aws

Benutzerhandbuch für Aurora

Amazon Aurora

Amazon Aurora: Benutzerhandbuch für Aurora

Table of Contents

Was ist Amazon Aurora?

Amazon Aurora (Aurora) ist eine vollständig verwaltete, mit MySQL und PostgreSQL kompatible relationale Datenbank-Engine. Sie wissen bereits, wie MySQL und PostgreSQL die Geschwindigkeit und Zuverlässigkeit von kommerziellen High-End-Datenbanken mit der Einfachheit und Kosteneffizienz von Open-Source-Datenbanken verbinden. Der Code, die Tools und Anwendungen, die Sie heute mit Ihren bestehenden MySQL- und PostgreSQL-Datenbanken verwenden, können auch mit Aurora verwendet werden. Bei manchen Workloads kann Aurora einen bis zu fünfmal höheren Durchsatz als MySQL und einen bis zu dreimal höheren Durchsatz als PostgreSQL liefern, ohne dass die meisten Ihrer bestehenden Anwendungen geändert werden müssen.

Aurora umfasst ein hochleistungsfähiges Speichersubsystem. Die mit MySQL und PostgreSQL kompatiblen Datenbank-Engines werden angepasst, um diesen schnellen verteilten Speicher zu nutzen. Der zugrunde liegende Speicher wächst bei Bedarf automatisch. Ein Aurora-Cluster-Volume kann auf eine maximale Größe von 128 tebibytes (TiB) anwachsen. Aurora automatisiert und standardisiert auch das Clustering und die Replikation von Datenbanken, die normalerweise zu den schwierigsten Aspekten der Datenbankkonfiguration und -verwaltung gehören.

Aurora ist Teil des verwalteten Datenbankservices Amazon Relational Database Service (Amazon RDS). Amazon RDS erleichtert die Einrichtung, den Betrieb und die Skalierung einer relationalen Datenbank in der Cloud. Wenn Sie noch keine Erfahrung mit Amazon RDS haben, beachten Sie die Informationen im Amazon Relational Database Service Benutzerhandbuch. Weitere Informationen zu den verschiedenen Datenbankoptionen, die in Amazon Web Services verfügbar sind, finden Sie unter Choosing the right database for your organization on AWS.

Themen

- Amazon Aurora-Sicherheit
- Hohe Verfügbarkeit für Amazon Aurora
- Replikation mit Amazon Aurora
- Abrechnung von DB-Instances für Aurora

Amazon-RDS-Modell der geteilten Verantwortung

Amazon RDS ist für das Hosting der Softwarekomponenten und der Infrastruktur von DB-Instances und DB-Clustern verantwortlich. Sie sind für die Abfrageoptimierung verantwortlich, d. h. für den Prozess der Anpassung von SQL-Abfragen, um die Leistung zu verbessern. Die Abfrageleistung hängt erheblich vom Datenbankdesign, der Datengröße, der Datenverteilung, der Anwendungs-Workload und den Abfragemustern ab, die stark variieren können. Überwachung und Optimierung sind hochgradig individualisierte Prozesse, für die Sie für Ihre RDS-Datenbanken verantwortlich sind. Sie können Erkenntnisse zur Amazon-RDS-Leistung und andere Tools verwenden, um problematische Abfragen zu identifizieren.

Funktionsweise von Amazon Amazon Aurora mit Amazon RDS

Die folgenden Punkte veranschaulichen die Beziehung zwischen Amazon Aurora und den in Amazon RDS verfügbaren standardmäßigen MySQL- und PostgreSQL-Engines:

- Sie wählen Aurora MySQL oder Aurora PostgreSQL als DB-Engine-Option aus, wenn Sie über Amazon RDS neue Datenbankserver einrichten.
- Aurora nutzt die bekannten Funktionen von Amazon Relational Database Service (Amazon RDS) für Verwaltung und Administration. Aurora verwendet die Amazon AWS Management Console RDS-Schnittstelle, AWS CLI Befehle und API-Operationen, um routinemäßige Datenbankaufgaben wie Bereitstellung, Patching, Sicherung, Wiederherstellung, Fehlererkennung und Reparatur zu erledigen.
- Aurora-Verwaltungsvorgänge umfassen in der Regel komplette Cluster von Datenbankservern, die durch Replikation synchronisiert werden, und keine einzelnen Datenbank-Instances. Durch das automatische Clustering, die automatische Replikation und Speicherzuweisung können selbst Ihre größten MySQL- und PostgreSQL-Bereitstellungen einfach und kosteneffizient eingerichtet, betrieben und skaliert werden.
- Durch Erstellen und Wiederherstellen von Snapshots oder Einrichtung einer unidirektionalen Replikation können Sie Daten aus Amazon RDS for MySQL und Amazon RDS for PostgreSQL in

Aurora einbringen. Sie können Push-Button-Migrationstools verwenden, um Ihre vorhandenen RDS für MySQL- und RDS für PostgreSQL-Anwendungen in Aurora zu konvertieren.

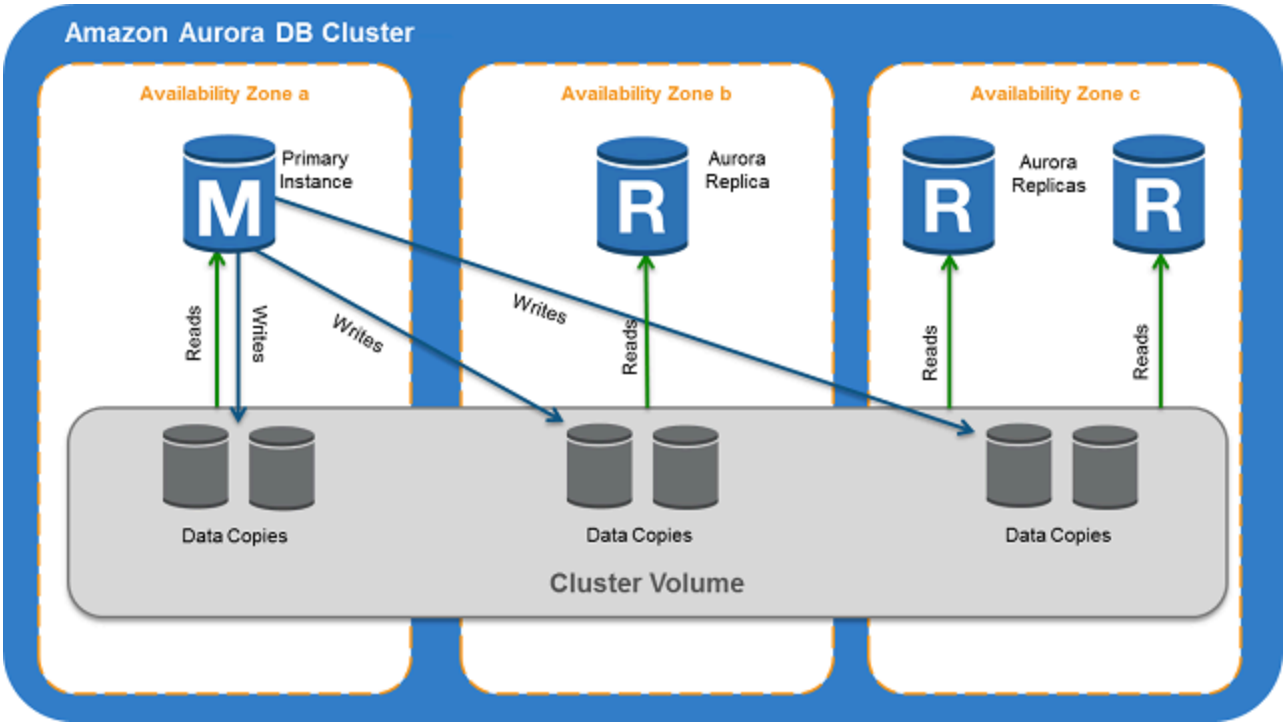
Bevor Sie Amazon Aurora verwenden, führen Sie die Schritte unter Einrichten Ihrer Umgebung für Amazon Aurora aus und sehen Sie sich anschließend im Abschnitt Amazon-Aurora-DB-Cluster die Konzepte und Funktionen von Aurora an.

Amazon-Aurora-DB-Cluster

Ein Amazon Aurora-DB-Cluster besteht aus einer oder mehreren DB-Instances und einem Cluster-Volume, das die Daten für diese DB-Instances verwaltet. Ein Aurora-Cluster-Volume ist ein virtuelles Datenbankspeicher-Volume, das sich über mehrere Availability Zones erstreckt, wobei jede Availability Zone über eine Kopie der DB-Cluster-Daten verfügt. Zwei Typen von DB-Instances bilden einen Aurora-DB-Cluster:

- Primäre DB-Instance – Unterstützt Lese- und Schreiboperationen und führt alle Datenänderungen im Cluster-Volume durch. Jeder Aurora-DB-Cluster verfügt über eine primäre DB-Instance.
- Aurora-Replica – Stellt eine Verbindung zu demselben Speichervolume wie die primäre DB-Instance her und unterstützt nur Lesevorgänge. Jeder Aurora-DB-Cluster kann zusätzlich zur primären DB-Instance bis zu 15 Aurora-Replicas besitzen. Sorgen Sie für eine hohe Verfügbarkeit, indem Sie die Aurora-Replikate in separaten Availability Zones platzieren. Aurora führt ein automatisches Failover auf ein Aurora-Replikat durch, falls die primäre DB-Instance nicht mehr verfügbar ist. Sie können die Failover-Priorität für Aurora-Replicas festlegen. Aurora-Replicas können auch schreibgeschützte Workloads von der primären DB-Instance auslagern.

Das folgende Diagramm veranschaulicht die Beziehung zwischen dem Cluster-Volume, der primären DB-Instance und Aurora-Replicas in einem Aurora-DB-Cluster.



> **Note**
>
> Dazu gehören bereitgestellte Cluster, Parallelabfragecluster, globale Datenbankcluster, Aurora Serverless-Cluster und alle MySQL 8.0-kompatiblen, 5.7-kompatiblen und PostgreSQL-kompatiblen Cluster.

Der Aurora-Cluster veranschaulicht die Trennung von Datenverarbeitungskapazität und Speicher. Beispielsweise ist eine Aurora-Konfiguration mit nur einer einzigen DB-Instance immer noch ein Cluster, da das zugrunde liegende Speichervolumen mehrere Speicherknoten umfasst, die auf mehrere Availability Zones (AZs) verteilt sind.

Ein-/Ausgabe (I/O)-Operationen in Aurora-DB-Clustern werden auf die gleiche Weise gezählt, unabhängig davon, ob sie sich auf einer Writer- oder Reader-DB-Instance befinden. Weitere Informationen finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora.

Amazon-Aurora-Versionen

Amazon Aurora verwendet Code wieder und behält die Kompatibilität mit den zugrunde liegenden MySQL- und PostgreSQL-DB-Engines bei. Aurora verfügt jedoch über eigene Versionsnummern, einen eigenen Release-Zyklus, einen eigenen Zeitplan für die Einstellung der Version usw. Im folgenden Abschnitt werden die gemeinsamen Punkte und Unterschiede erläutert. Mithilfe dieser Informationen können Sie entscheiden, welche Version Sie auswählen und wie Sie überprüfen können, welche Funktionen und Fehlerbehebungen in jeder Version verfügbar sind. Es kann Ihnen auch helfen, zu entscheiden, wie oft Sie ein Upgrade durchführen und wie Sie Ihren Upgrade-Prozess planen.

Themen

Relationale Datenbanken, die auf Aurora verfügbar sind

Die folgenden relationalen Datenbanken sind auf Aurora verfügbar:

- Amazon-Aurora-MySQL-kompatible Edition Weitere Informationen zur Nutzung finden Sie unter Arbeiten mit Amazon Aurora MySQL. Eine detaillierte Liste der verfügbaren Versionen finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.
- Amazon-Aurora-PostgreSQL-kompatible Edition Weitere Informationen zur Nutzung finden Sie unter Arbeiten mit Amazon Aurora PostgreSQL. Eine detaillierte Liste der verfügbaren Versionen finden Sie unter Amazon Aurora PostgreSQL-Aktualisierungen.

Unterschiede in den Versionsnummern zwischen Community-Datenbanken und Aurora

Jede Amazon-Aurora-Version ist mit einer bestimmten Community-Datenbankversion von MySQL oder PostgreSQL kompatibel. Sie können die Community-Version Ihrer Datenbank mithilfe der `version`-Funktion und die Aurora-Version mithilfe der `aurora_version`-Funktion finden.

Folgende Beispiele für Aurora MySQL und Aurora PostgreSQL werden gezeigt.

```
mysql> select version();
+------------------+
|   version()      |
+------------------+
|  5.7.12          |
+------------------+

mysql> select aurora_version(), @@aurora_version;
+------------------+------------------+
| aurora_version() | @@aurora_version |
+------------------+------------------+
| 2.08.1           | 2.08.1           |
+------------------+------------------+
```

```
postgres=> select version();
-------------------------------------------------------------------------------
PostgreSQL 11.7 on x86_64-pc-linux-gnu, compiled by gcc (GCC) 4.9.3, 64-bit
(1 row)

postgres=> select aurora_version();
aurora_version
----------------
3.2.2
```

Weitere Informationen erhalten Sie unter Überprüfen von Aurora MySQL-Versionen mit SQL und Identifizieren der Versionen von Amazon Aurora PostgreSQL.

Amazon-Aurora-Hauptversionen

Aurora-Versionen verwenden das Schema *major*.*minor*.*patch*. Eine Aurora-Hauptversion bezieht sich auf die MySQL- oder PostgreSQL-Community-Hauptversion, mit der Aurora kompatibel ist. Die Hauptversionen von Aurora MySQL und Aurora PostgreSQL stehen mindestens bis zum Ende des Lebenszyklus der Community für die entsprechende Community-Version zur Verfügung. Gegen eine Gebühr können Sie eine Hauptversion auch nach Ablauf des Standard-Supports von Aurora weiter ausführen. Weitere Informationen dazu finden Sie unter Verwenden von Amazon RDS Extended Support und Amazon Aurora – Preise.

Weitere Informationen zu den Hauptversionen von Aurora MySQL und dem Veröffentlichungskalender finden Sie unter Veröffentlichungskalender für Aurora MySQL-Hauptversionen.

Weitere Informationen zu den Hauptversionen von Aurora PostgreSQL und dem Veröffentlichungskalender finden Sie unter Veröffentlichungskalender für Aurora PostgreSQL-Hauptversionen.

> **Note**
>
> Amazon RDS Extended Support für Aurora MySQL Version 2 beginnt am 1. November 2024, Ihnen wird jedoch erst am 1. Dezember 2024 eine Gebühr berechnet. Zwischen dem 1. und 30. November 2024 sind alle Aurora MySQL Version 2-DB-Cluster durch Amazon RDS Extended Support abgedeckt.
> Amazon RDS Extended Support für PostgreSQL 11 beginnt am 1. März 2024, Ihnen wird jedoch erst am 1. April 2024 eine Gebühr berechnet. Zwischen dem 1. März und dem 31. März 2024 sind alle Aurora PostgreSQL Version 11-DB-Cluster durch Amazon RDS Extended Support abgedeckt.

Amazon-Aurora-Nebenversionen

Aurora-Versionen verwenden das Schema *major*.*minor*.*patch*. Eine Aurora-Nebenversion bietet inkrementelle Community- und Aurora-spezifische Verbesserungen des Services, zum Beispiel neue Funktionen und Fehlerkorrekturen.

Weitere Informationen zu Aurora MySQL-Nebenversionen und dem Veröffentlichungskalender finden Sie unter Veröffentlichungskalender für Aurora MySQL-Nebenversionen.

Weitere Informationen zu Aurora PostgreSQL-Nebenversionen und dem Veröffentlichungskalender finden Sie unter Veröffentlichungskalender für Aurora PostgreSQL-Nebenversionen.

Amazon-Aurora-Patchversionen

Aurora-Versionen verwenden das Schema *major*.*minor*.*patch*. Eine Aurora-Patchversion enthält wichtige Fehlerkorrekturen, die einer Nebenversion nach ihrer ersten Veröffentlichung hinzugefügt wurden (z. B. Aurora MySQL 2.10.0, 2.10.1, ..., 2.10.3). Während jede neue Nebenversion neue Aurora-Funktionen bietet, werden neue Patch-Versionen innerhalb einer bestimmten Nebenversion hauptsächlich verwendet, um wichtige Probleme zu beheben.

Weitere Informationen zu Patch-Vorgängen finden Sie unter Warten eines Amazon Aurora-DB-Clusters.

Erfahren Sie, was in jeder Amazon-Aurora-Version neu ist

Jede neue Aurora-Version enthält Versionshinweise, in denen die neuen Funktionen, Korrekturen, anderen Verbesserungen usw. aufgeführt sind, die für jede Version gelten.

Versionshinweise für Aurora MySQL finden Sie unter Versionshinweise für Aurora MySQL. Versionshinweise für Aurora PostgreSQL finden Sie unter Versionshinweise für Aurora PostgreSQL.

Angeben der Amazon-Aurora-Datenbankversion für Ihren Datenbank-Cluster

Sie können jede derzeit verfügbare Version (Haupt- und Nebenversion) angeben, wenn Sie einen neuen DB-Cluster mithilfe der Operation Datenbank erstellen in der Operation AWS Management Console, der oder der API AWS CLI angeben. `CreateDBCluster` Nicht jede Aurora Datenbankversion ist in jeder AWS -Region verfügbar.

Informationen zum Erstellen von Aurora-Clustern finden Sie unter Erstellen eines Amazon Aurora-DB Clusters. Informationen zum Ändern der Version eines vorhandenen Aurora-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Standard-Amazon-Aurora-Versionen

Wenn eine neue Aurora-Nebenversion im Vergleich zu einer vorherigen signifikante Verbesserungen enthält, wird sie als Standardversion für neue DB-Cluster markiert. In der Regel veröffentlichen wir zwei Standardversionen für jede Hauptversion pro Jahr.

Wir empfehlen, dass Sie Ihr DB-Cluster auf die aktuellste Standard-Nebenversion aktualisieren, da diese Version die neuesten Sicherheits- und Funktionskorrekturen enthält.

Automatische Unterversion-Upgrades

Sie können mit Aurora-Nebenversionen auf dem Laufenden bleiben, indem Sie für jede DB-Instance im Aurora-Cluster das automatische Upgrade der Nebenversion aktivieren. Aurora führt das automatische Upgrade nur durch, wenn alle DB-Instances in Ihrem Cluster diese Einstellung aktiviert haben. Automatische Nebenversions-Upgrades werden auf die standardmäßige Nebenversion durchgeführt.

Normalerweise planen wir zweimal im Jahr automatische Upgrades für DB-Cluster, bei denen die Einstellung Automatisches Upgrade der Nebenversion auf `Yes` gesetzt ist. Diese Upgrades werden während des Wartungsfensters gestartet, das Sie für den Cluster angeben. Weitere Informationen finden Sie unter Automatische Nebenversions-Upgrades für Aurora-DB-Cluster.

Automatische Upgrades von Nebenversionen werden im Voraus über ein Amazon-RDS-DB-Clusterereignis mit der Kategorie `maintenance` und der ID `RDS-EVENT-0156` kommuniziert. Weitere Informationen finden Sie unter Amazon RDS-Ereigniskategorien und Ereignisnachrichten für Aurora.

Wie lange bleiben Amazon-Aurora-Hauptversionen verfügbar?

Die Hauptversionen von Amazon Aurora stehen mindestens bis zum Ende des Lebenszyklus der Community für die entsprechende Community-Version zur Verfügung. Sie können die Daten des Ablaufs des Standard-Supports für Aurora verwenden, um Ihre Test- und Upgrade-Zyklen zu planen. Diese Daten stellen das früheste Datum dar, an dem ein Upgrade auf eine neuere Version erforderlich sein könnte. Weitere Informationen zu den Daten finden Sie unter Amazon-Aurora-Hauptversionen.

Bevor wir Sie bitten, auf eine neuere Hauptversion zu aktualisieren, und um Ihnen bei der Planung zu helfen, erinnern wir Sie in der Regel mindestens 12 Monate im Voraus daran. Wir tun dies, um

den detaillierten Upgrade-Prozess zu kommunizieren. Details umfassen das Timing bestimmter Meilensteine, die Auswirkungen auf Ihre DB-Cluster und die von Ihnen empfohlenen Aktionen. Es wird immer empfohlen, Ihre Anwendungen mit neuen Datenbankversionen gründlich zu testen, bevor Sie ein Upgrade der Hauptversion durchführen.

Wenn die Hauptversion das Ende des Standard-Supports für Aurora erreicht hat, werden alle DB-Cluster, auf denen noch die ältere Version ausgeführt wird, während eines geplanten Wartungsfensters automatisch auf eine Version mit erweitertem Support aktualisiert. Es können Gebühren für erweiterten Support anfallen. Weitere Informationen zu Amazon RDS Extended Support finden Sie unter Amazon RDS Extended Support verwenden.

Wie oft werden Amazon-Aurora-Nebenversionen veröffentlicht?

Im Allgemeinen werden Amazon-Aurora-Nebenversionen vierteljährlich veröffentlicht. Der Release-Zeitplan kann variieren, um zusätzliche Funktionen oder Korrekturen aufzunehmen.

Wie lange bleiben Amazon-Aurora-Nebenversionen verfügbar

Wir beabsichtigen, jede Amazon-Aurora-Nebenversion einer bestimmten Hauptversion für mindestens 12 Monate verfügbar zu machen. Am Ende dieses Zeitraums kann Aurora ein automatisches Nebenversions-Upgrade auf die nachfolgende Standard-Nebenversion anwenden. Ein solches Upgrade wird während des geplanten Wartungsfensters für jeden Cluster gestartet, auf dem noch die ältere Nebenversion ausgeführt wird.

Wir können eine Nebenversion einer bestimmten Hauptversion früher als in der üblichen 12-Monats-Frist ersetzen, wenn es kritische Angelegenheiten wie Sicherheitsprobleme gibt oder wenn die Hauptversion das Ende ihrer Lebensdauer erreicht hat.

Bevor Sie mit automatischen Upgrades von Nebenversionen beginnen, die sich dem Ende ihrer Lebensdauer nähern, erinnern wir Sie in der Regel drei Monate im Voraus daran. Wir tun dies, um den detaillierten Upgrade-Prozess zu kommunizieren. Details umfassen das Timing bestimmter Meilensteine, die Auswirkungen auf Ihre DB-Cluster und die von Ihnen empfohlenen Aktionen. Benachrichtigungen mit einer Vorlaufzeit von weniger als drei Monaten werden verwendet, wenn kritische Angelegenheiten wie Sicherheitsprobleme ein schnelleres Handeln erfordern.

Wenn Sie die Einstellung Automatisches Unterversion-Upgrade nicht aktiviert haben, erhalten Sie eine Erinnerung, aber keine RDS-Ereignisbenachrichtigung. Upgrades erfolgen innerhalb eines Wartungsfensters, nachdem die vorgeschriebene Upgrade-Frist abgelaufen ist.

Wenn Sie die Einstellung Automatisches Unterversion-Upgrade aktiviert haben, erhalten Sie eine Erinnerung und ein Ereignis des DB-Clusters von Amazon RDS mit der Kategorie `maintenance` und der ID `RDS-EVENT-0156`. Aktualisierungen erfolgen während des nächsten Wartungsfensters.

Weitere Informationen zu automatischen Unterversion-Upgrades finden Sie unter Automatische Nebenversions-Upgrades für Aurora-DB-Cluster.

Langzeit-Support für ausgewählte Amazon-Aurora-Nebenversionen

Für jede Aurora-Hauptversion werden bestimmte Nebenversionen als long-term-support (LTS-) Versionen bezeichnet und für mindestens drei Jahre verfügbar gemacht. Das heißt, mindestens eine Nebenversion pro Hauptversion wird länger als die typischen 12 Monate zur Verfügung gestellt. Wir erinnern in der Regel sechs Monate vor Ablauf dieser Frist daran. Wir tun dies, um den detaillierten Upgrade-Prozess zu kommunizieren. Details umfassen das Timing bestimmter Meilensteine, die Auswirkungen auf Ihre DB-Cluster und die von Ihnen empfohlenen Aktionen. Benachrichtigungen mit einer Vorlaufzeit von weniger als sechs Monaten werden verwendet, wenn kritische Angelegenheiten wie Sicherheitsprobleme ein schnelleres Handeln erfordern.

LTS-Nebenversionen enthalten nur wichtige Fehlerkorrekturen (über Patch-Versionen). Eine LTS-Version enthält keine neuen Funktionen, die nach ihrer Einführung veröffentlicht wurden. Einmal im Jahr werden DB-Cluster, die auf einer LTS-Nebenversion ausgeführt werden, auf die neueste Patch-Version der LTS-Version gepatcht. Wir führen diese Patches durch, um sicherzustellen, dass Sie von kumulativen Sicherheits- und Stabilitätsbehebungen profitieren. Wir können eine LTS-Nebenversion häufiger patchen, wenn kritische Fehlerbehebungen, z. B. für die Sicherheit, angewendet werden müssen.

> **Note**
>
> Um für die Dauer ihres Lebenszyklus auf einer LTS-Nebenversion zu bleiben, stellen Sie sicher, dass Sie das automatische Upgrade der Nebenversion für Ihre DB-Instances deaktivieren. Um zu vermeiden, dass Ihr DB-Cluster automatisch von der LTS-Nebenversion aktualisiert wird, legen Sie die Option Auto minor version upgrade (Automatisches Nebenversion-Upgrade) für alle DB-Instances in Ihrem Aurora-Cluster auf No fest.

Die Versionsnummern aller Aurora LTS-Versionen finden Sie unter Aurora MySQL Long-Term Support- (LTS, Langzeit-Support) Versionen und Aurora PostgreSQL Long-Term Support- (LTS, Langzeit-Support) Versionen.

Amazon RDS Extended Support für ausgewählte Aurora-Versionen

Mit Amazon RDS Extended Support können Sie Ihre Datenbank gegen Aufpreis auch nach Ablauf des Standard-Supportdatums von Aurora auf einer größeren Engine-Version weiter betreiben. Während des erweiterten RDS-Supports stellt Amazon RDS Patches für kritische und hohe CVEs bereit, wie sie in den CVSS-Schweregraden der National Vulnerability Database (NVD) definiert sind. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Extended Support.

RDS Extended Support ist nur für bestimmte Aurora-Versionen verfügbar. Weitere Informationen finden Sie unter Amazon-Aurora-Hauptversionen.

Manuelles Steuern, ob und wann Ihr Datenbank-Cluster auf neue Versionen aktualisiert wird

Automatische Nebenversions-Upgrades werden auf die standardmäßige Nebenversion durchgeführt. In der Regel planen wir automatische Upgrades zweimal pro Jahr für DB-Cluster, bei denen die Einstellung Automatisches Upgrade der Nebenversion aktiviert ist. Diese Upgrades werden während kundenspezifischer Wartungsfenster gestartet. Wenn Sie automatische Upgrades für Nebenversionen deaktivieren möchten, deaktivieren Sie das automatische Upgrade für Nebenversionen auf jeder DB-Instance innerhalb eines Aurora-Clusters. Aurora führt nur dann ein automatisches Upgrade der Nebenversion durch, wenn die Einstellung für alle DB-Instances in Ihrem Cluster aktiviert ist.

> **Note**
>
> Bei obligatorischen Upgrades wie dem Ende der Lebensdauer einer Nebenversion wird der DB-Cluster jedoch auch dann aktualisiert, wenn die Einstellung Automatisches Upgrade der Nebenversion deaktiviert ist. Sie erhalten eine Erinnerung, aber keine RDS-Ereignisbenachrichtigung. Upgrades erfolgen innerhalb eines Wartungsfensters, nachdem die vorgeschriebene Upgrade-Frist abgelaufen ist.

Da Upgrades von Hauptversionen ein gewisses Kompatibilitätsrisiko beinhalten, werden sie nicht automatisch ausgeführt. Sie müssen diese initiieren, außer im Fall eines Hauptversions-Upgrades aufgrund der Einstellung, wie zuvor erläutert. Es wird immer empfohlen, Ihre Anwendungen mit neuen Datenbankversionen gründlich zu testen, bevor Sie ein Upgrade der Hauptversion durchführen.

Weitere Informationen zum Aktualisieren eines DB-Clusters auf eine neue Aurora-Hauptversion finden Sie unter Upgrade von Amazon Aurora MySQL-DB-Clustern und Upgrade von DB-Clustern von Amazon Aurora PostgreSQL.

Erforderliche Amazon-Aurora-Upgrades

Bei bestimmten kritischen Fehlerbehebungen führen wir möglicherweise ein verwaltetes Upgrade auf eine neuere Patch-Stufe innerhalb derselben Nebenversion durch. Diese erforderlichen Upgrades erfolgen auch dann, wenn das automatische Upgrade der Nebenversion deaktiviert ist. Zuvor kommunizieren wir den detaillierten Upgrade-Prozess. Details umfassen das Timing bestimmter Meilensteine, die Auswirkungen auf Ihre DB-Cluster und die von Ihnen empfohlenen Aktionen. Solche verwalteten Upgrades werden automatisch durchgeführt. Jedes Upgrade wird innerhalb des Wartungsfensters des Clusters gestartet.

Testen Ihres DB-Clusters mit einer neuen Aurora-Version vor dem Upgrade

Sie können den Upgrade-Prozess und die Funktionsweise der neuen Version mit Ihrer Anwendung und Ihrer Workload testen. Verwenden Sie eine der folgenden Methoden:

- Klonen Sie Ihren Cluster mit der Funktion zum schnellen Klonen von Amazon-Aurora-Datenbanken. Führen Sie das Upgrade und alle Tests nach dem Upgrade auf dem neuen Cluster durch.
- Wiederherstellung aus einem Cluster-Snapshot, um einen neuen Aurora-Cluster zu erstellen. Sie können einen Cluster-Snapshot selbst aus einem vorhandenen Aurora-Cluster erstellen. Aurora erstellt außerdem automatisch periodische Snapshots für jeden deiner Cluster. Anschließend können Sie ein Versionsupdate für den neuen Cluster initiieren. Sie können mit der aktualisierten Kopie des Clusters experimentieren, bevor Sie entscheiden, ob Sie den ursprünglichen Cluster aktualisieren möchten.

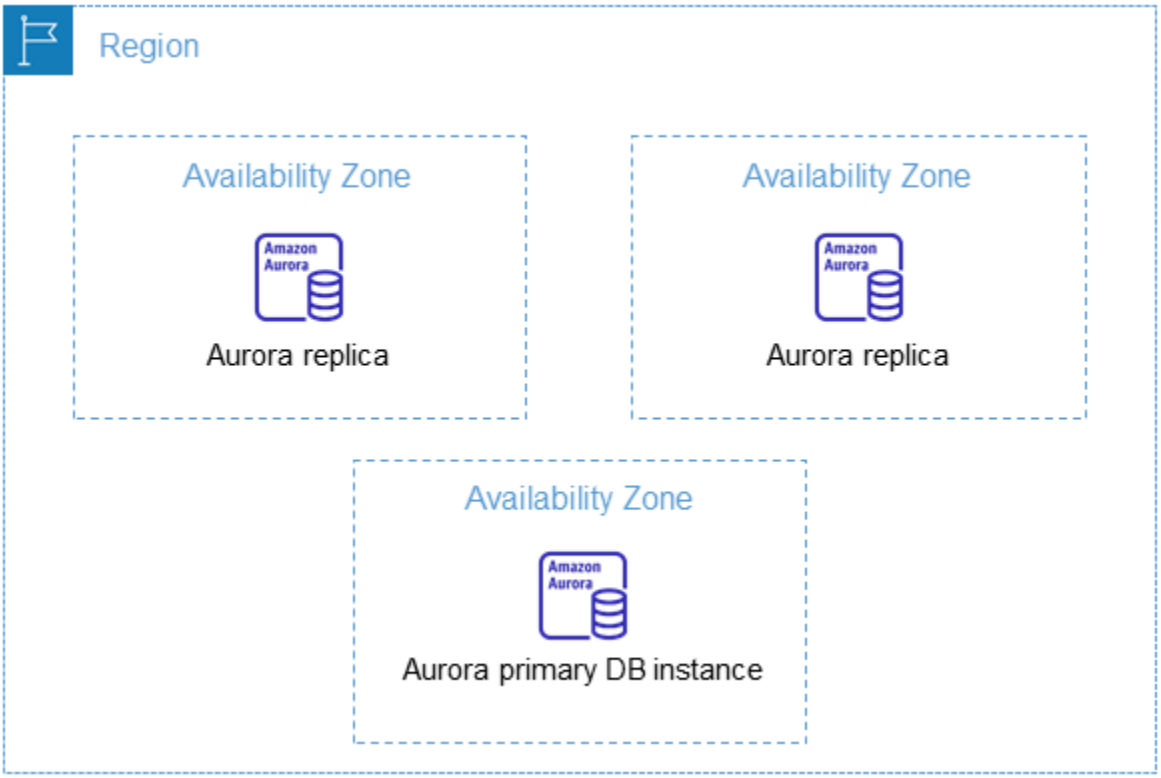
Weitere Informationen zu diesen Methoden zum Erstellen neuer Cluster zum Testen finden Sie unter Klonen eines Volumes für einen Amazon-Aurora-DB-Cluster und Erstellen eines DB-Cluster-Snapshots.

Regionen und Availability Zones

Amazon Cloud Computing-Ressourcen werden an mehreren Standorten weltweit gehostet. Diese Standorte bestehen aus AWS Regionen und Availability Zones. Jede AWS -Region ist ein separater geografischer Bereich. Jede AWS Region hat mehrere isolierte Standorte, die als Availability Zones bezeichnet werden.

> **Note**
>
> Informationen zur Suche nach den Availability Zones für eine AWS Region finden Sie unter Describe your Availability Zones in der Amazon EC2 EC2-Dokumentation.

Amazon betreibt state-of-the-art hochverfügbare Rechenzentren. Obwohl selten, können Fehler auftreten, die sich auf die Verfügbarkeit von DB-Instances auswirken, die sich am selben Speicherort befinden. Wenn Sie alle Ihre DB-Instances an einem Ort hosten, der von einem solchen Ausfall betroffen ist, ist keine Ihrer DB-Instances verfügbar.



Es ist wichtig, sich daran zu erinnern, dass jede AWS Region völlig unabhängig ist. Jede von Ihnen initiierte Amazon RDS-Aktivität (z. B. das Erstellen von Datenbank-Instances

oder das Auflisten verfügbarer Datenbank-Instances) wird nur in Ihrer aktuellen AWS Standardregion ausgeführt. Die AWS Standardregion kann in der Konsole oder durch Einstellen der `AWS_DEFAULT_REGION`Umgebungsvariablen geändert werden. Oder sie kann überschrieben werden, indem der `--region` Parameter mit der AWS Command Line Interface ()AWS CLI verwendet wird. Weitere Informationen finden Sie unter Konfigurieren der AWS Command Line Interface, insbesondere in den Abschnitten zu Umgebungsvariablen und zu den Befehlszeilenoptionen.

Amazon RDS unterstützt spezielle AWS Regionen namens AWS GovCloud (US). Diese wurden entwickelt, damit US-Regierungsbehörden und Kunden vertrauliche Workloads in die Cloud verschieben können. Die Regionen AWS GovCloud (US) gehen auf die spezifischen regulatorischen und Compliance-Anforderungen der US-Regierung ein. Weitere Informationen finden Sie unter Was ist AWS GovCloud (US)?

Um eine Amazon RDS-DB-Instance in einer bestimmten AWS Region zu erstellen oder mit ihr zu arbeiten, verwenden Sie den entsprechenden regionalen Service-Endpunkt.

> **Note**
>
> Aurora unterstützt keine Local Zones.

AWS Regionen

Jede AWS Region ist so konzipiert, dass sie von den anderen AWS Regionen isoliert ist. Dieser Entwurf sorgt für die größtmögliche Fehlertoleranz und Stabilität.

Wenn Sie Ihre Ressourcen anzeigen, sehen Sie nur die Ressourcen, die mit der von Ihnen angegebenen AWS Region verknüpft sind. Das liegt daran, dass AWS Regionen voneinander isoliert sind und wir Ressourcen nicht automatisch regionsübergreifend AWS replizieren.

Verfügbarkeit in Regionen

Wenn Sie mit einem Aurora-DB-Cluster über die Befehlszeilenschnittstelle oder API-Vorgänge arbeiten, stellen Sie sicher, dass Sie den regionalen Endpunkt angeben.

Themen

- Aurora MySQL-Verfügbarkeit in Regionen
- Aurora PostgreSQL-Verfügbarkeit in Regionen

Aurora MySQL-Verfügbarkeit in Regionen

Die folgende Tabelle zeigt die AWS Regionen, in denen Aurora MySQL derzeit verfügbar ist, und den Endpunkt für jede Region.

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
USA Ost (Ohio)	us-east-2	rds.us-east-2.amazonaws.com	HTTPS	
USA Ost (Nord-Virginia)	us-east-1	rds.us-east-1.amazonaws.com	HTTPS	
USA West (Nordkalifornien)	us-west-1	rds.us-west-1.amazonaws.com	HTTPS	
USA West (Oregon)	us-west-2	rds.us-west-2.amazonaws.com	HTTPS	
Afrika (Kapstadt)	af-south-1	rds.af-south-1.amazonaws.com	HTTPS	
Asien-Pazifik (Hongkong)	ap-east-1	rds.ap-east-1.amazonaws.com	HTTPS	
Asien-Pazifik (Hyderabad)	ap-south-2	rds.ap-south-2.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Jakarta)	ap-southeast-3	rds.ap-southeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	rds.ap-southeast-4.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	rds.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Kanada (Zentral)	ca-central-1	rds.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	rds.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	rds.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	rds.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	rds.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	rds.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	rds.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	rds.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	rds.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	rds.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	rds.il-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
Naher Osten (Bahrain)	me-south-1	rds.me-south-1.amazonaws.com	HTTPS	
Naher Osten (VAE)	me-central-1	rds.me-central-1.amazonaws.com	HTTPS	
Südamerika (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com	HTTPS	
AWS GovCloud (US-Ost)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com	HTTPS	
AWS GovCloud (US-West)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com	HTTPS	

Aurora PostgreSQL-Verfügbarkeit in Regionen

Die folgende Tabelle zeigt die AWS Regionen, in denen Aurora PostgreSQL derzeit verfügbar ist, und den Endpunkt für jede Region.

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
USA Ost (Ohio)	us-east-2	rds.us-east-2.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
USA Ost (Nord-Virginia)	us-east-1	rds.us-east-1.amazonaws.com	HTTPS	
USA West (Nordkalifornien)	us-west-1	rds.us-west-1.amazonaws.com	HTTPS	
USA West (Oregon)	us-west-2	rds.us-west-2.amazonaws.com	HTTPS	
Afrika (Kapstadt)	af-south-1	rds.af-south-1.amazonaws.com	HTTPS	
Asien-Pazifik (Hongkong)	ap-east-1	rds.ap-east-1.amazonaws.com	HTTPS	
Asien-Pazifik (Hyderabad)	ap-south-2	rds.ap-south-2.amazonaws.com	HTTPS	
Asien-Pazifik (Jakarta)	ap-southeast-3	rds.ap-southeast-3.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
Asien-Pazifik (Melbourne)	ap-southeast-4	rds.ap-southeast-4.amazonaws.com	HTTPS	
Asien-Pazifik (Mumbai)	ap-south-1	rds.ap-south-1.amazonaws.com	HTTPS	
Asien-Pazifik (Osaka)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com	HTTPS	
Asien-Pazifik (Seoul)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com	HTTPS	
Asien-Pazifik (Singapur)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com	HTTPS	
Asien-Pazifik (Sydney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com	HTTPS	
Asien-Pazifik (Tokio)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com	HTTPS	
Kanada (Zentral)	ca-central-1	rds.ca-central-1.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
Kanada West (Calgary)	ca-west-1	rds.ca-west-1.amazonaws.com	HTTPS	
Europa (Frankfurt)	eu-central-1	rds.eu-central-1.amazonaws.com	HTTPS	
Europa (Irland)	eu-west-1	rds.eu-west-1.amazonaws.com	HTTPS	
Europa (London)	eu-west-2	rds.eu-west-2.amazonaws.com	HTTPS	
Europa (Mailand)	eu-south-1	rds.eu-south-1.amazonaws.com	HTTPS	
Europa (Paris)	eu-west-3	rds.eu-west-3.amazonaws.com	HTTPS	
Europa (Spanien)	eu-south-2	rds.eu-south-2.amazonaws.com	HTTPS	
Europa (Stockholm)	eu-north-1	rds.eu-north-1.amazonaws.com	HTTPS	
Europa (Zürich)	eu-central-2	rds.eu-central-2.amazonaws.com	HTTPS	
Israel (Tel Aviv)	il-central-1	rds.il-central-1.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
Naher Osten (Bahrain)	me-south-1	rds.me-south-1.amazonaws.com	HTTPS	
Naher Osten (VAE)	me-central-1	rds.me-central-1.amazonaws.com	HTTPS	
Südamerika (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com	HTTPS	
AWS GovCloud (US-Ost)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com	HTTPS	
AWS GovCloud (US-West)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com	HTTPS	

Availability Zones

Eine Availability Zone ist ein isolierter Standort in einer bestimmten AWS-Region. Jede Region verfügt über mehrere Availability Zones (AZ), die eine hohe Verfügbarkeit für die Region bieten. Eine AZ wird durch den AWS Regionalcode gefolgt von einer Buchstabenkennung (z. B.`us-east-1a`) identifiziert. Wenn Sie die VPC und Subnetze erstellen, anstatt die Standard-VPC zu verwenden, definieren Sie jedes Subnetz in einer bestimmten AZ. Wenn Sie einen Aurora-DB-Cluster erstellen, erstellt Aurora die primäre Instance in einem der Subnetze in der DB-Subnetzgruppe der VPC. Auf diese Weise wird diese Instance mit einer von Aurora ausgewählten AZ verknüpft.

Jeder Aurora-DB-Cluster hostet Kopien seines Speichers in drei separaten AZs, die von Aurora automatisch aus den AZs in Ihrer DB-Subnetzgruppe ausgewählt werden. Jede DB-Instance im Cluster muss sich in einer dieser drei AZs befinden.

Wenn Sie eine DB-Instance in Ihrem Cluster erstellen, wählt Aurora automatisch eine geeignete AZ für diese Instance aus, wenn Sie keine AZ angeben.

Beschreiben Sie wie folgt mit dem Amazon-EC2-Befehl describe-availability-zones die Availability Zones in der angegebenen Region, die für Ihr Konto aktiviert sind.

```
aws ec2 describe-availability-zones --region region-name
```

Wenn Sie beispielsweise die Availability Zones in der Region USA Ost (Nord-Virginia) (us-east-1) beschreiben möchten, die für Ihr Konto aktiviert sind, führen Sie den folgenden Befehl aus:

```
aws ec2 describe-availability-zones --region us-east-1
```

Informationen dazu, wie Sie die AZ angeben, wenn Sie einen Cluster erstellen oder Instances hinzufügen, finden Sie unter Konfigurieren des Netzwerks für den DB-Cluster.

Lokale Zeitzone für Amazon Aurora-DB-Cluster

Standardmäßig ist die Zeitzone für ein Amazon Aurora-DB-Cluster auf die Universal Time Coordinated (UTC) eingestellt. Sie können die Zeitzone für Instances in Ihrem DB-Cluster stattdessen auf die lokale Zeitzone Ihrer Anwendung festlegen.

Legen Sie den Zeitzonenparameter auf einen der unterstützten Werte fest, um die lokale Zeitzone für einen DB-Cluster anzugeben. Diesen Parameter legen Sie in der Cluster-Parametergruppe für Ihren DB-Cluster fest.

- Für Aurora MySQL lautet der Name dieses Parameters `time_zone`. Informationen zu bewährten Methoden zum Festlegen des Parameters `time_zone` finden Sie unter Optimierung von Zeitstempeloperationen.
- Für Aurora PostgreSQL lautet der Name dieses Parameters `timezone`.

Wenn Sie den Parameter für ein DB-Cluster setzen, wird bei allen Instances in diesem DB-Cluster die neue lokale Zeitzone eingestellt. In einigen Fällen verwenden andere Aurora-DB-Cluster möglicherweise dieselbe Cluster-Parametergruppe. In diesem Fall wird für alle Instances in diesen DB-Clustern die neue lokale Zeitzone eingestellt. Weitere Informationen zu Parametern für Cluster-Ebenen finden Sie unter Amazon Aurora-DB-Cluster und DB-Instance-Parameter.

Nachdem Sie die lokale Zeitzone eingestellt haben, werden alle neuen Verbindungen zur Datenbank die Änderung reflektieren. In einigen Fällen haben Sie möglicherweise offene Verbindungen mit Ihrer

Datenbank, wenn Sie die lokale Zeitzone ändern. In diesem Fall sehen Sie die aktualisierte lokale Zeitzone nicht, nachdem Sie die Verbindung schließen und eine neue Verbindung öffnen.

Wenn Sie regionsübergreifend AWS replizieren, verwenden der Replikationsquell-DB-Cluster und das Replikat unterschiedliche Parametergruppen. Parametergruppen sind für eine AWS Region einzigartig. Damit Sie dieselbe lokale Zeitzone für jede Instance verwenden können, müssen Sie den Zeitzonenparameter in den Parametergruppen für die Replikationsquelle und für das Replikat festlegen.

Wenn Sie ein DB-Cluster aus einem DB-Cluster-Snapshot wiederherstellen, wird die lokale Zeitzone auf die Zeitzone UTC eingestellt. Sie können die Zeitzone auf Ihre lokale Zeitzone einstellen, nachdem die Wiederherstellung abgeschlossen ist. In einigen Fällen führen Sie möglicherweise eine zeitpunktbezogen Wiederherstellung eines DB-Clusters durch. In diesem Fall entspricht die lokale Zeitzone für den wiederhergestellten DB-Cluster der Zeitzoneneinstellung aus der Parametergruppe des wiederhergestellten DB-Clusters.

In der folgenden Tabelle sind einige Werte aufgeführt, die Sie für Ihre lokale Zeitzone festlegen können. Um alle verfügbaren Zeitzonen aufzulisten, können Sie die folgenden SQL-Abfragen verwenden:

- Aurora MySQL: `select * from mysql.time_zone_name;`
- Aurora PostgreSQL: `select * from pg_timezone_names;`

> **Note**
>
> Für einige Zeitzonen können Zeitwerte für bestimmte Datumsbereiche falsch gemeldet werden, worauf in der Tabelle hingewiesen wird. Für Zeitzonen in Australien wird die Zeitzonenabkürzung mit einem veralteten Wert zurückgegeben, worauf in der Tabelle hingewiesen wird.

Zeitzone	Hinweise
`Africa/Harare`	Diese Zeitzoneneinstellung kann vom 28. Februar 1903 21:49:40 GMT bis zum 28. Februar 1903 21:55:48 GMT falsche Werte zurückgeben.
`Africa/Monrovia`	

Zeitzone	Hinweise
`Africa/Nairobi`	Diese Zeitzoneneinstellung kann vom 31. Dezember 1939 21:30:00 GMT bis zum 31. Dezember 1959 21:15:15 GMT falsche Werte zurückgeben.
`Africa/Windhoek`	
`America/Bogota`	Diese Zeitzoneneinstellung kann vom 23. November 1914 04:56:16 GMT bis zum 23. November 1914 04:56:20 GMT falsche Werte zurückgeben.
`America/Caracas`	
`America/Chihuahua`	
`America/Cuiaba`	
`America/Denver`	
`America/Fortaleza`	In einigen Fällen wird bei einem DB-Cluster in der Region Südamerika (São Paulo) die Zeit für eine kürzlich geänderte Zeitzone Brasiliens nicht korrekt angezeigt. Setzen Sie in diesem Fall den Zeitzonenparameter des DB-Clusters auf `America/Fortaleza` zurück.
`America/Guatemala`	
`America/Halifax`	Diese Zeitzoneneinstellung kann vom 27. Oktober 1918 05:00:00 GMT bis zum 31. Oktober 1918 05:00:00 GMT falsche Werte zurückgeben.
`America/Manaus`	Wenn sich Ihr DB-Cluster in der Zeitzone Südamerika (Cuiaba) befindet und die erwartete Zeit für die kürzlich geänderte Zeitzone in Brasilien nicht korrekt angezeigt wird, setzen Sie den Zeitzonenparameter des DB-Clusters auf `America/Manaus` zurück.
`America/Matamoros`	
`America/Monterrey`	

Zeitzone	Hinweise
America/Montevideo	
America/Phoenix	
America/Tijuana	
Asia/Ashgabat	
Asia/Baghdad	
Asia/Baku	
Asia/Bangkok	
Asia/Beirut	
Asia/Calcutta	
Asia/Kabul	
Asia/Karachi	
Asia/Kathmandu	
Asia/Muscat	Diese Zeitzoneneinstellung kann vom 31. Dezember 1919 20:05:36 GMT bis zum 31. Dezember 1919 20:05:40 GMT falsche Werte zurückgeben.
Asia/Riyadh	Diese Zeitzoneneinstellung kann vom 13. März 1947 20:53:08 GMT bis zum 31. Dezember 1949 20:53:08 GMT falsche Werte zurückgeben.
Asia/Seoul	Diese Zeitzoneneinstellung kann vom 30. November 1904 15:30:00 GMT bis zum 07. September 1945 15:00:00 GMT falsche Werte zurückgeben.
Asia/Shanghai	Diese Zeitzoneneinstellung kann vom 31. Dezember 1927 15:54:08 GMT bis zum 02. Juni 1940 16:00:00 GMT falsche Werte zurückgeben.
Asia/Singapore	

Zeitzone	Hinweise
Asia/Taipei	Diese Zeitzoneneinstellung kann vom 30. September 1937 16:00:00 GMT bis zum 29. September 1979 15:00:00 GMT falsche Werte zurückgeben.
Asia/Tehran	
Asia/Tokyo	Diese Zeitzoneneinstellung kann vom 30. September 1937 15:00:00 GMT bis zum 31. Dezember 1937 15:00:00 GMT falsche Werte zurückgeben.
Asia/Ulaanbaatar	
Atlantic/Azores	Diese Zeitzoneneinstellung kann vom 24. Mai 1911 01:54:32 GMT bis zum 01. Januar 1912 01:54:32 GMT falsche Werte zurückgeben.
Australia/Adelaide	Die Abkürzung für diese Zeitzone wird als CST anstatt als ACDT/ACST zurückgegeben.
Australia/Brisbane	Die Abkürzung für diese Zeitzone wird als EST anstatt als AEDT/AEST zurückgegeben.
Australia/Darwin	Die Abkürzung für diese Zeitzone wird als CST anstatt als ACDT/ACST zurückgegeben.
Australia/Hobart	Die Abkürzung für diese Zeitzone wird als EST anstatt als AEDT/AEST zurückgegeben.
Australia/Perth	Die Abkürzung für diese Zeitzone wird als WST statt als AWST AWDT/ zurückgegeben.
Australia/Sydney	Die Abkürzung für diese Zeitzone wird als EST anstatt als AEDT/AEST zurückgegeben.
Brazil/East	
Canada/Saskatchewan	Diese Zeitzoneneinstellung kann vom 27. Oktober 1918 08:00:00 GMT bis zum 31. Oktober 1918 08:00:00 GMT falsche Werte zurückgeben.

Zeitzone	Hinweise
Europe/Amsterdam	
Europe/Athens	
Europe/Dublin	
Europe/Helsinki	Diese Zeitzoneneinstellung kann vom 30. April 1921 22:20:08 GMT bis zum 30. April 1921 22:20:11 GMT falsche Werte zurückgeben.
Europe/Paris	
Europe/Prague	
Europe/Sarajevo	
Pacific/Auckland	
Pacific/Guam	
Pacific/Honolulu	Diese Zeitzoneneinstellung kann vom 21. Mai 1933 11:30:00 GMT bis zum 30. September 1945 11:30:00 GMT falsche Werte zurückgeben.
Pacific/Samoa	Diese Zeitzoneneinstellung kann vom 01. Januar 1911 11:22:48 GMT bis zum 01. Januar 1950 11:30:00 GMT falsche Werte zurückgeben.
US/Alaska	
US/Central	
US/Eastern	
US/East-Indiana	
US/Pacific	
UTC	

Unterstützte Funktionen in Amazon Aurora by AWS-Region und der Aurora-DB-Engine

Aurora MySQL- und PostgreSQL-kompatible Datenbank-Engines unterstützen mehrere Amazon RDS- und Amazon Aurora-Funktionen und Optionen. Der Support variiert zwischen bestimmten Versionen der einzelnen Datenbank-Engines und in allen AWS-Regionen. Um die Versionsunterstützung und Verfügbarkeit der Aurora-Datenbank-Engine für eine bestimmte Funktion zu ermitteln AWS-Region, können Sie die folgenden Abschnitte verwenden.

Einige dieser Funktionen sind haben nur Aurora-Fähigkeiten. Beispielsweise werden globale Aurora-Datenbanken und die Unterstützung für die Integration mit AWS Machine-Learning-Diensten von Amazon RDS nicht unterstützt. Aurora Serverless Andere Funktionen, wie zum Beispiel Amazon RDS Proxy, werden von Amazon Aurora und Amazon RDS unterstützt.

Unterstützte Regionen und DB-Engines

- Tabellenkonventionen
- Unterstützte Regionen und Aurora-DB-Engines für Blue/Green-Bereitstellungen
- Unterstützte Regionen und Aurora-DB-Engines für Cluster-Speicherkonfigurationen
- Unterstützte Regionen und Aurora-DB-Engines für Datenbankaktivitätsstreams
- Unterstützte Regionen und Aurora-DB-Engines für den Export von Clusterdaten nach Amazon S3
- Unterstützte Regionen und Aurora-DB-Engines für den Export von Snapshot-Daten nach Amazon S3
- Unterstützte Regionen und DB-Engines für globale Aurora-Datenbanken
- Unterstützte Regionen und Aurora-DB-Engines für die IAM-Datenbankauthentifizierung
- Unterstützte Regionen und Aurora-DB-Engines für die Kerberos-Authentifizierung
- Unterstützte Regionen und DB-Engines für Aurora-Machine-Learning
- Unterstützte Regionen und Aurora-DB-Engines für Performance Insights
- Unterstützte Regionen und Aurora-DB-Engines für Zero-ETL-Integrationen mit Amazon Redshift
- Unterstützte Regionen und Aurora-DB-Engines für Amazon RDS Proxy
- Unterstützte Regionen und Aurora-DB-Engines für die Secrets Manager Manager-Integration
- Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2
- Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless Version 1
- Unterstützte Regionen und Aurora-DB-Engines für die RDS-Daten-API

- Unterstützte Regionen und Aurora-DB-Engines für Patching ohne Ausfallzeiten (ZDP)
- Unterstützte Regionen und DB-Engines für native Funktionen der Aurora-Engine

Tabellenkonventionen

In den Tabellen werden die folgenden Muster verwendet, um Versionsnummern und den Grad der Unterstützung anzugeben:

- Version x.y – Die spezifische Version allein wird unterstützt.
- Version x.y und höher – Die angegebene Version und alle höheren Unterversionen der jeweiligen Hauptversion werden unterstützt. Zum Beispiel bedeutet „Version 10.11 und höher“, dass die Versionen 10.11, 10.11.1 und 10.12 unterstützt werden.
- - — Die Funktion ist derzeit nicht für diese spezielle Aurora-Funktion für die angegebene Aurora-Datenbank-Engine oder in dieser speziellen Version verfügbar AWS-Region.

Unterstützte Regionen und Aurora-DB-Engines für Blue/Green-Bereitstellungen

Bei einer Blau/Grün-Bereitstellung wird eine Produktionsdatenbankumgebung in eine separate, synchronisierte Staging-Umgebung kopiert. Mithilfe von Blau/Grün-Bereitstellungen von Amazon RDS können Sie Änderungen an der Datenbank in der Staging-Umgebung vornehmen, ohne die Produktionsumgebung zu beeinträchtigen. Sie können beispielsweise die Haupt- oder Nebenversion der DB-Engine aktualisieren, Datenbankparameter ändern oder Schemaänderungen in der Staging-Umgebung vornehmen. Wenn Sie bereit sind, können Sie die Staging-Umgebung zur neuen Produktionsdatenbankumgebung hochstufen. Weitere Informationen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

Blau/Grün-Bereitstellungen mit Aurora MySQL

Die Funktion Blue/Green Deployments ist für alle Versionen von Aurora MySQL insgesamt verfügbar. AWS-Regionen

Blau/Grün-Bereitstellungen mit Aurora PostgreSQL

Die folgenden Regionen und Engine-Versionen sind für Blau/Grün-Bereitstellungen mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Alles AWS-Regionen	Version 16.1 und höher	Version 15.4 und höher	Version 14.9 und höher	Version 13.12 und höher	Version 12.16 und höher	Version 11.21 und höher

Unterstützte Regionen und Aurora-DB-Engines für Cluster-Speicherkonfigurationen

Amazon Aurora bietet zwei Speicherkonfigurationen für DB-Cluster, Aurora I/O-Optimized und Aurora Standard. Weitere Informationen finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora.

Aurora I/O-Optimized

Aurora I/O-Optimizedist in allen Versionen AWS-Regionen für die folgenden Amazon Aurora Aurora-Versionen verfügbar:

- Aurora MySQL Version 3.03.1 und höher
- Aurora PostgreSQL Versionen 16.1 und höher, 15.2 und höher, 14.7 und höher und 13.10 und höher

Aurora Standard

Aurora Standardist in allen AWS-Regionen Versionen von Aurora MySQL und Aurora PostgreSQL verfügbar.

Unterstützte Regionen und Aurora-DB-Engines für Datenbankaktivitätsstreams

Durch die Verwendung von Datenbank-Aktivitätsstreams in Aurora können Sie Alarme für die Prüfung von Aktivitäten in Ihrer Aurora-Datenbank überwachen und einstellen. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.

Datenbankaktivitäts-Streams werden im Hinblick auf die folgenden Funktionen nicht unterstützt:

- Aurora Serverless v1
- Aurora Serverless v2
- Babelfish für Aurora PostgreSQL

Themen

Datenbank-Aktivitätsstreams mit Aurora MySQL

Die folgenden Regionen und Engine-Versionen sind für Datenbankaktivitäts-Streams mit Aurora MySQL verfügbar.

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
USA Ost (Nord-Virginia)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
USA West (Nordkalifornien)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
USA West (Oregon)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Afrika (Kapstadt)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Asien-Pazifik (Hongkong)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Asien-Pazifik (Hyderabad)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Asien-Pazifik (Jakarta)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Asien-Pazifik (Mumbai)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Asien-Pazifik (Osaka)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Asien-Pazifik (Seoul)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Asien-Pazifik (Singapur)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Asien-Pazifik (Sydney)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Asien-Pazifik (Tokio)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Kanada (Zentral)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Kanada West (Calgary)	–	–
China (Peking)	–	–
China (Ningxia)	–	–
Europa (Frankfurt)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Europa (Irland)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Europa (London)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Europa (Milan)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Europa (Paris)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Europa (Spain)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Europa (Stockholm)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Europa (Zürich)	–	–
Israel (Tel Aviv)	–	–
Naher Osten (Bahrain)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Naher Osten (VAE)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher
Südamerika (São Paulo)	Alle verfügbaren Versionen	Aurora Version 2.11 und höher

Datenbank-Aktivitätsstreams mit Aurora PostgreSQL

Die folgenden Regionen und Engine-Versionen sind für Datenbankaktivitäts-Streams mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
USA Ost (Ohio)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
USA Ost (Nord-Virginia)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
USA West (Nordkalifornien)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
USA West (Oregon)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Afrika (Kapstadt)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Asien-Pazifik (Hongkong)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Hyderabad)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Jakarta)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Melbourne)	–	–	–	–	–	–
Asien-Pazifik (Mumbai)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Osaka)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Asien-Pazifik (Seoul)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Singapur)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Sydney)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Tokio)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Kanada (Zentral)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Kanada West (Calgary)	–	–	–	–	–	–

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
China (Peking)	–	–	–	–	–	–
China (Ningxia)	–	–	–	–	–	–
Europa (Frankfurt)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Europa (Irland)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Europa (London)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Europa (Milan)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Europa (Paris)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Europa (Spain)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Europa (Stockholm)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Europa (Zürich)	–	–	–	–	–	–
Israel (Tel Aviv)	–	–	–	–	–	–
Naher Osten (Bahrain)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Naher Osten (VAE)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher
Südamerika (São Paulo)	Version 16.1 und höher	Version 15.2 und höher	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Alle verfügbaren Versionen	Version 11.9 sowie Version 11.13 und höher

Unterstützte Regionen und Aurora-DB-Engines für den Export von Clusterdaten nach Amazon S3

Sie können DB-Cluster-Daten von Aurora in einen Amazon-S3-Bucket exportieren. Nachdem die Daten exportiert wurden, können Sie die exportierten Daten direkt mit Tools wie Amazon Athena oder Amazon Redshift Spectrum analysieren. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Daten nach Amazon S3.

Der Export von Clusterdaten nach S3 ist in folgenden AWS-Regionen verfügbar:

- Asien-Pazifik (Hongkong)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Kanada West (Calgary)

- China (Ningxia)
- Europe (Frankfurt)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Europa (Stockholm)
- Südamerika (São Paulo)
- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)

Themen

- Exportieren von Clusterdaten nach S3 mit Aurora MySQL
- Exportieren von Clusterdaten nach S3 mit Aurora PostgreSQL

Exportieren von Clusterdaten nach S3 mit Aurora MySQL

Alle derzeit verfügbaren Aurora-MySQL-Engine-Versionen unterstützen den Export von DB-Cluster-Daten nach Amazon S3. Weitere Informationen über Versionen finden Sie in den Versionshinweisen für Aurora MySQL.

Exportieren von Clusterdaten nach S3 mit Aurora PostgreSQL

Alle derzeit verfügbaren Aurora-PostgreSQL-Engine-Versionen unterstützen den Export von DB-Cluster-Daten nach Amazon S3. Weitere Informationen zu Versionen finden Sie unter Versionshinweise für Aurora PostgreSQL.

Unterstützte Regionen und Aurora-DB-Engines für den Export von Snapshot-Daten nach Amazon S3

Sie können DB-Cluster-Snapshot-Daten von Aurora in einen Amazon-S3-Bucket exportieren. Sie können manuelle Snapshots und automatisierte System-Snapshots exportieren. Nachdem die Daten exportiert wurden, können Sie die exportierten Daten direkt mit Tools wie Amazon Athena oder

Amazon Redshift Spectrum analysieren. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Snapshot-Daten nach Amazon S3.

Das Exportieren von Snapshots nach S3 ist in allen Versionen verfügbar, AWS-Regionen mit Ausnahme der folgenden:

- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Kanada West (Calgary)
- Europa (Spain)
- Europa (Zürich)
- Israel (Tel Aviv)
- Naher Osten (VAE)
- AWS GovCloud (US-Ost)
- AWS GovCloud (US-West)

Themen

- Exportieren von Snapshot-Daten nach S3 mit Aurora MySQL
- Exportieren von Snapshot-Daten nach S3 hat Aurora PostgreSQL

Exportieren von Snapshot-Daten nach S3 mit Aurora MySQL

Alle derzeit verfügbaren Aurora-MySQL-Engine-Versionen unterstützen den Export von DB-Cluster-Snapshot-Daten nach Amazon S3. Weitere Informationen über Versionen finden Sie in den Versionshinweisen für Aurora MySQL.

Exportieren von Snapshot-Daten nach S3 hat Aurora PostgreSQL

Alle derzeit verfügbaren Aurora-PostgreSQL-Engine-Versionen unterstützen den Export von DB-Cluster-Snapshot-Daten nach Amazon S3. Weitere Informationen zu Versionen finden Sie unter Versionshinweise für Aurora PostgreSQL.

Unterstützte Regionen und DB-Engines für globale Aurora-Datenbanken

Eine globale Aurora-Datenbank ist eine einzelne Datenbank, die sich über mehrere AWS-Regionen Datenbanken erstreckt und globale Lesevorgänge mit geringer Latenz und eine Notfallwiederherstellung nach einem Ausfall in der gesamten Region ermöglicht. Sie bietet integrierte Fehlertoleranz für Ihre Bereitstellung, da sich die DB-Instance nicht auf eine einzelne AWS-Region, sondern auf mehrere Regionen und verschiedene Availability Zones stützt. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Global Databases.

Themen

Globale Aurora-Datenbanken mit Aurora MySQL

Die folgenden Regionen und Engine-Versionen sind für globale Aurora-Datenbanken mit Aurora MySQL verfügbar.

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	Version 3.01.0 und höher	Version 2.07.0 und höher
USA Ost (Nord-Virginia)	Version 3.01.0 und höher	Version 2.07.0 und höher
USA West (Nordkalifornien)	Version 3.01.0 und höher	Version 2.07.0 und höher
USA West (Oregon)	Version 3.01.0 und höher	Version 2.07.0 und höher
Afrika (Kapstadt)	Version 3.01.0 und höher	Version 2.07.1 und höher
Asien-Pazifik (Hongkong)	Version 3.01.0 und höher	Version 2.07.1 und höher
Asien-Pazifik (Hyderabad)	Version 3.02.0 und höher	Version 2.11.2 und höher
Asien-Pazifik (Jakarta)	Version 3.01.0 und höher	Version 2.07.6 und höher
Asien-Pazifik (Melbourne)	Version 3.03.0 und höher	–
Asien-Pazifik (Mumbai)	Version 3.01.0 und höher	Version 2.07.0 und höher

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Asien-Pazifik (Osaka)	Version 3.01.0 und höher	Version 2.07.3 und höher
Asien-Pazifik (Seoul)	Version 3.01.0 und höher	Version 2.07.0 und höher
Asien-Pazifik (Singapur)	Version 3.01.0 und höher	Version 2.07.0 und höher
Asien-Pazifik (Sydney)	Version 3.01.0 und höher	Version 2.07.0 und höher
Asien-Pazifik (Tokio)	Version 3.01.0 und höher	Version 2.07.0 und höher
Kanada (Zentral)	Version 3.01.0 und höher	Version 2.07.0 und höher
Kanada West (Calgary)	Version 3.01.0 und höher	Version 2.07.0 und höher
China (Peking)	Version 3.01.0 und höher	Version 2.07.2 und höher
China (Ningxia)	Version 3.01.0 und höher	Version 2.07.2 und höher
Europa (Frankfurt)	Version 3.01.0 und höher	Version 2.07.0 und höher
Europa (Irland)	Version 3.01.0 und höher	Version 2.07.0 und höher
Europa (London)	Version 3.01.0 und höher	Version 2.07.0 und höher
Europa (Milan)	Version 3.01.0 und höher	Version 2.07.1 und höher
Europa (Paris)	Version 3.01.0 und höher	Version 2.07.0 und höher
Europa (Spain)	Version 3.02.0 und höher	–
Europa (Stockholm)	Version 3.01.0 und höher	Version 2.07.0 und höher
Europa (Zürich)	Version 3.02.0 und höher	–
Israel (Tel Aviv)	–	–
Naher Osten (Bahrain)	Version 3.01.0 und höher	Version 2.07.1 und höher
Naher Osten (VAE)	Version 3.02.0 und höher	–

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Südamerika (São Paulo)	Version 3.01.0 und höher	Version 2.07.1 und höher
AWS GovCloud (US-Ost)	Version 3.01.0 und höher	Version 2.07.0 und höher
AWS GovCloud (US-West)	Version 3.01.0 und höher	Version 2.07.0 und höher

Globale Aurora-Datenbanken unterstützen Aurora PostgreSQL

Die folgenden Regionen und Engine-Versionen sind für globale Aurora-Datenbanken mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
USA Ost (Ohio)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
USA Ost (Nord-Virginia)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
USA West (Nordkalifornien)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
USA West (Oregon)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
						11.13 und höher
Afrika (Kapstadt)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Hongkong)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Hyderabad)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Jakarta)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Melbourne)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Asien-Pazifik (Mumbai)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Osaka)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Seoul)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Singapur)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Sydney)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Asien-Pazifik (Tokio)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Kanada (Zentral)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Kanada West (Calgary)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
China (Peking)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
China (Ningxia)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Europa (Frankfurt)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Irland)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (London)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Milan)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Paris)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Europa (Spain)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Stockholm)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Zürich)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Israel (Tel Aviv)	–	–	–	–	–	–
Naher Osten (Bahrain)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Naher Osten (VAE)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Südamerika (São Paulo)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
AWS GovCloud (US-Ost)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
AWS GovCloud (US-West)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Unterstützte Regionen und Aurora-DB-Engines für die IAM-Datenbankauthentifizierung

Mit der IAM-Datenbankauthentifizierung in Aurora können Sie sich mithilfe der AWS Identity and Access Management (IAM) -Datenbankauthentifizierung bei Ihrem DB-Cluster authentifizieren. Mit dieser Authentifizierungsmethode benötigen Sie kein Passwort, um eine Verbindung mit einem DB-Cluster herzustellen. Stattdessen verwenden Sie ein Authentifizierungstoken. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung.

Themen

- IAM-Datenbank-Authentifizierung mit Aurora MySQL
- IAM-Datenbankauthentifizierung mit Aurora PostgreSQL

IAM-Datenbank-Authentifizierung mit Aurora MySQL

Die IAM-Datenbankauthentifizierung mit Aurora MySQL ist in allen Regionen für die folgenden Versionen verfügbar:

- Aurora MySQL 3 – alle verfügbaren Versionen
- Aurora MySQL 2 – alle verfügbaren Versionen

IAM-Datenbankauthentifizierung mit Aurora PostgreSQL

Die IAM-Datenbankauthentifizierung mit Aurora PostgreSQL ist in allen Regionen für die folgenden Versionen verfügbar:

- Aurora PostgreSQL 16 — Alle verfügbaren Versionen
- Aurora PostgreSQL 15 – alle verfügbaren Versionen
- Aurora PostgreSQL 14 – alle verfügbaren Versionen
- Aurora PostgreSQL 13 – alle verfügbaren Versionen
- Aurora PostgreSQL 12 – alle verfügbaren Versionen
- Aurora PostgreSQL 11 – alle verfügbaren Versionen

Unterstützte Regionen und Aurora-DB-Engines für die Kerberos-Authentifizierung

Durch die Verwendung der Kerberos-Authentifizierung mit Aurora können Sie die externe Authentifizierung von Datenbankbenutzern mit Kerberos und Microsoft Active Directory unterstützen. Die Verwendung von Kerberos und Active Directory bietet die Vorteile des Single Sign-Ons und der zentralisierten Authentifizierung von Datenbankbenutzern. Kerberos und Active Directory sind mit AWS Directory Service for Microsoft Active Directory, einer Funktion von verfügbar. AWS Directory Service Weitere Informationen finden Sie unter Kerberos-Authentifizierung.

Themen

- Kerberos-Authentifizierung mit Aurora MySQL
- Kerberos-Authentifizierung mit Aurora PostgreSQL

Kerberos-Authentifizierung mit Aurora MySQL

Die folgenden Regionen und Engine-Versionen sind für die Kerberos-Authentifizierung mit Aurora MySQL verfügbar.

Region	Aurora-MySQL-Version 3
USA Ost (Ohio)	Version 3.03.0 und höher
USA Ost (Nord-Virginia)	Version 3.03.0 und höher
USA West (Nordkalifornien)	Version 3.03.0 und höher
USA West (Oregon)	Version 3.03.0 und höher
Afrika (Kapstadt)	–
Asia Pacific (Hongkong)	–
Asien-Pazifik (Jakarta)	–
Asien-Pazifik (Mumbai)	Version 3.03.0 und höher
Asien-Pazifik (Osaka)	–
Asien-Pazifik (Seoul)	Version 3.03.0 und höher
Asien-Pazifik (Singapur)	Version 3.03.0 und höher
Asien-Pazifik (Sydney)	Version 3.03.0 und höher
Asien-Pazifik (Tokio)	Version 3.03.0 und höher
Kanada (Zentral)	Version 3.03.0 und höher
Kanada West (Calgary)	–
China (Peking)	Version 3.03.0 und höher
China (Ningxia)	Version 3.03.0 und höher
Europa (Frankfurt)	Version 3.03.0 und höher

Region	Aurora-MySQL-Version 3
Europa (Irland)	Version 3.03.0 und höher
Europa (London)	Version 3.03.0 und höher
Europa (Milan)	–
Europa (Paris)	Version 3.03.0 und höher
Europa (Spain)	–
Europa (Stockholm)	Version 3.03.0 und höher
Europa (Zürich)	–
Israel (Tel Aviv)	–
Naher Osten (Bahrain)	–
Naher Osten (VAE)	–
Südamerika (São Paulo)	Version 3.03.0 und höher
AWS GovCloud (US-Ost)	Version 3.03.0 und höher
AWS GovCloud (US-West)	Version 3.03.0 und höher

Kerberos-Authentifizierung mit Aurora PostgreSQL

Die folgenden Regionen und Engine-Versionen sind für die Kerberos-Authentifizierung mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
USA Ost (Ohio)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
USA Ost (Nord-Virginia)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
USA West (Nordkalifornien)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
USA West (Oregon)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Afrika (Kapstadt)	–	–	–	–	–	–
Asien-Pazifik (Hongkong)	–	–	–	–	–	–
Asien-Pazifik (Hyderabad)	–	–	–	–	–	–
Asien-Pazifik (Jakarta)	–	–	–	–	–	–
Asien-Pazifik (Melbourne)	–	–	–	–	–	–

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Asien-Pazifik (Mumbai)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Osaka)	–	–	–	–	–	–
Asien-Pazifik (Seoul)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Singapur)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Sydney)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Tokio)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Kanada (Zentral)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Kanada West (Calgary)	–	–	–	–	–	–
China (Peking)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
China (Ningxia)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Europa (Frankfurt)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Irland)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (London)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Milan)	–	–	–	–	–	–
Europa (Paris)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Spain)	–	–	–	–	–	–
Europa (Stockholm)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Zürich)	–	–	–	–	–	–
Israel (Tel Aviv)	–	–	–	–	–	–
Naher Osten (Bahrain)	–	–	–	–	–	–
Naher Osten (VAE)	–	–	–	–	–	–

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Südamerika (São Paulo)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
AWS GovCloud (US-Ost)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
AWS GovCloud (US-West)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen

Unterstützte Regionen und DB-Engines für Aurora-Machine-Learning

Durch die Verwendung von Amazon Aurora Machine Learning können Sie Ihren Aurora-DB-Cluster je nach Ihren Anforderungen in Amazon Comprehend oder Amazon SageMaker integrieren. Amazon Comprehend und SageMaker beide unterstützen unterschiedliche Anwendungsfälle für maschinelles Lernen. Amazon Comprehend ist ein verwalteter Dienst für die natürliche Sprachverarbeitung (NLP), der verwendet wird, um Informationen aus Dokumenten zu extrahieren. Durch die Verwendung von Aurora Machine Learning mit Amazon Comprehend können Sie die Stimmung von Text in Ihren Datenbanktabellen ermitteln. SageMaker ist ein Service für maschinelles Lernen mit vollem Funktionsumfang. Datenwissenschaftler verwenden Amazon, SageMaker um Modelle für maschinelles Lernen für eine Vielzahl von Inferenzaufgaben zu erstellen, zu trainieren und zu testen, z. B. zur Betrugserkennung. Durch die Verwendung von Aurora Machine Learning mit SageMaker können Datenbankentwickler die SageMaker Funktionalität im SQL-Code aufrufen.

Nicht alle AWS-Regionen unterstützen sowohl Amazon Comprehend als auch SageMaker, und nur bestimmte AWS-Regionen unterstützen Aurora Machine Learning und bieten somit Zugriff auf diese Dienste von einem Aurora-DB-Cluster aus. Der Integrationsprozess für Aurora Machine Learning ist außerdem je nach Datenbank-Engine unterschiedlich. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Machine Learning.

Themen

- Aurora Machine Learning mit Aurora MySQL
- Aurora Machine Learning mit Aurora PostgreSQL

Aurora Machine Learning mit Aurora MySQL

Aurora Machine Learning wird für Aurora MySQL unterstützt, wie in der Tabelle AWS-Regionen aufgeführt. Sie müssen nicht nur Ihre Version von Aurora MySQL verfügbar haben, sondern auch den Dienst unterstützen, den Sie verwenden möchten. AWS-Region Eine Liste, AWS-Regionen wo Amazon verfügbar SageMaker ist, finden Sie unter SageMaker Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz. Eine Liste, AWS-Regionen wo Amazon Comprehend verfügbar ist, finden Sie unter Amazon Comprehend Endpoints and Quotas in der. Allgemeine Amazon Web Services-Referenz

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	Version 3.01.0 und höher	Version 2.07 und höher
USA Ost (Nord-Virginia)	Version 3.01.0 und höher	Version 2.07 und höher
USA West (Nordkalifornien)	Version 3.01.0 und höher	Version 2.07 und höher
USA West (Oregon)	Version 3.01.0 und höher	Version 2.07 und höher
Afrika (Kapstadt)	–	–
Asia Pacific (Hongkong)	Version 3.01.0 und höher	Version 2.07 und höher
Asien-Pazifik (Hyderabad)	Version 3.01.0 und höher	Version 2.07 und höher
Asien-Pazifik (Jakarta)	Version 3.01.0 und höher	Version 2.07 und höher
Asien-Pazifik (Melbourne)	Version 3.01.0 und höher	Version 2.07 und höher
Asien-Pazifik (Mumbai)	Version 3.01.0 und höher	Version 2.07 und höher
Asien-Pazifik (Osaka)	Version 3.01.0 und höher	Version 2.07.3 und höher
Asien-Pazifik (Seoul)	Version 3.01.0 und höher	Version 2.07 und höher
Asien-Pazifik (Singapur)	Version 3.01.0 und höher	Version 2.07 und höher

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Asien-Pazifik (Sydney)	Version 3.01.0 und höher	Version 2.07 und höher
Asien-Pazifik (Tokio)	Version 3.01.0 und höher	Version 2.07 und höher
Kanada (Zentral)	Version 3.01.0 und höher	Version 2.07 und höher
Kanada West (Calgary)	Version 3.01.0 und höher	Version 2.07 und höher
China (Peking)	Version 3.01.0 und höher	Version 2.07 und höher
China (Ningxia)	Version 3.01.0 und höher	Version 2.07 und höher
Europa (Frankfurt)	Version 3.01.0 und höher	Version 2.07 und höher
Europa (Irland)	Version 3.01.0 und höher	Version 2.07 und höher
Europa (London)	Version 3.01.0 und höher	Version 2.07 und höher
Europa (Milan)	–	–
Europa (Paris)	Version 3.01.0 und höher	Version 2.07 und höher
Europa (Spain)	Version 3.01.0 und höher	Version 2.07 und höher
Europa (Stockholm)	Version 3.01.0 und höher	Version 2.07 und höher
Europa (Zürich)	Version 3.01.0 und höher	Version 2.07 und höher
Israel (Tel Aviv)	Version 3.01.0 und höher	Version 2.07 und höher
Naher Osten (Bahrain)	Version 3.01.0 und höher	Version 2.07 und höher
Naher Osten (VAE)	Version 3.01.0 und höher	Version 2.07 und höher
Südamerika (São Paulo)	Version 3.01.0 und höher	Version 2.07 und höher
AWS GovCloud (US-Ost)	Version 3.01.0 und höher	Version 2.07 und höher
AWS GovCloud (US-West)	Version 3.01.0 und höher	Version 2.07 und höher

Aurora Machine Learning mit Aurora PostgreSQL

Aurora Machine Learning wird für Aurora PostgreSQL unterstützt, wie in der AWS-Regionen Tabelle aufgeführt. Sie müssen nicht nur Ihre Version von Aurora PostgreSQL verfügbar haben, sondern auch den AWS-Region Dienst unterstützen, den Sie verwenden möchten. Eine Liste, AWS-Regionen wo Amazon verfügbar SageMaker ist, finden Sie unter SageMaker Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz. Eine Liste, AWS-Regionen wo Amazon Comprehend verfügbar ist, finden Sie unter Amazon Comprehend Endpoints and Quotas in der. Allgemeine Amazon Web Services-Referenz

Die folgenden Regionen und Engine-Versionen sind für Aurora Machine Learning mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
USA Ost (Ohio)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
USA Ost (Nord-Virginia)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
USA West (Nordkalifornien)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
USA West (Oregon)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Afrika (Kapstadt)	–	–	–	–	–	–
Asia Pacific	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
(Hongkong)						
Asien-Pazifik (Hyderabad)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Asien-Pazifik (Jakarta)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Asien-Pazifik (Melbourne)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Asien-Pazifik (Mumbai)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Asien-Pazifik (Osaka)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Asien-Pazifik (Seoul)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Asien-Pazifik (Singapur)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Asien-Pazifik (Sydney)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Asien-Pazifik (Tokio)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Kanada (Zentral)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Kanada West (Calgary)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
China (Peking)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
China (Ningxia)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Europa (Frankfurt)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Europa (Irland)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Europa (London)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Europa (Milan)	–	–	–	–	–	–
Europa (Paris)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Europa (Spain)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Europa (Stockholm)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Europa (Zürich)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Israel (Tel Aviv)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Naher Osten (Bahrain)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Naher Osten (VAE)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
Südamerika (São Paulo)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
AWS GovCloud (US-Ost)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher
AWS GovCloud (US-West)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3	Version 13.3 und höher	Version 12.4 und höher	Version 11.9, 11.12 und höher

Unterstützte Regionen und Aurora-DB-Engines für Performance Insights

Performance-Insights erweitert die vorhandenen Amazon-RDS-Überwachungsfunktionen, um die Leistung Ihrer Datenbank zu veranschaulichen und zu analysieren. Mit dem Performance-Insights-Dashboard können Sie die Datenbanklast Ihrer DB-Instance von Amazon RDS visualisieren und die Last nach Wartezeiten, SQL-Anweisungen, Hosts oder Benutzern filtern. Weitere Informationen finden Sie unter Übersicht über Performance-Insights für Amazon Aurora.

Informationen zur Unterstützung von Performance-Insights-Funktionen nach Region, DB-Engine und Instance-Klasse finden Sie unter DB-Engine-, Regions- und Instance-Klassenunterstützung von Amazon Aurora für Performance-Insights-Funktionen.

Themen

- Performance-Insights mit Aurora MySQL
- Performance-Insights mit Aurora PostgreSQL
- Performance-Insights mit Aurora Serverless

Performance-Insights mit Aurora MySQL

> **Note**
>
> Die Unterstützung der Engine-Version ist für Performance-Insights mit Aurora MySQL anders, wenn Sie parallele Abfragen aktiviert haben. Weitere Informationen zu parallelen Abfragen finden Sie unter Arbeiten mit Parallel Query für Amazon Aurora MySQL.

Themen

Performance-Insights mit Aurora MySQL und deaktivierter paralleler Abfragefunktion

Die folgenden Regionen und Engine-Versionen sind für Performance Insights mit Aurora MySQL und deaktivierter Parallelabfragefunktion verfügbar.

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	Alle Versionen	Alle Versionen
USA Ost (Nord-Virginia)	Alle Versionen	Alle Versionen
USA West (Nordkalifornien)	Alle Versionen	Alle Versionen
USA West (Oregon)	Alle Versionen	Alle Versionen
Afrika (Kapstadt)	Alle Versionen	Alle Versionen
Asien-Pazifik (Hongkong)	Alle Versionen	Alle Versionen
Asien-Pazifik (Hyderabad)	Alle Versionen	Alle Versionen
Asien-Pazifik (Jakarta)	Alle Versionen	Alle Versionen
Asien-Pazifik (Melbourne)	Alle Versionen	Alle Versionen
Asien-Pazifik (Mumbai)	Alle Versionen	Alle Versionen
Asien-Pazifik (Osaka)	Alle Versionen	Alle Versionen
Asien-Pazifik (Seoul)	Alle Versionen	Alle Versionen
Asien-Pazifik (Singapur)	Alle Versionen	Alle Versionen
Asien-Pazifik (Sydney)	Alle Versionen	Alle Versionen
Asien-Pazifik (Tokio)	Alle Versionen	Alle Versionen

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Kanada (Zentral)	Alle Versionen	Alle Versionen
Kanada West (Calgary)	Alle Versionen	Alle Versionen
China (Peking)	Alle Versionen	Alle Versionen
China (Ningxia)	Alle Versionen	Alle Versionen
Europa (Frankfurt)	Alle Versionen	Alle Versionen
Europa (Irland)	Alle Versionen	Alle Versionen
Europa (London)	Alle Versionen	Alle Versionen
Europa (Milan)	Alle Versionen	Alle Versionen
Europa (Paris)	Alle Versionen	Alle Versionen
Europa (Spain)	Alle Versionen	Alle Versionen
Europa (Stockholm)	Alle Versionen	Alle Versionen
Europa (Zürich)	Alle Versionen	Alle Versionen
Israel (Tel Aviv)	Alle Versionen	Alle Versionen
Naher Osten (Bahrain)	Alle Versionen	Alle Versionen
Naher Osten (VAE)	Alle Versionen	Alle Versionen
Südamerika (São Paulo)	Alle Versionen	Alle Versionen
AWS GovCloud (USA-Ost)	Alle Versionen	Alle Versionen
AWS GovCloud (US-West)	Alle Versionen	Alle Versionen

Performance-Insights mit Aurora MySQL und aktivierter paralleler Abfragefunktion

Die folgenden Regionen und Engine-Versionen sind für Performance Insights mit Aurora MySQL und aktivierter Parallelabfragefunktion verfügbar.

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	–	Version 2.09.0 und höher
USA Ost (Nord-Virginia)	–	Version 2.09.0 und höher
USA West (Nordkalifornien)	–	Version 2.09.0 und höher
USA West (Oregon)	–	Version 2.09.0 und höher
Afrika (Kapstadt)	–	Version 2.09.0 und höher
Asien-Pazifik (Hongkong)	–	Version 2.09.0 und höher
Asien-Pazifik (Hyderabad)	–	Alle Versionen
Asien-Pazifik (Jakarta)	–	Version 2.09.0 und höher
Asien-Pazifik (Melbourne)	–	Version 2.09.0 und höher
Asien-Pazifik (Mumbai)	–	Version 2.09.0 und höher
Asien-Pazifik (Osaka)	–	Version 2.09.0 und höher
Asien-Pazifik (Seoul)	–	Version 2.09.0 und höher
Asien-Pazifik (Singapur)	–	Version 2.09.0 und höher
Asien-Pazifik (Sydney)	–	Version 2.09.0 und höher
Asien-Pazifik (Tokio)	–	Version 2.09.0 und höher
Kanada (Zentral)	–	Version 2.09.0 und höher
Kanada West (Calgary)	–	Version 2.09.0 und höher
China (Peking)	–	Version 2.09.0 und höher

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
China (Ningxia)	–	Version 2.09.0 und höher
Europa (Frankfurt)	–	Version 2.09.0 und höher
Europa (Irland)	–	Version 2.09.0 und höher
Europa (London)	–	Version 2.09.0 und höher
Europa (Milan)	–	Version 2.09.0 und höher
Europa (Paris)	–	Version 2.09.0 und höher
Europa (Spain)	–	Version 2.09.0 und höher
Europa (Stockholm)	–	Version 2.09.0 und höher
Europa (Zürich)	–	Version 2.09.0 und höher
Israel (Tel Aviv)	–	Version 2.09.0 und höher
Naher Osten (Bahrain)	–	Version 2.09.0 und höher
Naher Osten (VAE)	–	Version 2.09.0 und höher
Südamerika (São Paulo)	–	Version 2.09.0 und höher
AWS GovCloud (US-Ost)	–	Version 2.09.0 und höher
AWS GovCloud (US-West)	–	Version 2.09.0 und höher

Performance-Insights mit Aurora PostgreSQL

Die folgenden Regionen und Engine-Versionen sind für Performance Insights mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11	Aurora PostgreSQL 10
USA Ost (Ohio)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
USA Ost (Nord-Virginia)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
USA West (Nordkalifornien)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
USA West (Oregon)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Afrika (Kapstadt)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Hongkong)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Hyderabad)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Jakarta)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11	Aurora PostgreSQL 10
Asien-Pazifik (Melbourne)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Mumbai)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Osaka)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Seoul)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Singapur)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Sydney)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Asien-Pazifik (Tokio)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Kanada (Zentral)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11	Aurora PostgreSQL 10
Kanada West (Calgary)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
China (Peking)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
China (Ningxia)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Frankfurt)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Irland)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (London)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Milan)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Paris)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Spain)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Stockholm)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Europa (Zürich)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11	Aurora PostgreSQL 10
Israel (Tel Aviv)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Naher Osten (Bahrain)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Naher Osten (VAE)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
Südamerika (São Paulo)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
AWS GovCloud (US-Ost)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen
AWS GovCloud (US-West)	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen	Alle Versionen

Performance-Insights mit Aurora Serverless

Aurora Serverless v2 unterstützt Performance Insights für alle MySQL-kompatiblen und PostgreSQL-kompatiblen Versionen. Wir empfehlen, die Mindestkapazität auf mindestens 2 Aurora-Kapazitätseinheiten (ACUs) einzustellen.

Aurora Serverless v1 unterstützt Performance Insights nicht.

Unterstützte Regionen und Aurora-DB-Engines für Zero-ETL-Integrationen mit Amazon Redshift

Bei Null-ETL-Integrationen von Amazon Aurora in Amazon Redshift handelt es sich um eine vollständig verwaltete Lösung, die Transaktionsdaten in Amazon Redshift verfügbar macht, nachdem diese in einen Aurora-Cluster geschrieben wurden. Weitere Informationen finden Sie unter .

Die folgenden Regionen und Engine-Versionen sind für Null-ETL-Integrationen in Amazon Redshift verfügbar.

Themen

Aurora MySQL Zero-ETL-Integrationen

Region	Aurora-MySQL-Version 3
USA Ost (Nord-Virginia)	Version 3.05.2 und höher
USA Ost (Ohio)	Version 3.05.2 und höher
USA West (Oregon)	Version 3.05.2 und höher
USA West (Nordkalifornien)	Version 3.05.2 und höher
Asien-Pazifik (Tokio)	Version 3.05.2 und höher
Asien-Pazifik (Singapur)	Version 3.05.2 und höher
Asien-Pazifik (Seoul)	Version 3.05.2 und höher
Asien-Pazifik (Mumbai)	Version 3.05.2 und höher
Asien-Pazifik (Hongkong)	Version 3.05.2 und höher
Asien-Pazifik (Osaka)	Version 3.05.2 und höher
Asien-Pazifik (Sydney)	Version 3.05.2 und höher

Region	Aurora-MySQL-Version 3
Europa (Frankfurt)	Version 3.05.2 und höher
Europa (Stockholm)	Version 3.05.2 und höher
Europa (Irland)	Version 3.05.2 und höher
Europa (Paris)	Version 3.05.2 und höher
Europa (London)	Version 3.05.2 und höher
Europa (Milan)	Version 3.05.2 und höher
Südamerika (São Paulo)	Version 3.05.2 und höher
Kanada (Zentral)	Version 3.05.2 und höher
Naher Osten (Bahrain)	Version 3.05.2 und höher
Afrika (Kapstadt)	Version 3.05.2 und höher
China (Peking)	Version 3.05.2 und höher
China (Ningxia)	Version 3.05.2 und höher

Aurora PostgreSQL Zero-ETL-Integrationen

Für die Vorabversion der Aurora PostgreSQL Zero-ETL-Integrationen mit Amazon Redshift müssen Sie Integrationen innerhalb der Amazon RDS Database Preview-Umgebung im Osten der USA (Ohio) (us-east-2) erstellen. AWS-Region In der Vorschauumgebung können Sie Beta-, Release Candidate- und frühe Produktionsversionen der PostgreSQL-Datenbank-Engine-Software testen.

Auf Ihrem Quell-DB-Cluster muss Aurora PostgreSQL ausgeführt werden (kompatibel mit PostgreSQL 15.4 und Zero-ETL Support).

Unterstützte Regionen und Aurora-DB-Engines für Amazon RDS Proxy

Amazon RDS Proxy ist ein vollständig verwalteter, hochverfügbarer Datenbank-Proxy, der Anwendungen durch Bündelung und gemeinsame Nutzung etablierter Datenbankverbindungen

skalierbarer macht. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

Themen

- Amazon RDS Proxy mit Aurora MySQL
- Amazon RDS Proxy mit Aurora PostgreSQL

Amazon RDS Proxy mit Aurora MySQL

Die folgenden Regionen und Engine-Versionen sind für RDS Proxy mit Aurora MySQL verfügbar.

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
USA Ost (Nord-Virginia)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
USA West (Nordkalifornien)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
USA West (Oregon)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Afrika (Kapstadt)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Hongkong)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Hyderabad)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Jakarta)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Melbourne)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Asien-Pazifik (Mumbai)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Osaka)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Seoul)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Singapur)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Sydney)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Asien-Pazifik (Tokio)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Kanada (Zentral)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Kanada West (Calgary)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
China (Peking)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
China (Ningxia)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Europa (Frankfurt)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Europa (Irland)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Europa (London)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Europa (Milan)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Europa (Paris)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Europa (Spain)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Europa (Stockholm)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Europa (Zürich)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Israel (Tel Aviv)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Naher Osten (Bahrain)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Naher Osten (VAE)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
Südamerika (São Paulo)	Version 3.01.0 und höher	Version 2.07 sowie Version 2.11 und höher
AWS GovCloud (USA-Ost)	–	–
AWS GovCloud (US-West)	–	–

Amazon RDS Proxy mit Aurora PostgreSQL

Die folgenden Regionen und Engine-Versionen sind für RDS Proxy mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
USA Ost (Ohio)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
USA Ost (Nord-Virginia)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
USA West (Nordkalifornien)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
USA West (Oregon)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Afrika (Kapstadt)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Hongkong)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
						11.13 und höher
Asien-Pazifik (Hyderabad)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Jakarta)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Melbourne)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Mumbai)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Osaka)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Asien-Pazifik (Seoul)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Singapur)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Sydney)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Asien-Pazifik (Tokio)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Kanada (Zentral)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Kanada West (Calgary)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
China (Peking)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
China (Ningxia)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Frankfurt)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Irland)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Europa (London)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Milan)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Paris)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Spain)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Europa (Stockholm)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
Europa (Zürich)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Israel (Tel Aviv)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Naher Osten (Bahrain)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Naher Osten (VAE)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
Südamerika (São Paulo)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.4 und höher	Version 12.8 und höher	Version 11.9 sowie Version 11.13 und höher
AWS GovCloud (US-Ost)	–	–	–	–	–	–

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13	Aurora PostgreSQL 12	Aurora PostgreSQL 11
AWS GovCloud (US-West)	–	–	–	–	–	–

Unterstützte Regionen und Aurora-DB-Engines für die Secrets Manager Manager-Integration

Mit AWS Secrets Manager können Sie hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Datenbankkennwörtern, durch einen API-Aufruf an Secrets Manager ersetzen, um das Geheimnis programmgesteuert abzurufen. Weitere Informationen zu Secrets Manager finden Sie im Benutzerhandbuch für AWS Secrets Manager.

Sie können angeben, dass Amazon Aurora das Hauptbenutzerpasswort in Secrets Manager für einen Aurora-DB-Cluster verwaltet. Aurora generiert das Passwort, speichert es in Secrets Manager und wechselt es regelmäßig. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager.

Secrets Manager ist für alle Aurora-DB-Engines und alle Versionen verfügbar.

Die Secrets Manager Manager-Integration ist in allen AWS-Regionen außer den folgenden verfügbar:

- Kanada West (Calgary)
- AWS GovCloud (US-Ost)
- AWS GovCloud (US-West)

Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2

Aurora Serverless v2 ist eine On-Demand-Funktion für die automatische Skalierung, die als kostengünstiger Ansatz für die Ausführung intermittierender oder unvorhersehbarer Workloads auf Amazon Aurora entwickelt wurde. Die Kapazität wird je nach Bedarf Ihrer Anwendungen hoch- oder herunterskaliert. Die Skalierung ist schneller und stärker granular als mit Aurora Serverless v1. Mit Aurora Serverless v2 kann jeder Cluster eine Writer-DB-Instance und mehrere Reader-DB-Instances enthalten. Sie können Aurora Serverless v2 und traditionelle bereitgestellte DB-Instances innerhalb

desselben Clusters kombinieren. Weitere Informationen finden Sie unter Verwenden von Aurora Serverless v2.

Themen

- Aurora Serverless v2 mit Aurora MySQL
- Aurora Serverless v2 mit Aurora PostgreSQL

Aurora Serverless v2 mit Aurora MySQL

Die folgenden Regionen und Engine-Versionen sind für Aurora Serverless v2 mit Aurora MySQL verfügbar.

Region	Aurora-MySQL-Version 3
USA Ost (Ohio)	Version 3.02.0 und höher
USA Ost (Nord-Virginia)	Version 3.02.0 und höher
USA West (Nordkalifornien)	Version 3.02.0 und höher
USA West (Oregon)	Version 3.02.0 und höher
Afrika (Kapstadt)	Version 3.02.0 und höher
Asien-Pazifik (Hongkong)	Version 3.02.0 und höher
Asien-Pazifik (Hyderabad)	Version 3.02.3 und höher
Asien-Pazifik (Jakarta)	Version 3.02.0 und höher
Asien-Pazifik (Melbourne)	Version 3.02.3 und höher
Asien-Pazifik (Mumbai)	Version 3.02.0 und höher
Asien-Pazifik (Osaka)	Version 3.02.0 und höher
Asien-Pazifik (Seoul)	Version 3.02.0 und höher
Asien-Pazifik (Singapur)	Version 3.02.0 und höher

Region	Aurora-MySQL-Version 3
Asien-Pazifik (Sydney)	Version 3.02.0 und höher
Asien-Pazifik (Tokio)	Version 3.02.0 und höher
Kanada (Zentral)	Version 3.02.0 und höher
Kanada West (Calgary)	Versionen 3.04.0, 3.04.1, 3.05.0, 3.05.1 und höher
China (Peking)	Version 3.02.2 und höher
China (Ningxia)	Version 3.02.2 und höher
Europa (Frankfurt)	Version 3.02.0 und höher
Europa (Irland)	Version 3.02.0 und höher
Europa (London)	Version 3.02.0 und höher
Europa (Milan)	Version 3.02.0 und höher
Europa (Paris)	Version 3.02.0 und höher
Europa (Spain)	Version 3.02.3 und höher
Europa (Stockholm)	Version 3.02.0 und höher
Europa (Zürich)	Version 3.02.3 und höher
Israel (Tel Aviv)	Versionen 3.02.3 und höher, 3.03.1 und höher
Naher Osten (Bahrain)	Version 3.02.0 und höher
Naher Osten (VAE)	Version 3.02.3 und höher
Südamerika (São Paulo)	Version 3.02.0 und höher
AWS GovCloud (US-Ost)	Version 3.02.2 und höher
AWS GovCloud (US-West)	Version 3.02.2 und höher

Aurora Serverless v2 mit Aurora PostgreSQL

Die folgenden Regionen und Engine-Versionen sind für Aurora Serverless v2 mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13
USA Ost (Ohio)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
USA Ost (Nord-Virginia)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
USA West (Nordkalifornien)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
USA West (Oregon)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Afrika (Kapstadt)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Asien-Pazifik (Hongkong)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Asien-Pazifik (Hyderabad)	Version 16.1 und höher	Version 15.2 und höher	Version 14.6 und höher	Version 13.9 und höher
Asien-Pazifik (Jakarta)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Asien-Pazifik (Melbourne)	Version 16.1 und höher	Version 15.2 und höher	Version 14.6 und höher	Version 13.9 und höher
Asien-Pazifik (Mumbai)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Asien-Pazifik (Osaka)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13
Asien-Pazifik (Seoul)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Asien-Pazifik (Singapur)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Asien-Pazifik (Sydney)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Asien-Pazifik (Tokio)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Kanada (Zentral)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Kanada West (Calgary)	Version 16.1 und höher	Version 15.3 und höher	Version 14.6, 14.8 und höher	Version 13.9, 13.11 und höher
China (Peking)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
China (Ningxia)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Europa (Frankfurt)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Europa (Irland)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Europa (London)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Europa (Milan)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13
Europa (Paris)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Europa (Spain)	Version 16.1 und höher	Version 15.2 und höher	Version 14.6 und höher	Version 13.9 und höher
Europa (Stockholm)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Europa (Zürich)	Version 16.1 und höher	Version 15.2 und höher	Version 14.6 und höher	Version 13.9 und höher
Israel (Tel Aviv)	Version 16.1 und höher	Version 15.2 und höher	Version 14.6 und höher	Version 13.9 und höher
Naher Osten (Bahrain)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
Naher Osten (VAE)	Version 16.1 und höher	Version 15.2 und höher	Version 14.6 und höher	Version 13.9 und höher
Südamerika (São Paulo)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
AWS GovCloud (US-Ost)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher
AWS GovCloud (US-West)	Version 16.1 und höher	Version 15.2 und höher	Version 14.3 und höher	Version 13.6 und höher

Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless Version 1

Aurora Serverless v1 ist eine On-Demand-Funktion für die automatische Skalierung, die als kostengünstiger Ansatz für die Ausführung intermittierender oder unvorhersehbarer Workloads auf

Amazon Aurora entwickelt wurde. Der Service kann automatisch starten, herunterfahren und die Kapazität je nach Bedarf Ihrer Anwendungen hoch- oder herunterskalieren. Dabei wird eine einzelne DB-Instance in jedem Cluster verwendet. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Serverless v1.

Themen

- Aurora Serverless v1 mit Aurora MySQL
- Aurora Serverless v1 mit Aurora PostgreSQL

Aurora Serverless v1 mit Aurora MySQL

Die folgenden Regionen und Engine-Versionen sind für Aurora Serverless v1 mit Aurora MySQL verfügbar.

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	–	Version 2.11.4
USA Ost (Nord-Virginia)	–	Ausführung 2.11.4
USA West (Nordkalifornien)	–	Ausführung 2.11.4
USA West (Oregon)	–	Ausführung 2.11.4
Afrika (Kapstadt)	–	–
Asien-Pazifik (Hongkong)	–	–
Asien-Pazifik (Hyderabad)	–	–
Asien-Pazifik (Jakarta)	–	–
Asien-Pazifik (Melbourne)	–	–
Asien-Pazifik (Mumbai)	–	Ausführung 2.11.4
Asien-Pazifik (Osaka)	–	–
Asien-Pazifik (Seoul)	–	Ausführung 2.11.4

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Asien-Pazifik (Singapur)	–	Ausführung 2.11.4
Asien-Pazifik (Sydney)	–	Ausführung 2.11.4
Asien-Pazifik (Tokio)	–	Ausführung 2.11.4
Kanada (Zentral)	–	Ausführung 2.11.4
Kanada West (Calgary)	–	–
China (Peking)	–	–
China (Ningxia)	–	Ausführung 2.11.4
Europa (Frankfurt)	–	Ausführung 2.11.4
Europa (Irland)	–	Ausführung 2.11.4
Europa (London)	–	Ausführung 2.11.4
Europa (Milan)	–	–
Europa (Paris)	–	Ausführung 2.11.4
Europa (Spain)	–	–
Europa (Stockholm)	–	–
Europa (Zürich)	–	–
Israel (Tel Aviv)	–	–
Naher Osten (Bahrain)	–	–
Naher Osten (VAE)	–	–
Südamerika (São Paulo)	–	–
AWS GovCloud (US-Ost)	–	–

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
AWS GovCloud (US-West)	–	–

Aurora Serverless v1 mit Aurora PostgreSQL

Die folgenden Regionen und Engine-Versionen sind für Aurora Serverless v1 mit Aurora PostgreSQL verfügbar.

Region	Aurora PostgreSQL 13
USA Ost (Ohio)	Ausführung 13.12
USA Ost (Nord-Virginia)	Ausführung 13.12
USA West (Nordkalifornien)	Ausführung 13.12
USA West (Oregon)	Ausführung 13.12
Afrika (Kapstadt)	–
Asien-Pazifik (Hongkong)	–
Asien-Pazifik (Hyderabad)	–
Asien-Pazifik (Jakarta)	–
Asien-Pazifik (Melbourne)	–
Asien-Pazifik (Mumbai)	Ausführung 13.12
Asien-Pazifik (Osaka)	–
Asien-Pazifik (Seoul)	Ausführung 13.12
Asien-Pazifik (Singapur)	Ausführung 13.12
Asien-Pazifik (Sydney)	Ausführung 13.12
Asien-Pazifik (Tokio)	Ausführung 13.12

Region	Aurora PostgreSQL 13
Kanada (Zentral)	Ausführung 13.12
Kanada West (Calgary)	–
China (Peking)	–
China (Ningxia)	–
Europa (Frankfurt)	Ausführung 13.12
Europa (Irland)	Ausführung 13.12
Europa (London)	Ausführung 13.12
Europa (Milan)	–
Europa (Paris)	Ausführung 13.12
Europa (Spain)	–
Europa (Stockholm)	–
Europa (Zürich)	–
Israel (Tel Aviv)	–
Naher Osten (Bahrain)	–
Naher Osten (VAE)	–
Südamerika (São Paulo)	–
AWS GovCloud (US-Ost)	–
AWS GovCloud (US-West)	–

Unterstützte Regionen und Aurora-DB-Engines für die RDS-Daten-API

Die RDS Data API (Data API) bietet eine Web-Services-Schnittstelle zu einem Amazon Aurora Aurora-DB-Cluster. Anstatt Datenbankverbindungen von Clientanwendungen aus zu verwalten, können Sie SQL-Befehle für einen HTTPS-Endpunkt ausführen. Weitere Informationen finden Sie unter Verwenden der RDS-Daten-API.

Für Aurora MySQL wird die Daten-API für Aurora Serverless v2 oder für bereitgestellte DB-Cluster nicht unterstützt.

Themen

Daten-API mit Aurora MySQL Serverless v1

Die folgenden Regionen und Engine-Versionen sind für Data API mit Aurora MySQL Serverless v1 verfügbar.

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	–	Version 2.11.3
USA Ost (Nord-Virginia)	–	Version 2.11.3
USA West (Nordkalifornien)	–	Version 2.11.3
USA West (Oregon)	–	Version 2.11.3
Afrika (Kapstadt)	–	–
Asien-Pazifik (Hongkong)	–	–
Asien-Pazifik (Hyderabad)	–	–
Asien-Pazifik (Jakarta)	–	–
Asien-Pazifik (Melbourne)	–	–

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Asien-Pazifik (Mumbai)	–	Version 2.11.3
Asien-Pazifik (Osaka)	–	–
Asien-Pazifik (Seoul)	–	Version 2.11.3
Asien-Pazifik (Singapur)	–	Version 2.11.3
Asien-Pazifik (Sydney)	–	Version 2.11.3
Asien-Pazifik (Tokio)	–	Version 2.11.3
Kanada (Zentral)	–	Version 2.11.3
Kanada West (Calgary)	–	–
China (Peking)	–	–
China (Ningxia)	–	Version 2.11.3
Europa (Frankfurt)	–	Version 2.11.3
Europa (Irland)	–	Version 2.11.3
Europa (London)	–	Version 2.11.3
Europa (Milan)	–	–
Europa (Paris)	–	Version 2.11.3
Europa (Spain)	–	–
Europa (Stockholm)	–	–
Europa (Zürich)	–	–
Israel (Tel Aviv)	–	–
Naher Osten (Bahrain)	–	–

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Naher Osten (VAE)	–	–
Südamerika (São Paulo)	–	–
AWS GovCloud (US-Ost)	–	–
AWS GovCloud (US-West)	–	–

Daten-API mit Aurora PostgreSQL Serverless v2 und bereitgestellt

Die folgenden Regionen und Engine-Versionen sind für die Daten-API mit Aurora PostgreSQL Serverless v2 und bereitgestellten DB-Clustern verfügbar.

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13
US East (Ohio)	–	–	–	–
USA Ost (Nord-Virginia)	Version 16.1 und höher	Version 15.3 und höher	Version 14.8 und höher	Version 13.11 und höher
USA West (Nordkalifornien)	–	–	–	–
USA West (Oregon)	Version 16.1 und höher	Version 15.3 und höher	Version 14.8 und höher	Version 13.11 und höher
Afrika (Kapstadt)	–	–	–	–
Asien-Pazifik (Hongkong)	–	–	–	–
Asien-Pazifik (Hyderabad)	–	–	–	–
Asien-Pazifik (Jakarta)	–	–	–	–

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13
Asien-Pazifik (Melbourne)	–	–	–	–
Asien-Pazifik (Mumbai)	–	–	–	–
Asia Pacific (Osaka)	–	–	–	–
Asia Pacific (Seoul)	–	–	–	–
Asien-Pazifik (Singapur)	–	–	–	–
Asien-Pazifik (Sydney)	–	–	–	–
Asien-Pazifik (Tokio)	Version 16.1 und höher	Version 15.3 und höher	Version 14.8 und höher	Version 13.11 und höher
Kanada (Zentral)	–	–	–	–
Kanada West (Calgary)	–	–	–	–
China (Peking)	–	–	–	–
China (Ningxia)	–	–	–	–
Europa (Frankfurt)	Version 16.1 und höher	Version 15.3 und höher	Version 14.8 und höher	Version 13.11 und höher
Europa (Irland)	–	–	–	–
Europa (London)	–	–	–	–

Region	Aurora PostgreSQL 16	Aurora PostgreSQL 15	Aurora PostgreSQL 14	Aurora PostgreSQL 13
Europa (Milan)	–	–	–	–
Europa (Paris)	–	–	–	–
Europa (Spain)	–	–	–	–
Europa (Stockholm)	–	–	–	–
Europa (Zürich)	–	–	–	–
Israel (Tel Aviv)	–	–	–	–
Naher Osten (Bahrain)	–	–	–	–
Naher Osten (VAE)	–	–	–	–
Südamerika (São Paulo)	–	–	–	–
AWS GovCloud (US-Ost)	–	–	–	–
AWS GovCloud (US-West)	–	–	–	–

Daten-API mit Aurora PostgreSQL Serverless v1

Die folgenden Regionen und Engine-Versionen sind für Data API mit Aurora PostgreSQL Serverless v1 verfügbar.

Region	Aurora PostgreSQL 13	Aurora PostgreSQL 11
USA Ost (Ohio)	Version 13.9	Version 11.18

Region	Aurora PostgreSQL 13	Aurora PostgreSQL 11
USA Ost (Nord-Virginia)	Version 13.9	Version 11.18
USA West (Nordkalifornien)	Version 13.9	Version 11.18
USA West (Oregon)	Version 13.9	Version 11.18
Afrika (Kapstadt)	–	–
Asien-Pazifik (Hongkong)	–	–
Asien-Pazifik (Hyderabad)	–	–
Asien-Pazifik (Jakarta)	–	–
Asien-Pazifik (Melbourne)	–	–
Asien-Pazifik (Mumbai)	Version 13.9	Version 11.18
Asien-Pazifik (Osaka)	–	–
Asien-Pazifik (Seoul)	Version 13.9	Version 11.18
Asien-Pazifik (Singapur)	Version 13.9	Version 11.18
Asien-Pazifik (Sydney)	Version 13.9	Version 11.18
Asien-Pazifik (Tokio)	Version 13.9	Version 11.18
Kanada (Zentral)	Version 13.9	Version 11.18
China (Peking)	–	–
China (Ningxia)	–	–
Europa (Frankfurt)	Version 13.9	Version 11.18
Europa (Irland)	Version 13.9	Version 11.18
Europa (London)	Version 13.9	Version 11.18

Region	Aurora PostgreSQL 13	Aurora PostgreSQL 11
Europa (Milan)	–	–
Europa (Paris)	Version 13.9	Version 11.18
Europa (Spain)	–	–
Europa (Stockholm)	–	–
Europa (Zürich)	–	–
Israel (Tel Aviv)	–	–
Naher Osten (Bahrain)	–	–
Naher Osten (VAE)	–	–
Südamerika (São Paulo)	–	–
AWS GovCloud (US-Ost)	–	–
AWS GovCloud (US-West)	–	–

Unterstützte Regionen und Aurora-DB-Engines für Patching ohne Ausfallzeiten (ZDP)

Das Durchführen von Upgrades für Aurora-DB-Cluster beinhaltet die Möglichkeit eines Ausfalls, wenn die Datenbank heruntergefahren wird und während sie aktualisiert wird. Wenn Sie das Upgrade starten, während die Datenbank ausgelastet ist, verlieren Sie standardmäßig alle Verbindungen und Transaktionen, die der DB-Cluster verarbeitet. Wenn Sie warten, bis die Datenbank im Leerlauf ist, um das Upgrade durchzuführen, müssen Sie möglicherweise lange warten.

Die Funktion Zero-Downtime-Patching (ZDP) versucht, Client-Verbindungen während eines Aurora-Upgrades auf Best-Effort-Basis aufrechtzuerhalten. Wenn das ZDP erfolgreich abgeschlossen wird, werden Anwendungssitzungen bewahrt und die Datenbank-Engine wird während der laufenden Aktualisierung neu gestartet. Der Neustart der Datenbank-Engine kann zu einem Abfall des Durchsatzes von eingen Sekunden bis 1 Minute führen.

Detaillierte Informationen zu den Bedingungen und Engine-Versionen, unter denen ZDP für Aurora-MySQL-Upgrades verfügbar ist, finden Sie unter Verwendung von Zero-Downtime-Patching (Patchen ohne Ausfallzeiten).

Detaillierte Informationen zu den Bedingungen und Engine-Versionen, unter denen ZDP für Aurora-PostgreSQL-Upgrades verfügbar ist, finden Sie unter Nebenversions-Upgrades und Zero-Downtime-Patching.

Unterstützte Regionen und DB-Engines für native Funktionen der Aurora-Engine

Aurora-Datenbank-Engines unterstützen auch zusätzliche Funktionen speziell für Aurora. Einige Engine-native Funktionen werden möglicherweise nur begrenzt unterstützt oder haben eingeschränkte Berechtigungen für eine bestimmte Aurora-DB-Engine, -Version oder Region.

Themen

- Engine-native Funktionen für Aurora MySQL
- Engine-native Funktionen für Aurora PostgreSQL

Engine-native Funktionen für Aurora MySQL

Im Folgenden sind die Engine-nativen Funktionen für Aurora MySQL aufgeführt.

- Erweitertes Auditing
- Backtrack
- Fehlersimulationsabfragen
- Clusterinterne Schreibweiterleitung
- Parallele Abfrage

Engine-native Funktionen für Aurora PostgreSQL

Im Folgenden sind die Engine-native Funktionen für Aurora PostgreSQL aufgeführt.

- Babelfish
- Fehlersimulationsabfragen
- Abfrageplanverwaltung

Amazon Aurora-Verbindungsverwaltung

Bei Amazon Aurora kommt in der Regel keine einzelne Instance, sondern ein Cluster von DB-Instances zum Einsatz. Jede Verbindung wird von einer bestimmten DB-Instance verarbeitet. Wenn Sie eine Verbindung zu einem Aurora-Cluster herstellen, verweisen der von Ihnen angegebene Hostname und Port auf einen zwischengeschalteten Handler, der als Endpunkt bezeichnet wird. Aurora verwendet den Endpunktmechanismus, um diese Verbindungen zu abstrahieren. Somit müssen Sie nicht alle Hostnamen fest codieren oder Ihre eigene Logik für den Verbindungsausgleich und die Umleitung von Verbindungen schreiben, wenn einige DB-Instances nicht verfügbar sind.

Bei bestimmten Aurora-Aufgaben führen verschiedene Instances oder Gruppen von Instances unterschiedliche Rollen aus. Beispielsweise verarbeitet die primäre Instance alle Data Definition Language (DDL)- und Data Manipulation Language (DML)-Anweisungen. Der schreibgeschützte Abfragedatenverkehr wird von bis zu 15 Aurora-Replicas verarbeitet.

Ihrem Anwendungsfall entsprechend können Sie mit Endpunkten jede Verbindung der entsprechenden Instance oder Gruppe von Instances zuordnen. Zum Ausführen von DDL-Anweisungen können Sie beispielsweise eine Verbindung mit der Instance herstellen, die als primäre Instance fungiert. Um Abfragen durchzuführen, können Sie eine Verbindung zum Reader-Endpunkt herstellen, wobei Aurora automatisch den Verbindungsausgleich zwischen allen Aurora Replicas durchführt. Bei Clustern mit DB-Instances unterschiedlicher Kapazitäten oder Konfigurationen besteht die Möglichkeit, eine Verbindung mit benutzerdefinierten Endpunkten herzustellen, die mit unterschiedlichen Untergruppen von DB-Instances verknüpft sind. Zur Diagnose und Optimierung können Sie eine Verbindung mit einem spezifischen Instance-Endpunkt herstellen, um die Details einer bestimmten DB-Instance zu untersuchen.

Themen

- AWS CLI End-to-End-Beispiel für benutzerdefinierte Endpunkte
- Verwenden der Instance-Endpunkte
- Funktionsweise von Aurora-Endpunkten mit hoher Verfügbarkeit

Typen von Aurora-Endpunkten

Ein Endpunkt wird als eine Aurora-spezifische URL dargestellt, die eine Hostadresse und einen Port enthält. In einem Aurora-DB-Cluster stehen die folgenden Endpunkt-Typen zur Verfügung:

Cluster-Endpunkt

Ein Cluster-Endpunkt (oder Writer-Endpunkt) für einen Aurora-DB-Cluster stellt eine Verbindung zur aktuellen primären DB-Instance für diesen DB-Cluster her. Nur dieser Endpunkt kann Schreibvorgänge wie z. B. DDL-Anweisungen durchführen. Aus diesem Grund sollten Sie eine Verbindung zum Cluster-Endpunkt herstellen, wenn Sie zum ersten Mal einen Cluster einrichten oder Ihr Cluster nur eine DB-Instance enthält.

Jeder Aurora-DB-Cluster verfügt über einen Cluster-Endpunkt und eine primäre DB-Instance.

Sie verwenden den Cluster-Endpunkt für alle Schreibvorgänge auf dem DB-Cluster, darunter Einfügungs-, Aktualisierungs- und Löschvorgänge sowie DDL-Änderungen. Sie können den Cluster-Endpunkt auch für Lesevorgänge nutzen, beispielsweise Abfragen.

Der Cluster-Endpunkt bietet Failover-Support für Lese-/Schreibverbindungen zum DB-Cluster. Wenn die aktuelle primäre DB-Instance eines DB-Clusters ausfällt, führt Aurora automatisch ein Failover zu einer neuen primären DB-Instance durch. Während eines Failovers bedient der DB-Cluster weiterhin Verbindungsanfragen von der neuen primären DB-Instance an den Cluster-Endpunkt mit minimaler Serviceunterbrechung.

Das folgende Beispiel zeigt einen Cluster-Endpunkt für einen Aurora MySQL-DB-Cluster.

```
mydbcluster.cluster-c7tj4example.us-east-1.rds.amazonaws.com:3306
```

Leser-Endpunkt

Ein Reader-Endpunkt für einen Aurora-DB-Cluster bietet Unterstützung für Verbindungsausgleich für schreibgeschützte Verbindungen zum DB-Cluster. Verwenden Sie den Leser-Endpunkt für Lesevorgänge, beispielsweise Abfragen. Durch die Verarbeitung dieser Anweisungen auf den

schreibgeschützten Aurora-Replikaten reduziert dieser Endpunkt den Overhead für die primäre Instance. Er hilft dem Cluster auch, die Kapazität für gleichzeitige `SELECT`-Abfragen zu skalieren, und dies proportional zur Anzahl der Aurora-Replikate im Cluster. Jeder Aurora-DB-Cluster verfügt über einen Reader-Endpunkt.

Wenn der Cluster eine oder mehrere Aurora Replicas enthält, verteilt der Leser-Endpunkt jede Verbindungsanfrage auf die Aurora Replicas. In diesem Fall können Sie nur schreibgeschützte Anweisungen wie `SELECT` in dieser Sitzung ausführen. Wenn der Cluster nur eine primäre Instance und keine Aurora-Replikate enthält, stellt der Reader-Endpunkt eine Verbindung zur primären Instance her. In diesem Fall können Sie Schreibvorgänge über den Endpunkt ausführen.

Das folgende Beispiel zeigt einen Leser-Endpunkt für einen Aurora MySQL-DB-Cluster.

```
mydbcluster.cluster-ro-c7tj4example.us-east-1.rds.amazonaws.com:3306
```

Benutzerdefinierter Endpunkt

Ein benutzerdefinierter Endpunkt für einen Aurora-Cluster ist ein von Ihnen gewählter Satz an DB-Instances. Wenn Sie eine Verbindung zum Endpunkt herstellen, führt Aurora einen Verbindungsausgleich durch und wählt eine der Instances in der Gruppe aus, die die Verbindung verarbeiten soll. Sie bestimmen, auf welche Instances sich dieser Endpunkt bezieht, und Sie entscheiden auch, welchen Zweck der Endpunkt erfüllen soll.

Ein Aurora-DB-Cluster verfügt über keine benutzerdefinierten Endpunkte. Ein benutzerdefinierter Endpunkt muss daher von Ihnen erstellt werden. Sie können für jeden bereitgestellten Aurora-Cluster oder Cluster von Aurora Serverless v2 bis zu fünf benutzerdefinierte Endpunkte erstellen. Für Aurora Serverless v1-Cluster können keine benutzerdefinierten Endpunkte verwendet werden.

Der benutzerdefinierte Endpunkt bietet ausgeglichene Datenbankverbindungen, die auf anderen Kriterien als der Schreibschutz- oder Lese-/Schreibfähigkeit der DB-Instances basieren. So können Sie z. B. einen benutzerdefinierten Endpunkt definieren, um eine Verbindung mit Instances herzustellen, die eine bestimmte AWS -Instance-Klasse oder eine bestimmte DB-Parametergruppe verwenden. Sie können dann bestimmte Benutzergruppen über diesen benutzerdefinierten Endpunkt informieren. Beispielsweise können Sie internen Benutzern Instances mit geringer Kapazität für die Berichterstellung oder Ad-hoc-Abfragen (einmalig) und dem Produktionsdatenverkehr Instances mit hohen Kapazitäten zuweisen.

Da die Verbindung mit jeder mit dem benutzerdefinierten Endpunkt verknüpften DB-Instance erfolgen kann, sollten Sie sicherstellen, dass alle DB-Instances innerhalb dieser Gruppe

bestimmte gemeinsame Eigenschaften aufweisen. Hierdurch wird sichergestellt, dass Leistung, Speicherkapazität usw. für alle Verbindungen mit diesem Endpunkt konsistent verfügbar sind.

Diese Funktion richtet sich an fortgeschrittene Benutzer mit besonderen Arten von Workloads, bei denen es nicht sinnvoll ist, wenn alle Aurora-Replicas im Cluster identisch sind. Mit benutzerdefinierten Endpunkten können Sie die Kapazität der DB-Instance vorhersagen, die für jede Verbindung verwendet wird. Bei der Verwendung von benutzerdefinierten Endpunkten wird der Reader-Endpunkt für diesen Cluster üblicherweise nicht verwendet.

Das folgende Beispiel zeigt einen benutzerdefinierten Endpunkt für eine DB-Instance in einem Aurora MySQL-DB-Cluster.

```
myendpoint.cluster-custom-c7tj4example.us-east-1.rds.amazonaws.com:3306
```

Instance-Endpunkt

Ein Instance-Endpunkt stellt innerhalb eines Aurora-Clusters eine Verbindung zu einer spezifischen DB-Instance her. Jede DB-Instance in einem DB-Cluster hat einen eigenen, spezifischen Instance-Endpunkt. Daher ist ein Instance-Endpunkt für die aktuelle primäre DB-Instance des DB-Clusters vorhanden und es steht ein Instance-Endpunkt für jedes der Aurora-Replicas im DB-Cluster zur Verfügung.

Der Instance-Endpunkt bietet direkte Kontrolle über Verbindungen zum DB-Cluster für Szenarien, in denen die Verwendung des Cluster-Endpunkts oder des Leser-Endpunkts möglicherweise nicht angemessen ist. Beispielsweise erfordert Ihre Client-Anwendung möglicherweise einen detaillierteren Verbindungsausgleich, der auf dem Workload-Typ basiert. In diesem Fall können Sie mehrere Clients so konfigurieren, dass sie Verbindungen zu verschiedenen Aurora-Replicas in einem DB-Cluster herstellen, um die Lese-Workloads zu verteilen. Ein Beispiel für die Verwendung von Instance-Endpunkten zur Verbesserung der Verbindungsgeschwindigkeit nach einem Failover für Aurora PostgreSQL finden Sie unter Schnelles Failover mit Amazon Aurora PostgreSQL. Ein Beispiel für die Verwendung von Instance-Endpunkten zur Verbesserung der Verbindungsgeschwindigkeit nach einem Failover für Aurora MySQL finden Sie unter MariaDB Connector/J failover support - case Amazon Aurora.

Das folgende Beispiel zeigt einen Instance-Endpunkt für eine DB-Instance in einem Aurora MySQL-DB-Cluster.

```
mydbinstance.c7tj4example.us-east-1.rds.amazonaws.com:3306
```

Anzeigen der Endpunkte für einen Aurora-Cluster

In der AWS Management Console sehen Sie den Cluster-Endpunkt, den Reader-Endpunkt und alle benutzerdefinierten Endpunkte auf der Detailseite für jeden Cluster. Der Instance-Endpunkt wird auf der Detailseite der jeweiligen Instance angezeigt. Beim Herstellen der Verbindung müssen Sie dem auf dieser Detailseite angezeigten Namen des Endpunkts die zugewiesene Portnummer (mit einem Doppelpunkt hinter der Nummer) anfügen.

Mit dem AWS CLI sehen Sie den Writer-, Reader- und alle benutzerdefinierten Endpunkte in der Ausgabe des Befehls describe-db-clusters. Der folgende Befehl zeigt beispielsweise die Endpunktattribute für alle Cluster in Ihrer aktuellen Region. AWS

```
aws rds describe-db-clusters --query '*[].
{Endpoint:Endpoint,ReaderEndpoint:ReaderEndpoint,CustomEndpoints:CustomEndpoints}'
```

Mit der Amazon RDS-API rufen Sie die Endpunkte ab, indem Sie die DescribeDB-Funktion aufrufen. ClusterEndpoints

Verwenden des Cluster-Endpunkts

Da jeder Aurora-Cluster über einen integrierten Cluster-Endpunkt verfügt, dessen Name und andere Attribute von Aurora verwaltet werden, kann ein solcher Endpunkt nicht erstellt, gelöscht oder geändert werden.

Den Cluster-Endpunkt verwenden Sie beim Verwalten Ihres Clusters, bei Extraktions-, Transformations- und Ladevorgängen (ETL) oder beim Entwickeln und Testen von Anwendungen. Der Cluster-Endpunkt stellt eine Verbindung zur primären Instance des Clusters her. Die primäre Instance ist die einzige DB-Instance, mit der Sie Tabellen und Indizes erstellen sowie `INSERT`-Anweisungen und andere DDL- und DML-Operationen ausführen können.

Die physische IP-Adresse, auf die der Cluster-Endpunkt verweist, wird geändert, wenn der Failover-Mechanismus für den Cluster eine neue DB-Instance zur primären Instance für Lese-Schreib-Operationen hochstuft. Wenn Sie irgendeine Form von Verbindungspooling oder sonstigem Multiplexing verwenden, sollten Sie bereit sein, diese für alle zwischengespeicherten DNS-Informationen zu leeren oder zu reduzieren. time-to-live Hierdurch wird sichergestellt, dass Sie keine Lese-Schreib-Verbindung mit einer DB-Instance herstellen, die nicht mehr verfügbar ist oder nach einem Failover schreibgeschützt ist.

Verwenden des Leser-Endpunkts

Sie nutzen den Reader-Endpunkt für schreibgeschützte Verbindungen Ihres Aurora-Clusters. Dieser Endpunkt verwendet einen Mechanismus für den Verbindungsausgleich, um Ihren Cluster bei der Bewältigung einer abfrageintensiven Arbeitslast zu unterstützen. Der Reader-Endpunkt ist der Endpunkt, den Sie Anwendungen zur Verfügung stellen, die Berichterstattung oder andere schreibgeschützte Operationen auf dem Cluster ausführen.

Der Reader-Endpunkt gleicht Verbindungen zu verfügbaren Aurora Replicas in einem Aurora-DB-Cluster aus. Es gleicht einzelne Abfragen nicht aus. Wenn Sie jede Abfrage ausgleichen möchten, um die Leselast für einen DB-Cluster zu verteilen, öffnen Sie für jede Abfrage eine neue Verbindung zum Reader-Endpunkt.

Jeder Aurora-Cluster verfügt über einen integrierten Cluster-Endpunkt verfügt, dessen Name zusammen mit anderen Attributen durch Aurora verwaltet wird. Sie können einen solchen Endpunkt nicht erstellen, löschen oder ändern.

Wenn Ihr Cluster nur eine primäre Instance und keine Aurora-Replikate enthält, stellt der Reader-Endpunkt eine Verbindung zur primären Instance her. In diesem Fall können Sie Schreibvorgänge über diesen Endpunkt ausführen.

> **Tip**
>
> Über RDS Proxy können Sie zusätzliche schreibgeschützte Endpunkte für einen Aurora-Cluster erstellen. Diese Endpunkte führen dieselbe Art von Verbindungsausgleich durch wie der Aurora-Reader-Endpunkt. Anwendungen können sich schneller mit den Proxy-Endpunkten wieder verbinden als der Aurora-Reader-Endpunkt, wenn Reader-Instances nicht verfügbar sind. Die Proxy-Endpunkte können auch andere Proxy-Funktionen wie Multiplexing nutzen. Weitere Informationen finden Sie unter Verwenden von Reader-Endpunkten mit Aurora-Clustern.

Verwenden von benutzerdefinierten Endpunkten

Benutzerdefinierte Endpunkte werden verwendet, um die Verbindungsverwaltung zu vereinfachen, wenn Ihr Cluster DB-Instances mit unterschiedlichen Kapazitäten und Konfigurationseinstellungen enthält.

Zuvor hätten Sie möglicherweise den CNAMES-Mechanismus verwendet, um DNS (Domain Name Service)-Aliasse Ihrer eigenen Domäne einzurichten und ähnliche Ergebnisse zu erzielen. Durch benutzerdefinierte Endpunkte müssen CNAME-Datensätze bei zu- oder abnehmender Größe Ihres Clusters nicht aktualisiert werden. Mit benutzerdefinierten Endpunkten können auch verschlüsselte Transport Layer Security (TLS)- und Secure Sockets Layer (SSL)-Verbindungen verwendet werden.

Anstatt für jeden bestimmten Zweck eine DB-Instance zu verwenden und eine Verbindung zu deren Instance-Endpunkt herzustellen, können Sie mehrere Gruppen spezifischer DB-Instances nutzen. In diesem Fall verfügt jede Gruppe über ihren eigenen benutzerdefinierten Endpunkt. Auf diese Weise kann Aurora den Verbindungsausgleich zwischen allen Instanzen durchführen, die für Aufgaben wie die Berichterstattung oder die Bearbeitung von Produktions- oder internen Anfragen vorgesehen sind. Die benutzerdefinierten Endpunkte verteilen die Verbindungen passiv auf die Instanzen und verwenden DNS, um die IP-Adresse einer der Instanzen nach dem Zufallsprinzip zurückzugeben. Sollte eine DB-Instance innerhalb einer Gruppe nicht mehr verfügbar sein, leitet Aurora nachfolgende Verbindungen benutzerdefinierter Endpunkte an eine der anderen DB-Instances weiter, die mit demselben Endpunkt verknüpft sind.

Themen

- Angeben der Eigenschaften für benutzerdefinierte Endpunkte
- Mitgliedschaftsregeln für benutzerdefinierte Endpunkte
- Verwalten von benutzerdefinierten Endpunkten

Angeben der Eigenschaften für benutzerdefinierte Endpunkte

Die maximale Länge des Namens für einen benutzerdefinierten Endpunkt beträgt 63 Zeichen. Der Name hat folgendes Format:

```
endpoint_name.cluster-custom-customer_DNS_identifier.AWS_Region.rds.amazonaws.com
```

Sie können den Namen eines benutzerdefinierten Endpunkts nicht für mehr als einen Cluster in derselben AWS-Region verwenden. Die Kunden-DNS-Kennung ist eine eindeutige Kennung, die mit Ihrer AWS-Konto eigenen ID verknüpft ist. AWS-Region

Jedem benutzerdefinierten Endpunkt ist ein Typ zugeordnet, der bestimmt, welche DB-Instances diesem Endpunkt zugeordnet werden können. Zurzeit kann der Typ entweder `READER` `WRITER` oder `ANY` sein. Für die benutzerdefinierten Endpunkttypen gelten die folgenden Überlegungen:

- Sie können den benutzerdefinierten Endpunkttyp nicht in der AWS Management Console auswählen. Alle benutzerdefinierten Endpunkte, die Sie über die erstellen, AWS Management Console haben einen Typ von`ANY`.

  Sie können den benutzerdefinierten Endpunkttyp mithilfe der AWS CLI oder der Amazon RDS-API festlegen und ändern.
- Nur Reader-DB-Instances können Teil eines benutzerdefinierten `READER`-Endpunkts sein.
- Sowohl Reader- als auch Writer-DB-Instances können Teil eines benutzerdefinierten `ANY`-Endpunkts sein. Aurora leitet Verbindungen zu Cluster-Endpunkten mit Typ `ANY` mit gleicher Wahrscheinlichkeit zu jeder zugehörigen DB-Instance. Der Typ `ANY` gilt für Cluster mit allen Replikationstopologien.
- Wenn Sie versuchen, einen benutzerdefinierten Endpunkt mit einem Typ zu erstellen, der mit der Replikationskonfiguration eines Clusters nicht kompatibel ist, zeigt Aurora eine Fehlermeldung an.

Mitgliedschaftsregeln für benutzerdefinierte Endpunkte

Wenn Sie eine DB-Instance einem benutzerdefinierten Endpunkt hinzufügen oder aus einem benutzerdefinierten Endpunkt entfernen, bleiben alle vorhandenen Verbindungen zu dieser DB-Instance bestehen.

Sie können eine Liste mit DB-Instances definieren, die im benutzerdefinierten Endpunkt enthalten oder aus diesem ausgeschlossen sein sollen. Wir bezeichnen diese Listen als statische bzw. als Ausschlusslisten. Sie können den Aufnahme- bzw. Ausschlussmechanismus verwenden, um die DB-Instances-Gruppen weiter aufzuteilen und sicherzustellen, dass der Satz an benutzerdefinierten Endpunkten alle DB-Instances im Cluster abdeckt. Jeder benutzerdefinierte Endpunkt kann nur einen dieser Listentypen enthalten.

In der AWS Management Console:

- Die Auswahl wird durch das Kontrollkästchen Attach future instances added to this cluster (Zukünftige Instances diesem Cluster anfügen) dargestellt. Wenn Sie das Kontrollkästchen deaktivieren, verwendet der benutzerdefinierte Endpunkt eine statische Liste, die nur die auf der Seite angegebenen DB-Instances enthält. Wenn Sie das Kontrollkästchen aktivieren, verwendet der benutzerdefinierte Endpunkt eine Ausschlussliste. In diesem Fall repräsentiert der benutzerdefinierte Endpunkt alle DB-Instances im Cluster (einschließlich zukünftig hinzugefügter DB-Instances) außer jenen, die auf der Seite nicht ausgewählt wurden.

- In der Konsole können Sie den Endpunkttyp nicht angeben. Jeder benutzerdefinierte Endpunkt, der mit der Konsole erstellt wurde, weist den Typ `ANY` auf.

  Daher ändert Aurora die Mitgliedschaft des benutzerdefinierten Endpunkts nicht, wenn DB-Instances aufgrund eines Failovers oder einer Hochstufung die Rollen zwischen Writer und Reader ändern.

In der AWS CLI und der Amazon RDS-API:

- Sie können den Endpunkttyp angeben. Wenn der Endpunkttyp auf `READER` oder `WRITER` gesetzt ist, wird die Endpunkt-Mitgliedschaft daher bei Failovers und Hochstufungen automatisch angepasst.

  Beispielsweise enthält ein benutzerdefinierter Endpunkt des Typs `READER` ein Aurora Replica, das anschließend zu einer Writer-Instance hochgestuft wird. Die neue Writer-Instance ist nicht mehr Teil des benutzerdefinierten Endpunkts.
- Sie können einzelne Mitglieder den Listen hinzufügen und sie aus den Listen entfernen, nachdem sie ihre Rollen geändert haben. Verwenden Sie den Befehl AWS CLI modify-db-cluster-endpoint oder den API-Vorgang ModifyDB. ClusterEndpoint

Sie können eine DB-Instance mit mehreren benutzerdefinierten Endpunkten verknüpfen. Angenommen, Sie fügen einem Cluster eine neue DB-Instance hinzu, oder eine DB-Instance wird von Aurora automatisch durch den Mechanismus der automatischen Skalierung hinzugefügt. In diesen Fällen wird die DB-Instance allen infrage kommenden benutzerdefinierten Endpunkten hinzugefügt. Welchen Endpunkten die DB-Instance hinzugefügt wird, hängt vom benutzerdefinierten Endpunkt des Typs `READER`, `WRITER` oder `ANY` sowie von statischen Listen oder Ausschlusslisten ab, die für jeden Endpunkt definiert wurden. Wenn der Endpunkt beispielsweise eine statische Liste von DB-Instances enthält, werden kürzlich hinzugefügte Aurora-Replicas nicht diesem Endpunkt hinzugefügt. Wenn der Endpunkt über eine Ausschlussliste verfügt, werden neu hinzugefügte Aurora-Replicas dem Endpunkt hinzugefügt, wenn sie nicht in der Ausschlussliste aufgeführt sind und ihre Rollen dem Typ des benutzerdefinierten Endpunkts entsprechen.

Wenn ein Aurora-Replica nicht mehr verfügbar ist, bleibt es weiterhin mit benutzerdefinierten Endpunkten verknüpft. Das Replica bleibt Teil des benutzerdefinierten Endpunkts, wenn es z. B. nicht voll funktionsfähig ist, angehalten wurde oder neu startet. Sie können jedoch erst dann eine Verbindung über diese Endpunkte zum Replica herstellen, wenn es wieder verfügbar ist.

Verwalten von benutzerdefinierten Endpunkten

Da neu erstellte Aurora-Cluster über keine benutzerdefinierten Endpunkte verfügen, müssen Sie diese Objekte selbst erstellen und verwalten. Sie tun dies mit der AWS Management Console AWS CLI, oder Amazon RDS-API.

> **Note**
>
> Sie müssen auch benutzerdefinierte Endpunkte für Aurora-Cluster erstellen und verwalten, die anhand von Snapshots wiederhergestellt wurden. Benutzerdefinierte Endpunkte sind nicht im Snapshot enthalten. Sie erstellen sie nach der Wiederherstellung erneut und wählen neue Endpunktnamen, wenn sich der wiederhergestellte Cluster in der gleichen Region wie der ursprüngliche Cluster befindet.

Um mit benutzerdefinierten Endpunkten von zu arbeiten AWS Management Console, navigieren Sie zur Detailseite für Ihren Aurora-Cluster und verwenden die Steuerelemente im Abschnitt Benutzerdefinierte Endpunkte.

Um mit benutzerdefinierten Endpunkten aus dem zu arbeiten AWS CLI, können Sie die folgenden Operationen verwenden:

- create-db-cluster-endpoint
- describe-db-cluster-endpoints
- modify-db-cluster-endpoint
- delete-db-cluster-endpoint

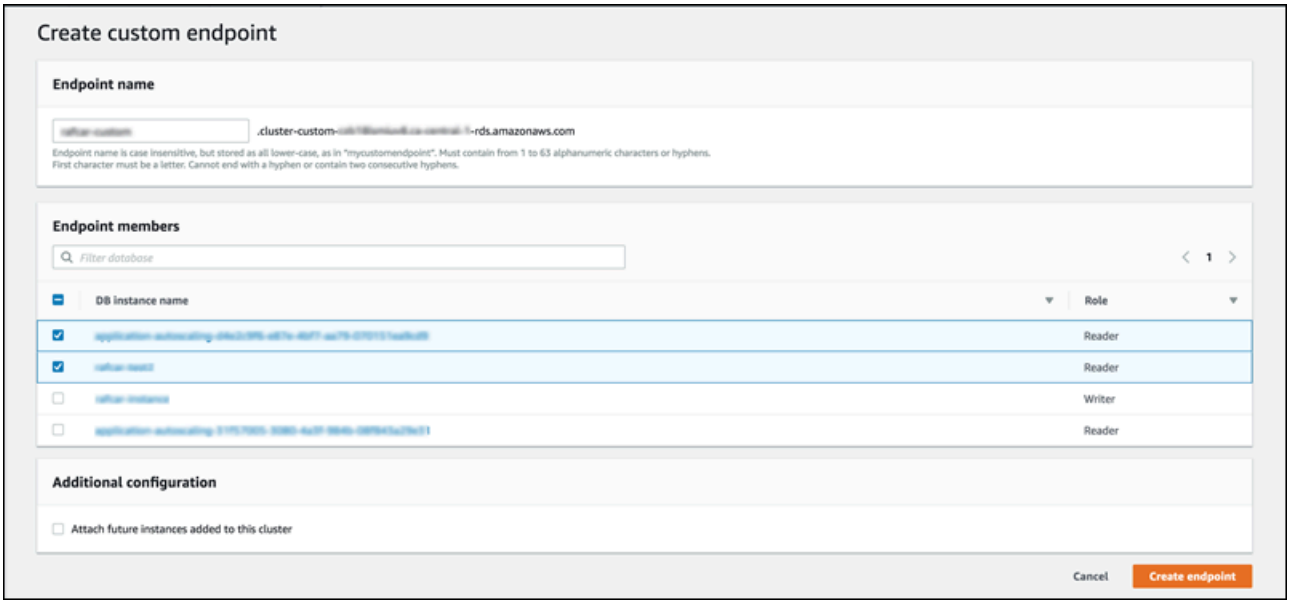
Sie können die folgenden Funktionen verwenden, um über die Amazon RDS-API mit benutzerdefinierten Endpunkten zu arbeiten:

- B wurde erstellt ClusterEndpoint
- BeschriebenDB ClusterEndpoints
- DB modifizieren ClusterEndpoint
- DB gelöscht ClusterEndpoint

Erstellen eines benutzerdefinierten Endpunkts

Konsole

Um einen benutzerdefinierten Endpunkt mit dem zu erstellen AWS Management Console, rufen Sie die Cluster-Detailseite auf und wählen Sie die **`Create custom endpoint`** Aktion im Abschnitt Endpoints aus. Wählen Sie einen Namen für den benutzerdefinierten Endpunkt aus. Dieser muss für Ihre Benutzer-ID und Region eindeutig sein. Um eine Liste von DB-Instances auszuwählen, die auch bei einer Erweiterung des Clusters gleich bleibt, lassen Sie das Kontrollkästchen Attach future instances added to this cluster (Zukünftige zu diesem Cluster hinzugefügte Instances anhängen) deaktiviert. Wenn Sie dieses Kontrollkästchen aktivieren, fügt der benutzerdefinierte Endpunkt dynamisch alle neuen Instances hinzu, wenn Sie sie zum Cluster hinzufügen.



Sie können den benutzerdefinierten Endpunkttyp `ANY` oder `READER` nicht in der AWS Management Console auswählen. Alle von Ihnen mit der AWS Management Console erstellten benutzerdefinierten Endpunkte haben den Typ `ANY`.

AWS CLI

Um einen benutzerdefinierten Endpunkt mit dem zu erstellen AWS CLI, führen Sie den Befehl create-db-cluster-endpoint aus.

Mit folgendem Befehl wird ein benutzerdefinierter Endpunkt erstellt, der an einen bestimmten Cluster angefügt ist. Zu Beginn wird der Endpunkt mit allen Aurora-Replica-Instances des Clusters verknüpft. Über einen nachfolgenden Befehl wird er mit einem spezifischen Satz an DB-Instances im Cluster verknüpft.

LinuxmacOSUnixFür, oder:

```
aws rds create-db-cluster-endpoint --db-cluster-endpoint-identifier custom-endpoint-
doc-sample \
  --endpoint-type reader \
  --db-cluster-identifier cluster_id

aws rds modify-db-cluster-endpoint --db-cluster-endpoint-identifier custom-endpoint-
doc-sample \
  --static-members instance_name_1 instance_name_2
```

Windows:

```
aws rds create-db-cluster-endpoint --db-cluster-endpoint-identifier custom-endpoint-
doc-sample ^
  --endpoint-type reader ^
  --db-cluster-identifier cluster_id

aws rds modify-db-cluster-endpoint --db-cluster-endpoint-identifier custom-endpoint-
doc-sample ^
  --static-members instance_name_1 instance_name_2
```

RDS-API

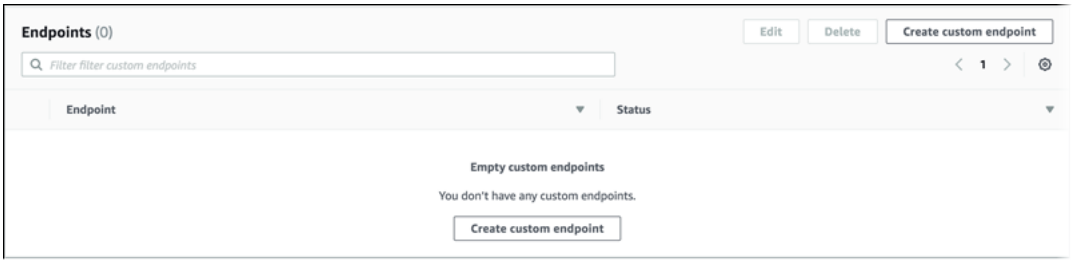
Um einen benutzerdefinierten Endpunkt mit der RDS-API zu erstellen, führen Sie den Vorgang CreateDB ClusterEndpoint aus.

Anzeigen von benutzerdefinierten Endpunkten

Konsole

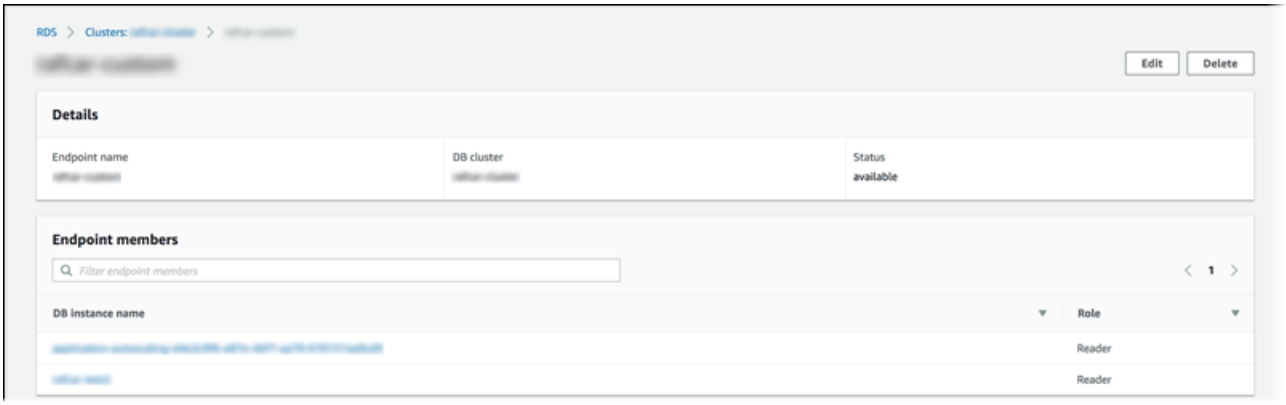
Um benutzerdefinierte Endpunkte mit dem anzuzeigen AWS Management Console, rufen Sie die Cluster-Detailseite für den Cluster auf und suchen Sie im Abschnitt Endpoints nach. Dieser Abschnitt enthält nur Informationen zu benutzerdefinierten Endpunkten. Die Details der integrierten Endpunkte sind im Abschnitt zu den wichtigsten Details aufgeführt. Um die Details für einen spezifischen benutzerdefinierten Endpunkt anzuzeigen, wählen Sie dessen Namen aus. Daraufhin wird die Detailseite für diesen Endpunkt geöffnet.

Der folgende Screenshot zeigt, dass die Liste der benutzerdefinierten Endpunkte für einen Aurora-Cluster zu Beginn leer ist.



Nachdem Sie einige benutzerdefinierte Endpunkte für diesen Cluster erstellt haben, werden diese im Abschnitt Endpoints (Endpunkte) angezeigt.

Auf der Detailseite sehen Sie, mit welchen DB-Instances der Endpunkt derzeit verknüpft ist.



Um darüber hinaus anzuzeigen, ob dem Cluster neu hinzugefügte DB-Instances automatisch auch in den Endpunkt integriert werden, rufen Sie die Seite Bearbeiten für den Endpunkt auf.

AWS CLI

Um benutzerdefinierte Endpunkte mit dem anzuzeigen AWS CLI, führen Sie den Befehl describe-db-cluster-endpoints aus.

Mit folgendem Befehl werden die benutzerdefinierten Endpunkte angezeigt, die mit einem bestimmten Cluster in einer bestimmten Region verknüpft sind. Die Ausgabe beinhaltet sowohl die integrierten Endpunkte als auch jeden benutzerdefinierten Endpunkt.

LinuxmacOSFürUnix, oder:

```
aws rds describe-db-cluster-endpoints --region region_name \
```

```
  --db-cluster-identifier cluster_id
```

Windows:

```
aws rds describe-db-cluster-endpoints --region region_name ^
  --db-cluster-identifier cluster_id
```

Im folgenden Beispiel wird der Befehl `describe-db-cluster-endpoints` mit einer Beispielausgabe gezeigt. Der `EndpointType` von `WRITER` oder `READER` bezeichnet die integrierten Schreib- und Lese- sowie schreibgeschützten Endpunkte des Clusters. Der `EndpointType` `CUSTOM` bezeichnet Endpunkte, die von Ihnen erstellt und deren verknüpfte DB-Instances von Ihnen ausgewählt werden. Einer der Endpunkte verfügt über ein Feld `StaticMembers`, das angibt, dass der Endpunkt mit einem genau bestimmten Satz an DB-Instances verknüpft ist. Dieses Feld kann nicht leer sein. Der andere Endpunkt verfügt über ein Feld `ExcludedMembers`, das angibt, dass der Endpunkt mit anderen als den unter `ExcludedMembers` aufgeführten DB-Instances verknüpft ist. Auch dieses Feld kann nicht leer sein. Die zweite Art benutzerdefinierter Endpunkte wird größer, um neue Instances zu berücksichtigen, die dem Cluster hinzufügt werden.

```
{
 "DBClusterEndpoints": [
  {
   "Endpoint": "custom-endpoint-demo.cluster-c7tj4example.ca-
central-1.rds.amazonaws.com",
   "Status": "available",
   "DBClusterIdentifier": "custom-endpoint-demo",
   "EndpointType": "WRITER"
  },
  {
   "Endpoint": "custom-endpoint-demo.cluster-ro-c7tj4example.ca-
central-1.rds.amazonaws.com",
   "Status": "available",
   "DBClusterIdentifier": "custom-endpoint-demo",
   "EndpointType": "READER"
  },
  {
   "CustomEndpointType": "ANY",
   "DBClusterEndpointIdentifier": "powers-of-2",
   "ExcludedMembers": [],
   "DBClusterIdentifier": "custom-endpoint-demo",
   "Status": "available",
   "EndpointType": "CUSTOM",
```

```
   "Endpoint": "powers-of-2.cluster-custom-c7tj4example.ca-
central-1.rds.amazonaws.com",
   "StaticMembers": [
     "custom-endpoint-demo-04",
     "custom-endpoint-demo-08",
     "custom-endpoint-demo-01",
     "custom-endpoint-demo-02"
   ],
   "DBClusterEndpointResourceIdentifier": "cluster-endpoint-
W7PE3TLLFNSHXQKFU6J6NV5FHU",
   "DBClusterEndpointArn": "arn:aws:rds:ca-central-1:111122223333:cluster-
endpoint:powers-of-2"
  },
  {
   "CustomEndpointType": "ANY",
   "DBClusterEndpointIdentifier": "eight-and-higher",
   "ExcludedMembers": [
     "custom-endpoint-demo-04",
     "custom-endpoint-demo-02",
     "custom-endpoint-demo-07",
     "custom-endpoint-demo-05",
     "custom-endpoint-demo-03",
     "custom-endpoint-demo-06",
     "custom-endpoint-demo-01"
   ],
   "DBClusterIdentifier": "custom-endpoint-demo",
   "Status": "available",
   "EndpointType": "CUSTOM",
   "Endpoint": "eight-and-higher.cluster-custom-123456789012.ca-
central-1.rds.amazonaws.com",
   "StaticMembers": [],
   "DBClusterEndpointResourceIdentifier": "cluster-endpoint-
W7PE3TLLFNSHYQKFU6J6NV5FHU",
   "DBClusterEndpointArn": "arn:aws:rds:ca-central-1:111122223333:cluster-
endpoint:eight-and-higher"
  }
 ]
}
```

RDS-API

Um benutzerdefinierte Endpunkte mit der RDS-API anzuzeigen, führen Sie den Vorgang DescribeDB .html aus ClusterEndpoints.

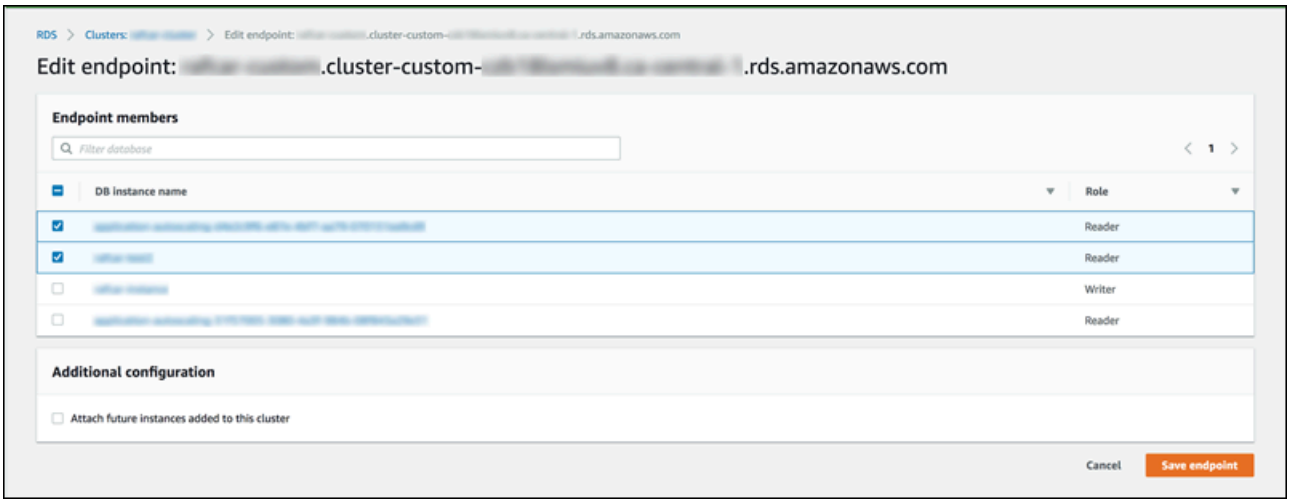
Bearbeiten eines benutzerdefinierten Endpunkts

Sie können die Eigenschaften eines benutzerdefinierten Endpunkts bearbeiten, um die mit dem Endpunkt verknüpften DB-Instances zu ändern. Sie können bei einem Endpunkt auch zwischen einer statischen und einer Ausschlussliste wechseln. Weitere Informationen zu diesen Endpunkteigenschaften finden Sie unter Mitgliedschaftsregeln für benutzerdefinierte Endpunkte.

Sie können einen benutzerdefinierten Endpunkt weiterhin verwenden oder eine Verbindung zu diesem herstellen, wenn die Änderungen einer Bearbeitungsaktion noch verarbeitet werden.

Konsole

Um einen benutzerdefinierten Endpunkt mit dem zu bearbeiten AWS Management Console, können Sie den Endpunkt auf der Cluster-Detailseite auswählen oder die Detailseite für den Endpunkt aufrufen und die Aktion Bearbeiten auswählen.



AWS CLI

Um einen benutzerdefinierten Endpunkt mit dem zu bearbeiten AWS CLI, führen Sie den Befehl modify-db-cluster-endpoint aus.

Mit den folgenden Befehlen wird der Satz an DB-Instances geändert, die für einen benutzerdefinierten Endpunkt gelten, und optional zwischen dem Verhalten einer statischen Liste oder einer Ausschlussliste gewechselt. Die Parameter `--static-members` und `--excluded-members` weisen eine durch Leerzeichen getrennte Liste von DB-Instance-Kennungen auf.

LinuxmacOSUnixFür, oder:

```
aws rds modify-db-cluster-endpoint --db-cluster-endpoint-identifier my-custom-endpoint
 \
  --static-members db-instance-id-1 db-instance-id-2 db-instance-id-3 \
  --region region_name

aws rds modify-db-cluster-endpoint --db-cluster-endpoint-identifier my-custom-endpoint
 \
  --excluded-members db-instance-id-4 db-instance-id-5 \
  --region region_name
```

Windows:

```
aws rds modify-db-cluster-endpoint --db-cluster-endpoint-identifier my-custom-endpoint
 ^
  --static-members db-instance-id-1 db-instance-id-2 db-instance-id-3 ^
  --region region_name

aws rds modify-db-cluster-endpoint --db-cluster-endpoint-identifier my-custom-endpoint
 ^
  --excluded-members db-instance-id-4 db-instance-id-5 ^
  --region region_name
```

RDS-API

Um einen benutzerdefinierten Endpunkt mit der RDS-API zu bearbeiten, führen Sie den Vorgang modifyDB ClusterEndpoint .html aus.

Löschen eines benutzerdefinierten Endpunkts

Konsole

Um einen benutzerdefinierten Endpunkt mit dem zu löschen AWS Management Console, rufen Sie die Cluster-Detailseite auf, wählen Sie den entsprechenden benutzerdefinierten Endpunkt aus und wählen Sie die Aktion Löschen aus.

AWS CLI

Um einen benutzerdefinierten Endpunkt mit dem zu löschen AWS CLI, führen Sie den Befehl delete-db-cluster-endpoint aus.

Mit folgendem Befehl wird ein benutzerdefinierter Endpunkt gelöscht: Sie müssen nicht den verknüpften Cluster, aber die Region angeben.

LinuxmacOSUnixFür, oder:

```
aws rds delete-db-cluster-endpoint --db-cluster-endpoint-identifier custom-end-point-id
 \
  --region region_name
```

Windows:

```
aws rds delete-db-cluster-endpoint --db-cluster-endpoint-identifier custom-end-point-id
 ^
  --region region_name
```

RDS-API

Um einen benutzerdefinierten Endpunkt mit der RDS-API zu löschen, führen Sie den Vorgang deleteDB ClusterEndpoint aus.

AWS CLI End-to-End-Beispiel für benutzerdefinierte Endpunkte

Das folgende Tutorial zeigt anhand von AWS CLI Beispielen mit Unix-Shell-Syntax, dass Sie einen Cluster mit mehreren „kleinen“ DB-Instances und einigen „großen“ DB-Instances definieren und benutzerdefinierte Endpunkte erstellen können, um eine Verbindung zu jeder Gruppe von DB-Instances herzustellen. Um ähnliche Befehle auf Ihrem eigenen System ausführen zu können, sollten Sie mit den Grundlagen der Arbeit mit Aurora-Clustern und der AWS CLI Verwendung vertraut sein, um Ihre eigenen Werte für Parameter wie Region, Subnetzgruppe und VPC-Sicherheitsgruppe bereitzustellen.

Dieses Beispiel verdeutlicht die ersten Einrichtungsschritte: das Erstellen eines Aurora-Clusters und das Hinzufügen von DB-Instances. Hierbei handelt es sich um einen heterogenen Cluster, weshalb nicht alle DB-Instances über die gleiche Kapazität verfügen. Die meisten Instances verwenden die AWS Instance-Klassedb.r4.4xlarge, aber die letzten beiden DB-Instances verwenden sie.

`db.r4.16xlarge` Bei jedem dieser `create-db-instance`-Beispielbefehle wird die Ausgabe auf dem Bildschirm angezeigt und eine Kopie der JSON-Datei zur späteren Prüfung gespeichert.

```
aws rds create-db-cluster --db-cluster-identifier custom-endpoint-demo --engine aurora-
mysql \
     --engine-version 8.0.mysql_aurora.3.02.0 --master-username $MASTER_USER --manage-
master-user-password \
     --db-subnet-group-name $SUBNET_GROUP  --vpc-security-group-ids $VPC_SECURITY_GROUP
 \
     --region $REGION

for i in 01 02 03 04 05 06 07 08
do
  aws rds create-db-instance --db-instance-identifier custom-endpoint-demo-${i} \
     --engine aurora --db-cluster-identifier custom-endpoint-demo --db-instance-class
 db.r4.4xlarge \
     --region $REGION \
     | tee custom-endpoint-demo-${i}.json
done

for i in 09 10
do
  aws rds create-db-instance --db-instance-identifier custom-endpoint-demo-${i} \
     --engine aurora --db-cluster-identifier custom-endpoint-demo --db-instance-class
 db.r4.16xlarge \
     --region $REGION \
     | tee custom-endpoint-demo-${i}.json
done
```

Die größeren Instances sind für spezialisierte Arten von Berichtsabfragen vorgesehen. Damit diese nicht auf die primäre Instance hochgestuft werden, wird im folgenden Beispiel gezeigt, wie der Hochstufungsebene für diese Instances die niedrigste Priorität zugewiesen wird. In diesem Beispiel wird die Option `--manage-master-user-password` zum Generieren des Hauptbenutzerpassworts und zum Verwalten dieses Passworts in Secrets Manager angegeben. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager. Alternativ können Sie die Option `--master-password` verwenden, um das Passwort selbst festzulegen und zu verwalten.

```
for i in 09 10
do
  aws rds modify-db-instance --db-instance-identifier custom-endpoint-demo-${i} \
```

```
    --region $REGION --promotion-tier 15
done
```

Angenommen, Sie möchten die zwei „größeren“ Instances nur für die ressourcenintensivsten Abfragen verwenden. Dazu können Sie zunächst einen benutzerdefinierten schreibgeschützten Endpunkt erstellen. Anschließend können Sie eine statische Liste von Elementen hinzufügen, sodass der Endpunkt nur mit diesen DB-Instances verbunden ist. Da sich diese Instances bereits in der niedrigsten Hochstufungsebene befinden, ist es unwahrscheinlich, dass eine von ihnen auf die primäre Instance hochgestuft wird. Sollte eine der Instances auf die primäre Instance hochgestuft worden sein, wäre sie über diesen Endpunkt nicht erreichbar, da der `READER`-Typ anstatt des `ANY`-Typs angegeben wurde.

Das folgende Beispiel verdeutlicht das Erstellen und Ändern von Endpunktbefehlen sowie eine JSON-Beispielausgabe mit dem ursprünglichen und geänderten Status des benutzerdefinierten Endpunkts.

```
$ aws rds create-db-cluster-endpoint --region $REGION \
    --db-cluster-identifier custom-endpoint-demo \
    --db-cluster-endpoint-identifier big-instances --endpoint-type reader
{
    "EndpointType": "CUSTOM",
    "Endpoint": "big-instances.cluster-custom-c7tj4example.ca-
central-1.rds.amazonaws.com",
    "DBClusterEndpointIdentifier": "big-instances",
    "DBClusterIdentifier": "custom-endpoint-demo",
    "StaticMembers": [],
    "DBClusterEndpointResourceIdentifier": "cluster-endpoint-
W7PE3TLLFNSHXQKFU6J6NV5FHU",
    "ExcludedMembers": [],
    "CustomEndpointType": "READER",
    "Status": "creating",
    "DBClusterEndpointArn": "arn:aws:rds:ca-central-1:111122223333:cluster-
endpoint:big-instances"
}

$ aws rds modify-db-cluster-endpoint --db-cluster-endpoint-identifier big-instances \
    --static-members custom-endpoint-demo-09 custom-endpoint-demo-10 --region $REGION
{
    "EndpointType": "CUSTOM",
    "ExcludedMembers": [],
    "DBClusterEndpointIdentifier": "big-instances",
```

```
    "DBClusterEndpointResourceIdentifier": "cluster-endpoint-
W7PE3TLLFNSHXQKFU6J6NV5FHU",
    "CustomEndpointType": "READER",
    "DBClusterEndpointArn": "arn:aws:rds:ca-central-1:111122223333:cluster-
endpoint:big-instances",
    "StaticMembers": [
        "custom-endpoint-demo-10",
        "custom-endpoint-demo-09"
    ],
    "Status": "modifying",
    "Endpoint": "big-instances.cluster-custom-c7tj4example.ca-
central-1.rds.amazonaws.com",
    "DBClusterIdentifier": "custom-endpoint-demo"
}
```

Der standardmäßige READER-Endpunkt des Clusters kann eine Verbindung entweder zur kleinen oder zur großen DB-Instance herstellen. Hierdurch wird das Vorhersagen der Abfrageleistung und der Skalierbarkeit bei einer hohen Auslastung des Clusters erschwert. Um den Workload zwischen den DB-Instance-Sätzen klar aufzuteilen, können Sie den standardmäßigen READER-Endpunkt ignorieren und einen zweiten benutzerdefinierten Endpunkt erstellen, der eine Verbindung mit den anderen DB-Instances herstellt. Im folgenden Beispiel wird dies erreicht, indem zunächst ein benutzerdefinierter Endpunkt erstellt und dann eine Ausschlussliste hinzugefügt wird. Alle anderen DB-Instances, die Sie dem Cluster später hinzufügen, werden automatisch in diesen Endpunkt integriert. Der Typ ANY signalisiert, dass dieser Endpunkt mit insgesamt acht Instances verknüpft ist: mit der primären Instance und sieben anderen Aurora-Replicas. Wenn im Beispiel der Typ READER verwendet würde, wäre der benutzerdefinierte Endpunkt nur mit den sieben Aurora-Replicas verknüpft.

```
$ aws rds create-db-cluster-endpoint --region $REGION --db-cluster-identifier custom-
endpoint-demo \
    --db-cluster-endpoint-identifier small-instances --endpoint-type any
{
    "Status": "creating",
    "DBClusterEndpointIdentifier": "small-instances",
    "CustomEndpointType": "ANY",
    "EndpointType": "CUSTOM",
    "Endpoint": "small-instances.cluster-custom-c7tj4example.ca-
central-1.rds.amazonaws.com",
    "StaticMembers": [],
    "ExcludedMembers": [],
    "DBClusterIdentifier": "custom-endpoint-demo",
```

```
    "DBClusterEndpointArn": "arn:aws:rds:ca-central-1:111122223333:cluster-
endpoint:small-instances",
    "DBClusterEndpointResourceIdentifier": "cluster-
endpoint-6RDDXQOC3AKKZT2PRD7ST37BMY"
}

$ aws rds modify-db-cluster-endpoint --db-cluster-endpoint-identifier small-instances \
    --excluded-members custom-endpoint-demo-09 custom-endpoint-demo-10 --region $REGION
{
    "DBClusterEndpointIdentifier": "small-instances",
    "DBClusterEndpointArn": "arn:aws:rds:ca-central-1:c7tj4example:cluster-
endpoint:small-instances",
    "DBClusterEndpointResourceIdentifier": "cluster-
endpoint-6RDDXQOC3AKKZT2PRD7ST37BMY",
    "CustomEndpointType": "ANY",
    "Endpoint": "small-instances.cluster-custom-c7tj4example.ca-
central-1.rds.amazonaws.com",
    "EndpointType": "CUSTOM",
    "ExcludedMembers": [
        "custom-endpoint-demo-09",
        "custom-endpoint-demo-10"
    ],
    "StaticMembers": [],
    "DBClusterIdentifier": "custom-endpoint-demo",
    "Status": "modifying"
}
```

Im folgenden Beispiel wird der Status der Endpunkte dieses Clusters geprüft. Mit dem `EndPointType` `WRITER` verfügt der Cluster immer noch über seinen ursprünglichen Cluster-Endpunkt, den Sie weiterhin für die Administration, für Extraktions-, Transformations- und Ladevorgänge (ETL) und andere Schreibvorgänge nutzen würden. Er verfügt immer noch über seinen ursprünglichen `READER`-Endpunkt, den Sie nicht verwenden würden, da jede zu ihm hergestellte Verbindung möglicherweise zu einer kleinen oder großen DB-Instance weitergeleitet wird. Die benutzerdefinierten Endpunkte machen dieses Verhalten vorhersehbar, da Verbindungen verwendet werden, die, je nach angegebenem Endpunkt, garantiert eine der kleinen oder großen DB-Instances verwenden.

```
$ aws rds describe-db-cluster-endpoints --region $REGION
{
    "DBClusterEndpoints": [
        {
            "EndpointType": "WRITER",
```

```
            "Endpoint": "custom-endpoint-demo.cluster-c7tj4example.ca-
central-1.rds.amazonaws.com",
            "Status": "available",
            "DBClusterIdentifier": "custom-endpoint-demo"
        },
        {
            "EndpointType": "READER",
            "Endpoint": "custom-endpoint-demo.cluster-ro-c7tj4example.ca-
central-1.rds.amazonaws.com",
            "Status": "available",
            "DBClusterIdentifier": "custom-endpoint-demo"
        },
        {
            "Endpoint": "small-instances.cluster-custom-c7tj4example.ca-
central-1.rds.amazonaws.com",
            "CustomEndpointType": "ANY",
            "DBClusterEndpointArn": "arn:aws:rds:ca-central-1:111122223333:cluster-
endpoint:small-instances",
            "ExcludedMembers": [
                "custom-endpoint-demo-09",
                "custom-endpoint-demo-10"
            ],
            "DBClusterEndpointResourceIdentifier": "cluster-
endpoint-6RDDXQOC3AKKZT2PRD7ST37BMY",
            "DBClusterIdentifier": "custom-endpoint-demo",
            "StaticMembers": [],
            "EndpointType": "CUSTOM",
            "DBClusterEndpointIdentifier": "small-instances",
            "Status": "modifying"
        },
        {
            "Endpoint": "big-instances.cluster-custom-c7tj4example.ca-
central-1.rds.amazonaws.com",
            "CustomEndpointType": "READER",
            "DBClusterEndpointArn": "arn:aws:rds:ca-central-1:111122223333:cluster-
endpoint:big-instances",
            "ExcludedMembers": [],
            "DBClusterEndpointResourceIdentifier": "cluster-endpoint-
W7PE3TLLFNSHXQKFU6J6NV5FHU",
            "DBClusterIdentifier": "custom-endpoint-demo",
            "StaticMembers": [
                "custom-endpoint-demo-10",
                "custom-endpoint-demo-09"
            ],
```

```
            "EndpointType": "CUSTOM",
            "DBClusterEndpointIdentifier": "big-instances",
            "Status": "available"
        }
    ]
}
```

In den abschließenden Beispielen wird gezeigt, wie nachfolgende Datenbankverbindungen zu den benutzerdefinierten Endpunkten eine Verbindung mit den zahlreichen DB-Instances im Aurora-Cluster herstellen. Der `small-instances`-Endpunkt stellt immer eine Verbindung zu den `db.r4.4xlarge`-DB-Instances her. Diese stellen die Hosts mit den niedrigeren Nummern in diesem Cluster dar.

```
$ mysql -h small-instances.cluster-custom-c7tj4example.ca-central-1.rds.amazonaws.com -
u $MYUSER -p
mysql> select @@aurora_server_id;
+--------------------------+
| @@aurora_server_id       |
+--------------------------+
| custom-endpoint-demo-02 |
+--------------------------+

$ mysql -h small-instances.cluster-custom-c7tj4example.ca-central-1.rds.amazonaws.com -
u $MYUSER -p
mysql> select @@aurora_server_id;
+--------------------------+
| @@aurora_server_id       |
+--------------------------+
| custom-endpoint-demo-07 |
+--------------------------+

$ mysql -h small-instances.cluster-custom-c7tj4example.ca-central-1.rds.amazonaws.com -
u $MYUSER -p
mysql> select @@aurora_server_id;
+--------------------------+
| @@aurora_server_id       |
+--------------------------+
| custom-endpoint-demo-01 |
+--------------------------+
```

Der `big-instances`-Endpunkt stellt immer eine Verbindung zu den `db.r4.16xlarge`-DB-Instances her, die die beiden höchst nummerierten Hosts in diesem Cluster sind.

```
$ mysql -h big-instances.cluster-custom-c7tj4example.ca-central-1.rds.amazonaws.com -u
 $MYUSER -p
mysql> select @@aurora_server_id;
+--------------------------+
| @@aurora_server_id       |
+--------------------------+
| custom-endpoint-demo-10 |
+--------------------------+

$ mysql -h big-instances.cluster-custom-c7tj4example.ca-central-1.rds.amazonaws.com -u
 $MYUSER -p
mysql> select @@aurora_server_id;
+--------------------------+
| @@aurora_server_id       |
+--------------------------+
| custom-endpoint-demo-09 |
+--------------------------+
```

Verwenden der Instance-Endpunkte

Jede DB-Instance in einem Aurora-Cluster verfügt über ihren eigenen integrierten Instance-Endpunkt, dessen Name und andere Attribute von Aurora verwaltet werden. Sie können einen solchen Endpunkt nicht erstellen, löschen oder ändern. Möglicherweise sind Sie mit Instance-Endpunkten vertraut, wenn Sie Amazon RDS verwenden. Bei Aurora verwenden Sie die Schreiber- und Leser-Endpunkte jedoch häufiger als die Instance-Endpunkte.

Im day-to-day Aurora-Betrieb verwenden Sie Instance-Endpunkte hauptsächlich zur Diagnose von Kapazitäts- oder Leistungsproblemen, die sich auf eine bestimmte Instance in einem Aurora-Cluster auswirken. Während eine Verbindung zu einer spezifischen Instance besteht, können Sie unter anderem deren Statusvariablen oder Metriken untersuchen. Hierdurch ist es möglich, Unterschiede zwischen den Aktivitäten verschiedener Cluster-Instances zu ermitteln.

In fortgeschrittenen Anwendungsfällen konfigurieren Sie einige DB-Instances möglicherweise anders als andere DB-Instances. Verwenden Sie in diesem Fall den Instance-Endpunkt, um eine direkte Verbindung mit einer Instance herzustellen, die kleiner oder größer ist oder sich auf eine andere Art von den anderen Instances unterscheidet. Legen Sie auch eine Failover-Priorität fest, damit diese spezielle DB-Instance bei einer Hochstufung zur primären Instance als letztes berücksichtigt wird. In solchen Fällen empfehlen wir, dass Sie nicht den Instance-Endpunkt, sondern benutzerdefinierte Endpunkte verwenden. Diese Vorgehensweise vereinfacht die Verbindungsverwaltung und trägt

zur Gewährleistung von hoher Verfügbarkeit bei, wenn Sie Ihrem Cluster weitere DB-Instances hinzufügen.

Funktionsweise von Aurora-Endpunkten mit hoher Verfügbarkeit

Verwenden Sie im Fall von Clustern, bei denen eine hohe Verfügbarkeit von großer Bedeutung ist, den Writer-Endpunkt für Lese-/Schreib- oder Allzweck-Verbindungen und den Leser-Endpunkt für schreibgeschützte Verbindungen. Die Schreiber- und Leser-Endpunkte verwalten das Failover von DB-Instances besser als Instance-Endpunkte. Im Gegensatz zu den Instance-Endpunkten ändern die Schreiber- und Leser-Endpunkte automatisch, mit welcher DB-Instance sie eine Verbindung herstellen, wenn eine DB-Instance in Ihrem Cluster nicht mehr verfügbar ist.

Wenn die primäre DB-Instance eines DB-Clusters ausfällt, führt Aurora automatisch ein Failover zu einer neuen primären DB-Instance durch. Dies geschieht entweder durch Hochstufung einer vorhandenen Aurora-Replica zu einer neuen primären DB-Instance oder durch Erstellen einer neuen primären DB-Instance. Bei einem Failover können Sie den Schreiber-Endpunkt verwenden, um die Verbindung zu der neu hochgestuften oder erstellten primären DB-Instance wiederherzustellen. Sie haben auch die Möglichkeit, den Leser-Endpunkt zu verwenden, um eine Verbindung zu einem der Aurora-Replicas im DB-Cluster wiederherzustellen. Während eines Failovers leitet der Reader-Endpunkt Verbindungen möglicherweise für kurze Zeit an die neue primäre DB-Instance eines DB-Clusters weiter, nachdem ein Aurora-Replica zur neuen primären DB-Instance hochgestuft wurde.

Wenn Sie Ihre Anwendungslogik so entwickeln, dass Verbindungen zu Instance-Endpunkten verwaltet werden können, ist es möglich, den daraus resultierenden Satz an verfügbaren DB-Instances im DB-Cluster manuell oder programmgesteuert zu ermitteln. Verwenden Sie den AWS CLI Befehl describe-db-clusters oder den RDS-API-Vorgang DescribeDBClusters, um die DB-Cluster- und Reader-Endpunkte, DB-Instances, ob DB-Instances Leser sind, und ihre Promotion-Stufen zu finden. Sie können dann die Instance-Klassen nach einem Failover bestätigen und eine Verbindung mit einem geeigneten Instance-Endpunkt herstellen.

Weitere Informationen zu Failovers finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.

Aurora DB-Instance-Klassen

Die DB-Instance-Klasse bestimmt die Berechnungs- und Speicherkapazität einer Amazon-Aurora-DB-Instance. Die benötigte DB-Instance-Klasse richtet sich nach Ihren Rechen- und Speicheranforderungen.

Eine DB-Instance-Klasse besteht sowohl aus dem DB-Instance-Klassentyp als auch aus der -größe. Beispielsweise ist db.r6g ein speicheroptimierter DB-Instance-Klassentyp, der von Graviton2-Prozessoren angetrieben wird. AWS Innerhalb des db.r6g-Instance-Klassentyps ist db.r6g.2xlarge eine DB-Instance-Klasse. Die Größe dieser Klasse ist 2xlarge.

Weitere Informationen zu Preisen der Instance-Klassen erhalten Sie unter Amazon RDS-Preise.

Themen

DB-Instance-Klassenarten

Amazon Aurora unterstützt DB-Instance-Klassen für die folgenden Anwendungsfälle:

- Aurora Serverless v2
- RAM-optimiert
- Spitzenlastleistung
- Optimierte Lesevorgänge

Weitere Informationen zu Amazon-EC2-Instance-Typen finden Sie unter Instance-Typen in der Amazon-EC2-Dokumentation.

Typ der Instance-Klasse von Aurora Serverless v2

Der folgende Typ von Aurora Serverless v2 ist verfügbar:

- db.serverless – Ein spezieller DB-Instance-Klassentyp, der von Aurora Serverless v2 verwendet wird. Aurora passt Rechen-, Speicher- und Netzwerkressourcen dynamisch an, wenn sich die Workload ändert. Details zur Verwendung finden Sie unter Verwenden von Aurora Serverless v2.

Typ arbeitsspeicheroptimierter Instance-Klassen

Die speicheroptimierte X-Familie unterstützt die folgenden Instance-Klassen:

- db.x2g — Instance-Klassen, die für speicherintensive Anwendungen optimiert sind und auf Graviton2-Prozessoren basieren. AWS Diese Instance-Klassen bieten niedrige Kosten pro GiB Speicher.

  Sie können eine DB-Instance so ändern, dass sie eine der DB-Instance-Klassen verwendet, die von Graviton2-Prozessoren unterstützt werden. AWS Führen Sie dazu die gleichen Schritte wie bei jeder anderen Änderung der DB-Instance aus.

Die speicheroptimierte R-Familie unterstützt die folgenden Typen von Instance-Klassen:

- db.r7g — Instance-Klassen, die auf Graviton3-Prozessoren basieren. AWS Diese Instance-Klassen eignen sich ideal für die Ausführung speicherintensiver Workloads.

  Sie können eine DB-Instance so ändern, dass sie eine der DB-Instance-Klassen verwendet, die von Graviton3-Prozessoren unterstützt werden. AWS Führen Sie dazu die gleichen Schritte wie bei jeder anderen Änderung der DB-Instance aus.
- db.r6g — Instance-Klassen, die auf Graviton2-Prozessoren basieren. AWS Diese Instance-Klassen eignen sich ideal für die Ausführung speicherintensiver Workloads

  Sie können eine DB-Instance so ändern, dass sie eine der DB-Instance-Klassen verwendet, die von Graviton2-Prozessoren unterstützt werden. AWS Führen Sie dazu die gleichen Schritte wie bei jeder anderen Änderung der DB-Instance aus.
- db.r6i – Instance-Klassen mit Unterstützung der skalierbaren Intel-Xeon-Prozessoren der 3. Generation. Diese Instance-Klassen sind SAP-zertifiziert und eignen sich ideal für die Ausführung speicherintensiver Workloads in Open-Source-Datenbanken wie MySQL und PostgreSQL.
- db.r4 – Diese Instance-Klassen werden nur für die Aurora-PostgreSQL-Versionen 11 und 12 unterstützt. Für alle Aurora PostgreSQL-DB-Cluster, die db.r4-DB-Instance-Klassen verwenden, empfehlen wir, so bald wie möglich ein Upgrade auf eine Instance-Klasse der höheren Generation durchzuführen.

Die db.r4-Instance-Klassen sind für die Cluster-Speicherkonfiguration Aurora I/O-Optimized nicht verfügbar.

- db.r3 – Instance-Klassen, die Speicheroptimierung bieten.

  Amazon Aurora hat den end-of-life Prozess für db.r3-DB-Instance-Klassen nach dem folgenden Zeitplan gestartet, der Upgrade-Empfehlungen enthält. Für alle DB-Cluster von Aurora MySQL, die DB-Instance-Klassen vom Typ „db.r3" verwenden, wird empfohlen, schnellstmöglichst auf eine DB-Instance-Klasse „db.r5“ oder höher zu aktualisieren.

Aktion oder Empfehlung	Datumsangaben
Sie können keine DB-Cluster von Aurora MySQL mehr erstellen, die DB-Instance-Klassen vom Typ „db.r3“ verwenden.	Jetzt
Amazon Aurora startete automatische Upgrades von DB-Clustern von Aurora MySQL, die DB-Instance-Klassen vom Typ „db.r3" verwenden, auf DB-Instance-Klassen vom Typ „db.r5“ oder höher.	31. Januar 2023

Instance-Klassen mit Spitzenlastleistung

Die folgenden DB-Instance-Klassentypen mit Spitzenlastleistung sind verfügbar:

- db.t4g — Allzweck-Instance-Klassen, die auf ARM-basierten Graviton2-Prozessoren basieren. AWS Diese Instance-Klassen bieten ein besseres Preis-Leistungs-Verhältnis als die DB-Instance-Klassen mit Spitzenlastleistung der vorherigen Generation für eine breite Palette von Allzweck-Workloads mit Spitzenleistung. Amazon RDS db.t4g-Instances sind für den unbegrenzten Modus konfiguriert. Das bedeutet, dass sie gegen eine zusätzliche Gebühr während eines 24-Stunden-Zeitfensters Burst-Leistung über die Baseline hinaus bieten können.

  Sie können eine DB-Instance so ändern, dass sie eine der DB-Instance-Klassen verwendet, die von Graviton2-Prozessoren unterstützt werden. AWS Führen Sie dazu die gleichen Schritte wie bei jeder anderen Änderung der DB-Instance aus.
- db.t3: Instance-Klassen, die ein Basisleistungsniveau bieten, mit der Möglichkeit, die volle CPU-Auslastung zu erreichen. Die db.t3-T3-Instances sind für den unbegrenzten Modus konfiguriert.

Diese Instance-Klassen bieten mehr Rechenkapazität als die vorherigen db.t2-Instance-Klassen. Sie werden vom AWS -Nitro System angetrieben, einer Kombination aus dedizierter Hardware und leichtem Hypervisor. Wir empfehlen, diese Instance-Klassen ausschließlich für das Entwickeln und Testen von Servern oder Nicht-Produktionsservern zu verwenden.

- db.t2: Instance-Klassen, die ein Basisleistungsniveau bieten, mit der Möglichkeit, die volle CPU-Auslastung zu erreichen. Die db.t2-Instances sind für den Unlimited-Modus konfiguriert. Wir empfehlen, diese Instance-Klassen ausschließlich für das Entwickeln und Testen von Servern oder Nicht-Produktionsservern zu verwenden.

  Die db.t2-Instance-Klassen sind für die Cluster-Speicherkonfiguration Aurora I/O-Optimized nicht verfügbar.

> **Note**
>
> Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Empfehlungen für die T-Instance-Typen finden Sie unter Verwendung von T-Instance-Klassen für Entwicklung und Tests.

Informationen zu den Hardware-Spezifikationen für DB-Instance-Klassen finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.

Instance-Klassentyp für optimierte Lesevorgänge

Folgende Instance-Klassentypen für optimierte Lesevorgänge sind verfügbar:

- AWS db.r6gd — Instance-Klassen, die von Graviton2-Prozessoren angetrieben werden. Diese Instance-Klassen eignen sich ideal für die Ausführung speicherintensiver Workloads und bieten lokalen NVMe-basierten SSD-Speicher auf Blockebene für Anwendungen, die lokalen Speicher mit hoher Geschwindigkeit und niedriger Latenz benötigen.
- db.r6id – Instance-Klassen mit skalierbaren Intel-Xeon-Prozessoren der 3. Generation. Diese Instance-Klassen sind SAP-zertifiziert und eignen sich ideal für speicherintensive Workloads. Sie bieten einen maximalen Speicher von 1 TiB und bis zu 7,6 TB direkt angeschlossenen NVMe-basierten SSD-Speicher.

Unterstützte DB-Engines für DB-Instance-Klassen

In der folgenden Tabelle finden Sie Details zu den unterstützten Amazon Aurora-DB-Instance-Klassen für die Aurora-DB-Engines.

Instance class	Aurora MySQL	Aurora PostgreSQL
db.serverless – Aurora Serverless v2-Instance-Klasse mit automatischer Kapazitätsskalierung		
db.serverless	Siehe Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2	Siehe Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2
db.x2g — speicheroptimierte Instanzklassen, die auf Graviton2-Prozessoren basieren AWS		
db.x2g.16xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.x2g.12xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.x2g.8xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.x2g.4xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.x2g.2xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.x2g.xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher

Instance class	Aurora MySQL	Aurora PostgreSQL
db.x2g.large	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.r6gd — Optimierte Reads-Instanzklassen, die auf Graviton2-Prozessoren basieren AWS		
db.r6gd.16xlarge	Nein	15.4 und höher, 14.9 und höher
db.r6gd.12xlarge	Nein	15.4 und höher, 14.9 und höher
db.r6gd.8xlarge	Nein	15.4 und höher, 14.9 und höher
db.r6gd.4xlarge	Nein	15.4 und höher, 14.9 und höher
db.r6gd.2xlarge	Nein	15.4 und höher, 14.9 und höher
db.r6gd.xlarge	Nein	15.4 und höher, 14.9 und höher
db.r6id – Instance-Klassen für optimierte Lesevorgänge		
db.r6id.32xlarge	Nein	15.4 und höher, 14.9 und höher
db.r6id.24xlarge	Nein	15.4 und höher, 14.9 und höher
db.r7g — speicheroptimierte Instanzklassen, die auf Graviton3-Prozessoren basieren AWS		
db.r7g.16xlarge	2.12.0 und höher, 3.03.1 und höher	15.2 und höher, 14.7 und höher, 13.10 und höher
db.r7g.12xlarge	2.12.0 und höher, 3.03.1 und höher	15.2 und höher, 14.7 und höher, 13.10 und höher
db.r7g.8xlarge	2.12.0 und höher, 3.03.1 und höher	15.2 und höher, 14.7 und höher, 13.10 und höher
db.r7g.4xlarge	2.12.0 und höher, 3.03.1 und höher	15.2 und höher, 14.7 und höher, 13.10 und höher

Instance class	Aurora MySQL	Aurora PostgreSQL
db.r7g.2xlarge	2.12.0 und höher, 3.03.1 und höher	15.2 und höher, 14.7 und höher, 13.10 und höher
db.r7g.xlarge	2.12.0 und höher, 3.03.1 und höher	15.2 und höher, 14.7 und höher, 13.10 und höher
db.r7g.large	2.12.0 und höher, 3.03.1 und höher	15.2 und höher, 14.7 und höher, 13.10 und höher
db.r6g — speicheroptimierte Instanzklassen, die auf Graviton2-Prozessoren basieren AWS		
db.r6g.16xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.r6g.12xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.r6g.8xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.r6g.4xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.r6g.2xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.r6g.xlarge	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher

Instance class	Aurora MySQL	Aurora PostgreSQL
db.r6g.large	2.09.2 und höher, 2.10.0 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.8 und höher, 11.9, 11.12 und höher
db.r6i – arbeitsspeicheroptimierte Instance-Klassen		
db.r6i.32xlarge	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r6i.24xlarge	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r6i.16xlarge	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r6i.12xlarge	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r6i.8xlarge	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r6i.4xlarge	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r6i.2xlarge	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r6i.xlarge	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r6i.large	2.11.0 und höher, 3.02.1 und höher	15.2 und höher, 14.3 und höher, 13.5 und höher, 12.9 und höher
db.r5 – arbeitsspeicheroptimierte Instance-Klassen		
db.r5.24xlarge	Alle Versionen 2.x; 3.01.0 und höher	Alle aktuell verfügbaren Versionen

Instance class	Aurora MySQL	Aurora PostgreSQL
db.r5.16xlarge	Alle Versionen 2.x; 3.01.0 und höher	Alle aktuell verfügbaren Versionen
db.r5.12xlarge	Alle Versionen 2.x; 3.01.0 und höher	Alle aktuell verfügbaren Versionen
db.r5.8xlarge	Alle Versionen 2.x; 3.01.0 und höher	Alle aktuell verfügbaren Versionen
db.r5.4xlarge	Alle Versionen 2.x; 3.01.0 und höher	Alle aktuell verfügbaren Versionen
db.r5.2xlarge	Alle Versionen 2.x; 3.01.0 und höher	Alle aktuell verfügbaren Versionen
db.r5.xlarge	Alle Versionen 2.x; 3.01.0 und höher	Alle aktuell verfügbaren Versionen
db.r5.large	Alle Versionen 2.x; 3.01.0 und höher	Alle aktuell verfügbaren Versionen
db.r4 – arbeitsspeicheroptimierte Instance-Klassen		
db.r4.16xlarge	Alle Versionen 2.x; wird in 3.01.0 und höher nicht unterstützt	Nein
db.r4.8xlarge	Alle Versionen 2.x; nicht unterstützt in 3.01.0 und höher	Nein
db.r4.4xlarge	Alle Versionen 2.x; nicht unterstützt in 3.01.0 und höher	Nein
db.r4.2xlarge	Alle Versionen 2.x; nicht unterstützt in 3.01.0 und höher	Nein
db.r4.xlarge	Alle Versionen 2.x; nicht unterstützt in 3.01.0 und höher	Nein

Instance class	Aurora MySQL	Aurora PostgreSQL
db.r4.large	Alle Versionen 2.x; nicht unterstützt in 3.01.0 und höher	Nein
db.t4g — Instance-Klassen mit hervorragender Leistung, die auf Graviton2-Prozessoren basieren AWS		
db.t4g.2xlarge	Nein	Nein
db.t4g.xlarge	Nein	Nein
db.t4g.large	2.11.1 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.7 und höher, 11.12 und höher
db.t4g.medium	2.11.1 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.7 und höher, 11.12 und höher
db.t4g.klein	Nein	Nein
db.t3 – Instance-Klassen mit Spitzenlastleistung		
db.t3.2xlarge	Nein	Nein
db.t3.xlarge	Nein	Nein
db.t3.large	2.11.1 und höher, 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.7 und höher, 11.12 und höher
db.t3.medium	Alle 2.x-Versionen; 3.01.0 und höher	15.2 und höher, 14.3 und höher, 13.3 und höher, 12.7 und höher, 11.12 und höher
db.t3.small	Alle 2.x-Versionen; in 3.01.0 und höher nicht unterstützt	Nein
db.t3.micro	Nein	Nein

Instance class	Aurora MySQL	Aurora PostgreSQL
db.t2 – Instance-Klassen mit Spitzenlastleistung		
db.t2.Medium	Alle 2.x-Versionen; in 3.01.0 und höher nicht unterstützt	Nein
db.t2.small	Alle 2.x-Versionen; in 3.01.0 und höher nicht unterstützt	Nein

Ermitteln der Unterstützung für DB-Instance-Klassen in AWS-Regionen

Zur Bestimmung der DB-Instance-Klassen, die von jeder DB-Engine in einer bestimmten AWS-Region unterstützt werden, stehen mehrere Ansätze zur Verfügung. Sie können die AWS Management ConsoleAmazon RDS-Preisseite oder den Befehl AWS CLI describe-orderable-db-instance-options verwenden.

> **Note**
>
> Wenn Sie Operationen mit dem ausführen AWS Management Console, werden automatisch die unterstützten DB-Instance-Klassen für eine bestimmte DB-Engine, DB-Engine-Version und angezeigt. AWS-Region Beispiele für Vorgänge, die Sie ausführen können, sind das Erstellen und Ändern einer DB-Instance.

Inhalt

Verwenden der Amazon RDS-Preisseite zur Bestimmung der DB-Instance-Klassenunterstützung in AWS-Regionen

Sie können die Seite Amazon Aurora Pricing verwenden, um die DB-Instance-Klassen zu bestimmen, die von jeder DB-Engine in einer bestimmten AWS-Region unterstützt werden.

So verwenden Sie die Preisseite, um die DB-Instance-Klassen zu bestimmen, die von jeder Engine in einer Region unterstützt werden

1. Gehen Sie zu Amazon Aurora Pricing.
2. Wählen Sie im Bereich AWS Pricing Calculator eine Amazon Aurora-Engine aus.
3. Wählen Sie unter Region auswählen eine AWS-Region aus.
4. Wählen Sie unter Cluster-Konfigurationsoption eine Konfigurationsoption aus.
5. Verwenden Sie den Abschnitt für kompatible Instances, um sich die unterstützten DB-Instance-Klassen anzusehen.
6. (Optional) Wählen Sie andere Optionen im Rechner und dann Zusammenfassung speichern und anzeigen oder Service speichern und hinzufügen aus.

Verwenden Sie die AWS CLI , um die Unterstützung der DB-Instance-Klasse zu ermitteln in AWS-Regionen

Sie können den verwenden AWS CLI , um zu ermitteln, welche DB-Instance-Klassen für bestimmte DB-Engines und DB-Engine-Versionen in einem unterstützt AWS-Region werden.

Um die folgenden AWS CLI Beispiele zu verwenden, geben Sie gültige Werte für die DB-Engine, die DB-Engine-Version, die DB-Instance-Klasse und ein AWS-Region. Die folgende Tabelle zeigt die gültigen DB-Engine-Werte.

Engine-Name	Engine-Wert in CLI-Befehlen	Weitere Informationen zu den Versionen
MySQL 5.7-kompatibles Aurora und 8.0-compatible Aurora	`aurora-mysql`	Aktualisierungen der Datenbank-Engine für Amazon Aurora MySQL Version 2 und Aktualisierungen der Datenbank-Engine für Amazon-Aurora-MySQL-Version 3 in den Versionshinweisen für Aurora MySQL

Engine-Name	Engine-Wert in CLI-Befehlen	Weitere Informationen zu den Versionen
Aurora PostgreSQL	`aurora-postgresql`	Versionshinweise für Aurora PostgreSQL

Hinweise zu AWS-Region Namen finden Sie unterAWS Regionen.

Die folgenden Beispiele zeigen, wie die Unterstützung von DB-Instance-Klassen AWS-Region mithilfe des Befehls AWS CLI describe-orderable-db-instance-options ermittelt werden kann.

Themen

- Auflistung der DB-Instance-Klassen, die von einer bestimmten DB-Engine-Version in einer AWS-Region unterstützt werden
- Auflisten der DB-Engine-Versionen, die eine bestimmte DB-Instance-Klasse in einer AWS-Region unterstützen

Auflistung der DB-Instance-Klassen, die von einer bestimmten DB-Engine-Version in einer AWS-Region unterstützt werden

Führen Sie den folgenden Befehl aus, um die DB-Instance-Klassen aufzulisten, die von einer bestimmten DB-Engine-Version unterstützt werden. AWS-Region

Für LinuxmacOS, oderUnix:

```
aws rds describe-orderable-db-instance-options --engine engine --engine-version version
 \
    --query "OrderableDBInstanceOptions[].
{DBInstanceClass:DBInstanceClass,SupportedEngineModes:SupportedEngineModes[0]}" \
    --output table \
    --region region
```

Windows:

```
aws rds describe-orderable-db-instance-options --engine engine --engine-version version
 ^
    --query "OrderableDBInstanceOptions[].
{DBInstanceClass:DBInstanceClass,SupportedEngineModes:SupportedEngineModes[0]}" ^
    --output table ^
```

```
    --region region
```

Die Ausgabe zeigt auch die Engine-Modi, die für jede DB-Instance-Klasse unterstützt werden.

Der folgende Befehl listet beispielsweise die unterstützten DB-Instance-Klassen für Version 13.6 der Aurora-PostgreSQL-DB-Engine in USA Ost (Nord-Virginia) auf.

Für LinuxmacOS, oderUnix:

```
aws rds describe-orderable-db-instance-options --engine aurora-postgresql --engine-
version 15.3 \
    --query "OrderableDBInstanceOptions[].
{DBInstanceClass:DBInstanceClass,SupportedEngineModes:SupportedEngineModes[0]}" \
    --output table \
    --region us-east-1
```

Windows:

```
aws rds describe-orderable-db-instance-options --engine aurora-postgresql --engine-
version 15.3 ^
    --query "OrderableDBInstanceOptions[].
{DBInstanceClass:DBInstanceClass,SupportedEngineModes:SupportedEngineModes[0]}"  ^
    --output table ^
    --region us-east-1
```

Auflisten der DB-Engine-Versionen, die eine bestimmte DB-Instance-Klasse in einer AWS-Region unterstützen

Um die DB-Engine-Versionen aufzulisten, die eine bestimmte DB-Instance-Klasse in einer AWS-Region unterstützen, führen Sie den folgenden Befehl aus.

Für LinuxmacOS, oderUnix:

```
aws rds describe-orderable-db-instance-options --engine engine --db-instance-
class DB_instance_class \
    --query "OrderableDBInstanceOptions[].
{EngineVersion:EngineVersion,SupportedEngineModes:SupportedEngineModes[0]}" \
    --output table \
    --region region
```

Windows:

```
aws rds describe-orderable-db-instance-options --engine engine --db-instance-
class DB_instance_class ^
    --query "OrderableDBInstanceOptions[].
{EngineVersion:EngineVersion,SupportedEngineModes:SupportedEngineModes[0]}" ^
    --output table ^
    --region region
```

Die Ausgabe zeigt auch die Engine-Modi, die für jede DB-Engine-Version unterstützt werden.

Der folgende Befehl listet beispielsweise die DB-Engine-Versionen der RDS for Aurora PostgreSQL-DB-Engine auf, welche die db.r5.large DB-Instance-Klasse in US East (N. Virginia) unterstützen.

Für LinuxmacOS, oderUnix:

```
aws rds describe-orderable-db-instance-options --engine aurora-postgresql --db-
instance-class db.r7g.large \
    --query "OrderableDBInstanceOptions[].
{EngineVersion:EngineVersion,SupportedEngineModes:SupportedEngineModes[0]}" \
    --output table \
    --region us-east-1
```

Windows:

```
aws rds describe-orderable-db-instance-options --engine aurora-postgresql --db-
instance-class db.r7g.large ^
    --query "OrderableDBInstanceOptions[].
{EngineVersion:EngineVersion,SupportedEngineModes:SupportedEngineModes[0]}" ^
    --output table ^
    --region us-east-1
```

Hardware-Spezifikationen für DB-Instance-Klassen für Aurora

Die folgende Terminologie wird zum Beschreiben der Hardwarespezifikationen für DB-Instance-Klassen verwendet:

vCPU

Die Anzahl der virtuellen zentralen Verarbeitungseinheiten (Central Processing Units, CPUs). Eine virtuelle CPU ist eine Kapazitätseinheit, mit der Sie DB-Instance-Klassen vergleichen können. Anstatt einen bestimmten Prozessor für mehrere Monate oder Jahre zu erwerben oder

zu leasen, wird jetzt Kapazität stundenweise gemietet. Unser Ziel ist es, eine konsistente und spezifische Menge an CPU-Kapazität innerhalb der Grenzen der zugrunde liegenden Hardware zur Verfügung zu stellen.

EC2-Recheneinheiten

Das relative Maß der ganzzahligen Rechenleistung einer Amazon EC2-Instance. Um den Entwicklern den Vergleich zwischen den CPU-Kapazitäten der verschiedenen Instance-Klassen zu erleichtern, haben wir eine Amazon EC2-Recheneinheit definiert. Die einer bestimmten Instance zugewiesene CPU-Menge wird in diesen EC2 Compute Units ausgedrückt. Ein ECU entspricht derzeit einem CPU-Kapazitätsäquivalent eines 1,0–1,2 GHz-2007 Opteron- oder -2007 Xeon-Prozessors.

Arbeitsspeicher (GiB)

Der Arbeitsspeicher (RAM) in Gibibytes, der der DB-Instance zugeteilt ist. Häufig ist das Verhältnis zwischen Arbeitsspeicher- und vCPU konsistent. Beispielsweise hat die Instance-Klasse db.r4 das gleiche Verhältnis von Speicher zu vCPU wie die Instance-Klasse db.r5. Für die meisten Anwendungsfälle bietet die Instance-Klasse db.r5 jedoch eine bessere und konsistentere Performance als die Instance-Klasse db.r4.

Max. EBS-Bandbreite (Mbit/s)

Die maximale EBS-Bandbreite in Megabit pro Sekunde. Dividieren Sie durch 8, um den erwarteten Durchsatz in Megabyte pro Sekunde zu erhalten.

> **Note**
>
> Diese Zahl bezieht sich auf die I/O-Bandbreite für den lokalen Speicher innerhalb der DB-Instance. Sie gilt nicht für die Kommunikation mit dem Aurora-Clustervolume.

Netzwerkbandbreite

Die Netzwerkgeschwindigkeit relativ zu anderen DB-Instance-Klassen.

In der folgenden Tabelle finden Sie Hardware-Details zu den Amazon RDS-DB-Instance-Klassen für Aurora.

Informationen zur Aurora-DB-Engine-Unterstützung für die einzelnen DB-Instance-Klassen finden Sie unter Unterstützte DB-Engines für DB-Instance-Klassen.

Instance-Klasse	vCPU	EC2-Recheneinheiten	Arbeitsspeicher (GiB)	Max. Bandbreite (Mbit/s) des lokalen Speichers	Netzwerkleistung (Gbit/s)
db.x1 – Speicheroptimierte Instance-Klassen					
db.x2g.16xlarge	64	—	1024	19.000	25
db.x2g.12xlarge	48	—	768	14.250	20
db.x2g.8xlarge	32	—	512	9.500	12
db.x2g.4xlarge	16	—	256	4.750	Bis zu 10
db.x2g.2xlarge	8	—	128	Bis zu 4750.	Bis zu 10
db.x2g.xlarge	4	—	64	Bis zu 4750.	Bis zu 10
db.x2g.large	2	—	32	Bis zu 4750.	Bis zu 10
db.r7g – arbeitsspeicheroptimierte Instance-Klassen mit AWS -Graviton3-Prozessoren					
db.r7g.16xlarge	64	—	512	20 000	30
db.r7g.12xlarge	48	—	384	15 000	22,5
db.r7g.8xlarge	32	—	256	10.000	15
db.r7g.4xlarge	16	—	128	Bis zu 10 000*	Bis zu 15
db.r7g.2xlarge	8	—	64	Bis zu 10 000*	Bis zu 15
db.r7g.xlarge	4	—	32	Bis zu 10 000*	Bis zu 12,5

Instance-Klasse	vCPU	EC2-Recheneinheiten	Arbeitsspeicher (GiB)	Max. Bandbreite (Mbit/s) des lokalen Speichers	Netzwerkleistung (Gbit/s)
db.r7g.large	2	—	16	Bis zu 10 000*	Bis zu 12,5
db.r6g – arbeitsspeicheroptimierte Instance-Klassen mit AWS -Graviton2-Prozessoren					
db.r6g.16xlarge	64	—	512	19.000	25
db.r6g.12xlarge	48	—	384	13.500	20
db.r6g.8xlarge	32	—	256	9 000	12
db.r6g.4xlarge	16	—	128	4.750	Bis zu 10
db.r6g.2xlarge	8	—	64	Bis zu 4750.	Bis zu 10
db.r6g.xlarge	4	—	32	Bis zu 4750.	Bis zu 10
db.r6g.large	2	—	16	Bis zu 4750.	Bis zu 10
db.r6i – arbeitsspeicheroptimierte Instance-Klassen					
db.r6i.32xlarge	128	—	1,024	40 000	50
db.r6i.24xlarge	96	—	768	30 000	37,5
db.r6i.16xlarge	64	—	512	20 000	25
db.r6i.12xlarge	48	—	384	15 000	18,75
db.r6i.8xlarge	32	—	256	10.000	12,5
db.r6i.4xlarge	16	—	128	Bis zu 10 000*	Bis zu 12,5

Instance-Klasse	vCPU	EC2-Recheneinheiten	Arbeitsspeicher (GiB)	Max. Bandbreite (Mbit/s) des lokalen Speichers	Netzwerkleistung (Gbit/s)
db.r6i.2xlarge	8	—	64	Bis zu 10 000*	Bis zu 12,5
db.r6i.xlarge	4	—	32	Bis zu 10 000*	Bis zu 12,5
db.r6i.large	2	—	16	Bis zu 10 000*	Bis zu 12,5
db.r5 – arbeitsspeicheroptimierte Instance-Klassen					
db.r5.24xlarge	96	347	768	19.000	25
db.r5.16xlarge	64	264	512	13.600	20
db.r5.12xlarge	48	173	384	9.500	12
db.r5.8xlarge	32	132	256	6.800	10
db.r5.4xlarge	16	71	128	4.750	Bis zu 10
db.r5.2xlarge	8	38	64	Bis zu 4750.	Bis zu 10
db.r5.xlarge	4	19	32	Bis zu 4750.	Bis zu 10
db.r5.large	2	10	16	Bis zu 4750.	Bis zu 10
db.r4 – arbeitsspeicheroptimierte Instance-Klassen					
db.r4.16xlarge	64	195	488	14.000	25
db.r4.8xlarge	32	99	244	7.000	10
db.r4.4xlarge	16	53	122	3.500	Bis zu 10

Instance-Klasse	vCPU	EC2-Recheneinheiten	Arbeitsspeicher (GiB)	Max. Bandbreite (Mbit/s) des lokalen Speichers	Netzwerkleistung (Gbit/s)
db.r4.2xlarge	8	27	61	1.700	Bis zu 10
db.r4.xlarge	4	13.5	30,5	850	Bis zu 10
db.r4.large	2	7	15,25	425	Bis zu 10
db.t4g – Instance-Klassen mit Spitzenlastleistung					
db.t4g.large	2	—	8	Bis zu 2.780	Bis zu 5
db.t4g.medium	2	—	4	Bis zu 2 085	Bis zu 5
db.t3 – Instance-Klassen mit Spitzenlastleistung					
db.t3.large	2	Variable	8	Bis zu 2.048	Bis zu 5
db.t3.medium	2	Variable	4	Bis zu 1.536	Bis zu 5
db.t3.small	2	Variable	2	Bis zu 1.536	Bis zu 5
db.t2 – Instance-Klassen mit Spitzenlastleistung					
db.t2.Medium	2	Variable	4	—	Mittel
db.t2.small	1	Variable	2	—	Niedrig

Amazon Aurora-Speicher und -Zuverlässigkeit

Im Folgenden können Sie mehr über das Aurora-Speichersubsystem erfahren. Aurora verwendet eine verteilte und gemeinsam genutzte Speicherarchitektur, die ein wichtiger Faktor für Leistung, Skalierbarkeit und Zuverlässigkeit für Aurora-Cluster ist.

Themen

Übersicht über Amazon-Aurora-Speicher

Aurora-Daten werden im Cluster-Volume gespeichert. Hierbei handelt es sich um ein einzelnes, virtuelles Volume, das SSD-Laufwerke verwendet. Ein Cluster-Volume besteht aus Datenkopien, die sich zwischen drei Availability Zones in einer einzelnen AWS-Region befinden. Da Daten automatisch zwischen Availability Zones repliziert werden, bleiben Ihre Daten sehr lange beständig, mit einer geringeren Wahrscheinlichkeit für Datenverlust. Durch diese Replikation wird eine höhere Verfügbarkeit Ihrer Datenbank bei einem Failover sichergestellt. Dies ist möglich, weil die Datenkopien bereits in den anderen Availability Zones vorhanden sind und Datenanfragen für die DB-Instances in Ihrem DB-Cluster weiterhin bearbeitet werden. Die Menge der replizierten Daten ist unabhängig von der Anzahl der DB-Instances in Ihrem Cluster.

Aurora verwendet separaten lokalen Speicher für nicht persistente, temporäre Dateien. Dazu gehören Dateien, die für Zwecke wie das Sortieren großer Datensätze während der Abfrageverarbeitung oder für die Indexerstellung verwendet werden. Weitere Informationen finden Sie unter Temporäre Speicherlimits für Aurora MySQL und Temporäre Speicherlimits für Aurora PostgreSQL.

Inhalt des Cluster-Volumes

Das Aurora-Cluster-Volume enthält all Ihre Benutzerdaten, Schema-Objekte sowie interne Metadaten wie die Systemtabellen und das Binärprotokoll. Beispielsweise speichert Aurora alle Tabellen, Indizes, Binary Large Objects (BLOBs) oder gespeicherte Prozeduren eines Aurora-Clusters im Cluster-Volume.

Die verschiedene Speicherquellen nutzende Architektur von Aurora sorgt dafür, dass Ihre Daten von den DB-Instances im Cluster unabhängig sind. So können Sie eine DB-Instance schnell hinzufügen, weil Aurora keine neue Kopie der Tabellendaten erstellt. Stattdessen stellt die DB-Instance eine Verbindung zum freigegebenen Volume her, das bereits alle Daten von Ihnen enthält. Sie können eine DB-Instance aus einem Cluster entfernen, ohne die zugrunde liegenden Daten aus dem Cluster entfernen zu müssen. Aurora entfernt die Daten nur, wenn Sie den gesamten Cluster löschen.

Speicherkonfigurationen für DB-Cluster von Amazon Aurora

Amazon Aurora bietet zwei Speicherkonfigurationen für DB-Cluster:

- Aurora I/O-Optimized – Verbessertes Preis-Leistungs-Verhältnis und bessere Vorhersagbarkeit für I/O-intensive Anwendungen. Sie zahlen nur für die Nutzung und Speicherung Ihrer DB-Cluster, ohne zusätzliche Gebühren für Lese- und Schreib-I/O-Operationen.

  Aurora I/O-Optimized ist am besten geeignet, wenn Ihre I/O-Ausgaben 25 % oder mehr Ihrer gesamten Aurora-Datenbankausgaben ausmachen.

  Sie können Aurora I/O-Optimized auswählen, wenn Sie einen DB-Cluster mit einer DB-Engine-Version erstellen oder ändern, die die Cluster-Konfiguration von Aurora I/O-Optimized unterstützt. Sie können jederzeit von Aurora I/O-Optimized zu Aurora Standard wechseln.
- Aurora Standard – Kostengünstige Preise für viele Anwendungen mit moderater I/O-Auslastung. Neben der Auslastung und Speicherung Ihrer DB-Cluster zahlen Sie auch einen Standardsatz pro 1 Million Anfragen für I/O-Operationen.

  Aurora Standard ist am besten geeignet, wenn Ihre I/O-Ausgaben 25 % oder weniger Ihrer gesamten Aurora-Datenbankausgaben ausmachen.

  Sie können alle 30 Tage von Aurora Standard auf Aurora I/O-Optimized wechseln. Es gibt keine Ausfallzeiten, wenn Sie von Aurora Standard zu Aurora I/O-Optimizedoder von Aurora I/O-Optimized zu wechselnAurora Standard.

Weitere Informationen zu AWS-Region und zur Unterstützung der Versionen finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Cluster-Speicherkonfigurationen.

Weitere Informationen zu den Preisen für Speicherkonfigurationen von Amazon Aurora finden Sie unter Amazon Aurora: Preise.

Informationen zur Auswahl der Speicherkonfiguration beim Erstellen eines DB-Clusters finden Sie unter Erstellen eines DB-Clusters. Informationen zum Ändern der Speicherkonfiguration für einen DB-Cluster finden Sie unter Einstellungen für Amazon Aurora.

Wie sich die Größe des Aurora-Speichers automatisch ändert

Aurora-Cluster-Volumes nehmen automatisch an Größe zu, wenn die Datenmenge in Ihrer Datenbank zunimmt. Die maximale Größe für ein Aurora-Cluster-Volumen beträgt je nach Version

der DB-Engine 128 Tebibyte (TiB) oder 64 TiB. Weitere Informationen zur maximalen Größe für eine bestimmte Version finden Sie unter Amazon Aurora-Größenbeschränkungen. Diese automatische Speicherskalierung wird mit einem leistungsstarken und hochverteilten Speicher-Subsystem kombiniert. Dadurch ist Aurora eine gute Wahl für Ihre wichtigen Unternehmensdaten, wenn Ihre Hauptziele Zuverlässigkeit und Hochverfügbarkeit sind.

Informationen zum Anzeigen des Volume-Status finden Sie unter Anzeigen des Volume-Status für einen Aurora MySQL-DB-Cluster oder Anzeigen des Volume-Status für einen Aurora PostgreSQL-DB-Cluster. Um die Speicherkosten mit anderen Prioritäten auszugleichen, Speicherskalierung beschreibt , wie die Amazon-Aurora-Metriken `AuroraVolumeBytesLeftTotal` und `VolumeBytesUsed` in überwacht werden CloudWatch.

Wenn Aurora-Daten entfernt werden, wird der für diese Daten zugewiesene Speicherplatz freigegeben. Beispiele für das Entfernen von Daten sind das Löschen oder Abschneiden einer Tabelle. Diese automatische Reduzierung der Speichernutzung hilft Ihnen, Speichergebühren zu minimieren.

> **Note**
>
> Die hier beschriebenen Speicherlimits und das dynamische Größenanpassungsverhalten gelten für persistente Tabellen und andere Daten, die auf dem Cluster-Volume gespeichert sind.
> Für Aurora PostgreSQL werden temporäre Tabellendaten in der lokalen DB-Instance gespeichert.
> Bei Aurora MySQL Version 2 werden temporäre Tabellendaten standardmäßig auf dem Cluster-Volume für Writer-Instances und im lokalen Speicher für Reader-Instances gespeichert. Weitere Informationen finden Sie unter Speicher-Engine für temporäre Tabellen auf der Festplatte.
> Bei Aurora MySQL Version 3 werden temporäre Tabellendaten in der lokalen DB-Instance oder auf dem Cluster-Volume gespeichert. Weitere Informationen finden Sie unter Neues temporäres Tabellenverhalten in Aurora-MySQL-Version 3.
> Die maximale Größe temporärer Tabellen im lokalen Speicher ist durch die maximale lokale Speichergröße der DB-Instance begrenzt. Die lokale Speichergröße hängt von der Instance-Klasse ab, die Sie verwenden. Weitere Informationen finden Sie unter Temporäre Speicherlimits für Aurora MySQL und Temporäre Speicherlimits für Aurora PostgreSQL.

Einige Speicherfunktionen, wie die maximale Größe eines Cluster-Volumes und die automatische Größenanpassung beim Entfernen von Daten, hängen von der Aurora-Version des Clusters ab. Weitere Informationen finden Sie unter Speicherskalierung. Außerdem erfahren Sie, wie Sie Speicherprobleme vermeiden und den zugewiesenen Speicher und freien Speicherplatz in Ihrem Cluster überwachen können.

Informationen zur Abrechnung des Aurora-Datenspeichers

Auch wenn ein Aurora-Cluster-Volume auf bis zu 128 tebibytes (TiB) anwachsen kann, werden Ihnen nur die Kosten für den Speicherplatz berechnet, den Sie in einem Aurora-Cluster-Volume verwenden. In früheren Aurora-Versionen konnte das Cluster-Volume Speicherplatz wiederverwenden, der beim Entfernen von Daten freigegeben wurde, der zugewiesene Speicherplatz nahm jedoch nie ab. Wenn Aurora-Daten jetzt entfernt werden, z. B. durch Löschen einer Tabelle oder Datenbank, verringert sich der insgesamt zugewiesene Speicherplatz um einen vergleichbaren Betrag. So können Sie Speicherkosten senken, indem Sie Tabellen, Indizes, Datenbanken usw. löschen, die Sie nicht mehr benötigen.

> **Tip**
>
> Bei früheren Versionen ohne die Funktion für die dynamische Größenanpassung muss die Speicherverwendung für einen Cluster zurückgesetzt werden, um einen logischen Dump auszuführen und auf einem neuen Cluster wiederherzustellen. Diese Operation kann bei großen Datenmengen sehr lange dauern. Wenn eine solche Situation auftritt, sollten Sie das Upgrade Ihres Clusters auf eine Version durchführen, die die dynamische Größenanpassung des Volumes unterstützt.

Informationen dazu, welche Aurora-Versionen die dynamische Größenanpassung unterstützen und wie Sie Speicherkosten durch Überwachen der Speichernutzung für Ihren Cluster minimieren können, finden Sie unter Speicherskalierung. Informationen zur Speicherabrechnung von Aurora-Backups finden Sie unter Grundlegendes zur Backup-Speicher-Nutzung in Amazon Aurora. Weitere Informationen über die Preise für Aurora-Datenspeicher finden Sie unter Amazon RDS for Aurora: Preise.

Amazon Aurora-Zuverlässigkeit

Aurora ist darauf ausgelegt, zuverlässig, beständig und fehlertolerant zu sein. Sie können Ihren Aurora-DB-Cluster so gestalten, dass eine bessere Verfügbarkeit erzielt wird, indem Sie

beispielsweise Aurora-Replicas hinzufügen und in verschiedenen Availability Zones platzieren. Zudem beinhaltet Aurora mehrere automatische Funktionen, die es zu einer verlässlichen Datenbanklösung machen.

Themen

Automatische Speicherplatzreparatur

Da Aurora mehrere Kopien Ihrer Daten in drei Availability Zones aufbewahrt, sind die Risiken für einen laufwerksbedingten Verlust von Daten stark reduziert. Aurora erkennt automatisch Fehler in den Laufwerk-Volumes, aus denen das Cluster-Volume besteht. Wenn ein Segment eines Laufwerk-Volumes ausfällt, repariert Aurora das Segment umgehend. Wenn Aurora das Laufwerk-Segment repariert, verwendet es die Daten in den anderen Volumes des Cluster-Volumes, um sicherzustellen, dass die Daten im reparierten Segment auf dem aktuellen Stand sind. Dadurch vermeidet Aurora Datenverlust und reduziert die Notwendigkeit, eine point-in-time Wiederherstellung durchzuführen, um nach einem Festplattenausfall wiederherzustellen.

Überlebensfähiger Seiten-Cache

Bei Aurora wird der Seiten-Cache jeder DB-Instance in einem von der Datenbank separaten Prozess verwaltetet, was dem Seiten-Cache ermöglicht, unabhängig von der Datenbank zu überleben. (Der Seiten-Cache wird auch als InnoDB-Puffer-Pool in Aurora MySQL und Puffer-Cache in Aurora PostgreSQL bezeichnet.)

Im unwahrscheinlichen Fall eines Datenbankausfalls bleibt der Seiten-Cache im Arbeitsspeicher, was aktuelle Datenseiten im Seiten-Cache „warm“ hält, wenn die Datenbank neu gestartet wird. Dies bringt einen Leistungsgewinn, da umgangen werden kann, dass die ersten Abfragen Lese-I/O-Operationen zum „Aufwärmen“ des Seiten-Caches ausführen müssen.

Bei Aurora MySQL ist das Verhalten des Seiten-Caches beim Neustart und Failover wie folgt:

- Versionen vor 2.10 – Wenn die Writer-DB-Instance neu gestartet wird, bleibt der Seiten-Cache der Writer-Instance erhalten, während Reader-DB-Instances ihre Seiten-Caches verlieren.
- Version 2.10 und höher – Sie können die Writer-Instance ohne die Reader-Instances neu starten.

  - Wenn die Reader-Instances beim Neustart der Writer-Instance nicht neu gestartet werden, verlieren sie ihre Seiten-Caches nicht.
  - Wenn die Reader-Instances beim Neustart der Writer-Instance neu gestartet werden, verlieren sie ihre Seiten-Caches.
- Wenn eine Reader-Instance neu gestartet wird, überleben die Seiten-Caches auf den Writer- und Reader-Instances.
- Wenn der DB-Cluster ein Failover ausführt, wirkt sich dies ähnlich aus wie ein Neustart einer Writer-Instance. Auf der neuen Writer-Instance (zuvor die Reader-Instance) bleibt der Seiten-Cache erhalten, aber auf der Reader-Instance (zuvor der Writer-Instance) überlebt der Seiten-Cache nicht.

Bei Aurora PostgreSQL können Sie die Cluster-Cache-Verwaltung verwenden, um den Seiten-Cache einer bestimmten Reader-Instance beizubehalten, die nach dem Failover zur Writer-Instance wird. Weitere Informationen finden Sie unter Schnelle Wiederherstellung nach Failover mit der Cluster-Cacheverwaltung für Aurora PostgreSQL.

Wiederherstellung nach ungeplanten Neustarts

Aurora ist für die nahezu umgehende Wiederherstellung nach einem ungeplanten Neustart und die weitere Bereitstellung Ihrer Anwendungsdaten ohne das Binärprotokoll ausgelegt. Aurora führt die Wiederherstellung asynchron auf parallelen Threads durch, sodass Ihre Datenbank nach einem ungeplanten Neustart sofort geöffnet und verfügbar ist.

Weitere Informationen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster und Optimierungen reduzieren die Neustartzeit der Datenbank.

Die folgenden Betrachtungen gelten für eine Binärprotokollierung und die Wiederherstellung nach einem ungeplanten Neustart auf Aurora MySQL:

- Die Aktivierung der Binärprotokollierung auf Aurora wirkt sich direkt auf die Wiederherstellungsdauer nach einem ungeplanten Neustart aus, da die DB-Instance gezwungen wird, das Binärprotokoll wiederherzustellen.
- Der Typ der Binärprotokollierung wirkt sich auf die Größe und die Effizienz der Protokollierung aus. Einige Formate protokollieren dieselbe Menge an Datenbankaktivitäten mehr Informationen in den Binärprotokollen auf als andere. Die folgenden Einstellungen für den Parameter `binlog_format` führen zu unterschiedlichen Mengen an Protokolldaten:
  - `ROW` – die meisten Protokolldaten

  - `STATEMENT` – die wenigsten Protokolldaten
  - `MIXED` – Eine mittlere Menge an Protokolldaten, was normalerweise die beste Kombination von Datenintegrität und Leistung darstellt

  Die Menge der Binärprotokolldaten wirkt sich auf die Wiederherstellungszeit aus. Wenn in den Binärprotokollen mehr Daten protokolliert sind, muss die DB-Instance bei der Wiederherstellung mehr Daten verarbeiten, was wiederum die Wiederherstellungsdauer erhöht.
- Um den Rechenaufwand zu reduzieren und die Wiederherstellungszeiten mit der Binärprotokollierung zu verbessern, können Sie das erweiterte Binärprotokoll verwenden. Das erweiterte Binärprotokoll verbessert die Datenbankwiederherstellungszeit um bis zu 99 %. Weitere Informationen finden Sie unter Einrichten eines erweiterten Binärprotokolls.
- Aurora benötigt die Binärprotokolle nicht, um Daten innerhalb eines DB-Clusters zu replizieren oder eine point-in-time Wiederherstellung (PITR) durchzuführen.
- Wenn Sie das Binärprotokoll nicht für die externe Replikation (oder einen externen Binärprotokoll-Stream) benötigen, empfehlen wir Ihnen, den Parameter `binlog_format` auf `OFF` zu setzen, um die Binärprotokollierung zu deaktivieren. Dies reduziert die Wiederherstellungsdauer.

Weitere Informationen über die Binärprotokollierung und Replikation in Aurora finden Sie unter Replikation mit Amazon Aurora. Weitere Informationen über die Auswirkungen der Verwendung unterschiedlicher MySQL-Replikationstypen finden Sie unter Vorteile und Nachteile einer auf Anweisungen und einer auf Zeilen basierenden Replikation in der MySQL-Dokumentation.

Amazon Aurora-Sicherheit

Die Sicherheit für Amazon Aurora wird auf drei Ebenen verwaltet:

- Mit AWS Identity and Access Management (IAM) können Sie steuern, wer Verwaltungsaktionen in Amazon RDS für Aurora-DB-Cluster und DB-Instances ausführen darf. Wenn Sie eine Verbindung zu AWS mithilfe von IAM-Anmeldeinformationen herstellen, muss Ihr AWS-Konto über IAM-Richtlinien verfügen, die die erforderlichen Berechtigungen zum Ausführen von Amazon-RDS-Verwaltungsvorgängen gewähren. Weitere Informationen finden Sie unter Identity and Access Management für Amazon Aurora.

  Wenn Sie IAM verwenden, um auf die Amazon-RDS-Konsole zuzugreifen, müssen Sie sich zuerst mit Ihren Anmeldeinformationen bei der AWS Management Console anmelden und anschließend die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds öffnen.

- Aurora-DB-Cluster müssen in einer Virtual Private Cloud (VPC) basierend auf dem Amazon VPC-Service erstellt werden. Mithilfe einer VPC-Sicherheitsgruppe können Sie steuern, welche Geräte und Amazon EC2-Instances Verbindungen zum Endpunkt und Port der DB-Instance für Aurora-DB-Cluster in einer VPC herstellen können. Diese Endpunkt- und Portverbindungen können mithilfe von Transport Layer Security (TLS)/Secure Sockets Layer (SSL) erstellt werden. Zusätzlich können Firewall-Regeln in Ihrem Unternehmen steuern, ob in Ihrem Unternehmen verwendete Geräte Verbindungen mit einer DB-Instance herstellen dürfen. Weitere Informationen zu VPCs finden Sie unter Amazon VPCs und Amazon Aurora.
- Um Anmeldungen und Berechtigungen für einen Amazon Aurora-DB-Cluster zu authentifizieren, können Sie einen der folgenden Ansätze oder eine Kombination aus diesen wählen.
  - Sie können denselben Ansatz wie bei einer eigenständigen DB-Instance in MySQL oder PostgreSQL wählen.

    Techniken zur Authentifizierung von Anmeldungen und Berechtigungen für eigenständige MySQL- oder PostgreSQL-DB-Instances, wie z. B. die Verwendung von SQL-Befehlen oder die Änderung von Datenbankschematabellen, funktionieren auch mit Aurora. Weitere Informationen finden Sie unter Sicherheit in Amazon Aurora MySQL oder Sicherheit in Amazon Aurora PostgreSQL.
  - Sie können die IAM-Datenbank-Authentifizierung verwenden.

    Mit der IAM-Datenbank-Authentifizierung authentifizieren Sie sich bei Ihrem Aurora-DB-Cluster, indem Sie einen Benutzer oder eine IAM-Rolle und ein Authentifizierungstoken verwenden. Ein Authentifizierungstoken ist ein eindeutiger Wert, der mithilfe des Signatur-Version 4-Signiervorgangs erstellt wird. Durch das Verwenden der IAM-Datenbank-Authentifizierung können Sie dieselben Anmeldeinformationen verwenden, um den Zugang zu Ihren AWS-Ressourcen und Ihrer Datenbank zu steuern. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung.
  - Sie können die Kerberos-Authentifizierung für Aurora PostgreSQL und Aurora MySQL verwenden.

    Sie können Kerberos verwenden, um Benutzer zu authentifizieren, wenn diese sich mit Ihrem DB-Cluster von Aurora PostgreSQL und Aurora MySQL verbinden. In diesem Fall arbeitet der DB-Cluster mit AWS Directory Service for Microsoft Active Directory, um die Kerberos-Authentifizierung zu aktivieren. AWS Directory Service for Microsoft Active Directory wird auch AWS Managed Microsoft AD genannt. Wenn Sie alle Ihre Anmeldeinformationen im selben Verzeichnis aufbewahren, können Sie Zeit und Mühe sparen. Sie haben einen zentralen Ort für die Speicherung und Verwaltung von Anmeldeinformationen für mehrere DB-Cluster. Die

Verwendung eines Verzeichnisses kann auch Ihr allgemeines Sicherheitsprofil verbessern. Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung mit Aurora PostgreSQL und Verwenden der Kerberos-Authentifizierung für Aurora MySQL.

Weitere Informationen zur Sicherheitskonfiguration finden Sie unter Sicherheit in Amazon Aurora.

Verwenden von SSL mit Aurora-DB-Clustern

Amazon Aurora-DB-Cluster unterstützten Secure Sockets Layer (SSL)-Verbindungen von Anwendungen mithilfe desselben Prozesses und desselben öffentlichen Schlüssels wie Amazon RDS-DB-Instances. Weitere Informationen finden Sie unter Sicherheit in Amazon Aurora MySQL, Sicherheit in Amazon Aurora PostgreSQL oder Verwenden von TLS/SSL mit Aurora Serverless v1.

Hohe Verfügbarkeit für Amazon Aurora

Die Amazon-Aurora-Architektur beinhaltet eine Trennung von Speicher und Rechenleistung. Aurora enthält einige Hochverfügbarkeitsfunktionen, die sich auf die Daten in Ihrem DB-Cluster beziehen. Die Daten bleiben auch dann sicher, wenn einige oder alle DB-Instances im Cluster nicht mehr verfügbar sind. Weitere Hochverfügbarkeitsfunktionen gelten für die DB-Instances. Diese Funktionen stellen sicher, dass eine oder mehrere DB-Instances bereit sind, Datenbankanforderungen Ihrer Anwendung zu verarbeiten.

Themen

- Hohe Verfügbarkeit für Aurora-Daten
- Hohe Verfügbarkeit für Aurora-DB-Instances
- Hohe Verfügbarkeit über AWS -Regionen hinweg mit globalen Aurora-Datenbanken
- Fehlertoleranz für einen Aurora-DB-Cluster
- Hochverfügbarkeit mit Amazon-RDS-Proxy

Hohe Verfügbarkeit für Aurora-Daten

Aurora speichert Kopien der Daten in einem DB-Cluster über mehrere Availability Zones in einer einzigen AWS-Region. Dieser Speichervorgang von Aurora erfolgt unabhängig davon, ob die DB-Instances im DB-Cluster mehrere Availability Zones umfassen. Weitere Informationen zu finden Sie unter Auror Verwalten eines Amazon Aurora-DB-Clusters.

Wenn Daten in die primäre DB-Instance geschrieben werden, repliziert Aurora die Daten synchron über die Availability Zones auf sechs Speicherknoten, die Ihrem Cluster-Volume zugeordnet sind. Auf diese Weise werden eine Datenredundanz erreicht, das Blockieren von I/Os verhindert und Latenzspitzen bei System-Backups minimiert. Wenn Sie eine DB-Instance mit hoher Verfügbarkeit ausführen, kann dies die Verfügbarkeit bei geplanten Systemwartungen verbessern. Außerdem kann dies Ihre Datenbanken bei Ausfällen und bei Nichtverfügbarkeit von Availability Zones schützen. Weitere Informationen über Availability Zones finden Sie unter Regionen und Availability Zones.

Hohe Verfügbarkeit für Aurora-DB-Instances

Nachdem Sie die primäre (Writer–) Instance erstellt haben, können Sie bis zu 15 schreibgeschützte Aurora-Replikate erstellen. Die Aurora-Replikate werden auch als Reader-Instances bezeichnet.

Während des day-to-day Betriebs können Sie einen Teil der Arbeit für leseintensive Anwendungen auslagern, indem Sie die Reader-Instances zur Verarbeitung von `SELECT` Abfragen verwenden. Wenn sich ein Problem auf die primäre Instance auswirkt, übernimmt eine dieser Reader-Instances als primäre Instance. Dieser Mechanismus wird als Failover bezeichnet. Viele Aurora-Funktionen gelten für den Failover-Mechanismus. Beispielsweise erkennt Aurora Datenbankprobleme und aktiviert den Failover-Mechanismus bei Bedarf automatisch. Aurora verfügt jedoch über Funktionen, die die Zeit für den Abschluss des Failovers verkürzen. Dadurch wird die Zeit minimiert, in der die Datenbank während eines Failovers nicht zum Schreiben verfügbar ist.

Aurora ist so konzipiert, dass die Wiederherstellung so schnell wie möglich erfolgt. Der schnellste Wiederherstellungspfad besteht darin, häufig neu zu starten oder ein Failover auf dieselbe DB-Instance durchzuführen. Der Neustart ist schneller und mit weniger Overhead verbunden als ein Failover.

Um eine Verbindungszeichenfolge zu verwenden, die auch dann unverändert bleibt, wenn ein Failover eine neue primäre Instance heraufstuft, stellen Sie eine Verbindung mit dem Cluster-Endpunkt her. Der Cluster-Endpunkt stellt stets die aktuelle primäre Instance im Cluster dar. Weitere Informationen zum Cluster-Endpunkt finden Sie unter Amazon Aurora-Verbindungsverwaltung.

> **Tip**
>
> Innerhalb jeder stellen Availability Zones (AZs) Standorte dar AWS-Region, die sich voneinander unterscheiden, um im Falle von Ausfällen Isolierung zu bieten. Wir empfehlen Ihnen, die primäre Instance und die Reader-Replikate in Ihrem DB-Cluster über mehrere Availability Zones zu verteilen, um die Verfügbarkeit Ihres DB-Clusters zu verbessern. Auf

diese Weise verursacht ein Problem, das eine gesamte Availability Zone betrifft, keinen Ausfall für Ihren Cluster.
Sie können einen Multi-AZ-DB-Cluster einrichten, indem Sie beim Erstellen des Clusters eine einfache Auswahl treffen. Sie können die AWS Management Console, AWS CLI oder die Amazon-RDS-API benutzen. Sie können einen vorhandenen Aurora-DB-Cluster auch in einen Multi-AZ-DB-Cluster konvertieren, indem Sie eine neue Reader-DB-Instance hinzufügen und eine andere Availability Zone angeben.

Hohe Verfügbarkeit über AWS -Regionen hinweg mit globalen Aurora-Datenbanken

Für hohe Verfügbarkeit über mehrere hinweg können AWS-RegionenSie globale Aurora-Datenbanken einrichten. Jede globale Aurora-Datenbank erstreckt sich über mehrere AWS-Regionen, was globale Lesevorgänge mit niedriger Latenz und Notfallwiederherstellung nach Ausfällen in einer ermöglicht AWS-Region. Aurora übernimmt automatisch die Replikation aller Daten und Aktualisierungen vom primären AWS-Region in jede der sekundären Regionen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Global Databases.

Fehlertoleranz für einen Aurora-DB-Cluster

Ein Aurora-DB-Cluster ist darauf ausgelegt, fehlertolerant zu sein. Das Cluster-Volume erstreckt sich über mehrere Availability Zones (AZs) in einem einzigen AWS-Regionund jede Availability Zone enthält eine Kopie der Cluster-Volume-Daten. Diese Funktionalität bedeutet, dass Ihr DB-Cluster einen Fehler in einer Availability Zone ohne Datenverlust und mit einer nur sehr kurzen Unterbrechung des Services toleriert.

Wenn die primäre Instance in einem DB-Cluster ausfällt, führt ein automatisches Failover auf eine von zwei Arten zu einer neuen primären Instance:

- Durch das Hochstufen einer bestehenden Aurora-Replica zu einer neuen primären Instance
- Durch das Erstellen einer neuen primären Instance

Wenn ein DB-Cluster über ein oder mehrere Aurora verfügt, wird eine Aurora-Replica während eines Ausfallereignisses zur primären Instance hochgestuft. Ein Fehlerereignis hat eine kurze Unterbrechung zufolge, während die Lese- und Schreibvorgänge mit einer Ausnahme fehlschlagen. Jedoch wird der Service im Normalfall in weniger als 60 Sekunden und oft sogar schon nach

30 Sekunden wiederhergestellt. Wir empfehlen Ihnen, mindestens ein oder mehrere Aurora Replicas in zwei oder mehreren verschiedenen Availability Zones zu erstellen, um die Verfügbarkeit Ihres DB-Clusters zu erhöhen.

> **Tip**
>
> In Aurora MySQL 2.10 und höher können Sie die Verfügbarkeit während eines Failovers verbessern, indem Sie mehr als eine Reader-DB-Instance in einem Cluster haben. In Aurora MySQL 2.10 und höher startet Aurora nur die Writer-DB-Instance und die Reader-Instance neu, auf die das Failover erfolgt ist. Andere Reader-Instances im Cluster bleiben während eines Failovers verfügbar, um Abfragen über Verbindungen zum Reader-Endpunkt fortzusetzen.
> Sie können die Verfügbarkeit auch während eines Failovers verbessern, indem Sie RDS-Proxy mit Ihrem Aurora-DB-Cluster verwenden. Weitere Informationen finden Sie unter Hochverfügbarkeit mit Amazon-RDS-Proxy.

Sie können die Reihenfolge, in der Ihre Aurora Replicas auf die primäre Instance nach einem Ausfall hochgestuft werden, anpassen, indem Sie jedem Replica eine Priorität zuweisen. Prioritäten liegen im Bereich zwischen 0 als höchste Priorität und 15 als niedrigste Priorität. Wenn die primäre Instance ausfällt, stuft Amazon RDS die Aurora-Replica mit der höchsten Priorität zur neuen primären Instance hoch. Sie können die Priorität eines Aurora Replica jederzeit anpassen. Das Ändern der Priorität löst kein Failover aus.

Mehrere Aurora Replicas können dieselbe Priorität haben, was zu Hochstufungsebenen führt. Wenn zwei oder mehrere Aurora-Replicas dieselbe Priorität haben, stuft Amazon RDS die größte Replica hoch. Wenn zwei oder mehrere Aurora-Replicas dieselbe Priorität und Größe haben, stuft Amazon RDS eine beliebige Replica auf derselben Hochstufungsebene hoch.

Wenn der DB-Cluster keine Aurora-Replikate hat, wird die primäre Instance bei einem Fehlerereignis in derselben AZ neu erstellt. Ein Fehlerereignis hat eine Unterbrechung zufolge, während die Lese- und Schreibvorgänge mit einer Ausnahme fehlschlagen. Der Service wird wiederhergestellt, wenn die primäre Instance erstellt wird. Dies dauert im Normalfall weniger als 10 Minuten. Das Hochstufen eines Aurora Replicas auf eine primäre Instance funktioniert viel schneller als das Erstellen einer neuen primären Instance.

Angenommen, die primäre Instance in Ihrem Cluster ist aufgrund eines Ausfalls, der sich auf eine gesamte AZ auswirkt, nicht verfügbar. In diesem Fall hängt die Möglichkeit, eine neue primäre Instance online zu stellen, davon ab, ob Ihr Cluster eine Multi-AZ-Konfiguration verwendet.

- Wenn Ihr bereitgestellter oder Aurora Serverless v2-Cluster Reader-Instances in anderen AZs enthält, verwendet Aurora den Failover-Mechanismus, um eine dieser Reader-Instances als neue primäre Instance hochzustufen.
- Wenn Ihr bereitgestellter oder Aurora Serverless v2-Cluster nur eine einzelne DB-Instance enthält oder wenn sich die primäre Instance und alle Reader-Instances in derselben AZ befinden, müssen Sie manuell eine oder mehrere neue DB-Instances in einer anderen AZ erstellen.
- Wenn Ihr Cluster Aurora Serverless v1 verwendet, erstellt Aurora automatisch eine neue DB-Instance in einer anderen AZ. Dieser Prozess erfordert jedoch eine Host-Ersetzung und dauert daher länger als ein Failover.

> **Note**
>
> Amazon Aurora unterstützt auch die Replikation mit einer externen MySQL-Datenbank oder einer RDS-MySQL-DB-Instance. Weitere Informationen finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).

Hochverfügbarkeit mit Amazon-RDS-Proxy

Mit RDS-Proxy können Sie Anwendungen erstellen, die Datenbankfehler transparent tolerieren können, ohne komplexen Fehlerbehandlungscode schreiben zu müssen. Der Proxy leitet den Datenverkehr automatisch an eine neue Datenbank-Instance weiter, wobei Anwendungsverbindungen erhalten bleiben. Außerdem umgeht er Domain Name System (DNS)-Caches, um die Failover-Zeiten für Aurora-Multi-AZ-Datenbanken um bis zu 66 % zu reduzieren. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

Replikation mit Amazon Aurora

Es gibt mehrere Replikations-Optionen für Aurora. Jeder Aurora-DB-Cluster verfügt über eine integrierte Replikation zwischen mehreren DB-Instances im selben Cluster. Sie können auch die Replikation mit Ihrem Aurora-Cluster als Quelle oder Ziel einrichten. Wenn Sie Daten in oder aus

einem Aurora-Cluster replizieren, können Sie zwischen integrierten Funktionen wie Aurora globalen Datenbanken oder den herkömmlichen Replikationsmechanismen für die MySQL- oder PostgreSQL-DB-Engines wählen. Sie können die geeigneten Optionen auswählen, je nachdem, welche die richtige Kombination aus Hochverfügbarkeit, Komfort und Leistung für Ihre Anforderungen bietet. In den folgenden Abschnitten wird erläutert, wie und wann Sie die jeweilige Technik wählen.

Themen

Aurora-Replikate

Wenn Sie eine zweite, dritte und so weiter DB-Instance in einem bereitgestellten Aurora-DB-Cluster erstellen, wird Aurora automatisch die Replikation von der Writer-DB-Instance zu allen anderen DB-Instances einrichten. Diese anderen DB-Instances sind schreibgeschützt und werden als Aurora-Replicas bezeichnet. Wir bezeichnen sie auch als Reader-Instances, wenn wir besprechen, wie Sie Writer- und Reader-DB-Instances innerhalb eines Clusters kombinieren können.

Aurora-Replicas haben zwei Hauptzwecke. Sie können über sie Abfragen stellen, um die Lesevorgänge für Ihre Anwendung zu skalieren. In der Regel tun Sie dies, indem Sie eine Verbindung zum Reader-Endpunkt des Clusters herstellen. Auf diese Weise kann Aurora die Last für schreibgeschützte Verbindungen auf so viele Aurora-Replicas verteilen, wie Sie im Cluster haben. Aurora-Replicas tragen auch dazu bei, die Verfügbarkeit zu erhöhen. Wenn die Writer-Instance in einem Cluster nicht verfügbar ist, stuft Aurora automatisch eine der Reader-Instances hoch, um ihren Platz als neuer Autor einzunehmen.

Ein Aurora-DB-Cluster kann bis zu 15 Aurora-Replicas enthalten. Die Aurora-Replikate können über die Availability Zones verteilt werden, über die sich ein DB-Cluster innerhalb einer AWS -Region erstreckt.

Die Daten in Ihrem DB-Cluster haben ihre eigenen Hochverfügbarkeits- und Zuverlässigkeitsfunktionen, unabhängig von den DB-Instances im Cluster. Wenn Sie mit den Aurora-Speicherfunktionen nicht vertraut sind, lesen Sie Übersicht über Amazon-Aurora-Speicher. Das DB-Cluster-Volume besteht physisch aus mehreren Kopien der Daten für den DB-Cluster. Die primäre Instance und die Aurora-Replicas im DB-Cluster sehen die Daten im Cluster-Volume als ein einziges logisches Volume.

Daher geben alle Aurora-Replikate die gleichen selben Daten als Abfrageergebnisse bei minimaler Replikatsverzögerung zurück. Diese Verzögerung beträgt in der Regel sehr viel weniger als 100 Millisekunden nach dem Schreiben einer Aktualisierung durch die primäre Instance. Die Replica-Verzögerung variiert in Abhängigkeit vom Veränderungsgrad in der Datenbank. In den Zeitabschnitten, in denen sehr viele Schreibvorgänge in der Datenbank durchgeführt werden, könnte es zu einer erhöhten Replica-Verzögerung kommen.

> **Note**
>
> Aurora Replica wird neu gestartet, wenn die Kommunikation mit der Writer-DB-Instance in den folgenden Aurora-PostgreSQL-Versionen länger als 60 Sekunden unterbrochen wird:
>
> - 14.6 und ältere Versionen
> - 13.9 und ältere Versionen
> - 12.13 und ältere Versionen
> - Alle Versionen von Aurora PostgreSQL 11

Aurora Replicas funktionieren für das Skalieren von Lesevorgängen, da sie in Ihrem Cluster-Volume vollständig für Lesevorgänge bereit stehen. Schreibvorgänge werden von der primären Instance verwaltet. Da das Cluster-Volume zwischen allen Instances in Ihrem DB-Cluster geteilt wird, bedeutet es nur einen geringen Aufwand, um eine Kopie der Daten für die einzelnen Aurora-Replicas zu replizieren.

Sie können Aurora Replicas als Failover-Vorgaben verwenden, um die Verfügbarkeit zu erhöhen. Das heißt, wenn die primäre Instance ausfällt, wird ein Aurora-Replikat zur primären Instance heraufgestuft. Es gibt dann eine kurze Unterbrechung, während der Lese- und Schreibanfragen an die primäre Instance mit einer Ausnahme fehlschlagen.

Die Hochstufung einer Aurora-Replica per Failover ist eine viel schnellere Methode als die Neuerstellung der primären Instance. Wenn Ihr Aurora-DB-Cluster keine Aurora-Replikate enthält, steht Ihr DB-Cluster während der Wiederherstellung Ihrer DB-Instance nach dem Ausfall nicht zur Verfügung.

Bei einem Failover werden möglicherweise einige der Aurora-Replikate je nach Version der DB-Engine neu gestartet. In Aurora MySQL 2.10 und höher startet Aurora nur die Writer-DB-Instance und das Failover-Ziel während eines Failovers neu. Informationen zum Neustartverhalten verschiedener Aurora-DB-Engine-Versionen finden Sie unter Neustart eines Amazon Aurora DB-Clusters oder einer

Amazon Aurora DB-Instance. Hinweise dazu, was mit Seitencaches beim Neustart oder Failover geschieht, finden Sie unterÜberlebensfähiger Seiten-Cache.

Für Szenarien mit hoher Verfügbarkeit empfehlen wir Ihnen, mindestens ein Aurora-Replikat zu erstellen. Diese sollten dieselbe DB-Instance-Class haben wie die primäre Instance und in verschiedenen Availability Zones für Ihren Aurora-DB-Cluster liegen. Weitere Informationen über Aurora-Replikate als Failover-Ziele finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.

Sie können keine verschlüsselte Aurora-Replica für einen unverschlüsselten Aurora-DB-Cluster erstellen. Sie können keine unverschlüsselte Aurora-Replica für einen verschlüsselten Aurora-DB-Cluster erstellen.

> **Tip**
>
> Sie können Aurora-Replicas innerhalb eines Aurora-Clusters als Ihre einzige Form der Replikation verwenden, um Ihre Daten hochverfügbar zu halten. Sie können die integrierte Aurora-Replikation auch mit den anderen Arten der Replikation kombinieren. Dies kann dazu beitragen, ein zusätzliches Maß an hoher Verfügbarkeit und geografischer Verteilung Ihrer Daten zu gewährleisten.

Details zum Erstellen von Aurora-Replicas finden Sie unter Hinzufügen von Aurora-Replicas zu einem DB-Cluster.

Replikation mit Aurora MySQL

Zusätzlich zu Aurora-Replicas haben Sie die folgenden Möglichkeiten für Replikationen mit Aurora MySQL:

- Aurora MySQL-DB-Cluster in verschiedenen - AWS Regionen.
  - Sie können Daten über mehrere Regionen mithilfe einer Aurora globalen Datenbank replizieren. Details hierzu finden Sie unter Hohe Verfügbarkeit über AWS -Regionen hinweg mit globalen Aurora-Datenbanken.
  - Sie können ein Aurora-Lesereplikat eines Aurora MySQL-DB-Clusters in einer anderen - AWS Region erstellen, indem Sie die MySQL-Binlog-Replikation (Binärprotokoll) verwenden. Jeder Cluster kann über bis zu fünf auf diese Weise erstellte Lesereplikate verfügen, die sich jeweils in einer anderen Region befinden.

- Zwei Aurora-MySQL-DB Cluster in der gleichen Region, indem Sie mit dem MySQL-Binärprotokoll (binlog) eine Replikation einrichten.
- Eine RDS-for-MySQL-DB-Instance als Datenquelle und ein Aurora-MySQL-DB-Cluster, indem Sie ein Aurora-Lesereplikat einer RDS-for-MySQL-DB-Instance erstellen. Üblicherweise verwenden Sie diese Methode eher bei Migrationsvorgängen nach Aurora MySQL als für die fortlaufende Replikation.

Weitere Informationen zur Replikation mit Aurora MySQL finden Sie unter Replikation mit Amazon Aurora My SQL.

Replikation mit Aurora PostgreSQL

Zusätzlich zu Aurora-Replicas haben Sie die folgenden Möglichkeiten für Replikationen mit Aurora PostgreSQL:

- Ein primärer Aurora-DB-Cluster in einer Region und bis zu fünf schreibgeschützte sekundäre DB-Cluster in verschiedenen Regionen unter Verwendung einer globalen Aurora-Datenbank. Aurora PostgreSQL unterstützt keine regionsübergreifenden Aurora-Replikate. Sie können jedoch die globale Aurora-Datenbank verwenden, um die Lesefunktionen Ihres DB-Clusters von Aurora PostgreSQL auf mehr als eine AWS Region zu skalieren und die Verfügbarkeitsziele zu erreichen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Global Databases.
- Zwei Aurora-PostgreSQL-DB-Cluster in derselben Region, indem die logische Replikationsfunktion von PostgreSQL verwendet wird.
- Eine RDS-for-PostgreSQL-DB-Instance als Datenquelle und ein Aurora-PostgreSQL-DB-Cluster, indem ein Aurora-Lesereplikat einer RDS-for-PostgreSQL-DB-Instance erstellt wird. Üblicherweise verwenden Sie diese Methode eher bei Migrationsvorgängen nach Aurora PostgreSQL als für die fortlaufende Replikation.

Weitere Informationen zur Replikation mit Aurora PostgreSQL finden Sie unter Replikation mit Amazon Aurora PostgreSQL.

Abrechnung von DB-Instances für Aurora

Von Amazon RDS in einem Aurora-Cluster bereitgestellte Instances werden basierend auf den folgenden Komponenten abgerechnet:

- DB-Instance-Stunden (pro Stunde): Basierend auf der DB-Instance-Klasse der DB-Instance (z. B. db.t2.small oder db.m4.large). Die Preise werden auf Stundenbasis aufgeführt, aber Rechnungen werden jetzt auf die Sekunde genau kalkuliert und zeigen die Zeiten im Dezimalformat an. Die RDS-Nutzung wird pro Sekunde berechnet, wobei mindestens für 10 Minuten zu zahlen ist. Weitere Informationen finden Sie unter Aurora DB-Instance-Klassen.
- Speicher (pro GiB pro Monat: Die Speicherkapazität, die Sie für die DB-Instance bereitstellen lassen. Bei einer Skalierung Ihrer zur Verfügung gestellten Speicherkapazität im laufenden Monat werden die Gebühren entsprechend anteilig erfasst. Weitere Informationen finden Sie unter Amazon Aurora-Speicher und -Zuverlässigkeit.
- Ein-/Ausgabe (I/O)-Anforderungen (pro 1 Mio. Anfragen) – Gesamtzahl der Speicher-I/O-Anforderungen, die Sie in einem Abrechnungszeitraum ausgeführt haben, nur für die DB-Clusterkonfiguration von Aurora Standard.

  Weitere Informationen zur I/O-Abrechnung von Amazon Aurora finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora.
- Backup-Speicher (pro GiB pro Monat) – Ein Backup-Speicher ist Speicher, der automatisierten Datenbanksicherungen und allen aktiven Datenbank-Snapshots zugeordnet ist, die Sie erstellt haben. Wenn Sie die Aufbewahrungszeit Ihrer Backups erhöhen oder zusätzliche Datenbank-Snapshots erstellen, belegt Ihre Datenbank dementsprechend mehr Backup-Speicher. Die sekundengenaue Abrechnung gilt nicht für den Backup-Speicher (gemessen in GB/Monat).

  Weitere Informationen finden Sie unter Sichern und Wiederherstellen eines Amazon-Aurora-DB-Clusters.
- Datenübertragung (pro GB) Datenübertragung in und aus Ihrer DB-Instance vom oder zum Internet und von oder zu anderen AWS-Regionen.

Amazon RDS bietet die folgenden Kaufoptionen, um Ihnen die Möglichkeit zu bieten, Ihre Kosten basierend auf Ihren Anforderungen zu optimieren.

- On-Demand instances (On-Demand-Instances) – Sie bezahlen stundenweise für DB-Instance-Stunden, die Sie nutzen. Die Preise werden auf Stundenbasis aufgeführt, aber Rechnungen werden jetzt auf die Sekunde genau kalkuliert und zeigen die Zeiten im Dezimalformat an. Die RDS-Nutzung wird jetzt pro Sekunde berechnet, wobei mindestens für 10 Minuten zu zahlen ist.
- Reserved instances (Reserved Instances) – Reservieren Sie eine DB-Instance für einen Zeitraum von einem oder drei Jahren und erhalten Sie einen im Vergleich zu den Preisen für eine On-Demand-DB-Instance erheblichen Rabatt. Durch die Nutzung von Reserved Instances können Sie

mehrere Instances innerhalb einer Stunde in Betrieb nehmen, starten, löschen oder beenden und die Reserved Instance-Rabatte für alle Instances erhalten.

- Aurora Serverless v2 – Aurora Serverless v2 bietet On-Demand-Kapazität, bei der die Abrechnungseinheit Aurora Capacity Unit (ACU)-Stunden anstelle von DB-Instance-Stunden ist. Die Aurora Serverless v2-Kapazität steigt und sinkt in einem von Ihnen angegebenen Bereich, abhängig von der Last Ihrer Datenbank. Sie können einen Cluster konfigurieren, dessen gesamte Kapazität Aurora Serverless v2 ist. Sie können auch ein Kombination aus Aurora Serverless v2 und On-Demand oder reservierten bereitgestellten Instances konfigurieren. Weitere Informationen zur Funktionsweise von Aurora Serverless v2-ACUs finden Sie unter Funktionsweise von Aurora Serverless v2.

Informationen zur Preisgestaltung von Aurora finden Sie in der Aurora-Preisliste.

Themen

- On-Demand-DB-Instances für Aurora
- Reservierte DB-Instances für Aurora

On-Demand-DB-Instances für Aurora

Amazon-RDS-On-Demand-DB-Instances werden basierend auf der Klasse der DB-Instance abgerechnet (z. B. db.t3.small oder db.m5.large). Informationen zu Amazon RDS-Preisen finden Sie auf der Amazon RDS-Produktseite.

Die Abrechnung für eine DB-Instance beginnt, sobald die DB-Instance verfügbar ist. Die Preise werden auf Stundenbasis aufgeführt, aber Rechnungen werden jetzt auf die Sekunde genau kalkuliert und zeigen die Zeiten im Dezimalformat an. Die Amazon-RDS-Nutzung wird pro Sekunde berechnet, wobei mindestens für 10 Minuten zu zahlen ist. Im Falle einer abrechenbaren Konfigurationsänderung, wie Skalierung der Rechen- oder Speicherkapazität, wird Ihnen eine Mindestdauer von 10 Minuten in Rechnung gestellt. Die Abrechnung wird solange fortgesetzt, bis die DB-Instance beendet wird, was beim Löschen der DB-Instance oder beim Ausfall der DB-Instance passiert.

Wenn Sie nicht mehr mit Gebühren für Ihre DB-Instance belastet werden wollen, müssen Sie diese stoppen oder löschen, um zu vermeiden, dass zusätzliche Stunden der DB-Instance in Rechnung gestellt werden. Weitere Informationen über die Zustände der DB-Instance, die Ihnen in Rechnung gestellt werden, finden Sie unter Anzeigen von DB-Instance-Status in einem Aurora-Cluster.

Angehaltene DB-Instances

Während Ihre DB-Instance angehalten wird, werden nur Gebühren für bereitgestellten Speicher in Rechnung gestellt, einschließlich bereitgestellter IOPS. Es werden Ihnen auch Gebühren für den Backup-Speicher berechnet, einschließlich des Speichers für manuelle Snapshots und automatische Backups innerhalb des von Ihnen festgelegten Aufbewahrungsfensters. Für DB-Instance-Stunden werden Ihnen keine Gebühren in Rechnung gestellt.

Multi-AZ-DB-Instances

Wenn Sie angeben, dass Ihre DB-Instance eine Multi-AZ-Bereitstellung sein soll, werden Ihnen die Multi-AZ-Preise in Rechnung gestellt, wie auf der Seite Amazon RDS-Preise aufgelistet..

Reservierte DB-Instances für Aurora

Mit Reserved DB-Instances können Sie eine DB-Instance für eine ein- oder dreijährige Laufzeit reservieren. Reservierte DB-Instances bieten Ihnen einen deutlichen Rabatt im Vergleich zu den bedarfsorientierten Preisen für DB-Instances. Bei reservierten DB-Instances handelt es sich nicht um physische Instances, sondern um einen Fakturierungsrabatt für die Nutzung gewisser On-Demand-Instances in Ihrem Konto. Rabatte für Reserved DB-Instances sind an den Instance-Typ und die AWS-Region gebunden.

Der allgemeine Prozess für das Arbeiten mit reservierten DB-Instances ist: Zuerst Informationen über verfügbare reservierte DB-Instance-Angebote erhalten, dann ein reserviertes DB-Instance-Angebot kaufen und schließlich Informationen über Ihre vorhandenen reservierten DB-Instances erhalten.

Übersicht über Reservierte DB-Instances

Wenn Sie eine Reserved DB-Instance in Amazon RDS kaufen, erwerben Sie eine Verpflichtung, eine reduzierte Rate für einen bestimmten DB-Instance-Typ für die Dauer der Reserved DB-Instance zu erhalten. Um eine Amazon RDS Reserved DB-Instance zu verwenden, erstellen Sie eine neue DB-Instance, genau wie bei einer On-Demand-Instance.

Die neu erstellte DB-Instance muss mit den Spezifikationen der Reserved DB-Instance in folgenden Punkten übereinstimmen:

- AWS-Region
- DB-Engine (Die Versionsnummer der DB-Engine muss nicht übereinstimmen.)
- DB-Instance-Typ

Wenn die Spezifikationen der neuen DB-Instance mit einer vorhandenen Reserved DB-Instance für Ihr Konto übereinstimmen, wird Ihnen der angebotene diskontierte Preis für die Reserved DB-Instance in Rechnung gestellt. Andernfalls wird der DB-Instance eine On-Demand-Rate berechnet.

Sie können eine DB-Instance, die Sie als Reserved-DB-Instance verwenden, ändern. Wenn die Änderung innerhalb der Spezifikationen der reservierten DB-Instance liegt, gilt der diskontierte Preis teilweise oder vollständig für die geänderte DB-Instance. Wenn die Änderung außerhalb der Spezifikationen liegt, z. B. die Änderung der Instance-Klasse, gilt der diskontierte Preis nicht mehr. Weitere Informationen finden Sie unter Größenflexible Reservierte DB-Instances.

Themen

- Angebotstypen
- Flexibilität bezüglich der Konfiguration des Aurora-DB-Clusters
- Größenflexible Reservierte DB-Instances
- Abrechnungsbeispiele für Reserved DB-Instances von Aurora
- Löschen einer Reserved DB-Instance

Weitere Informationen zu reservierten DB-Instances samt Preisen finden Sie unter Amazon RDS Reserved Instances.

Angebotstypen

Reservierte DB-Instances sind in drei Varianten verfügbar – Keine Vorauszahlung, Teilweise Vorauszahlung und Vollständige Vorauszahlung. Auf diese Weise können Sie die Amazon RDS-Kosten auf der Basis der erwarteten Nutzung optimieren.

Keine Vorabzahlung

Diese Option ermöglicht den Zugriff auf eine reservierte DB-Instance, ohne dass eine Vorauszahlung erforderlich ist. Ihre reservierte DB-Instance ohne Vorauszahlung rechnet für jede Stunde innerhalb der Laufzeit einen ermäßigten Stundensatz ab, unabhängig von der Nutzung, und es ist keine Vorauszahlung erforderlich. Diese Option ist lediglich als Reservierung für die Dauer eines Jahres verfügbar.

Teilweise Vorauszahlung

Diese Option beruht darauf, dass ein Teil der reservierten DB-Instance im Voraus bezahlt wird. Die innerhalb der Laufzeit verbleibenden Stunden werden unabhängig von der Nutzung zu einem vergünstigten Stundensatz berechnet. Diese Option ersetzt die vorherige Heavy Utilization-Option.

Komplette Vorauszahlung

Die vollständige Zahlung erfolgt zu Beginn der Laufzeit, unabhängig von der Nutzungsdauer und ohne weitere Kosten innerhalb der Restlaufzeit.

Wenn Sie die konsolidierte Fakturierung nutzen, werden alle Konten in der Organisation wie ein einziges Konto behandelt. Das bedeutet, dass alle Konten in der Organisation den stündlichen Kostenvorteil für Reserved DB-Instances erhalten können, die durch ein anderes Konto erworben wurden. Weitere Informationen zur konsolidierten Fakturierung finden Sie unter Reservierte Amazon-RDS-DB-Instances im Benutzerhandbuch AWS -Fakturierungs- und Kostenverwaltung.

Flexibilität bezüglich der Konfiguration des Aurora-DB-Clusters

Sie können Reserved DB-Instances von Aurora mit beiden DB-Cluster-Konfigurationen verwenden:

- Aurora I/O-Optimized – Sie zahlen nur für die Nutzung und Speicherung Ihrer DB-Cluster, ohne zusätzliche Gebühren für Lese- und Schreib-I/O-Operationen.
- Aurora Standard – Neben der Auslastung und Speicherung Ihrer DB-Cluster zahlen Sie auch einen Standardsatz pro 1 Million Anfragen für I/O-Operationen.

Aurora berücksichtigt automatisch den Preisunterschied zwischen diesen Konfigurationen. Aurora I/O-Optimizedverbraucht 30 % mehr normalisierte Einheiten pro Stunde als Aurora Standard.

Weitere Informationen zu den Speicherkonfigurationen von Aurora-Clustern finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora. Weitere Informationen zu den Preisen für Speicherkonfigurationen von Aurora-Clustern finden Sie unter Amazon Aurora: Preise.

Größenflexible Reservierte DB-Instances

Beim Kauf einer Reserved DB-Instance wird unter anderem die Instance-Klasse angegeben, z. B. db.r5.large. Weitere Informationen zu DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.

Wenn Sie eine DB-Instance haben und diese auf größere Kapazität skalieren müssen, wird Ihre Reserved DB-Instance automatisch auf Ihre skalierte DB-Instance angewendet. Das heißt, Ihre Reserved DB-Instances werden automatisch auf alle DB-Instance-Klassengrößen angewendet. Größenflexible reservierte DB-Instances sind für DB-Instances mit derselben AWS-Region DB-Engine verfügbar. Größenflexible Reserved DB-Instances können nur innerhalb ihres Instance-Klassentyps skalieren. Eine Reserved DB-Instance für das Modell db.r5.large kann beispielsweise auf das Modell db.r5.xlarge angewendet werden, nicht aber auf db.r6g.large, da es sich bei db.r5 und db.r6g um unterschiedliche Instance-Klassentypen handelt.

Vorteile von Reserved DB-Instances gelten auch für Multi-AZ- und Single-AZ-Konfigurationen. Flexibilität bedeutet, dass Sie zwischen Konfigurationen innerhalb desselben DB-Instance-Klassentyps frei wechseln können. Sie können beispielsweise von einer Single-AZ-Bereitstellung, die auf einer großen DB-Instance (vier normalisierte Einheiten pro Stunde) ausgeführt wird, zu einer Multi-AZ-Bereitstellung wechseln, die auf zwei mittleren DB-Instances ausgeführt wird (2+2 = 4 normalisierte Einheiten pro Stunde).

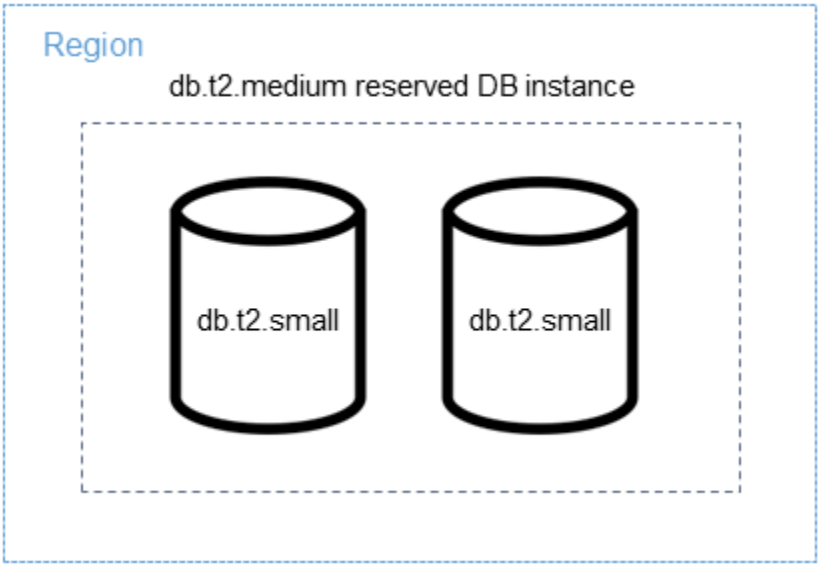
Größenflexible reservierte DB-Instances sind für die folgenden Aurora-Datenbank-Engines verfügbar:

- Aurora MySQL
- Aurora PostgreSQL

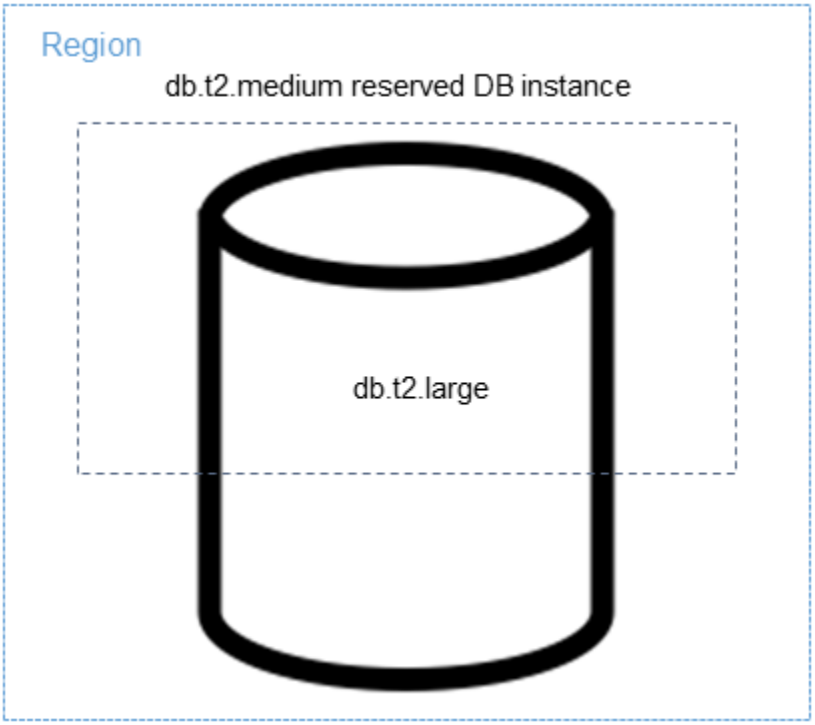
Sie können die Nutzung für verschiedene Reserved DB-Instance-Größen vergleichen, indem Sie normalisierte Einheiten pro Stunde verwenden. Beispielsweise entspricht eine Nutzungseinheit auf zwei db.r3.large DB-Instances acht normalisierten Nutzungseinheiten pro Stunde auf einem db.r3.small. Die folgende Tabelle zeigt die Anzahl von normalisierten Einheiten pro Stunde für jede DB-Instance-Größe.

Instance-Größe	Normalisierte Einheiten pro Stunde für eine DB-Instance, Aurora Standard	Normalisierte Einheiten pro Stunde für eine DB-Instance, Aurora I/O-Optimized	Normalisierte Einheiten pro Stunde für drei DB-Instances (Writer und zwei Reader), Aurora Standard	Normalisierte Einheiten pro Stunde für drei DB-Instances (Writer und zwei Reader), Aurora I/O-Optimized
small	1	1.3	3	3.9
Medium	2	2.6	6	7.8
large	4	5.2	12	15,6
xlarge	8	10.4	24	31,2
2xlarge	16	20,8	48	62,4
4xlarge	32	41,6	96	124,8
8xlarge	64	83,2	192	249,6
12xlarge	96	124,8	288	374,4
16xlarge	128	166,4	384	499,2
24xlarge	192	249,6	576	748,8
32xlarge	256	332,8	768	998,4

Angenommen, Sie kaufen eine Reserved `db.t2.medium`-DB-Instance und haben zwei `db.t2.small`-DB-Instances in Ihrem Konto, die in der gleichen AWS-Region ausgeführt werden. In diesem Fall wird der Rabatt in vollem Umfang auf beide Instances angewendet.



Wenn in Ihrem Konto eine `db.t2.large` Instance ausgeführt wird AWS-Region, wird der Abrechnungsvorteil alternativ auf 50 Prozent der Nutzung der DB-Instance angerechnet.



> **Note**
>
> Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter DB-Instance-Klassenarten.

Abrechnungsbeispiele für Reserved DB-Instances von Aurora

Die folgenden Beispiele veranschaulichen die Preise für Reserved DB-Instances für Aurora-DB-Cluster, die sowohl die DB-Cluster-Konfiguration Aurora Standard als auch die Konfiguration Aurora I/O-Optimized verwenden.

Beispiel mit Aurora Standard

Der Preis für eine Reserved DB-Instance bietet keinen Rabatt für die Kosten in Verbindung mit Speicher, Backups und I/O. Das folgende Beispiel veranschaulicht die Gesamtkosten pro Monat für eine Reserved DB-Instance:

- Eine Reserved Single-AZ-DB-Instance von Aurora MySQL der Klasse db.r5.large in der Region USA Ost (Nord-Virginia) kostet 0,19 USD pro Stunde oder 138,70 USD pro Monat.
- Aurora-Speicher zu einem Preis von 0,10 USD pro GiB pro Monat (ungefähr 45,60 USD pro Monat in diesem Beispiel).
- Aurora-I/O zu einem Preis von 0,20 USD pro 1 Millionen Anforderungen (ungefähr 20 USD pro Monat in diesem Beispiel).
- Aurora-Sicherungsspeicher zu einem Preis von 0,021 USD pro GiB pro Monat (ungefähr 30 USD pro Monat in diesem Beispiel).

Wenn Sie die Kosten all dieser Optionen (138,70 USD + 45,60 USD + 20 USD + 30 USD) mit der Reserved DB-Instance addieren, liegen die monatlichen Gesamtkosten bei 234,30 USD.

Wenn Sie sich statt für eine Reserved DB-Instance für eine On-Demand-DB-Instance entscheiden, kostet eine Single-AZ-Instance der Klasse db.r5.large von Aurora MySQL in der Region USA Ost (Nord-Virginia) 0,29 USD pro Stunde oder 217,50 USD pro Monat. Wenn Sie die Kosten all dieser Optionen (217,50 USD + 45,60 USD + 20 USD + 30 USD) mit der On-Demand-DB-Instance addieren, liegen die monatlichen Gesamtkosten bei 313,10 USD. Sie sparen fast 79 USD pro Monat, indem Sie die reservierte DB-Instance verwenden.

Beispiel für die Verwendung eines Aurora Standard DB-Clusters mit zwei Reader-Instances

Um Reserved Instances für Aurora-DB-Cluster zu verwenden, kaufen Sie einfach eine Reserved Instance für jede DB-Instance im Cluster.

Gehen wir noch einmal auf das erste Beispiel ein und nehmen an, Sie verfügen über einen DB-Cluster von Aurora MySQL mit einer Writer-DB-Instance und zwei Aurora Replicas, also insgesamt drei DB-Instances im Cluster. Für die beiden Aurora Replicas fallen keine zusätzlichen Speicher- oder Backup-Kosten an. Wenn Sie drei Reserved DB-Instances von Aurora MySQL der Klasse db.r5.large kaufen, belaufen sich die Kosten auf 234,30 USD (für die Writer-DB-Instance) + 2 * (138,70 USD + 20 USD I/O pro Aurora Replica), was insgesamt 551,70 USD pro Monat entspricht.

Die entsprechenden On-Demand-Kosten für einen DB-Cluster von Aurora MySQL mit einer Writer-DB-Instance und zwei Aurora Replicas betragen 313,10 USD + 2 * (217,50 USD + 20 USD I/O pro Instance), also insgesamt 788,10 USD pro Monat. Sie sparen fast 236,40 USD pro Monat, wenn Sie die Reserved DB-Instances verwenden.

Beispiel mit Aurora I/O-Optimized

Sie können Ihre vorhandenen Aurora Standard Reserved DB-Instances mit Aurora I/O-Optimized wiederverwenden. Um die Vorteile Ihrer Reserved Instance-Rabatte mit Aurora I/O-Optimized in vollem Umfang nutzen zu können, können Sie 30 % zusätzliche Reserved Instances kaufen, die Ihren aktuellen Reserved Instances ähneln.

Die folgende Tabelle zeigt Beispiele dafür, wie Sie die zusätzlichen Reserved Instances abschätzen können, wenn Sie Aurora I/O-Optimized verwenden. Wenn es sich bei den erforderlichen Reserved Instances um einen Bruchteil handelt, können Sie die Größenflexibilität nutzen, die Reserved Instances bieten, um auf eine ganze Zahl zu kommen. In diesen Beispielen bezieht sich „aktuell“ auf die Aurora Standard Reserved Instances, über die Sie jetzt verfügen. Zusätzliche Reserved Instances sind die Anzahl der Aurora Standard Reserved Instances, die Sie kaufen müssen, um Ihre aktuellen Reserved Instance-Rabatte bei Verwendung von Aurora I/O-Optimized beizubehalten.

DB-Instance-Klasse	Aktuelle Aurora Standard Reserved Instances	Reserved Instances, die für Aurora I/O-Optimized erforderlich sind	Zusätzlich erforderliche Reserved Instances	Zusätzlich erforderliche Reserved Instances bei Nutzung der Größenflexibilität
db.r6g.large	10	10 * 1,3 = 13	3 * db.r6g.large	3 * db.r6g.large
db.r6g.4xlarge	20	20 * 1,3 = 26	6 * db.r6g.4x large	6 * db.r6g.4x large
db.r6g.12xlarge	5	5 * 1,3 = 6,5	1,5 * db.r6g.12 xlarge	db.r6g.12xlarge, r6g.4xlarge und r6g.2xlarge jeweils einmal (0,5 * db.r6g.12 xlarge = 1 * db.r6g.4xlarge + 1 * db.r6g.2x large)
db.r6i.24xlarge	15	15 * 1,3 = 19,5	4,5 * db.r6i.24 xlarge	4 * db.r6i.24 xlarge + 1 * db.r6i.12xlarge (0,5 * db.r6i.24 xlarge = 1 * db.r6i.12xlarge)

Beispiel für die Verwendung eines Aurora I/O-Optimized DB-Clusters mit zwei Reader-Instances

Sie verfügen über einen DB-Cluster von Aurora MySQL mit einer Writer-DB-Instance und zwei Aurora Replicas, also insgesamt drei DB-Instances im Cluster. Diese verwenden die DB-Cluster-Konfiguration Aurora I/O-Optimized. Um Reserved DB-Instances für diesen Cluster zu verwenden, müssten Sie vier Reserved DB-Instances derselben DB-Instance-Klasse kaufen. Drei DB-Instances verbrauchen mit Aurora I/O-Optimized 3,9 normalisierte Einheiten pro Stunde, verglichen mit 3

normalisierten Einheiten pro Stunde für drei DB-Instances mit Aurora Standard. Sie sparen jedoch die monatlichen I/O-Kosten für jede DB-Instance.

> **Note**
>
> Die Preise in diesem Beispiel sind Beispiele und entsprechen möglicherweise nicht den tatsächlichen Preisen. Informationen zur Preisgestaltung von Aurora finden Sie unter Aurora-Preise.

Löschen einer Reserved DB-Instance

In den Bedingungen für eine Reserved DB-Instance ist eine einjährige oder dreijährige Verpflichtung enthalten. Sie können eine Reserved DB-Instance nicht stornieren. Sie können jedoch eine DB-Instance löschen, die durch einen Rabatt für eine Reserved DB-Instance abgedeckt ist. Der Vorgang zum Löschen einer DB-Instance, für die ein Rabatt für eine Reserved DB-Instance gilt, ist der gleiche wie für jede andere DB-Instance.

Die Vorabkosten werden Ihnen in Rechnung gestellt, unabhängig davon, ob Sie die Ressourcen nutzen.

Wenn Sie eine DB-Instance löschen, die durch einen Rabatt für eine Reserved DB-Instance gedeckt ist, können Sie eine andere DB-Instance mit kompatiblen Spezifikationen starten und den ermäßigten Preis während der Reservierungslaufzeit (ein Jahr oder drei Jahre) erhalten. In diesem Fall erhalten Sie den Rabatt während des Reservierungszeitraums (ein Jahr oder drei Jahre).

Arbeiten mit reservierten DB-Instances

Sie können die AWS Management Console, und die RDS-API verwenden AWS CLI, um mit reservierten DB-Instances zu arbeiten.

Konsole

Sie können die verwenden AWS Management Console , um mit reservierten DB-Instances zu arbeiten, wie in den folgenden Verfahren gezeigt.

Preise und Informationen zu verfügbaren Angeboten für reservierte DB-Instances erhalten

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Reserved instances (Reservierte Instances) aus.
3. Klicken Sie auf Reserved DB-Instance kaufen.
4. Um die Produktbeschreibung einzusehen, wählen Sie die DB-Engine und den Lizenztyp aus.
5. Wählen Sie für DB-Instance-Klasse die DB-Instance-Klasse aus.
6. Wählen Sie für Bereitstellungsoption aus, ob Sie eine Single-AZ- oder eine Multi-AZ-Bereitstellung der DB-Instance wünschen.

> **Note**
>
> Bei Reserved Instances von Amazon Aurora ist die Bereitstellungsoption grundsätzlich auf Single-AZ-DB-Instance festgelegt. Wenn Sie jedoch einen Aurora-DB-Cluster erstellen, lautet die Standardbereitstellungsoption Ein Aurora-Replikat oder einen Reader in einer anderen AZ erstellen (Multi-AZ).
> Sie müssen eine Reserved DB-Instance für jede Instance erwerben, die Sie verwenden möchten, einschließlich Aurora Replicas. Daher müssen Sie für Multi-AZ-Bereitstellungen in Aurora zusätzliche reservierte DB-Instances erwerben.

7. Für Laufzeit wählen Sie die Zeitspanne aus, für welche die DB-Instance reserviert werden soll.
8. Wählen Sie für Angebotstyp den Angebotstyp aus.

   Nachdem Sie die Angebotsart ausgewählt haben, werden Ihnen die Preisinformationen angezeigt.

> **Important**
>
> Klicken Sie auf Abbrechen, um den Kaufvorgang für die Reserved DB-Instance abzubrechen und Kosten zu vermeiden.

Nachdem Sie Informationen über die verfügbaren reservierten DB-Instance-Angebote erhalten haben, können Sie diese Informationen verwenden, um ein Angebot zu erwerben, wie in der folgenden Vorgehensweise gezeigt.

Kauf einer reservierten DB-Instance

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Reserved instances (Reservierte Instances) aus.
3. Klicken Sie auf Reserved DB-Instance kaufen.
4. Um die Produktbeschreibung einzusehen, wählen Sie die DB-Engine und den Lizenztyp aus.
5. Wählen Sie für DB-Instance-Klasse die DB-Instance-Klasse aus.
6. Wählen Sie für Multi-AZ-Bereitstellung aus, ob Sie eine Single-AZ- oder eine Multi-AZ-Bereitstellung der DB-Instance wünschen.

   > **Note**
   >
   > Bei Reserved Instances von Amazon Aurora ist die Bereitstellungsoption grundsätzlich auf Single-AZ-DB-Instance festgelegt. Wenn Sie einen DB-Cluster von Amazon Aurora aus Ihrer Reserved DB-Instance erstellen, ist der DB-Cluster automatisch als Multi-AZ eingerichtet. Sie müssen eine Reserved DB-Instance für jede DB-Instance erwerben, die Sie verwenden möchten, einschließlich Aurora Replicas.

7. Für die Auswahl des Laufzeit wählen Sie die Zeitspanne aus, für welche die DB-Instance reserviert werden soll.
8. Wählen Sie für Angebotstyp den Angebotstyp aus.

   Nachdem Sie die Angebotsart ausgewählt haben, werden Ihnen die Preisinformationen angezeigt.
9. (Optional) Sie können den Reserved DB-Instances, die Sie kaufen, Ihre eigene Kennung zuweisen, um die Übersicht zu behalten. Geben Sie unter Reservierte ID eine Kennzeichnung für Ihre reservierte DB-Instance ein.
10. Wählen Sie Absenden aus.

    Ihre Reserved DB-Instance wird gekauft und dann in der Liste Reserved Instances angezeigt.

Nachdem Sie reservierte DB-Instances gekauft haben, erhalten Sie Informationen über Ihre reservierten DB-Instances, wie in der folgenden Vorgehensweise gezeigt.

Um Informationen über reservierte DB-Instances für Ihr AWS Konto zu erhalten

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Bereich Navigation die Option Reserved Instances (Reservierte Instances) aus.

Es erscheinen die reservierten DB-Instances für Ihr Konto. Um detaillierte Informationen zu einer bestimmten Reserved DB-Instance anzuzeigen, wählen Sie diese in der Liste aus. Sie können dann detaillierte Informationen über diese Instance im Detailbereich am unteren Rand der Konsole anzeigen.

AWS CLI

Sie können die verwenden AWS CLI , um mit reservierten DB-Instances zu arbeiten, wie in den folgenden Beispielen gezeigt.

Example Erhalten von verfügbaren Reserved DB-Instance-Angeboten

Rufen Sie den AWS CLI Befehl auf, um Informationen über verfügbare Angebote für reservierte DB-Instances zu erhalten `describe-reserved-db-instances-offerings`.

```
aws rds describe-reserved-db-instances-offerings
```

Diese Aktion führt zu folgender oder einer ähnlichen Ausgabe:

```
OFFERING  OfferingId                            Class         Multi-AZ  Duration  Fixed
 Price  Usage Price  Description  Offering Type
OFFERING  438012d3-4052-4cc7-b2e3-8d3372e0e706  db.r3.large   y         1y
 1820.00 USD  0.368 USD    mysql        Partial  Upfront
OFFERING  649fd0c8-cf6d-47a0-bfa6-060f8e75e95f  db.r3.small   n         1y
 227.50 USD  0.046 USD    mysql        Partial  Upfront
OFFERING  123456cd-ab1c-47a0-bfa6-12345667232f  db.r3.small   n         1y
 162.00 USD   0.00 USD    mysql        All      Upfront
    Recurring Charges:   Amount  Currency  Frequency
    Recurring Charges:   0.123   USD       Hourly
OFFERING  123456cd-ab1c-37a0-bfa6-12345667232d  db.r3.large   y         1y
 700.00 USD   0.00 USD    mysql        All      Upfront
    Recurring Charges:   Amount  Currency  Frequency
    Recurring Charges:   1.25    USD       Hourly
OFFERING  123456cd-ab1c-17d0-bfa6-12345667234e  db.r3.xlarge  n         1y
 4242.00 USD   2.42 USD    mysql        No       Upfront
```

Nachdem Sie Informationen über die verfügbaren reservierten DB-Instance-Angebote erhalten haben, können Sie diese Informationen verwenden, um ein Angebot zu erwerben.

Um eine reservierte DB-Instance zu erwerben, verwenden Sie den AWS CLI Befehl purchase-reserved-db-instances-offeringmit den folgenden Parametern:

- `--reserved-db-instances-offering-id` – Die ID des Angebots, das Sie erwerben möchten Siehe das vorhergehende Beispiel, um die Angebots-ID zu erhalten.
- `--reserved-db-instance-id` – Sie können den Reserved DB-Instances, die Sie kaufen, Ihre eigene Kennung zuweisen, um die Übersicht zu behalten.

Example Kauf einer Reserved DB-Instance

Im folgenden Beispiel wird das reservierte DB-Instance-Angebot mit der ID *649fd0c8-cf6d-47a0-bfa6-060f8e75e95f gekauft und der Identifier von zugewiesen*. *MyReservation*

LinuxmacOSUnixFür, oder:

```
aws rds purchase-reserved-db-instances-offering \
    --reserved-db-instances-offering-id 649fd0c8-cf6d-47a0-bfa6-060f8e75e95f \
    --reserved-db-instance-id MyReservation
```

Windows:

```
aws rds purchase-reserved-db-instances-offering ^
    --reserved-db-instances-offering-id 649fd0c8-cf6d-47a0-bfa6-060f8e75e95f ^
    --reserved-db-instance-id MyReservation
```

Daraufhin erhalten Sie ein Ergebnis, das dem hier dargestellten entspricht:

```
RESERVATION  ReservationId      Class        Multi-AZ  Start Time
 Duration  Fixed Price  Usage Price  Count  State           Description  Offering Type
RESERVATION  MyReservation      db.r3.small  y         2011-12-19T00:30:23.247Z  1y
    455.00 USD   0.092 USD    1      payment-pending  mysql        Partial  Upfront
```

Nachdem Sie Reserved DB-Instances gekauft haben, erhalten Sie Informationen über Ihre Reserved DB-Instances.

Um Informationen über reservierte DB-Instances für Ihr AWS Konto zu erhalten, rufen Sie den AWS CLI Befehl auf describe-reserved-db-instances, wie im folgenden Beispiel gezeigt.

Example Erhalten von Reserved DB-Instances

```
aws rds describe-reserved-db-instances
```

Daraufhin erhalten Sie ein Ergebnis, das dem hier dargestellten entspricht:

```
RESERVATION  ReservationId     Class        Multi-AZ  Start Time
 Duration  Fixed Price  Usage Price  Count  State    Description  Offering Type
RESERVATION  MyReservation     db.r3.small  y         2011-12-09T23:37:44.720Z  1y
   455.00 USD   0.092 USD    1      retired  mysql        Partial  Upfront
```

RDS-API

Sie können die RDS-API verwenden, um mit Reserved DB-Instances zu arbeiten:

- Um Informationen zu verfügbaren Reserved DB-Instance-Angeboten zu erhalten, rufen Sie die Amazon RDS-API-Aktion auf `DescribeReservedDBInstancesOfferings`.
- Nachdem Sie Informationen über die verfügbaren reservierten DB-Instance-Angebote erhalten haben, können Sie diese Informationen verwenden, um ein Angebot zu erwerben. Rufen Sie dazu die RDS-API-Operation `PurchaseReservedDBInstancesOffering` mit den folgenden Parametern auf:
  - `--reserved-db-instances-offering-id` – Die ID des Angebots, das Sie erwerben möchten
  - `--reserved-db-instance-id` – Sie können den Reserved DB-Instances, die Sie kaufen, Ihre eigene Kennung zuweisen, um die Übersicht zu behalten.
- Nachdem Sie Reserved DB-Instances gekauft haben, erhalten Sie Informationen über Ihre Reserved DB-Instances. Rufen Sie die Aktion `DescribeReservedDBInstances`-RDS-API auf.

Abrechnung für Reserved DB-Instances

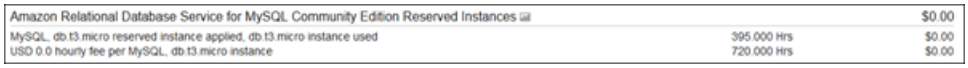
Sie können die Abrechnung für Ihre reservierten DB-Instances im Abrechnungs-Dashboard im AWS Management Console.

So zeigen Sie Reserved DB-Instance Abrechnung an

1. Melden Sie sich bei der an AWS Management Console.
2. Wählen Sie im Kontomenü oben rechts Abrechnungs-Dashboard aus.
3. Wählen Sie oben rechts im Dashboard Rechnungsdetails aus.

4. Erweitern Sie unter AWS -Servicegebühren den Dienst für relationale Datenbanken.
5. Erweitern Sie den AWS-Region Ort, an dem sich Ihre reservierten DB-Instances befinden, z. B. US West (Oregon).

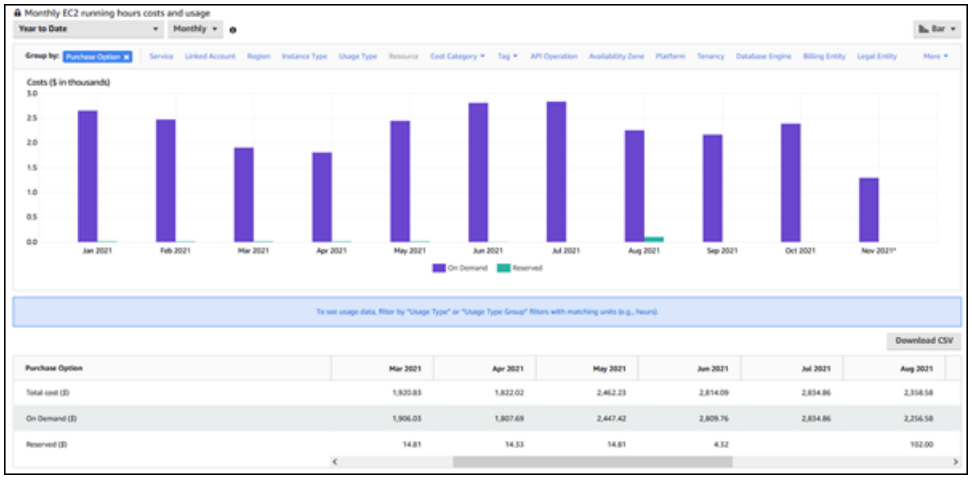
   Ihre reservierten DB-Instances und ihre stündlichen Gebühren für den aktuellen Monat werden unter Amazon Relational Database Service for ***Datenbank-Engine*** Reserved Instances angezeigt.

   Die reservierte DB-Instance in diesem Beispiel wurde „All Upfront“ gekauft, daher fallen keine Stundengebühren an.
6. Wählen Sie das Cost Explorer-Symbol (Balkendiagramm) neben der Überschrift Reserved Instances.

   Der Cost Explorer zeigt die monatlichen EC2-Betriebsstundenkosten und das Nutzungsdiagramm an.
7. Deaktivieren Sie den Filter Verwendungstyp-Gruppe rechts neben dem Diagramm.
8. Wählen Sie den Zeitraum und die Zeiteinheit aus, für die Sie die Nutzungskosten untersuchen möchten.

   Das folgende Beispiel zeigt die Nutzungskosten für On-Demand- und reservierte DB-Instances für das bisherige Jahr bis nach Monaten an.

   Die Kosten für reservierte DB-Instance von Januar bis Juni 2021 sind monatliche Gebühren für eine Partial-Upfront-Instance, während die Kosten im August 2021 eine einmalige Gebühr für eine All Upfront-Instance sind.

Der Rabatt der reservierten Instances für die Partial Upfront-Instance lief im Juni 2021 aus, die DB-Instance wurde jedoch nicht gelöscht. Nach dem Ablaufdatum wurde es einfach zum On-Demand-Tarif berechnet.

Einrichten Ihrer Umgebung für Amazon Aurora

Bevor Sie Amazon Aurora zum ersten Mal verwenden, führen Sie die folgenden Aufgaben aus.

Themen

Wenn Sie bereits über eine verfügen AWS-Konto, Ihre Aurora-Anforderungen kennen und lieber die Standardeinstellungen für IAM- und VPC-Sicherheitsgruppen verwenden möchten, fahren Sie mit fort. Erste Schritte mit Amazon Aurora

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Ermitteln der Anforderungen

Die Grundbausteine für Aurora sind DB-Cluster. Einem DB-Cluster können eine oder mehrere DB-Instances angehören. Ein DB-Cluster gibt eine Netzwerkadresse, den sogenannten Cluster-Endpunkt, an. Ihre Anwendungen verbinden sich immer dann mit dem vom DB-Cluster gezeigten Cluster-Endpunkt, wenn sie auf die Datenbanken zugreifen müssen, die in diesem DB-Cluster erstellt wurden. Die Informationen, die Sie beim Erstellen des DB-Clusters angeben, steuern Konfigurationselemente wie Arbeitsspeicher, Datenbank-Engine und -Version, Netzwerkkonfiguration, Sicherheit und Wartungszeiträume.

Bevor Sie einen DB-Cluster und eine Sicherheitsgruppe erstellen, müssen Sie Ihre DB-Cluster- und Netzwerkanforderungen kennen. Hier einige wichtige Dinge, die Sie berücksichtigen sollten:

- Ressourcenanforderungen – Welche Anforderungen haben Sie an den Arbeitsspeicher und den Prozessor für Ihre Anwendung oder Ihren Service? Sie verwenden diese Einstellungen, wenn Sie bestimmen, welche DB-Instance-Klasse Sie beim Erstellen Ihres DB-Clusters nutzen. Spezifikationen für alle verfügbaren DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.
- VPC, Subnetz und Sicherheitsgruppe– Ihr DB-Cluster befindet sich in einer Virtual Private Cloud (VPC). Um eine Verbindung zu einem DB-Cluster herzustellen, müssen Regeln für Sicherheitsgruppen konfiguriert werden. Die folgende Liste beschreibt die Regeln für jede VPC-Option:
  - Standard-VPC — Wenn Ihr AWS Konto über eine Standard-VPC in der AWS Region verfügt, ist diese VPC für die Unterstützung von DB-Clustern konfiguriert. Wenn Sie beim Erstellen des DB-Clusters die Standard-VPC angeben:
    - Sie müssen eine VPC-Sicherheitsgruppe anlegen, die Verbindungen von der Anwendung oder dem Service zum Aurora-DB-Cluster autorisiert. Verwenden Sie die Option Sicherheitsgruppe auf der VPC-Konsole oder AWS CLI um VPC-Sicherheitsgruppen zu erstellen. Weitere Informationen finden Sie unter Schritt 3: Erstellen einer VPC-Sicherheitsgruppe.
    - Sie müssen die Standard-DB-Subnetzgruppe angeben. Wenn dies der erste DB-Cluster ist, den Sie in der AWS Region erstellt haben, erstellt Amazon RDS bei der Erstellung des DB-Clusters die Standard-DB-Subnetzgruppe.
  - Benutzerdefinierte VPC – wenn Sie beim Erstellen eines DB-Clusters eine benutzerdefinierte VPC angeben möchten:
    - Sie müssen eine VPC-Sicherheitsgruppe anlegen, die Verbindungen von der Anwendung oder dem Service zum Aurora-DB-Cluster autorisiert. Verwenden Sie die Option Sicherheitsgruppe auf der VPC-Konsole oder AWS CLI um VPC-Sicherheitsgruppen zu erstellen. Weitere Informationen finden Sie unter Schritt 3: Erstellen einer VPC-Sicherheitsgruppe.
    - Die VPC muss bestimmte Anforderungen erfüllen, um DB-Cluster bereitzustellen, z. B. das Vorhandensein von zwei Subnetzen in jeweils einer separaten Availability Zone. Weitere Informationen finden Sie unter Amazon VPCs und Amazon Aurora.
    - Sie müssen eine DB-Subnetzgruppe angeben, die definiert, welche Subnetze in dieser VPC vom DB-Cluster genutzt werden können. Weitere Informationen erhalten Sie im Abschnitt "DB-Subnetzgruppen" unter Arbeiten mit einer DB-Cluster in einer VPC.

- Hohe Verfügbarkeit: Benötigen Sie Failover-Unterstützung? Bei Aurora erstellt eine Multi-AZ-Bereitstellung eine primäre Instance sowie Aurora-Replicas. Sie können die primäre Instance und Aurora-Replicas so konfigurieren, dass sie sich in verschiedenen Availability Zones befinden, um Failover-Support zu erhalten. Wir empfehlen Multi-AZ-Bereitstellungen, um die hohe Verfügbarkeit von Produktions-Workloads sicherzustellen. Für Entwicklungs- und Testzwecke reicht gewöhnlich eine Bereitstellung ohne Multi-AZ. Weitere Informationen finden Sie unter Hohe Verfügbarkeit für Amazon Aurora.
- IAM-Richtlinien: Verfügt Ihr AWS Konto über Richtlinien, die die für die Durchführung von Amazon RDS-Vorgängen erforderlichen Berechtigungen gewähren? Wenn Sie eine Verbindung AWS mit IAM-Anmeldeinformationen herstellen, muss Ihr IAM-Konto über IAM-Richtlinien verfügen, die die für die Durchführung von Amazon RDS-Vorgängen erforderlichen Berechtigungen gewähren. Weitere Informationen finden Sie unter Identity and Access Management für Amazon Aurora.
- Offene Ports: Welchen TCP/IP-Port fragt Ihre Datenbank ab? Die Firewalls einiger Unternehmen blockieren möglicherweise Verbindungen zum Standard-Port für Ihre Datenbank-Engine. Wenn die Firewall Ihres Unternehmens den Standardport blockiert, wählen Sie einen anderen Port für den neuen DB-Cluster aus. Nach dem Erstellen eines DB-Clusters, der einen angegebenen Port abfragt, können Sie diesen Port ändern, indem Sie den DB-Cluster modifizieren.
- AWS Region: In welcher AWS Region möchten Sie Ihre Datenbank haben? Indem sich die Datenbank nahe bei der Anwendung oder dem Webdienst befindet, könnten Netzwerklatenzen verringert werden. Weitere Informationen finden Sie unter Regionen und Availability Zones.

Sobald Ihnen die benötigten Informationen zur Erstellung der Sicherheitsgruppe und des DB-Clusters vorliegen, fahren Sie mit dem nächsten Schritt fort.

Ermöglichen des Zugriffs auf den DB-Cluster in der VPC durch Erstellen einer Sicherheitsgruppe

Ihr DB-Cluster wird in einer VPC erstellt. Sicherheitsgruppen bieten Zugriff auf den DB-Cluster in der VPC. Sie fungieren als Firewall für die zugeordneten DB-Cluster und steuern den ein- und ausgehenden Datenverkehr auf der Cluster-Ebene. DB-Cluster werden standardmäßig mit einer Firewall und einer Standard-Sicherheitsgruppe erstellt, die den Zugriff auf den DB-Cluster verhindert. Sie müssen daher einer Sicherheitsgruppe Regeln hinzufügen, die es Ihnen ermöglichen, eine Verbindung zu Ihrem DB-Cluster herzustellen. Verwenden Sie die Netzwerk- und Konfigurationsinformationen, die Sie im vorherigen Schritt festgelegt haben, um Regeln für den Zugriff auf Ihren DB-Cluster festzulegen.

Wenn beispielsweise eine Anwendung auf eine Datenbank in Ihrem DB-Cluster in einer VPC zugreifen soll, müssen Sie eine benutzerdefinierte TCP-Regel hinzufügen, die den Portbereich und IP-Adressen angibt, mit denen die Anwendung auf die Datenbank zugreift. Befindet sich eine Anwendung auf einer Amazon-EC2-Instance, können Sie die VPC-Sicherheitsgruppe verwenden, die Sie für die Amazon-EC2-Instance eingerichtet haben.

Sie können die Konnektivität zwischen einer Amazon-EC2-Instance und einem DB-Cluster konfigurieren, wenn Sie den DB-Cluster erstellen. Weitere Informationen finden Sie unter Automatische Netzwerkkonnektivität mit einer EC2-Instance konfigurieren.

> **Tip**
>
> Sie können die Netzwerkkonnektivität zwischen einer Amazon-EC2-Instance und einem DB-Cluster automatisch beim Erstellen des DB-Clusters einrichten. Weitere Informationen finden Sie unter Automatische Netzwerkkonnektivität mit einer EC2-Instance konfigurieren.

Weitere Informationen zum Erstellen einer VPC zur Verwendung mit Aurora finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4). Informationen zu gängigen Szenarien für den Zugriff auf eine DB-Instance finden Sie unter Szenarien für den Zugriff auf eine DB-Cluster in einer VPC.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Melden Sie sich bei der Amazon VPC-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/vpc.

   > **Note**
   >
   > Stellen Sie sicher, dass Sie sich in der VPC-Konsole befinden, nicht in der RDS-Konsole.

2. Wählen Sie in der oberen rechten Ecke von die AWS Region aus AWS Management Console, in der Sie Ihre VPC-Sicherheitsgruppe und Ihren DB-Cluster erstellen möchten. Die Liste der Amazon-VPC-Ressourcen für diese AWS -Region sollte zeigen, dass Sie über mindestens eine VPC und mehrere Subnetze verfügen. Wenn Sie dies nicht tun, haben Sie in dieser AWS Region keine Standard-VPC.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
4. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.

Die Seite Sicherheitsgruppe erstellen wird angezeigt.

5. Geben Sie im Feld Grundlegende Details den Namen der Sicherheitsgruppe und die Beschreibung ein. Wählen Sie unter VPC die VPC aus, in der Sie Ihren DB-Cluster erstellen möchten.
6. Wählen Sie in Eingehende Regeln die Option Regel hinzufügen.
   a. Wählen Sie für Type (Typ) die Option Custom TCP (Benutzerdefiniertes TCP) aus.
   b. Geben Sie für Portbereich den Portwert ein, der für Ihren DB-Cluster verwendet werden soll.
   c. Wählen Sie für Source (Quelle) den Namen einer Sicherheitsgruppe oder geben Sie den IP-Adressbereich (CIDR-Wert) ein, von dem aus Sie auf den DB-Cluster zugreifen. Wenn Sie Meine IP auswählen, ermöglicht dies den Zugriff auf den DB-Cluster von der in Ihrem Browser erkannten IP-Adresse.
7. Wenn Sie weitere IP-Adressen oder andere Portbereiche hinzufügen müssen, wählen Sie Regel hinzufügen und geben Sie die Informationen für die Regel ein.
8. (Optional) Fügen Sie inRegeln für ausgehenden Datenverkehr Regeln für ausgehenden Datenverkehr hinzu. Standardmäßig ist der gesamte ausgehende Datenverkehr zugelassen.
9. Wählen Sie Sicherheitsgruppe erstellen aus.

Sie können die soeben erstellte VPC-Sicherheitsgruppe als Sicherheitsgruppe beim Anlegen Ihres DB-Clusters verwenden.

> **Note**
>
> Wenn Sie eine Standard-VPC verwenden, wird eine Standard-Subnetzgruppe für Sie angelegt, die alle Subnetze der VPC umfasst. Wenn Sie einen DB-Cluster erstellen, können Sie die Standard-VPC auswählen und Standard für die DB-Subnetzgruppe verwenden.

Nachdem Sie die Setup-Anforderungen erfüllt haben, können Sie einen DB-Cluster mit Ihren Anforderungen und Ihrer Sicherheitsgruppe erstellen, indem Sie den Anweisungen in Erstellen eines Amazon Aurora-DB Clusters. Informationen zu den ersten Schritten beim Erstellen eines DB-Clusters, der eine bestimmte DB-Engine verwendet, finden Sie unter Erste Schritte mit Amazon Aurora.

Erste Schritte mit Amazon Aurora

In diesem Abschnitt finden Sie heraus, wie Sie mit Amazon RDS einen Aurora-DB-Cluster erstellen und eine Verbindung mit diesem herstellen.

Bei den folgenden Prozeduren handelt es sich um Tutorials, die die Grundlagen der ersten Schritte mit Aurora demonstrieren. In den späteren Abschnitten werden erweiterte Aurora-Konzepte und -Verfahren vorgestellt, z. B. die verschiedenen Endpunkte und die Skalierung von Aurora-Clustern.

> **Important**
>
> Sie müssen die Aufgaben im Abschnitt Einrichten Ihrer Umgebung für Amazon Aurora abschließen, um einen DB-Cluster erstellen oder eine Verbindung mit einer DB-Instance herstellen zu können.

Themen

- Erstellen und Verbinden mit einem DB-Cluster von Aurora MySQL
- Erstellen eines DB-Clusters von Aurora PostgreSQL und Herstellen einer Verbindung
- Tutorial: Erstellen eines Webservers und einer eines Amazon Aurora-DB-Clusters

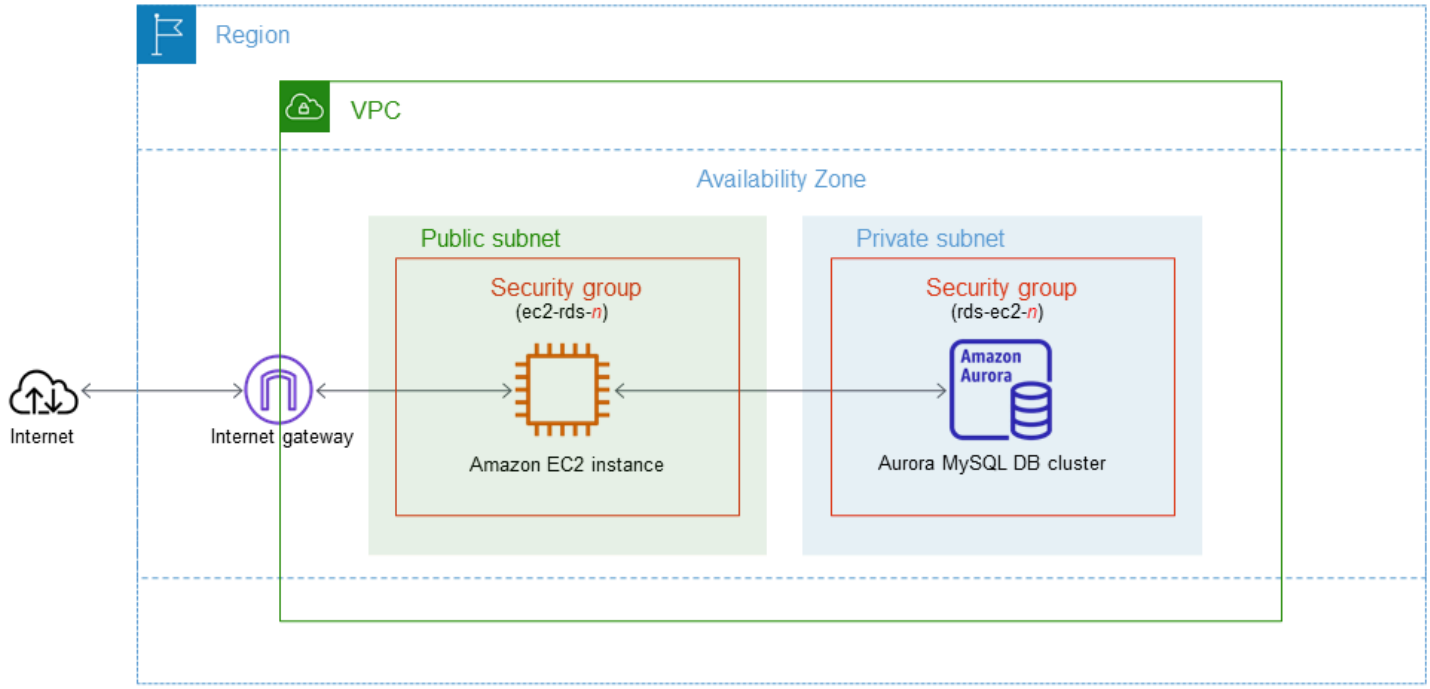
Erstellen und Verbinden mit einem DB-Cluster von Aurora MySQL

In diesem Tutorial werden eine EC2-Instance und ein DB-Cluster von Aurora MySQL erstellt. Das Tutorial zeigt, wie Sie mit einem Standard-MySQL-Client von der EC2-Instance aus auf den DB-Cluster zugreifen. Als bewährte Methode erstellt dieses Tutorial einen privaten DB-Cluster in einer Virtual Private Cloud (VPC). In den meisten Fällen können andere Ressourcen in derselben VPC, wie EC2-Instances, auf den DB-Clusterzugreifen, Ressourcen außerhalb der VPC können jedoch nicht darauf zugreifen.

Nach Abschluss des Tutorials gibt es in jeder Availability Zone im VPC ein öffentliches und ein privates Subnetz. In einer Availability Zone befindet sich die EC2-Instance im öffentlichen Subnetz und die DB-Instance im privaten Subnetz.

> **Important**
>
> Für die Erstellung eines AWS Kontos fallen keine Gebühren an. Wenn Sie dieses Tutorial abschließen, können Ihnen jedoch Kosten für die AWS Ressourcen entstehen, die Sie verwenden. Sie können diese Ressourcen nach Abschluss des Tutorials löschen, wenn sie nicht mehr benötigt werden.

Das folgende Diagramm zeigt die Konfiguration nach Abschluss des Tutorials.



In diesem Tutorial können Sie Ihre Ressourcen mithilfe einer der folgenden Methoden erstellen:

1. Verwenden Sie das AWS Management Console - Schritt 1: Erstellen einer EC2-Instance und Schritt 2:Erstellen eines DB-Clusters von Aurora MySQL
2. Verwenden Sie AWS CloudFormation , um die Datenbank-Instance und die EC2-Instance zu erstellen - (Optional) Erstellen Sie eine VPC, eine EC2-Instanz und einen Aurora MySQL-Cluster mithilfe von AWS CloudFormation

Die erste Methode verwendet Easy Create, um einen privaten Aurora MySQL-DB-Cluster mit dem zu erstellen AWS Management Console. Hier geben Sie nur den DB-Engine-Typ, die DB-Instance-Größe und die DB-Cluster-ID an. Easy Create (Einfache Erstellung) verwendet für die anderen Konfigurationsoptionen die Standardeinstellung.

Wenn Sie stattdessen Standard Create verwenden, können Sie bei der Erstellung eines DB-Clusters weitere Konfigurationsoptionen angeben. Zu diesen Optionen gehören Einstellungen für Verfügbarkeit, Sicherheit, Backups und Wartung. Wenn Sie einen öffentliche DB-Cluster erstellen möchten, müssen Sie Standarderstellung verwenden. Weitere Informationen finden Sie unter the section called “Erstellen eines DB-Clusters”.

Themen

Voraussetzungen

Bevor Sie die Schritte in diesem Abschnitt abschließen, stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

- Melden Sie sich an für ein AWS-Konto
- Erstellen Sie einen Benutzer mit Administratorzugriff

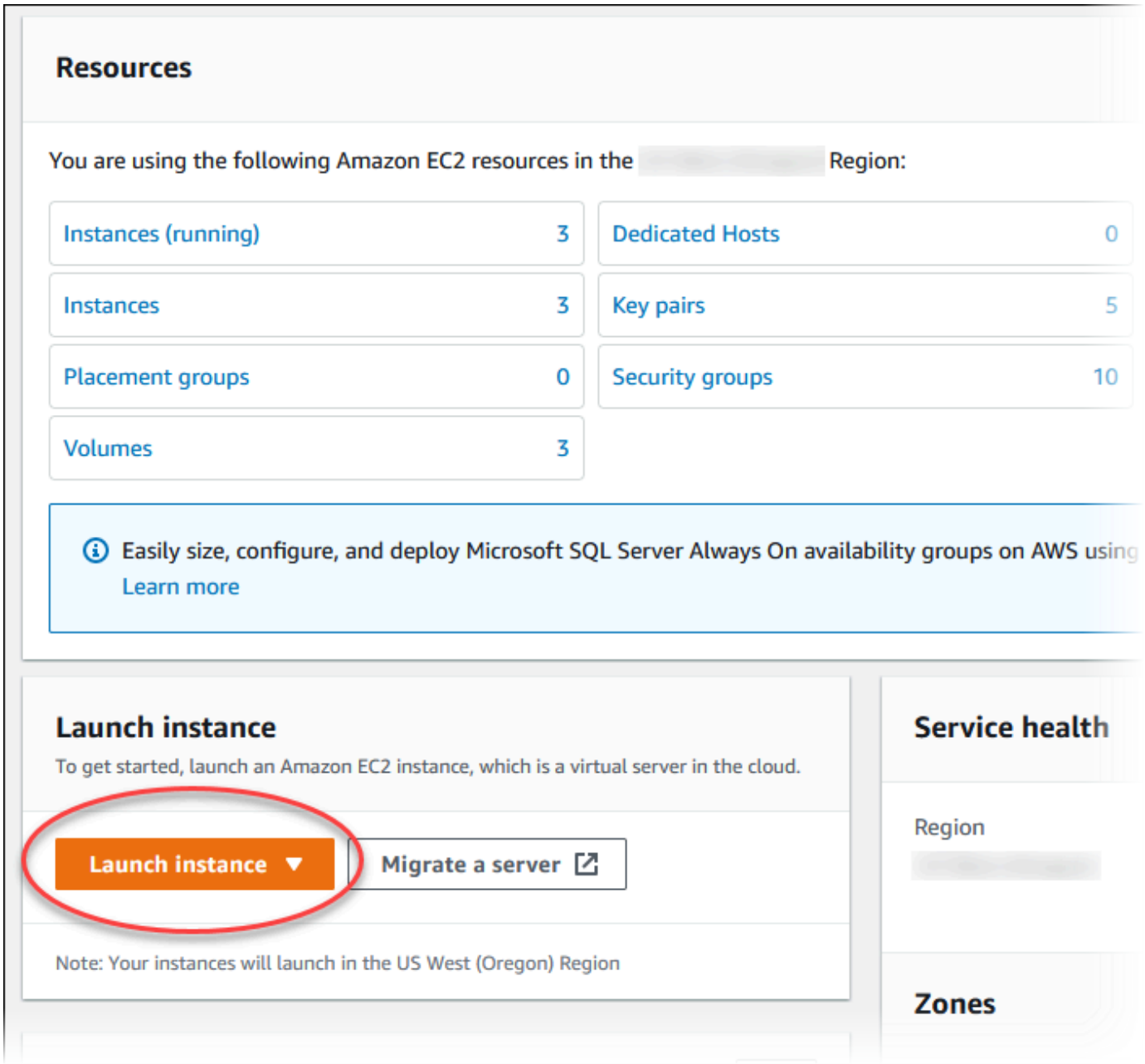
Schritt 1: Erstellen einer EC2-Instance

Erstellen Sie eine Amazon-EC2-Instance, um eine Verbindung mit Ihrer Datenbank herzustellen.

So erstellen Sie eine EC2-Instance

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie in der oberen rechten Ecke von die aus AWS Management Console, AWS-Region in der Sie die EC2-Instance erstellen möchten.
3. Wählen Sie EC2-Dashboard und anschließend Instance starten wie im Folgenden gezeigt.

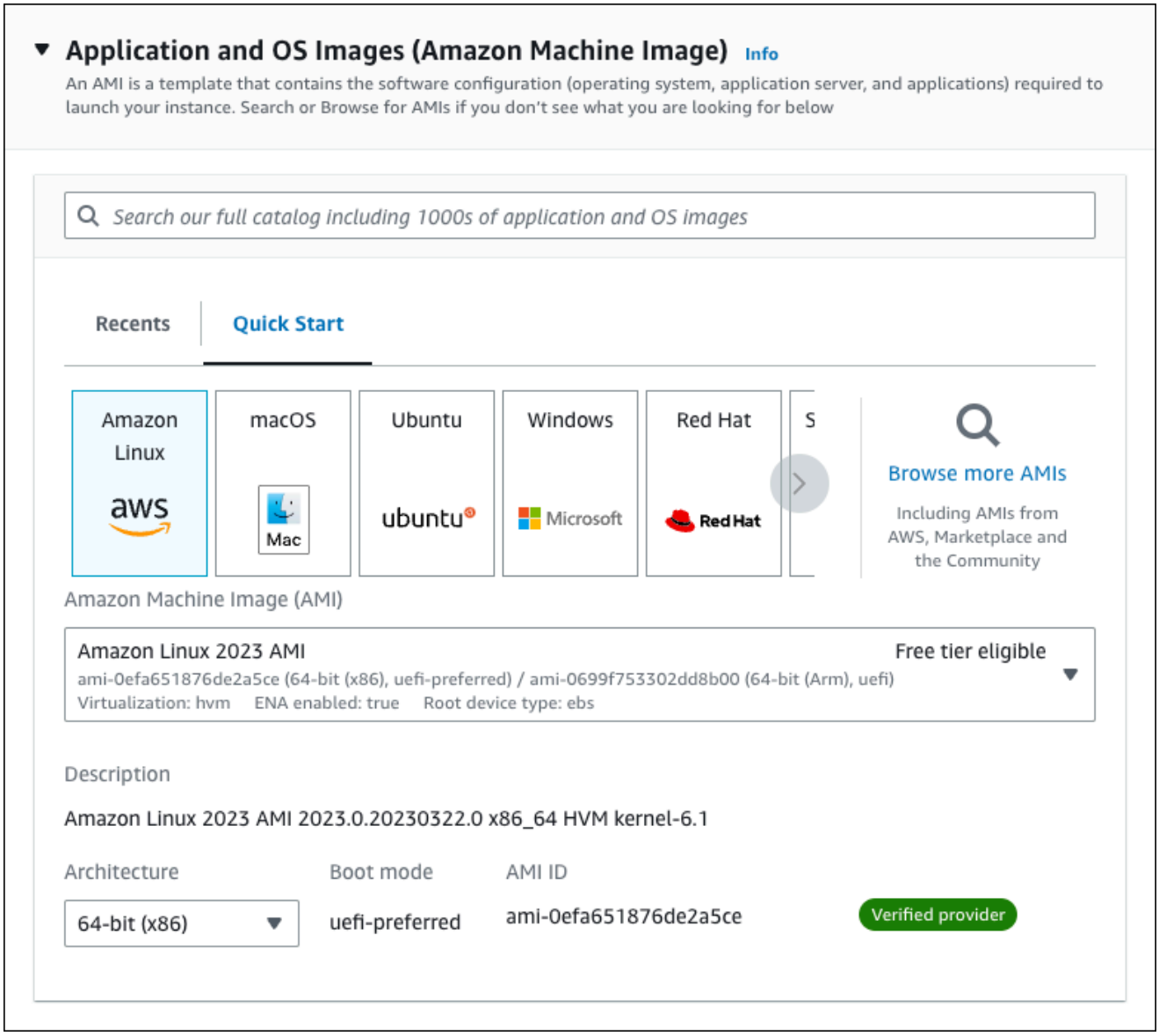


Die Seite Eine Instance starten wird geöffnet.

4. Wählen Sie auf der Seite Eine Instance starten die folgenden Einstellungen aus.

   a. Geben Sie unter Name and tags (Name und Tags) als Name den Namen **`ec2-database-connect`** ein.

b. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Amazon Linux und dann die Registerkarte Amazon Linux 2023 AMI aus. Übernehmen Sie für alle anderen Einstellungen die Standardwerte.



c. Wählen Sie unter Instance type (Instance-Typ) den Wert t2.micro aus.

d. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) einen Key pair name (Schlüsselpaarname), um ein vorhandenes Schlüsselpaar zu verwenden. Wenn Sie ein neues Schlüsselpaar für die Amazon-EC2-Instance erstellen möchten, wählen Sie Create new key pair (Neues Schlüsselpaar erstellen) aus und erstellen sie das Schlüsselpaar im Fenster Create key pair (Schlüsselpaar erstellen).

Weitere Informationen zum Erstellen eines neuen Schlüsselpaars finden Sie unter Create a key pair im Amazon EC2 EC2-Benutzerhandbuch.

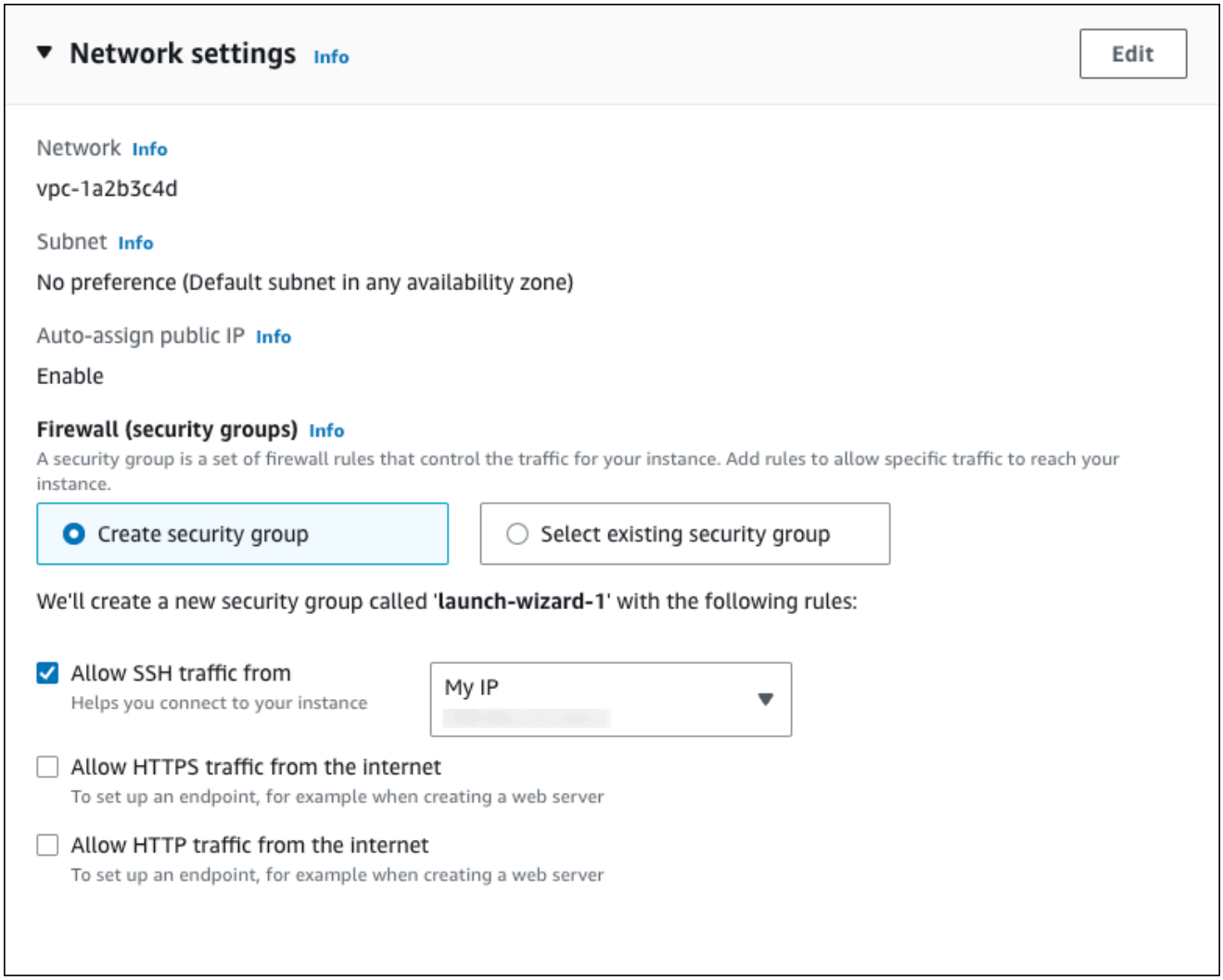
e. Wählen Sie in Netzwerkeinstellungen für SSH-Verkehr zulassen die Quelle von SSH-Verbindungen mit der EC2-Instance aus.

Sie können My IP (Meine IP) auswählen, wenn die angezeigte IP-Adresse für SSH-Verbindungen korrekt ist. Andernfalls können Sie die IP-Adresse, die für die Verbindung mit EC2-Instances in Ihrer VPC verwendet werden soll, mit Secure Shell (SSH) ermitteln. Um Ihre öffentliche IP-Adresse zu ermitteln, können Sie in einem anderen Browserfenster oder einer anderen Registerkarte den Service unter https://checkip.amazonaws.com verwenden. Ein Beispiel für eine IP-Adresse ist 192.0.2.1/32.

In vielen Fällen können Sie eine Verbindung über einen Internetdienstanbieter (ISP) oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen. Bestimmen Sie in diesem Fall den Bereich der IP-Adressen, die von Client-Computern verwendet werden.

> **Warning**
>
> Wenn Sie `0.0.0.0/0` für den SSH-Zugriff verwenden, ermöglichen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen EC2-Instances. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Für die Produktion sollten Sie nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre EC2-Instances autorisieren.

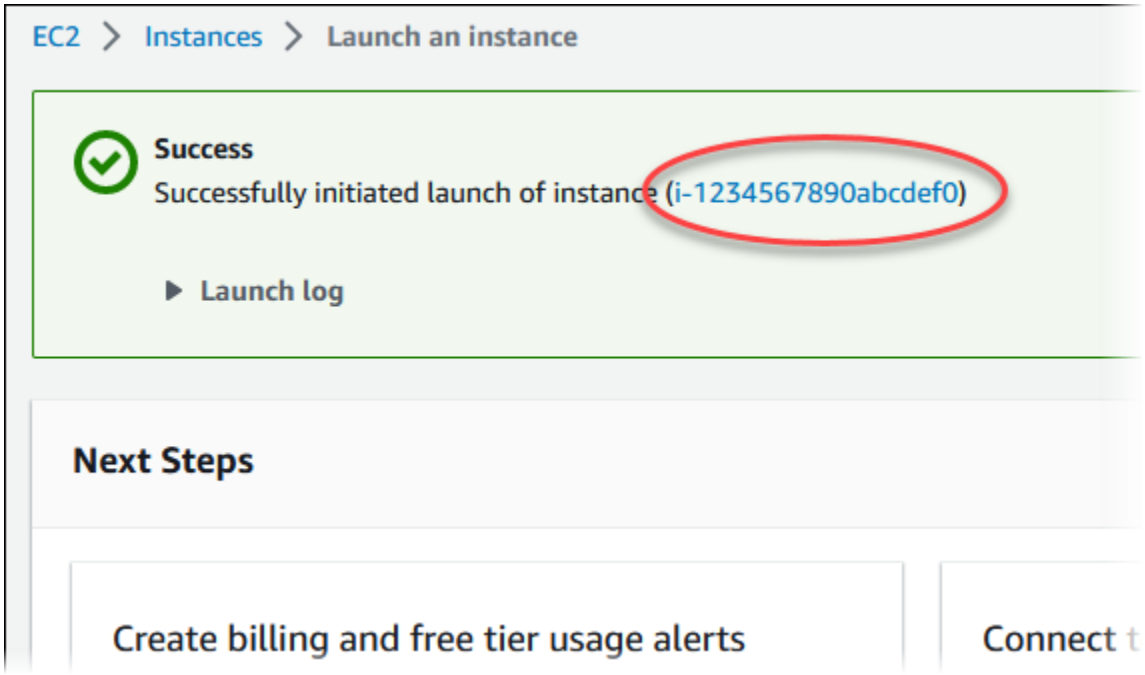
Die folgende Abbildung zeigt ein Beispiel für den Bereich Netzwerkeinstellungen.



f. Übernehmen Sie die Standardwerte für die übrigen Abschnitte.

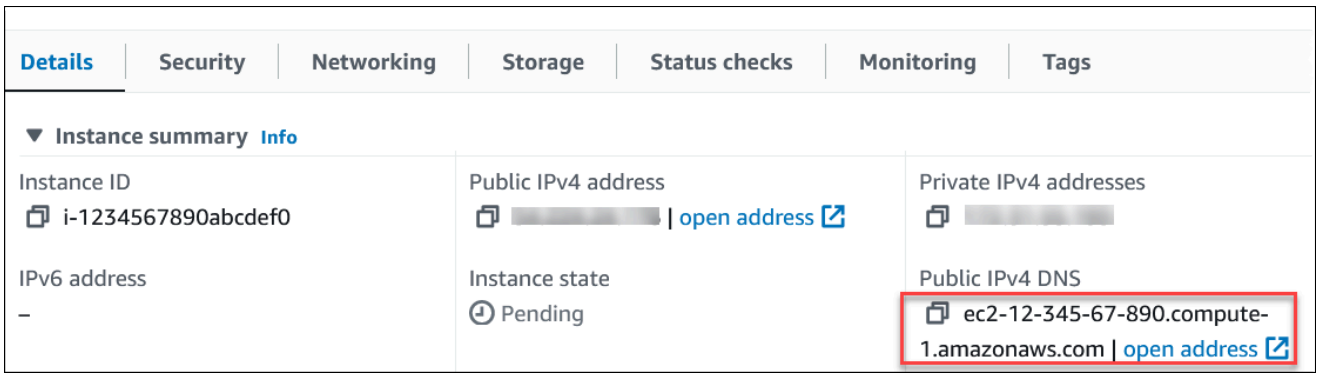
g. Prüfen Sie die Zusammenfassung Ihrer EC2-Instance-Konfiguration im Fenster Zusammenfassung; wenn Sie bereit sind, wählen Sie Instance starten.

5. Notieren Sie auf der im Folgenden gezeigten Seite Startstatus die Kennung für die neue EC2-Instance, beispielsweise: `i-1234567890abcdef0`.

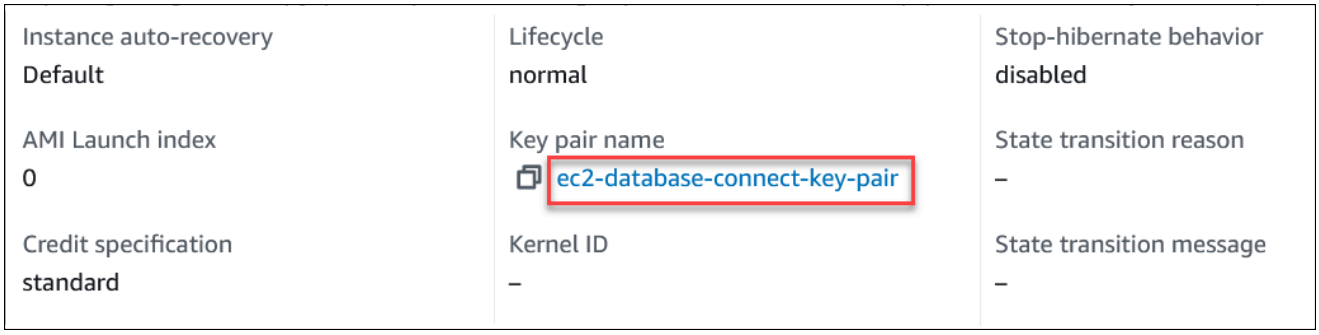


6. Wählen Sie die EC2-Instance-Kennung aus, um die Liste der EC2-Instances zu öffnen. Wählen Sie dann Ihre EC2-Instance aus.
7. Notieren Sie sich die folgenden Werte auf der Registerkarte Details. Diese benötigen Sie, wenn Sie eine Verbindung über SSH herstellen:

   a. Notieren Sie sich unter Instance-Zusammenfassung den Wert für Public IPv4 DNS.



   b. Notieren Sie sich unter Instance-Details den Wert für Schlüsselpaarname.



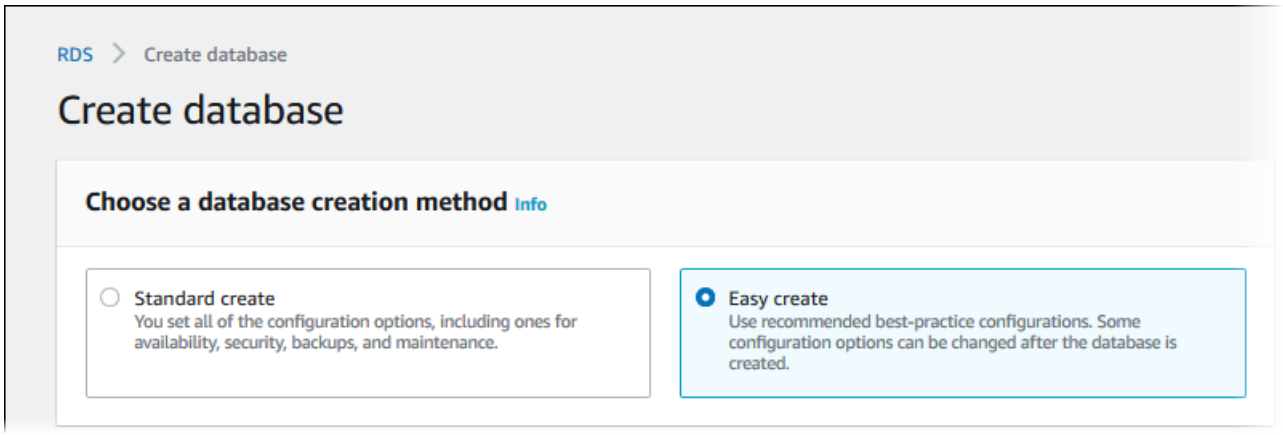
8. Warten Sie, bis der Instance-Status Ihrer EC2-Instance den Status Wird ausgeführt hat, bevor Sie fortfahren.

Schritt 2:Erstellen eines DB-Clusters von Aurora MySQL

In diesem Beispiel verwenden Sie Einfache Erstellung, um einen DB-Cluster von Aurora MySQL mit einer DB-Instance-Klasse vom Typ „db.r6g.large“ zu erstellen.

So erstellen Sie einen DB-Cluster von Aurora MySQL mit der Option „Einfache Erstellung“

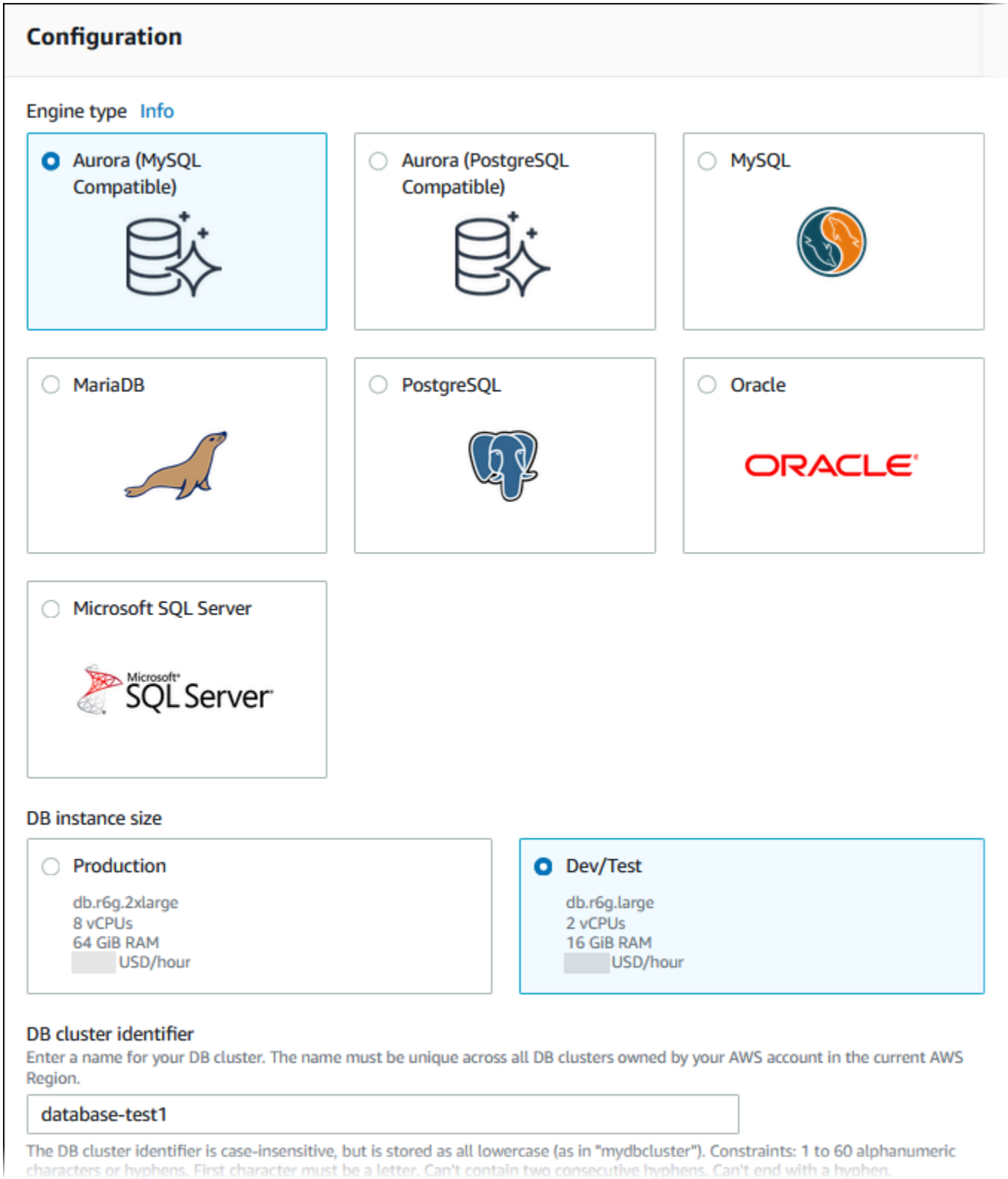
1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der oberen rechten Ecke der Amazon RDS-Konsole den aus, AWS-Region in dem Sie den DB-Cluster erstellen möchten.
3. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
4. Wählen Sie Datenbank erstellen aus und vergewissern Sie sich, dass Einfache Erstellung ausgewählt ist.



5. Wählen Sie unter Konfiguration die Option Aurora (MySQL-kompatibel) als Engine-Typ aus.

6. Wählen Sie in DB instance size (DB-Instance-Größe) die Option Dev/Test (Entwicklung/Testen) aus.
7. Geben Sie unter DB-Cluster-Kennung die Zeichenfolge **`database-test1`** ein.

   Die Seite Datenbank erstellen sollte ähnlich wie in der folgenden Abbildung gezeigt aussehen.



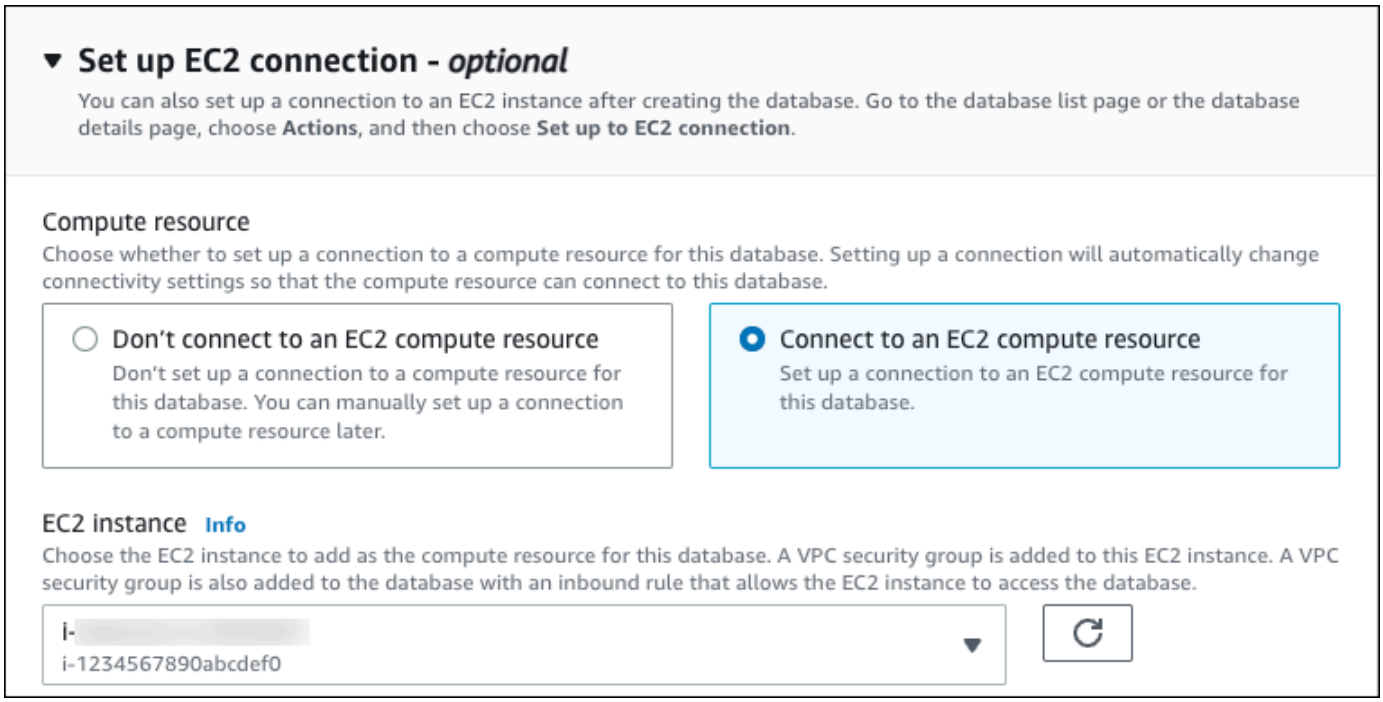
8. Geben Sie unter Hauptbenutzername einen Namen für den Hauptbenutzer ein oder behalten Sie den Standardnamen bei.

9. Um für den DB-Cluster ein automatisch generiertes Hauptpasswort zu verwenden, wählen Sie Passwort automatisch generieren aus.

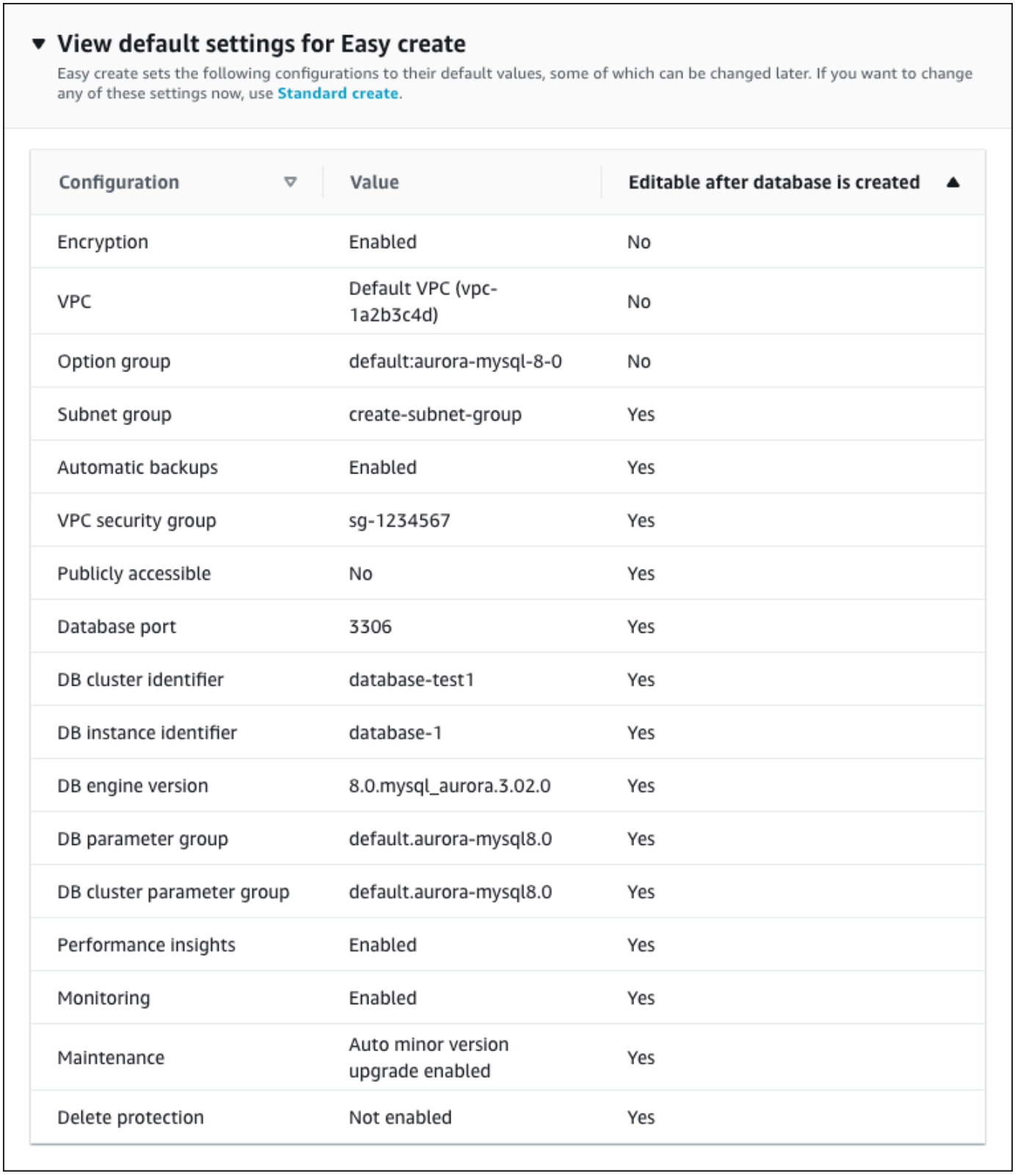
   Um das Hauptpasswort einzugeben, deaktivieren Sie das Kontrollkästchen Passwort automatisch generieren und geben Sie anschließend dasselbe Passwort in Hauptpasswort und Passwort bestätigen ein.

10. Um eine Verbindung mit der EC2-Instance einzurichten, die Sie zuvor erstellt haben, öffnen Sie EC2-Verbindung einrichten – optional.

    Wählen Sie Mit einer EC2-Datenverarbeitungsressource verbinden aus. Wählen Sie die EC2-Instance aus, die Sie zuvor erstellt haben.



11. (Optional) Öffnen Sie Anzeigen von Standardeinstellungen für eine einfache Erstellung.



View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use **Standard create**.

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-1a2b3c4d)	No
Option group	default:aurora-mysql-8-0	No
Subnet group	create-subnet-group	Yes
Automatic backups	Enabled	Yes
VPC security group	sg-1234567	Yes
Publicly accessible	No	Yes
Database port	3306	Yes
DB cluster identifier	database-test1	Yes
DB instance identifier	database-1	Yes
DB engine version	8.0.mysql_aurora.3.02.0	Yes
DB parameter group	default.aurora-mysql8.0	Yes
DB cluster parameter group	default.aurora-mysql8.0	Yes
Performance insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto minor version upgrade enabled	Yes
Delete protection	Not enabled	Yes

Sie können die Standardeinstellungen von Einfache Erstellung einsehen. Die Spalte Nach Erstellung der Datenbank editierbar zeigt, welche Optionen Sie nach der Datenbankerstellung ändern können.

- Wenn für eine Einstellung Nein in dieser Spalte steht und Sie eine andere Einstellung verwenden möchten, können Sie Standarderstellung verwenden, um den DB-Cluster zu erstellen.
- Wenn für eine Einstellung Ja in dieser Spalte steht und Sie eine andere Einstellung verwenden möchten, können Sie entweder Standarderstellung auswählen, um den DB-Cluster zu erstellen, oder den DB-Cluster nach der Erstellung ändern, um die Einstellung zu ändern.

12. Wählen Sie Datenbank erstellen aus.

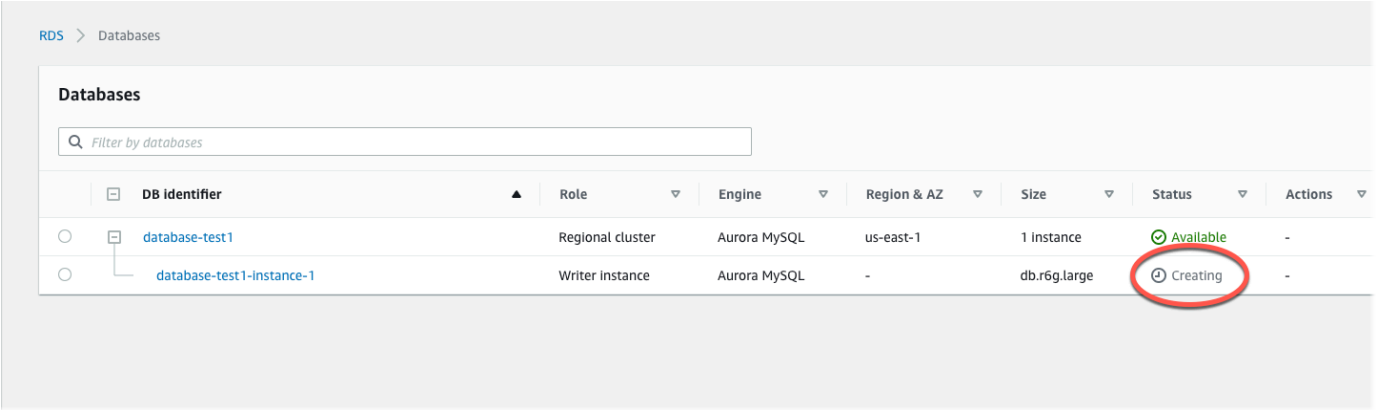
    Um den Hauptbenutzernamen und das Passwort für den DB-Cluster anzuzeigen, wählen Sie Anmeldeinformationen anzeigen aus.

    Sie können den angezeigten Benutzernamen und das angezeigte Passwort verwenden, um als Hauptbenutzer eine Verbindung mit dem DB-Cluster herzustellen.

    > **Important**
    >
    > Sie können dieses Passwort für den Hauptbenutzer nicht erneut anzeigen. Wenn Sie es nicht notieren, müssen Sie es möglicherweise ändern.
    > Wenn Sie das Passwort für den Hauptbenutzer ändern müssen, nachdem der DB-Cluster verfügbar wurde, können Sie den DB-Cluster entsprechend ändern. Weitere Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

13. Wählen Sie in der Liste Datenbanken den Namen des neuen DB-Clusters von Aurora MySQL aus.

    Die Writer-Instance hat den Status Wird erstellt, bis der DB-Cluster bereit ist und verwendet werden kann.



Wenn sich der Status der Writer-Instance in Verfügbar ändert, können Sie die Verbindung mit dem DB-Cluster herstellen. Je nach Klasse und Speicherort der DB-Instance kann es bis zu 20 Minuten dauern, bis der neue DB-Cluster verfügbar ist.

(Optional) Erstellen Sie eine VPC, eine EC2-Instanz und einen Aurora MySQL-Cluster mithilfe von AWS CloudFormation

Anstatt die Konsole zum Erstellen Ihrer VPC, EC2-Instance und Ihres Aurora MySQL-DB-Clusters AWS CloudFormation zu verwenden, können Sie AWS Ressourcen bereitstellen, indem Sie die Infrastruktur als Code behandeln. Um Ihnen zu helfen, Ihre AWS Ressourcen in kleinere und besser verwaltbare Einheiten zu organisieren, können Sie die AWS CloudFormation Nested-Stack-Funktionalität verwenden. Weitere Informationen finden Sie unter Einen Stack auf der AWS CloudFormation Konsole erstellen und Mit verschachtelten Stacks arbeiten.

> **Important**
>
> AWS CloudFormation ist kostenlos, aber die Ressourcen, die CloudFormation erstellt werden, sind live. Es fallen die üblichen Nutzungsgebühren für diese Ressourcen an, bis Sie sie kündigen. Die Gesamtgebühren sind minimal. Informationen darüber, wie Sie Gebühren minimieren können, finden Sie unter AWS Kostenloses Kontingent.

Gehen Sie wie folgt vor, um Ihre Ressourcen mithilfe der AWS CloudFormation Konsole zu erstellen:

- Schritt 1: Laden Sie die CloudFormation Vorlage herunter
- Schritt 2: Konfigurieren Sie Ihre Ressourcen mit CloudFormation

Laden Sie die CloudFormation Vorlage herunter

Eine CloudFormation Vorlage ist eine JSON- oder YAML-Textdatei, die die Konfigurationsinformationen zu den Ressourcen enthält, die Sie im Stack erstellen möchten. Diese Vorlage erstellt zusammen mit dem Aurora-Cluster auch eine VPC und einen Bastion-Host für Sie.

Um die Vorlagendatei herunterzuladen, öffnen Sie den folgenden Link: Aurora MySQL CloudFormation template.

Klicken Sie auf der Github-Seite auf die Schaltfläche Rohdatei herunterladen, um die YAML-Vorlagendatei zu speichern.

Konfigurieren Sie Ihre Ressourcen mit CloudFormation

> **Note**
>
> Bevor Sie diesen Vorgang starten, stellen Sie sicher, dass Sie ein Schlüsselpaar für eine EC2-Instance in Ihrem AWS-Konto haben. Weitere Informationen finden Sie unter Amazon-EC2-Schlüsselpaare und Linux-Instances.

Wenn Sie die AWS CloudFormation Vorlage verwenden, müssen Sie die richtigen Parameter auswählen, um sicherzustellen, dass Ihre Ressourcen ordnungsgemäß erstellt werden. Führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
2. Wählen Sie Stapel erstellen aus.
3. Wählen Sie im Abschnitt Vorlage angeben die Option Eine Vorlagendatei von Ihrem Computer hochladen und dann Weiter aus.
4. Legen Sie auf der Seite „Stack-Details angeben“ die folgenden Parameter fest:
   a. Setzen Sie den Stacknamen auf AurMySQL TestStack.
   b. Legen Sie unter Parameter Availability Zones fest, indem Sie zwei Availability Zones auswählen.
   c. Wählen Sie unter Linux Bastion Host configuration für Key Name ein key pair aus, um sich bei Ihrer EC2-Instance anzumelden.
   d. Stellen Sie in den Linux Bastion Host-Konfigurationseinstellungen den zulässigen IP-Bereich auf Ihre IP-Adresse ein. Um mithilfe von Secure Shell (SSH) eine Verbindung zu EC2-Instances

in Ihrer VPC herzustellen, ermitteln Sie Ihre öffentliche IP-Adresse mithilfe des Dienstes unter https://checkip.amazonaws.com. Ein Beispiel für eine IP-Adresse ist 192.0.2.1/32.

> **Warning**
>
> Wenn Sie `0.0.0.0/0` für den SSH-Zugriff verwenden, ermöglichen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen EC2-Instances. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Für die Produktion sollten Sie nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre EC2-Instances autorisieren.

e. Stellen Sie unter Allgemeine Datenbankkonfiguration die Datenbankinstanzklasse auf db.r6g.large ein.

f. Setzen Sie den Datenbanknamen auf. **`database-test1`**

g. Geben Sie unter Datenbank-Master-Benutzername einen Namen für den Masterbenutzer ein.

h. Stellen Sie `false` für dieses Tutorial das DB-Master-Benutzerpasswort mit Secrets Manager verwalten auf ein.

i. Geben Sie für das Datenbankkennwort ein Passwort Ihrer Wahl ein. Merken Sie sich dieses Passwort für weitere Schritte im Tutorial.

j. Stellen Sie die Multi-AZ-Bereitstellung auf ein`false`.

k. Behalten Sie für alle anderen Einstellungen die Standardwerte bei. Klicken Sie auf Weiter, um fortzufahren.

5. Behalten Sie auf der Seite „Stack-Optionen konfigurieren“ alle Standardoptionen bei. Klicken Sie auf Weiter, um fortzufahren.
6. Wählen Sie auf der Seite „Stack überprüfen“ die Option Senden aus, nachdem Sie die Datenbank- und Linux-Bastion-Host-Optionen überprüft haben.

Sehen Sie sich nach Abschluss der Stack-Erstellung die Stacks mit Namen BastionStackund AMSNS an, um die Informationen zu notieren, die Sie für die Verbindung mit der Datenbank benötigen. Weitere Informationen finden Sie unter AWS CloudFormation Stack-Daten und Ressourcen anzeigen auf der. AWS Management Console

Schritt 3: Herstellen einer Verbindung mit einem DB-Cluster von Aurora MySQL

Sie können für die Verbindung mit dem DB-Cluster eine beliebige SQL-Client-Standardanwendung verwenden. In diesem Beispiel stellen Sie eine Verbindung mit einem DB-Cluster von Aurora MySQL mithilfe des mysql-Befehlszeilen-Clients her.

So stellen Sie eine Verbindung mit dem DB-Cluster von Aurora MySQL her

1. Suchen Sie nach dem Endpunkt (DNS-Name) und der Portnummer der Writer-Instance für Ihren DB-Cluster.

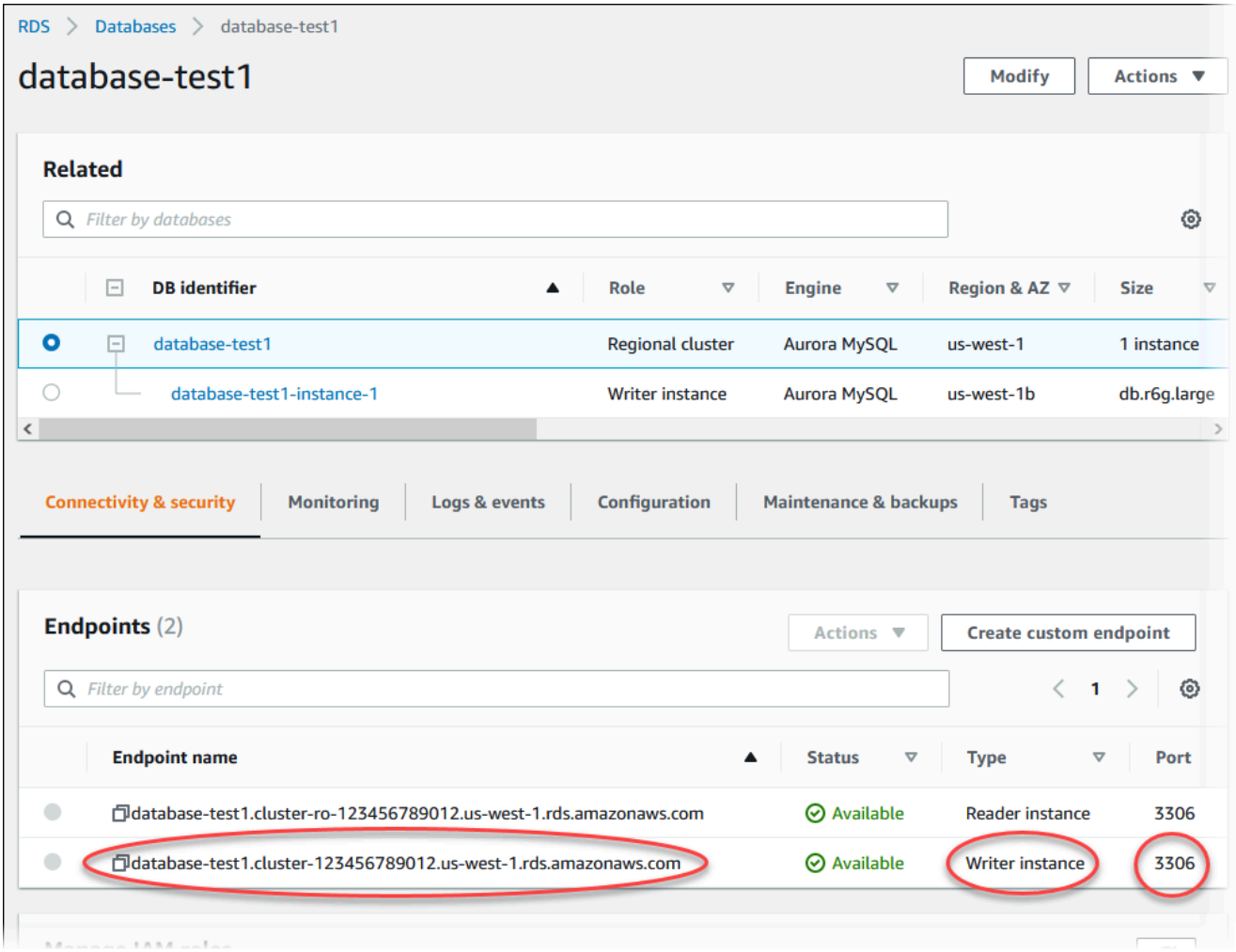
    a. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

    b. Wählen Sie oben rechts in der Amazon-RDS-Konsole die AWS-Region für den DB-Cluster aus.

    c. Wählen Sie im Navigationsbereich Datenbanken aus.

    d. Wählen Sie den Namen des DB-Clusters von Aurora MySQL aus, um dessen Details anzuzeigen.

    e. Kopieren Sie auf der Registerkarte Konnektivität und Sicherheit den Endpunkt der Writer-Instance. Notieren Sie sich auch die Portnummer. Sie benötigen sowohl den Endpunkt als auch die Portnummer, um die Verbindung mit dem DB-Cluster herzustellen.



2. Stellen Sie eine Verbindung zu der EC2-Instance her, die Sie zuvor erstellt haben, indem Sie den Schritten unter Connect to your Linux Instance im Amazon EC2 EC2-Benutzerhandbuch folgen.

   Wir empfehlen, dass Sie eine Verbindung mit Ihrer EC2-Instance mithilfe von SSH herstellen. Wenn das SSH-Client-Dienstprogramm unter Windows, Linux oder Mac installiert ist, können Sie mit dem folgenden Befehlsformat eine Verbindung mit der Instance herstellen:

   ```
   ssh -i location_of_pem_file ec2-user@ec2-instance-public-dns-name
   ```

   Nehmen wir zum Beispiel an, das `ec2-database-connect-key-pair.pem` in `/dir1` unter Linux gespeichert und das öffentliche IPv4-DNS für Ihre EC2-Instance `ec2-12-345-678-90.compute-1.amazonaws.com` ist. In diesem Fall würde Ihr SSH-Befehl wie folgt aussehen:

```
ssh -i /dir1/ec2-database-connect-key-pair.pem ec2-
user@ec2-12-345-678-90.compute-1.amazonaws.com
```

3. Installieren Sie die neuesten Fehlerbehebungen und Sicherheitsupdates, indem Sie die Software auf Ihrer EC2-Instance aktualisieren. Führen Sie dazu den folgenden Befehl aus.

   > **Note**
   >
   > Mit der Option `-y` werden die Updates installiert, ohne um Bestätigung zu bitten. Um Updates vor der Installation zu überprüfen, lassen Sie diese Option aus.

   ```
   sudo dnf update -y
   ```

4. Führen Sie den folgenden Befehl aus, um den mysql-Befehlszeilen-Client von MariaDB auf Amazon Linux 2023 zu installieren:

   ```
   sudo dnf install mariadb105
   ```

5. Stellen Sie eine Verbindung mit dem DB-Cluster von Aurora MySQL her. Geben Sie z. B. den folgenden Befehl ein. Mit dieser Aktion können Sie eine Verbindung mit dem DB-Cluster von Aurora MySQL mithilfe des MySQL-Clients herstellen.

   Ersetzen Sie den Endpunkt der Writer-Instance für *`endpoint`* und den Hauptbenutzernamen, den Sie für *`admin`* verwendet haben. Geben Sie das Master-Passwort ein, das Sie bei der Aufforderung zur Eingabe eines Passworts verwendet haben.

   ```
   mysql -h endpoint -P 3306 -u admin -p
   ```

   Nachdem Sie das Passwort für den Benutzer eingegeben haben, sollte eine Ausgabe wie die folgende angezeigt werden.

   ```
   Welcome to the MariaDB monitor.  Commands end with ; or \g.
   Your MySQL connection id is 217
   Server version: 8.0.23 Source distribution

   Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
   ```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Weitere Informationen zum Herstellen einer Verbindung mit einem DB-Cluster von Aurora MySQL finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora MySQL-DB-Cluster. Wenn Sie sich nicht mit Ihrem DB-Cluster verbinden können, erhalten Sie unter Verbindung zur Amazon RDS-DB-Instance kann nicht hergestellt werden Hilfe.

Aus Sicherheitsgründen empfiehlt es sich, verschlüsselte Verbindungen zu verwenden. Verwenden Sie eine unverschlüsselte MySQL Verbindung nur, wenn sich Client und Server in derselben VPC befinden und das Netzwerk vertrauenswürdig ist. Weitere IInformationen zur Verwendung verschlüsselter Verbindungen finden Sie unter Mit SSL eine Verbindung zu Aurora MySQL herstellen.

6. SQL-Befehle ausführen

   Der folgende SQL-Befehl zeigt z B. das aktuelle Datum und die aktuelle Zeit an:

   ```
   SELECT CURRENT_TIMESTAMP;
   ```

Schritt 4: Löschen der EC2-Instance und des DB-Clusters

Nachdem Sie eine Verbindung mit der Beispiel-EC2-Instance und dem DB-Cluster, die Sie erstellt haben, hergestellt und diese erkundet haben, löschen Sie sie, damit Ihnen dafür keine weiteren Kosten entstehen.

Wenn Sie früher AWS CloudFormation Ressourcen erstellt haben, überspringen Sie diesen Schritt und fahren Sie mit dem nächsten Schritt fort.

So löschen Sie die EC2-Instance

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die EC2- Instance aus, und wählen Sie Instance-Status, Instance beenden.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.

Weitere Informationen zum Löschen einer EC2-Instance finden Sie unter Terminate your Instance im Amazon EC2 EC2-Benutzerhandbuch.

So löschen Sie den DB-Cluster

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Databases (Datenbanken) und anschließend die DB-Instance aus, die mit dem DB-Cluster verknüpft ist.
3. Klicken Sie bei Actions auf Delete.
4. Deaktivieren Sie das Kontrollkästchen Abschließenden Snapshot erstellen?.
5. Bestätigen Sie, und wählen Sie Löschen.

Wenn alle mit einem DB-Cluster verknüpften DB-Instances gelöscht sind, wird der DB-Cluster automatisch gelöscht.

(Optional) Löschen Sie die EC2-Instance und den DB-Cluster, die mit erstellt wurden CloudFormation

Wenn Sie früher AWS CloudFormation Ressourcen erstellt haben, löschen Sie den CloudFormation Stack, nachdem Sie sich mit der EC2-Beispiel-Instance und dem DB-Cluster verbunden und diese erkundet haben, sodass Ihnen diese nicht mehr in Rechnung gestellt werden.

Um die Ressourcen zu löschen CloudFormation

1. Öffnen Sie die AWS CloudFormation Konsole.
2. Wählen Sie auf der Seite Stacks in der CloudFormation Konsole den Root-Stack aus (den Stack ohne den Namen VPCStack BastionStack oder AMSNS).
3. Wählen Sie Löschen aus.
4. Wählen Sie Stack löschen aus, wenn Sie zur Bestätigung aufgefordert werden.

Weitere Informationen zum Löschen eines Stacks in CloudFormation finden Sie im AWS CloudFormation Benutzerhandbuch unter Löschen eines Stacks auf der AWS CloudFormation Konsole.

(Optional) Verbinden Sie Ihren DB-Cluster mit einer Lambda-Funktion

Sie können Ihren DB-Cluster von Aurora MySQL auch mit einer Lambda-Serverless-Rechenressource verbinden. Mit Lambda-Funktionen können Sie Code ausführen, ohne die Infrastruktur bereitstellen oder verwalten zu müssen. Eine Lambda-Funktion ermöglicht es Ihnen auch, automatisch auf Codeausführungsanfragen jeder Größenordnung zu reagieren, von einem Dutzend Ereignissen pro Tag bis hin zu Hunderten von Ereignissen pro Sekunde. Weitere Informationen finden Sie unter Automatisches Verbinden einer Lambda-Funktion mit einem Aurora-DB-Cluster.

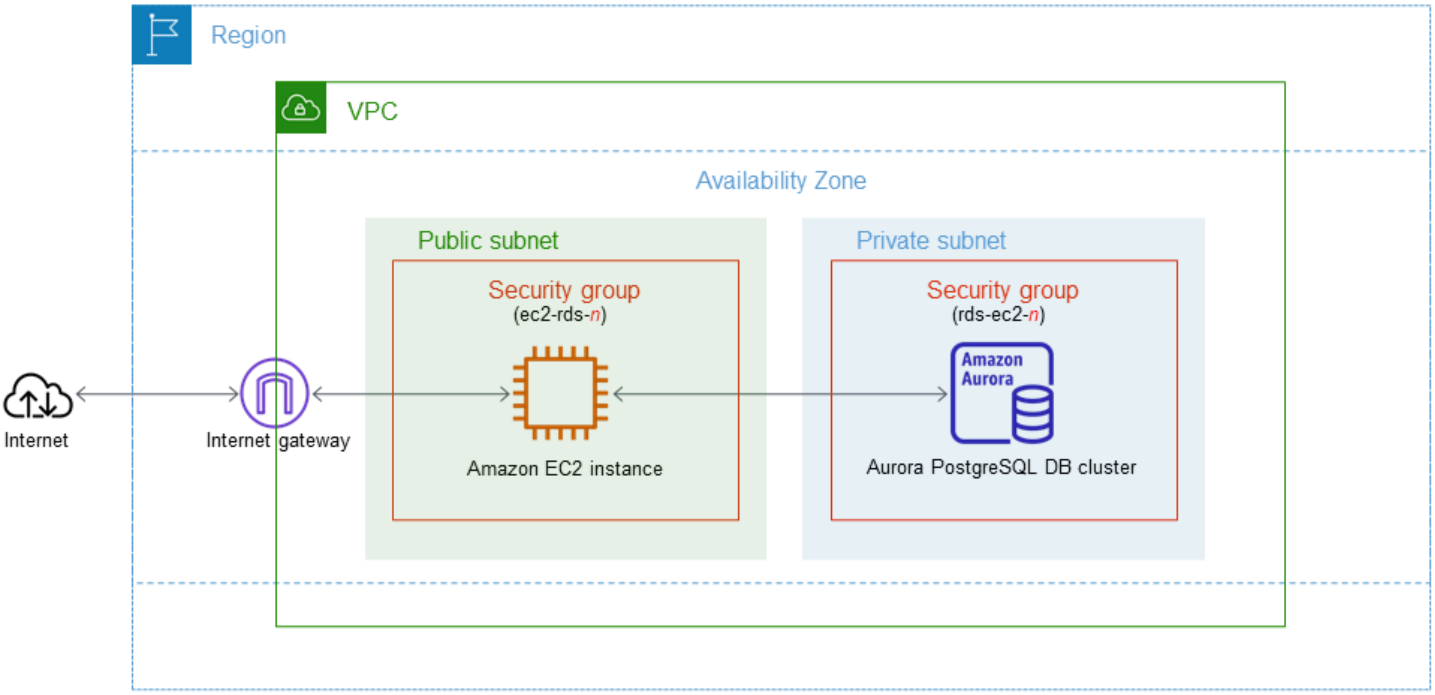
Erstellen eines DB-Clusters von Aurora PostgreSQL und Herstellen einer Verbindung

In diesem Tutorial werden eine EC2-Instance und ein DB-Cluster von Aurora PostgreSQL erstellt. Das Tutorial zeigt, wie Sie mit einem Standard-PostgreSQL-Client von der EC2-Instance aus auf den DB-Cluster zugreifen. Als bewährte Methode erstellt dieses Tutorial einen privaten DB-Cluster in einer Virtual Private Cloud (VPC). In den meisten Fällen können andere Ressourcen in derselben VPC, wie EC2-Instances, auf den DB-Clusterzugreifen, Ressourcen außerhalb der VPC können jedoch nicht darauf zugreifen.

Nach Abschluss des Tutorials gibt es in jeder Availability Zone im VPC ein öffentliches und ein privates Subnetz. In einer Availability Zone befindet sich die EC2-Instance im öffentlichen Subnetz und die DB-Instance im privaten Subnetz.

> **Important**
>
> Für die Erstellung eines AWS Kontos fallen keine Gebühren an. Wenn Sie dieses Tutorial abschließen, können Ihnen jedoch Kosten für die AWS Ressourcen entstehen, die Sie verwenden. Sie können diese Ressourcen nach Abschluss des Tutorials löschen, wenn sie nicht mehr benötigt werden.

Das folgende Diagramm zeigt die Konfiguration nach Abschluss des Tutorials.



In diesem Tutorial können Sie Ihre Ressourcen mithilfe einer der folgenden Methoden erstellen:

1. Verwenden Sie das AWS Management Console - Schritt 1: Erstellen einer EC2-Instance und Schritt 2: Erstellen eines DB-Clusters von Aurora PostgreSQL
2. Verwenden Sie AWS CloudFormation , um die Datenbank-Instance und die EC2-Instance zu erstellen - (Optional) Erstellen Sie eine VPC, eine EC2-Instanz und einen Aurora PostgreSQL-Cluster mit AWS CloudFormation

Die erste Methode verwendet Easy Create, um einen privaten Aurora PostgreSQL-DB-Cluster mit dem zu erstellen. AWS Management Console Hier geben Sie nur den DB-Engine-Typ, die DB-Instance-Größe und die DB-Cluster-ID an. Easy Create (Einfache Erstellung) verwendet für die anderen Konfigurationsoptionen die Standardeinstellung.

Wenn Sie stattdessen Standard Create verwenden, können Sie bei der Erstellung eines DB-Clusters weitere Konfigurationsoptionen angeben. Zu diesen Optionen gehören Einstellungen für Verfügbarkeit, Sicherheit, Backups und Wartung. Wenn Sie einen öffentliche DB-Cluster erstellen möchten, müssen Sie Standarderstellung verwenden. Weitere Informationen finden Sie unter the section called “Erstellen eines DB-Clusters”.

Themen

- Voraussetzungen

Voraussetzungen

Bevor Sie die Schritte in diesem Abschnitt abschließen, stellen Sie sicher, dass Sie folgende Voraussetzungen erfüllen:

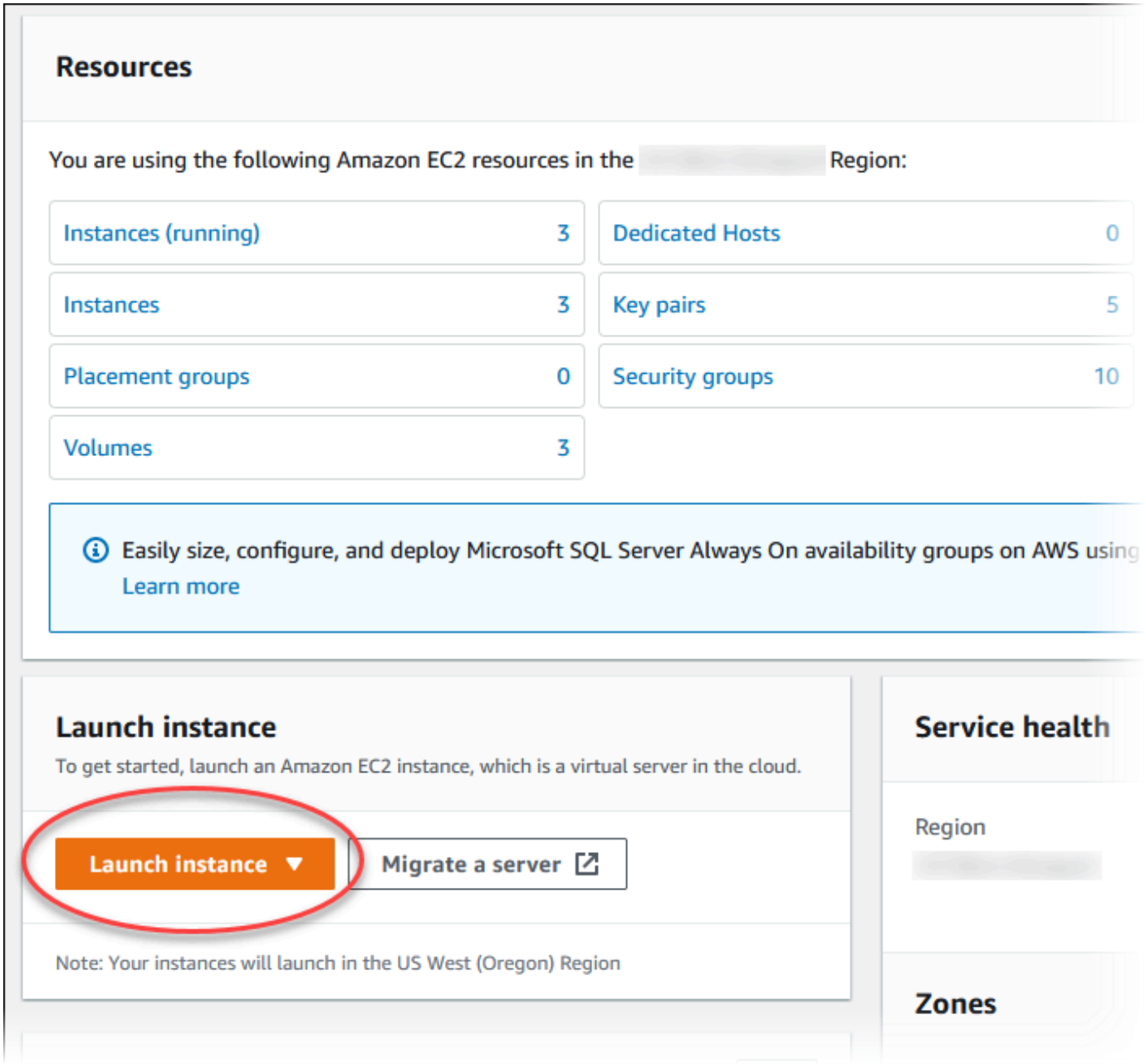
- Melden Sie sich an für ein AWS-Konto
- Erstellen Sie einen Benutzer mit Administratorzugriff

Schritt 1: Erstellen einer EC2-Instance

Erstellen Sie eine Amazon-EC2-Instance, um eine Verbindung mit Ihrer Datenbank herzustellen.

So erstellen Sie eine EC2-Instance

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der oberen rechten Ecke von die aus AWS Management Console, AWS-Region in der Sie die EC2-Instance erstellen möchten.
3. Wählen Sie EC2-Dashboard und anschließend Instance starten wie im Folgenden gezeigt.

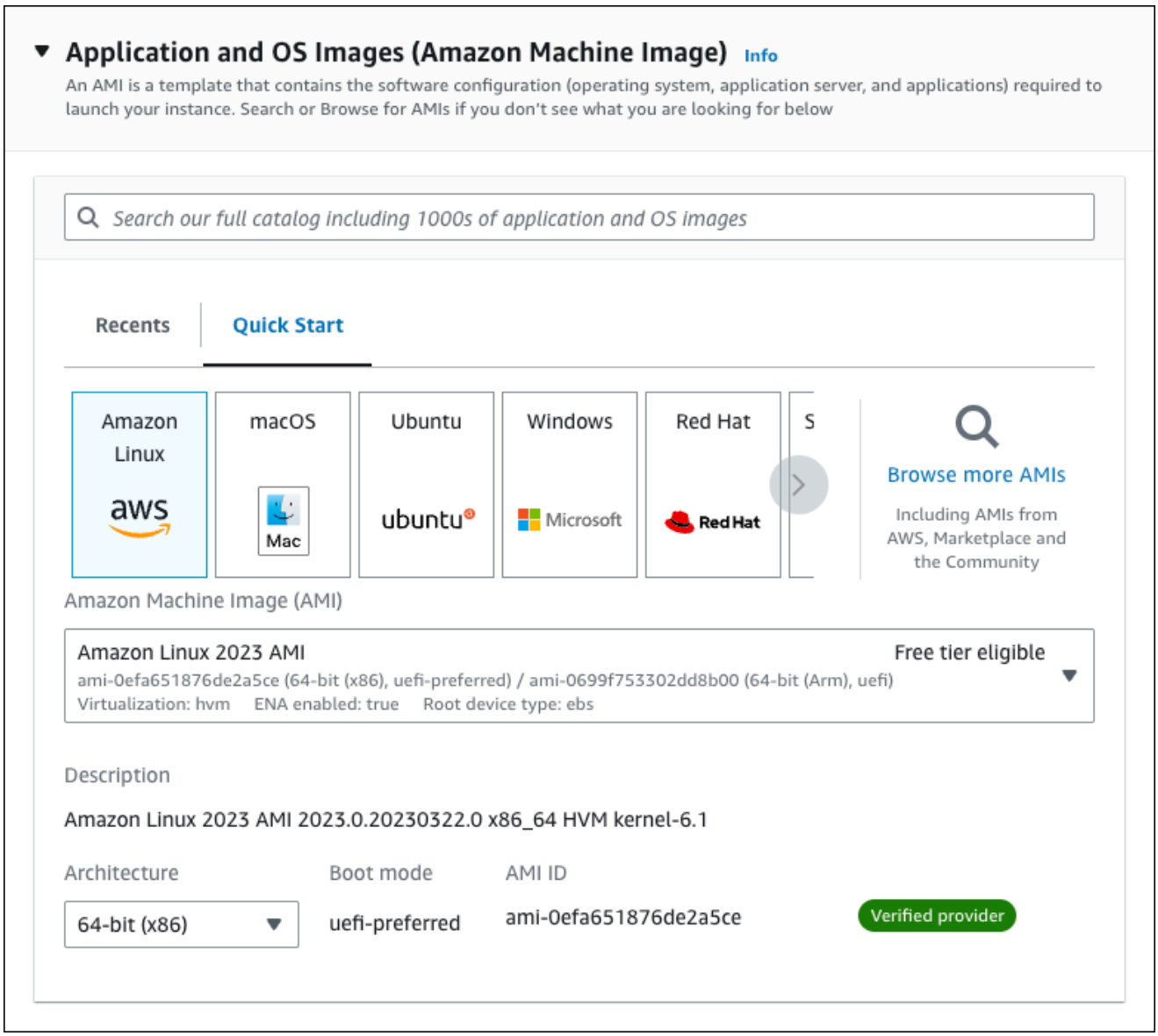


Die Seite Eine Instance starten wird geöffnet.

4. Wählen Sie auf der Seite Eine Instance starten die folgenden Einstellungen aus.

   a. Geben Sie unter Name and tags (Name und Tags) als Name den Namen **`ec2-database-connect`** ein.

   b. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Amazon Linux und dann die Registerkarte Amazon Linux 2023 AMI aus. Übernehmen Sie für alle anderen Einstellungen die Standardwerte.



c. Wählen Sie unter Instance type (Instance-Typ) den Wert t2.micro aus.

d. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) einen Key pair name (Schlüsselpaarname), um ein vorhandenes Schlüsselpaar zu verwenden. Wenn Sie ein neues Schlüsselpaar für die Amazon-EC2-Instance erstellen möchten, wählen Sie Create new key pair (Neues Schlüsselpaar erstellen) aus und erstellen sie das Schlüsselpaar im Fenster Create key pair (Schlüsselpaar erstellen).

   Weitere Informationen zum Erstellen eines neuen Schlüsselpaars finden Sie unter Create a key pair im Amazon EC2 EC2-Benutzerhandbuch.

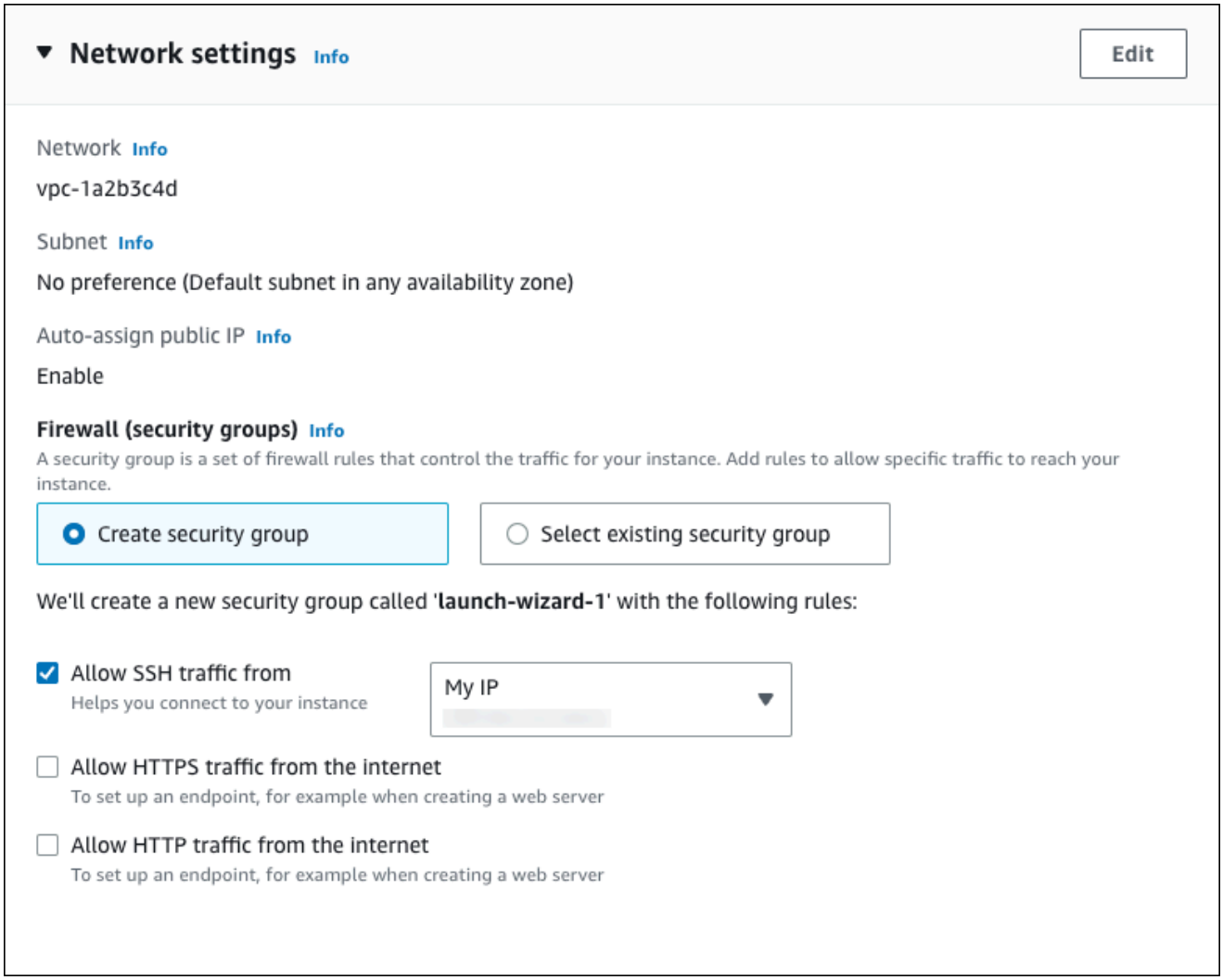
e. Wählen Sie in Netzwerkeinstellungen für SSH-Verkehr zulassen die Quelle von SSH-Verbindungen mit der EC2-Instance aus.

Sie können My IP (Meine IP) auswählen, wenn die angezeigte IP-Adresse für SSH-Verbindungen korrekt ist. Andernfalls können Sie die IP-Adresse, die für die Verbindung mit EC2-Instances in Ihrer VPC verwendet werden soll, mit Secure Shell (SSH) ermitteln. Um Ihre öffentliche IP-Adresse zu ermitteln, können Sie in einem anderen Browserfenster oder einer anderen Registerkarte den Service unter https://checkip.amazonaws.com verwenden. Ein Beispiel für eine IP-Adresse ist 192.0.2.1/32.

In vielen Fällen können Sie eine Verbindung über einen Internetdienstanbieter (ISP) oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen. Bestimmen Sie in diesem Fall den Bereich der IP-Adressen, die von Client-Computern verwendet werden.

> **Warning**
>
> Wenn Sie `0.0.0.0/0` für den SSH-Zugriff verwenden, ermöglichen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen EC2-Instances. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Für die Produktion sollten Sie nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre EC2-Instances autorisieren.

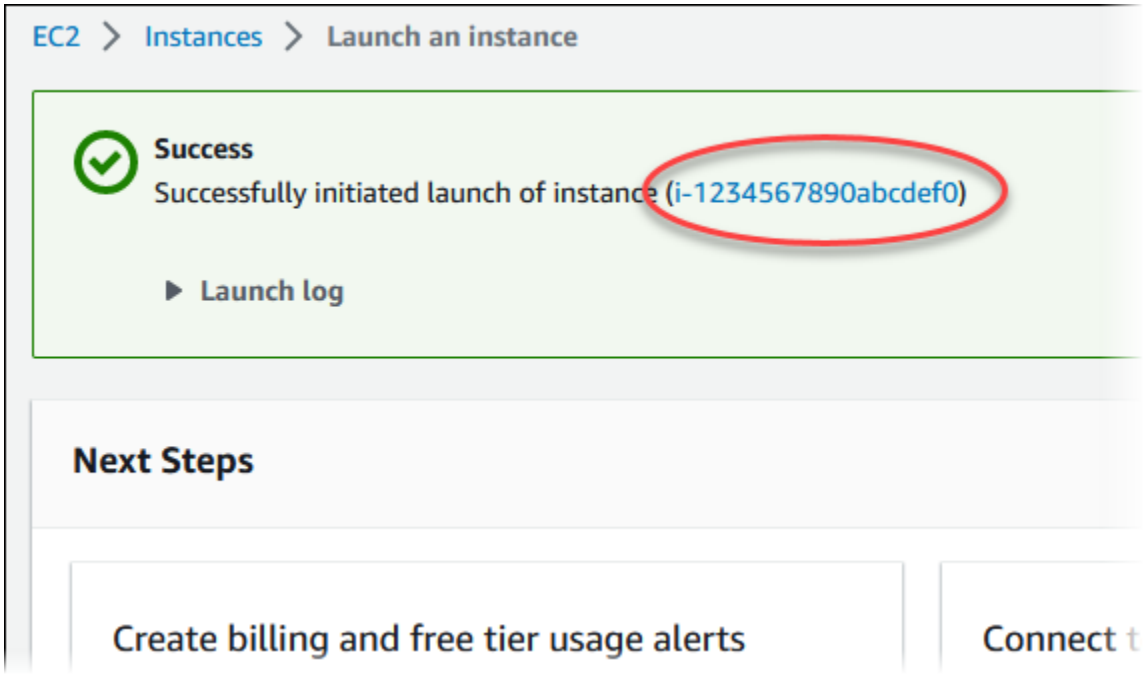
Die folgende Abbildung zeigt ein Beispiel für den Bereich Netzwerkeinstellungen.



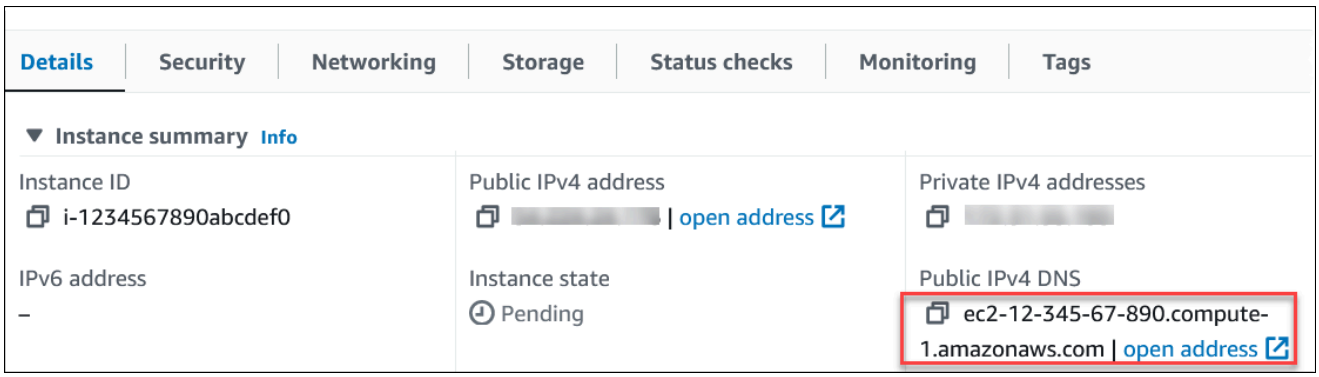
f. Übernehmen Sie die Standardwerte für die übrigen Abschnitte.

g. Prüfen Sie die Zusammenfassung Ihrer EC2-Instance-Konfiguration im Fenster Zusammenfassung; wenn Sie bereit sind, wählen Sie Instance starten.

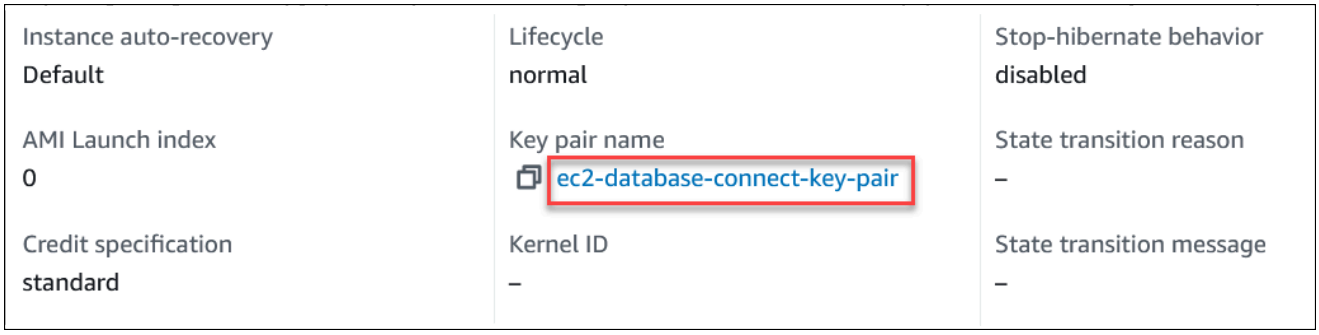
5. Notieren Sie auf der im Folgenden gezeigten Seite Startstatus die Kennung für die neue EC2-Instance, beispielsweise: `i-1234567890abcdef0`.



6. Wählen Sie die EC2-Instance-Kennung aus, um die Liste der EC2-Instances zu öffnen. Wählen Sie dann Ihre EC2-Instance aus.
7. Notieren Sie sich die folgenden Werte auf der Registerkarte Details. Diese benötigen Sie, wenn Sie eine Verbindung über SSH herstellen:
   a. Notieren Sie sich unter Instance-Zusammenfassung den Wert für Public IPv4 DNS.



   b. Notieren Sie sich unter Instance-Details den Wert für Schlüsselpaarname.



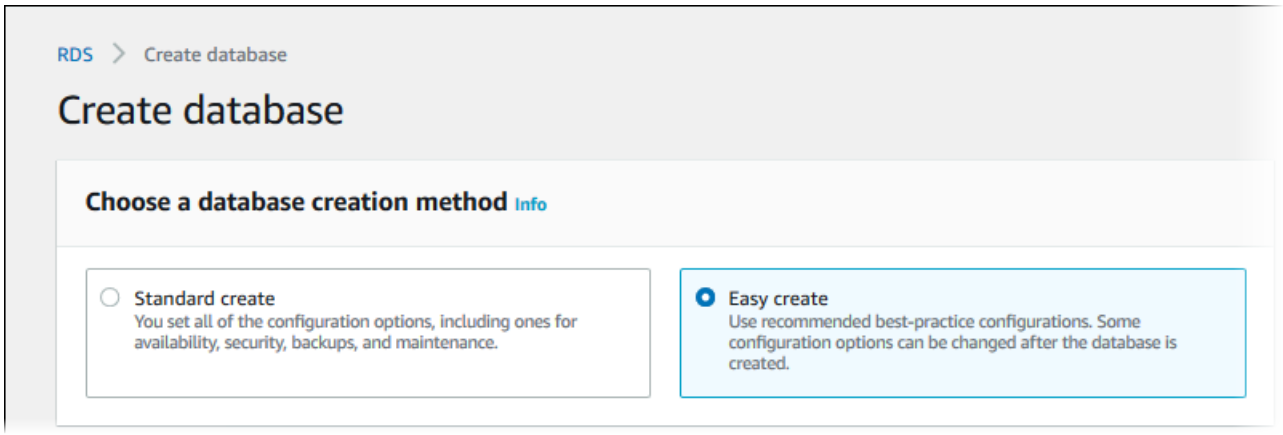
8. Warten Sie, bis der Instance-Status Ihrer EC2-Instance den Status Wird ausgeführt hat, bevor Sie fortfahren.

Schritt 2: Erstellen eines DB-Clusters von Aurora PostgreSQL

In diesem Beispiel verwenden Sie Einfache Erstellung, um einen DB-Cluster von Aurora PostgreSQL mit einer DB-Instance-Klasse vom Typ „db.t4g.large“ zu erstellen.

So erstellen Sie einen DB-Cluster von Aurora PostgreSQL der Option „Einfache Erstellung“

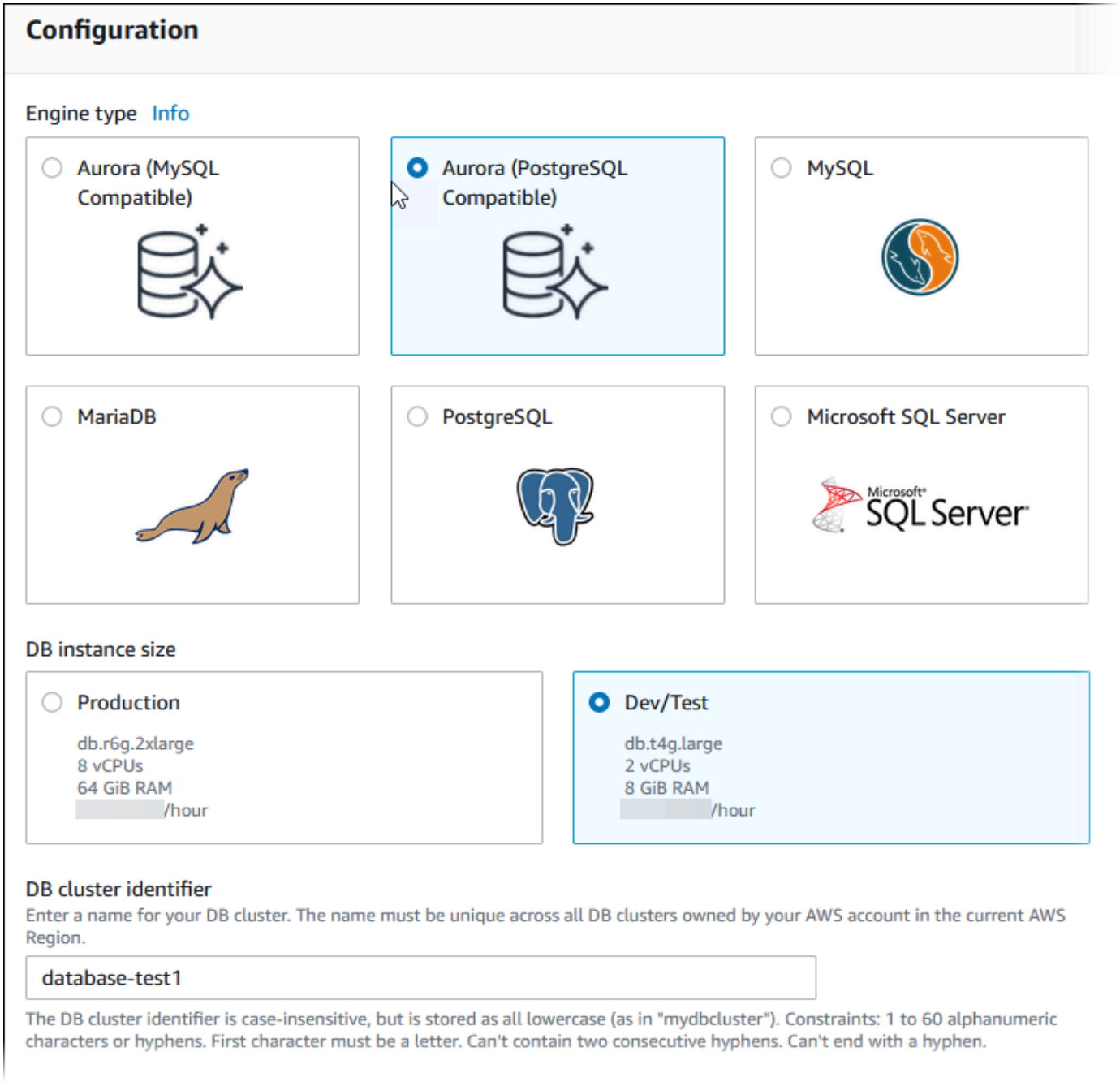
1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie rechts oben in der Amazon-RDS-Konsole die AWS-Region aus, in der Sie den DB-Cluster erstellen möchten.
3. Wählen Sie im Navigationsbereich Datenbanken aus.
4. Wählen Sie Datenbank erstellen aus und vergewissern Sie sich, dass Einfache Erstellung ausgewählt ist.



5. Wählen Sie unter Konfiguration die Option Aurora (PostgreSQL-kompatibel) als Engine-Typ aus.

6. Wählen Sie in DB instance size (DB-Instance-Größe) die Option Dev/Test (Entwicklung/Testen) aus.
7. Geben Sie unter DB-Cluster-Kennung die Zeichenfolge **`database-test1`** ein.

   Die Seite Datenbank erstellen sollte ähnlich wie in der folgenden Abbildung gezeigt aussehen.



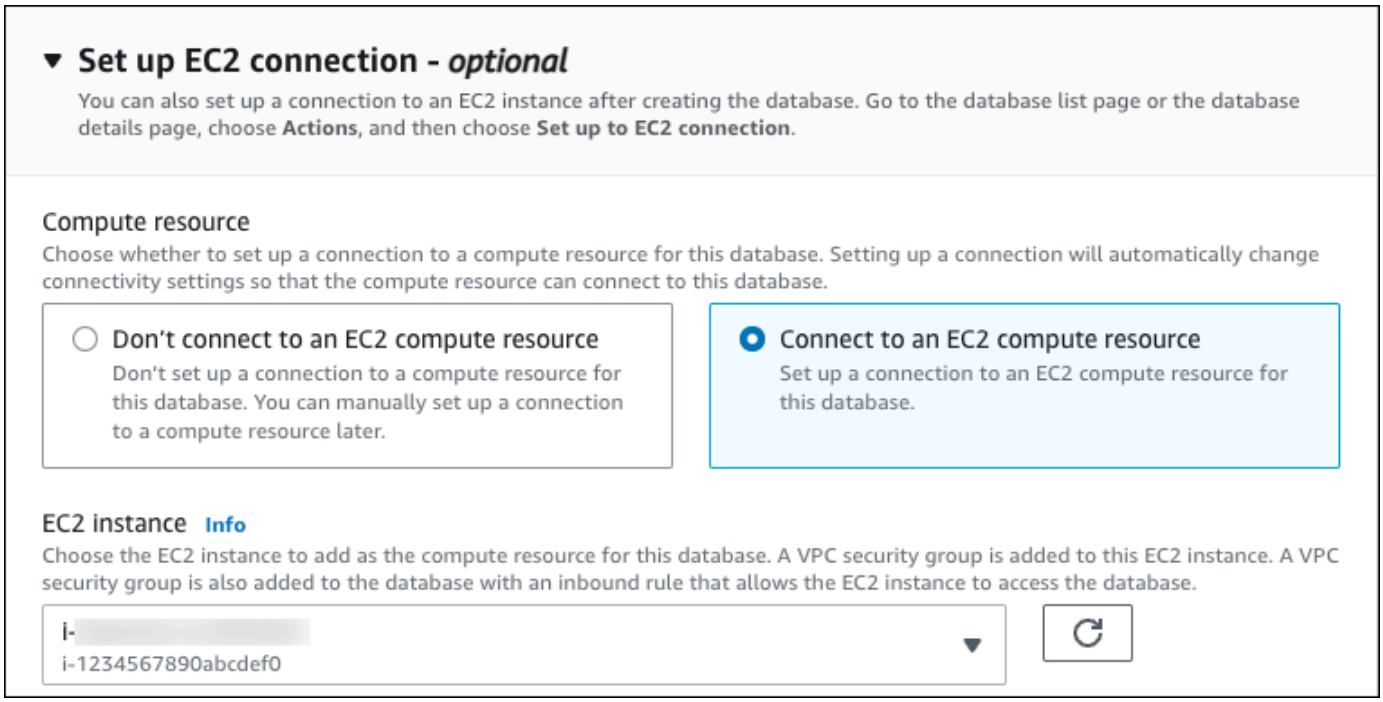
8. Geben Sie im Feld Hauptbenutzername einen Namen für den Benutzer ein oder behalten Sie den Standardnamen (**`postgres`**) bei.

9. Um für den DB-Cluster ein automatisch generiertes Hauptpasswort zu verwenden, wählen Sie Passwort automatisch generieren aus.

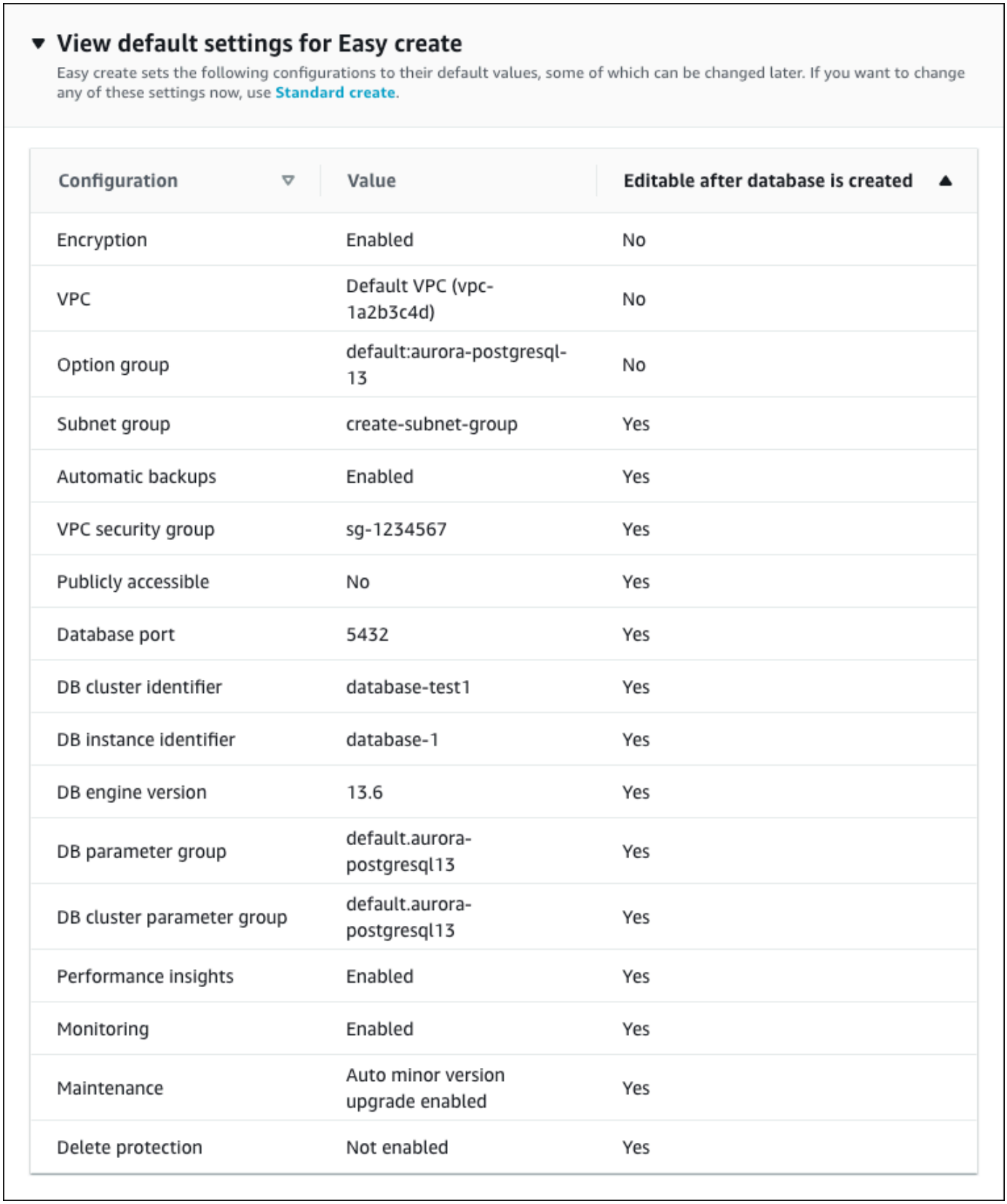
   Um das Hauptpasswort einzugeben, deaktivieren Sie das Kästchen Passwort automatisch generieren und geben Sie anschließend dasselbe Passwort in Hauptpasswort und Passwort bestätigen ein.

10. Um eine Verbindung mit der EC2-Instance einzurichten, die Sie zuvor erstellt haben, öffnen Sie EC2-Verbindung einrichten – optional.

    Wählen Sie Mit einer EC2-Datenverarbeitungsressource verbinden aus. Wählen Sie die EC2-Instance aus, die Sie zuvor erstellt haben.



11. (Optional) Öffnen Sie Anzeigen von Standardeinstellungen für eine einfache Erstellung.



View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use **Standard create**.

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-1a2b3c4d)	No
Option group	default:aurora-postgresql-13	No
Subnet group	create-subnet-group	Yes
Automatic backups	Enabled	Yes
VPC security group	sg-1234567	Yes
Publicly accessible	No	Yes
Database port	5432	Yes
DB cluster identifier	database-test1	Yes
DB instance identifier	database-1	Yes
DB engine version	13.6	Yes
DB parameter group	default.aurora-postgresql13	Yes
DB cluster parameter group	default.aurora-postgresql13	Yes
Performance insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto minor version upgrade enabled	Yes
Delete protection	Not enabled	Yes

Sie können die Standardeinstellungen von Einfache Erstellung einsehen. Die Spalte Nach Erstellung der Datenbank editierbar zeigt, welche Optionen Sie nach der Datenbankerstellung ändern können.

- Wenn für eine Einstellung Nein in dieser Spalte steht und Sie eine andere Einstellung verwenden möchten, können Sie Standarderstellung verwenden, um den DB-Cluster zu erstellen.
- Wenn für eine Einstellung Ja in dieser Spalte steht und Sie eine andere Einstellung verwenden möchten, können Sie entweder Standarderstellung auswählen, um den DB-Cluster zu erstellen, oder den DB-Cluster nach der Erstellung ändern, um die Einstellung zu ändern.

12. Wählen Sie Datenbank erstellen aus.

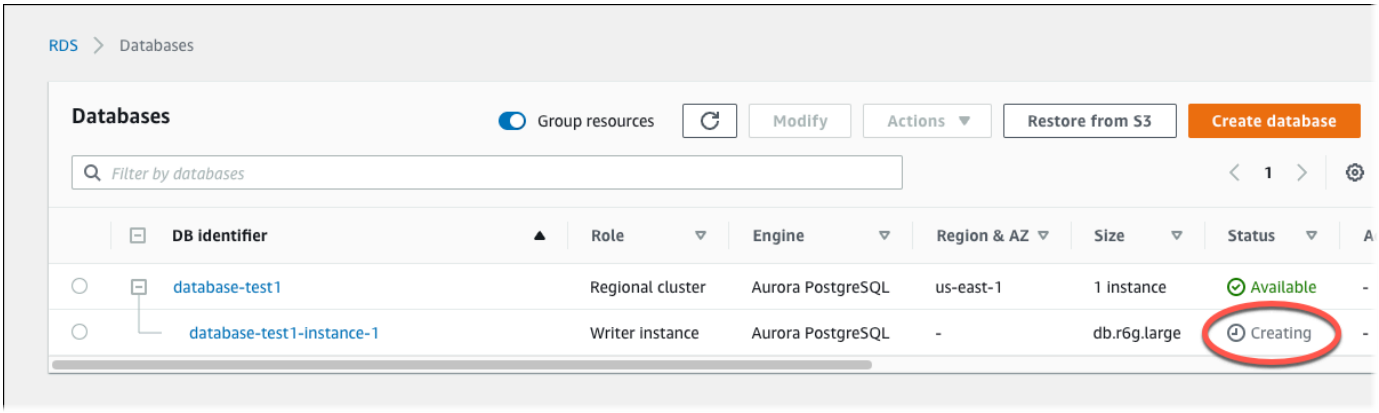
    Um den Hauptbenutzernamen und das Passwort für den DB-Cluster anzuzeigen, wählen Sie Anmeldeinformationen anzeigen aus.

    Sie können den angezeigten Benutzernamen und das angezeigte Passwort verwenden, um als Hauptbenutzer eine Verbindung mit dem DB-Cluster herzustellen.

    > **Important**
    >
    > Sie können dieses Passwort für den Hauptbenutzer nicht erneut anzeigen. Wenn Sie es nicht notieren, müssen Sie es möglicherweise ändern.
    > Wenn Sie das Passwort für den Hauptbenutzer ändern müssen, nachdem der DB-Cluster verfügbar wurde, können Sie den DB-Cluster entsprechend ändern. Weitere Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

13. Wählen Sie in der Liste Datenbanken den Namen des neuen DB-Clusters von Aurora PostgreSQL aus.

    Die Writer-Instance hat den Status Wird erstellt, bis der DB-Cluster bereit ist und verwendet werden kann.



Wenn sich der Status der Writer-Instance in Verfügbar ändert, können Sie die Verbindung mit dem DB-Cluster herstellen. Je nach Klasse und Speicherort der DB-Instance kann es bis zu 20 Minuten dauern, bis der neue DB-Cluster verfügbar ist.

(Optional) Erstellen Sie eine VPC, eine EC2-Instanz und einen Aurora PostgreSQL-Cluster mit AWS CloudFormation

Anstatt die Konsole zum Erstellen Ihrer VPC, EC2-Instance und Ihres Aurora PostgreSQL-DB-Clusters AWS CloudFormation zu verwenden, können Sie AWS Ressourcen bereitstellen, indem Sie die Infrastruktur als Code behandeln. Um Ihnen zu helfen, Ihre AWS Ressourcen in kleinere und besser verwaltbare Einheiten zu organisieren, können Sie die Nested-Stack-Funktionalität verwenden. AWS CloudFormation Weitere Informationen finden Sie unter Einen Stack auf der AWS CloudFormation Konsole erstellen und Mit verschachtelten Stacks arbeiten.

> **Important**
>
> AWS CloudFormation ist kostenlos, aber die Ressourcen, die CloudFormation erstellt werden, sind live. Es fallen die üblichen Nutzungsgebühren für diese Ressourcen an, bis Sie sie kündigen. Die Gesamtgebühren sind minimal. Informationen darüber, wie Sie Gebühren minimieren können, finden Sie unter AWS Kostenloses Kontingent.

Gehen Sie wie folgt vor, um Ihre Ressourcen mithilfe der AWS CloudFormation Konsole zu erstellen:

- Schritt 1: Laden Sie die CloudFormation Vorlage herunter
- Schritt 2: Konfigurieren Sie Ihre Ressourcen mit CloudFormation

Laden Sie die CloudFormation Vorlage herunter

Eine CloudFormation Vorlage ist eine JSON- oder YAML-Textdatei, die die Konfigurationsinformationen zu den Ressourcen enthält, die Sie im Stack erstellen möchten. Diese Vorlage erstellt zusammen mit dem Aurora-Cluster auch eine VPC und einen Bastion-Host für Sie.

Um die Vorlagendatei herunterzuladen, öffnen Sie den folgenden Link: Aurora CloudFormation PostgreSQL-Vorlage.

Klicken Sie auf der Github-Seite auf die Schaltfläche Rohdatei herunterladen, um die YAML-Vorlagendatei zu speichern.

Konfigurieren Sie Ihre Ressourcen mit CloudFormation

> **Note**
>
> Bevor Sie diesen Vorgang starten, stellen Sie sicher, dass Sie ein Schlüsselpaar für eine EC2-Instance in Ihrem AWS-Konto haben. Weitere Informationen finden Sie unter Amazon-EC2-Schlüsselpaare und Linux-Instances.

Wenn Sie die AWS CloudFormation Vorlage verwenden, müssen Sie die richtigen Parameter auswählen, um sicherzustellen, dass Ihre Ressourcen ordnungsgemäß erstellt werden. Führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
2. Wählen Sie Stapel erstellen aus.
3. Wählen Sie im Abschnitt Vorlage angeben die Option Eine Vorlagendatei von Ihrem Computer hochladen und dann Weiter aus.
4. Legen Sie auf der Seite „Stack-Details angeben“ die folgenden Parameter fest:
   a. Setzen Sie den Stacknamen auf AurPostgreSQL TestStack.
   b. Legen Sie unter Parameter Availability Zones fest, indem Sie zwei Availability Zones auswählen.
   c. Wählen Sie unter Linux Bastion Host configuration für Key Name ein key pair aus, um sich bei Ihrer EC2-Instance anzumelden.
   d. Stellen Sie in den Linux Bastion Host-Konfigurationseinstellungen den zulässigen IP-Bereich auf Ihre IP-Adresse ein. Um mithilfe von Secure Shell (SSH) eine Verbindung zu EC2-Instances

in Ihrer VPC herzustellen, ermitteln Sie Ihre öffentliche IP-Adresse mithilfe des Dienstes unter https://checkip.amazonaws.com. Ein Beispiel für eine IP-Adresse ist 192.0.2.1/32.

> **Warning**
>
> Wenn Sie `0.0.0.0/0` für den SSH-Zugriff verwenden, ermöglichen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen EC2-Instances. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Für die Produktion sollten Sie nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre EC2-Instances autorisieren.

e. Stellen Sie unter Allgemeine Datenbankkonfiguration die Datenbankinstanzklasse auf db.t4g.large ein.

f. Setzen Sie den Datenbanknamen auf. **`database-test1`**

g. Geben Sie unter Datenbank-Master-Benutzername einen Namen für den Masterbenutzer ein.

h. Stellen Sie `false` für dieses Tutorial das DB-Master-Benutzerpasswort mit Secrets Manager verwalten auf ein.

i. Geben Sie für das Datenbankkennwort ein Passwort Ihrer Wahl ein. Merken Sie sich dieses Passwort für weitere Schritte im Tutorial.

j. Stellen Sie die Multi-AZ-Bereitstellung auf ein`false`.

k. Behalten Sie für alle anderen Einstellungen die Standardwerte bei. Klicken Sie auf Weiter, um fortzufahren.

5. Behalten Sie auf der Seite „Stack-Optionen konfigurieren“ alle Standardoptionen bei. Klicken Sie auf Weiter, um fortzufahren.
6. Wählen Sie auf der Seite „Stack überprüfen“ die Option Senden aus, nachdem Sie die Datenbank- und Linux-Bastion-Host-Optionen überprüft haben.

Sehen Sie sich nach Abschluss der Stack-Erstellung die Stacks mit Namen BastionStackund APGNS an, um die Informationen zu notieren, die Sie für die Verbindung mit der Datenbank benötigen. Weitere Informationen finden Sie unter AWS CloudFormation Stack-Daten und Ressourcen anzeigen auf der. AWS Management Console

Schritt 3: Herstellen einer Verbindung mit einem DB-Cluster von Aurora PostgreSQL

Sie können für die Verbindung mit dem DB-Cluster eine beliebige PostgreSQL-Client-Standardanwendung verwenden. In diesem Beispiel stellen Sie eine Verbindung mit einem DB-Cluster von Aurora PostgreSQL mithilfe des psql-Befehlszeilen-Clients her.

So stellen Sie eine Verbindung mit einem DB-Cluster von Aurora PostgreSQL her

1. Suchen Sie nach dem Endpunkt (DNS-Name) und der Portnummer der Writer-Instance für Ihren DB-Cluster.

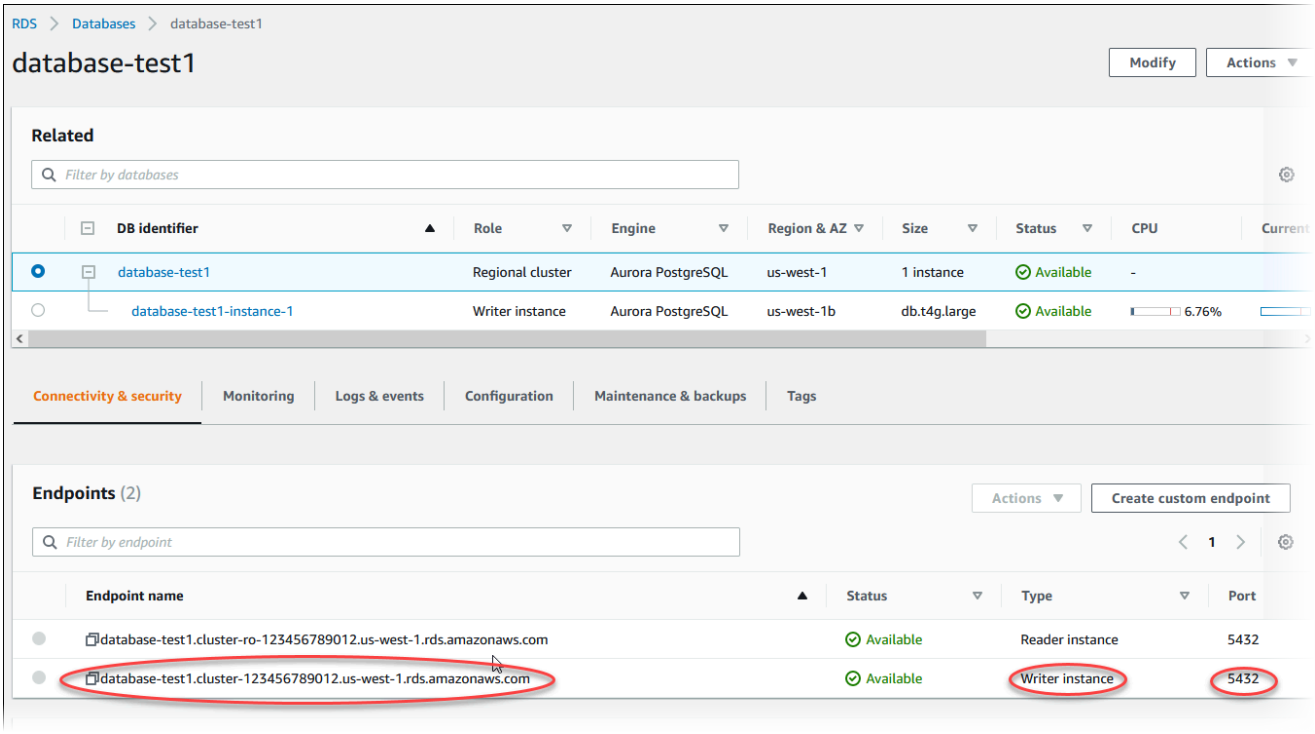
    a. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

    b. Wählen Sie in der oberen rechten Ecke der Amazon RDS-Konsole den AWS-Region für den DB-Cluster aus.

    c. Wählen Sie im Navigationsbereich Datenbanken aus.

    d. Wählen Sie den Namen des DB-Clusters von Aurora PostgreSQL aus, um dessen Details anzuzeigen.

    e. Kopieren Sie auf der Registerkarte Konnektivität und Sicherheit den Endpunkt der Writer-Instance. Notieren Sie sich auch die Portnummer. Sie benötigen sowohl den Endpunkt als auch die Portnummer, um die Verbindung mit dem DB-Cluster herzustellen.



2. Stellen Sie eine Verbindung zu der EC2-Instance her, die Sie zuvor erstellt haben, indem Sie den Schritten unter Connect to your Linux Instance im Amazon EC2 EC2-Benutzerhandbuch folgen.

   Wir empfehlen, dass Sie eine Verbindung mit Ihrer EC2-Instance mithilfe von SSH herstellen. Wenn das SSH-Client-Dienstprogramm unter Windows, Linux oder Mac installiert ist, können Sie mit dem folgenden Befehlsformat eine Verbindung mit der Instance herstellen:

   ```
   ssh -i location_of_pem_file ec2-user@ec2-instance-public-dns-name
   ```

   Nehmen wir zum Beispiel an, das `ec2-database-connect-key-pair.pem` in `/dir1` unter Linux gespeichert und das öffentliche IPv4-DNS für Ihre EC2-Instance `ec2-12-345-678-90.compute-1.amazonaws.com` ist. Ihr SSH-Befehl würde wie folgt aussehen:

   ```
   ssh -i /dir1/ec2-database-connect-key-pair.pem ec2-
   user@ec2-12-345-678-90.compute-1.amazonaws.com
   ```

3. Installieren Sie die neuesten Fehlerbehebungen und Sicherheitsupdates, indem Sie die Software auf Ihrer EC2-Instance aktualisieren. Führen Sie dazu den folgenden Befehl aus.

> **Note**
>
> Mit der Option `-y` werden die Updates installiert, ohne um Bestätigung zu bitten. Um Updates vor der Installation zu überprüfen, lassen Sie diese Option aus.

```
sudo dnf update -y
```

4. Installieren Sie den psql-Befehlszeilen-Client von PostgreSQL auf Amazon Linux 2023 mit dem folgenden Befehl:

```
sudo dnf install postgresql15
```

5. Stellen Sie eine Verbindung mit dem DB-Cluster von Aurora PostgreSQL her. Geben Sie z. B. den folgenden Befehl ein. Mit dieser Aktion können Sie mithilfe des psql-Clients eine Verbindung mit dem DB-Cluster von Aurora PostgreSQL herstellen.

   Ersetzen Sie den Endpunkt der Writer-Instance für *`endpoint`*, den Namen der Datenbank `--dbname`, mit der Sie eine Verbindung für *`postgres`* herstellen möchten, und den Hauptbenutzernamen, den Sie für *`postgres`* verwendet haben. Geben Sie das Master-Passwort ein, das Sie bei der Aufforderung zur Eingabe eines Passworts verwendet haben.

```
psql --host=endpoint --port=5432 --dbname=postgres --username=postgres
```

   Nachdem Sie das Passwort für den Benutzer eingegeben haben, sollte eine Ausgabe wie die folgende angezeigt werden.

```
psql (14.3, server 14.6)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256,
 compression: off)
Type "help" for help.

postgres=>
```

   Weitere Informationen zum Herstellen einer Verbindung mit einem DB-Cluster von Aurora PostgreSQL finden Sie unter Herstellen einer Verbindung mit einem Amazon-Aurora-PostgreSQL-DB-Cluster. Wenn Sie sich nicht mit Ihrem DB-Cluster verbinden können, erhalten Sie unter Verbindung zur Amazon RDS-DB-Instance kann nicht hergestellt werden Hilfe.

Aus Sicherheitsgründen empfiehlt es sich, verschlüsselte Verbindungen zu verwenden. Verwenden Sie eine unverschlüsselte PostgreSQL-Verbindung nur, wenn sich Client und Server in derselben VPC befinden und das Netzwerk vertrauenswürdig ist. Weitere IInformationen zur Verwendung verschlüsselter Verbindungen finden Sie unter Sicherung von Aurora-PostgreSQL-Daten mit SSL/TLS.

6. SQL-Befehle ausführen

   Der folgende SQL-Befehl zeigt z B. das aktuelle Datum und die aktuelle Zeit an:

   ```
   SELECT CURRENT_TIMESTAMP;
   ```

Schritt 4: Löschen der EC2-Instance und des DB-Clusters

Nachdem Sie eine Verbindung mit der Beispiel-EC2-Instance und dem DB-Cluster, die Sie erstellt haben, hergestellt und diese erkundet haben, löschen Sie sie, damit Ihnen dafür keine weiteren Kosten entstehen.

Wenn Sie früher AWS CloudFormation Ressourcen erstellt haben, überspringen Sie diesen Schritt und fahren Sie mit dem nächsten Schritt fort.

So löschen Sie die EC2-Instance

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die EC2- Instance aus, und wählen Sie Instance-Status, Instance beenden.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.

Weitere Informationen zum Löschen einer EC2-Instance finden Sie unter Terminate your Instance im Amazon EC2 EC2-Benutzerhandbuch.

So löschen Sie einen DB-Cluster

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie Databases (Datenbanken) und anschließend die DB-Instance aus, die mit dem DB-Cluster verknüpft ist.
3. Klicken Sie bei Actions auf Delete.
4. Wählen Sie Delete (Löschen).

   Wenn alle mit einem DB-Cluster verknüpften DB-Instances gelöscht sind, wird der DB-Cluster automatisch gelöscht.

(Optional) Löschen Sie die EC2-Instance und den DB-Cluster, die mit erstellt wurden CloudFormation

Wenn Sie früher AWS CloudFormation Ressourcen erstellt haben, löschen Sie den CloudFormation Stack, nachdem Sie sich mit der EC2-Beispiel-Instance und dem DB-Cluster verbunden und diese erkundet haben, sodass Ihnen diese nicht mehr in Rechnung gestellt werden.

Um die Ressourcen zu löschen CloudFormation

1. Öffnen Sie die AWS CloudFormation Konsole.
2. Wählen Sie auf der Seite Stacks in der CloudFormation Konsole den Root-Stack aus (den Stack ohne den Namen VPCStack BastionStack oder APGNS).
3. Wählen Sie Löschen aus.
4. Wählen Sie Stack löschen aus, wenn Sie zur Bestätigung aufgefordert werden.

Weitere Informationen zum Löschen eines Stacks in CloudFormation finden Sie im AWS CloudFormation Benutzerhandbuch unter Löschen eines Stacks auf der AWS CloudFormation Konsole.

(Optional) Verbinden Sie Ihren DB-Cluster mit einer Lambda-Funktion

Sie können Ihren Aurora PostgreSQL-DB-Cluster auch mit einer serverlosen Lambda-Rechenressource verbinden. Mit Lambda-Funktionen können Sie Code ausführen, ohne die Infrastruktur bereitstellen oder verwalten zu müssen. Eine Lambda-Funktion ermöglicht es Ihnen auch, automatisch auf Codeausführungsanfragen jeder Größenordnung zu reagieren, von einem Dutzend Ereignissen pro Tag bis hin zu Hunderten von Ereignissen pro Sekunde. Weitere Informationen finden Sie unter Automatisches Verbinden einer Lambda-Funktion mit einem Aurora-DB-Cluster.

Tutorial: Erstellen eines Webservers und einer eines Amazon Aurora-DB-Clusters

Dieses Tutorial veranschaulicht, wie Sie einen Apache-Webserver mit PHP installieren und eine MariaDB-, MySQL- oder PostgreSQL-Datenbank erstellen. Der Webserver wird auf einer Amazon-EC2-Instance unter Verwendung von Amazon Linux 2023 ausgeführt und Sie können zwischen einem Aurora-MySQL- oder Aurora-PostgreSQL-DB-Cluster wählen. Die Amazon EC2-Instance und die / der DB-Cluster werden beide in einer virtuellen privaten Cloud (VPC) auf der Basis des Amazon VPC-Service ausgeführt.

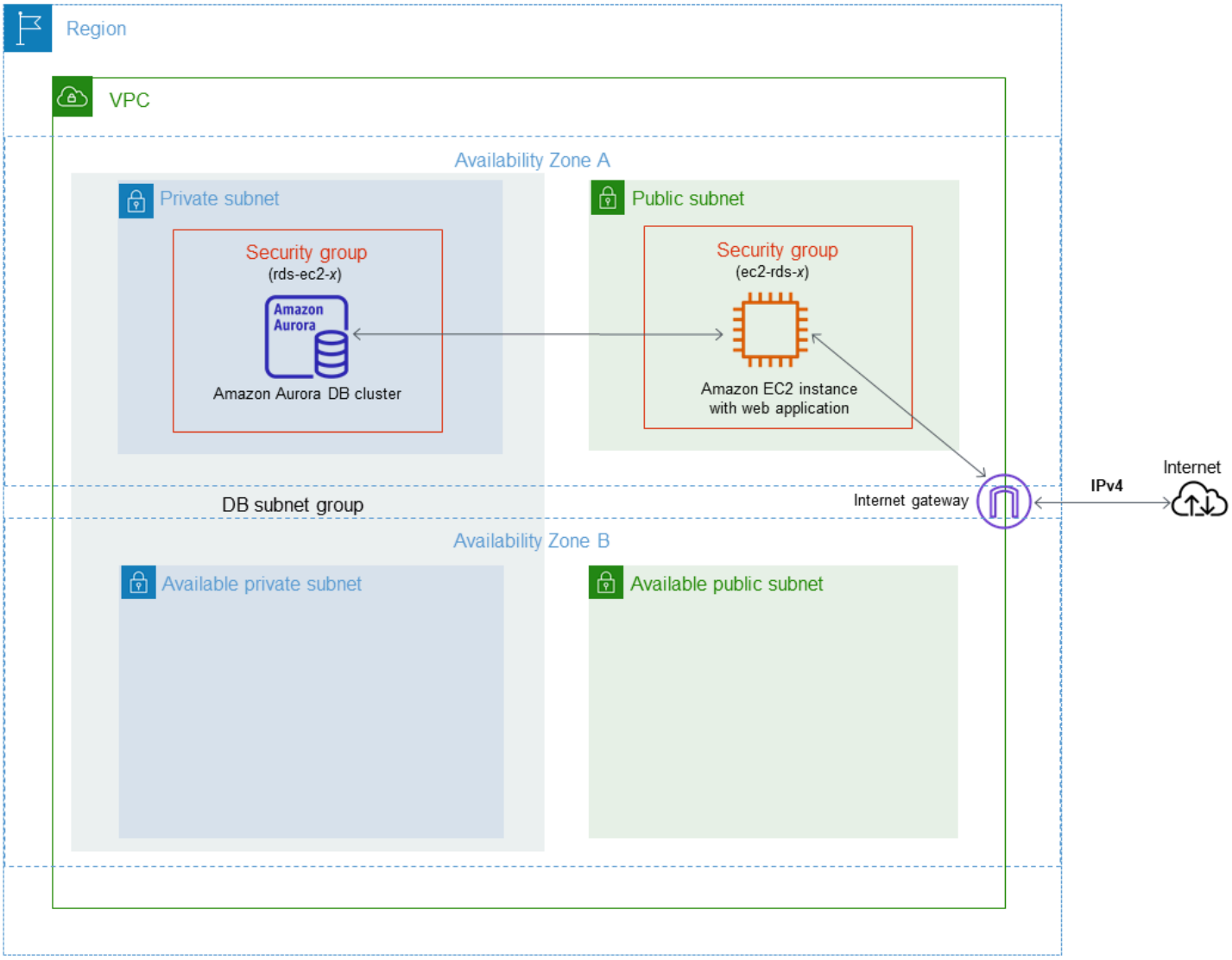
> **Important**
>
> Die Einrichtung eines AWS-Kontos ist kostenlos. Bei Durchführung dieses Tutorials können jedoch Kosten für die von Ihnen verwendeten AWS-Ressourcen anfallen. Sie können diese Ressourcen nach Abschluss des Tutorials löschen, wenn sie nicht mehr benötigt werden.

> **Note**
>
> Dieses Tutorial funktioniert mit Amazon Linux 2023 und möglicherweise nicht mit anderen Linux-Versionen.

Im folgenden Tutorial erstellen Sie eine EC2-Instance, die die Standard-VPC, Subnetze und die Sicherheitsgruppe für Ihr AWS-Konto verwendet. In diesem Tutorial erhalten Sie Informationen zum Erstellen des DB-Clusters und richten die Verbindung mit der EC2-Instance, die Sie erstellt haben, automatisch ein. Das Tutorial zeigt Ihnen dann, wie Sie den Webserver auf der EC2-Instance installieren. Sie verbinden Ihren Webserver in der VPC mit Ihrem DB-Cluster in der VPC mithilfe des DB-Cluster-Writer-Endpunkts.

1. Starten einer EC2-Instance
2. Erstellen eines Amazon Aurora-DB-Clusters
3. Installieren eines Webservers auf Ihrer EC2-Instance

Das folgende Diagramm zeigt die Konfiguration nach Abschluss des Tutorials.



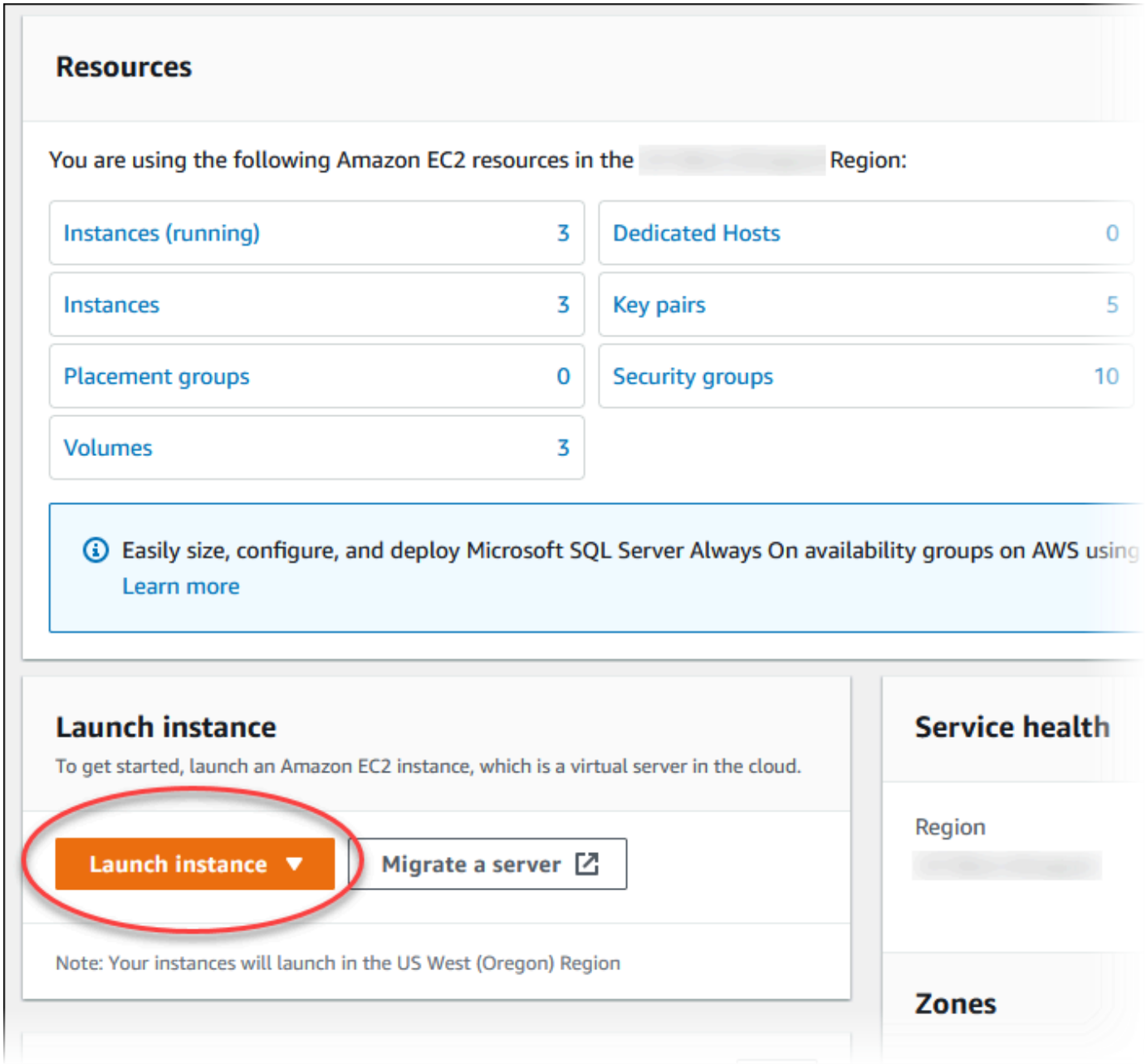
> **Note**
>
> Nach Abschluss des Tutorials gibt es in jeder Availability Zone im VPC ein öffentliches und ein privates Subnetz. Dieses Tutorial verwendet die Standard-VPC für Ihr AWS-Kontound richtet automatisch die Verbindung zwischen Ihrer EC2-Instance und dem DB-Cluster ein. Wenn Sie stattdessen lieber eine neue VPC für dieses Szenario konfigurieren möchten, führen Sie die Aufgaben in Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4) aus.

Starten einer EC2-Instance

Erstellen Sie im öffentlichen Subnetz Ihrer VPC eine Amazon-EC2-Instance.

Starten Sie EC2-Instances wie folgt:

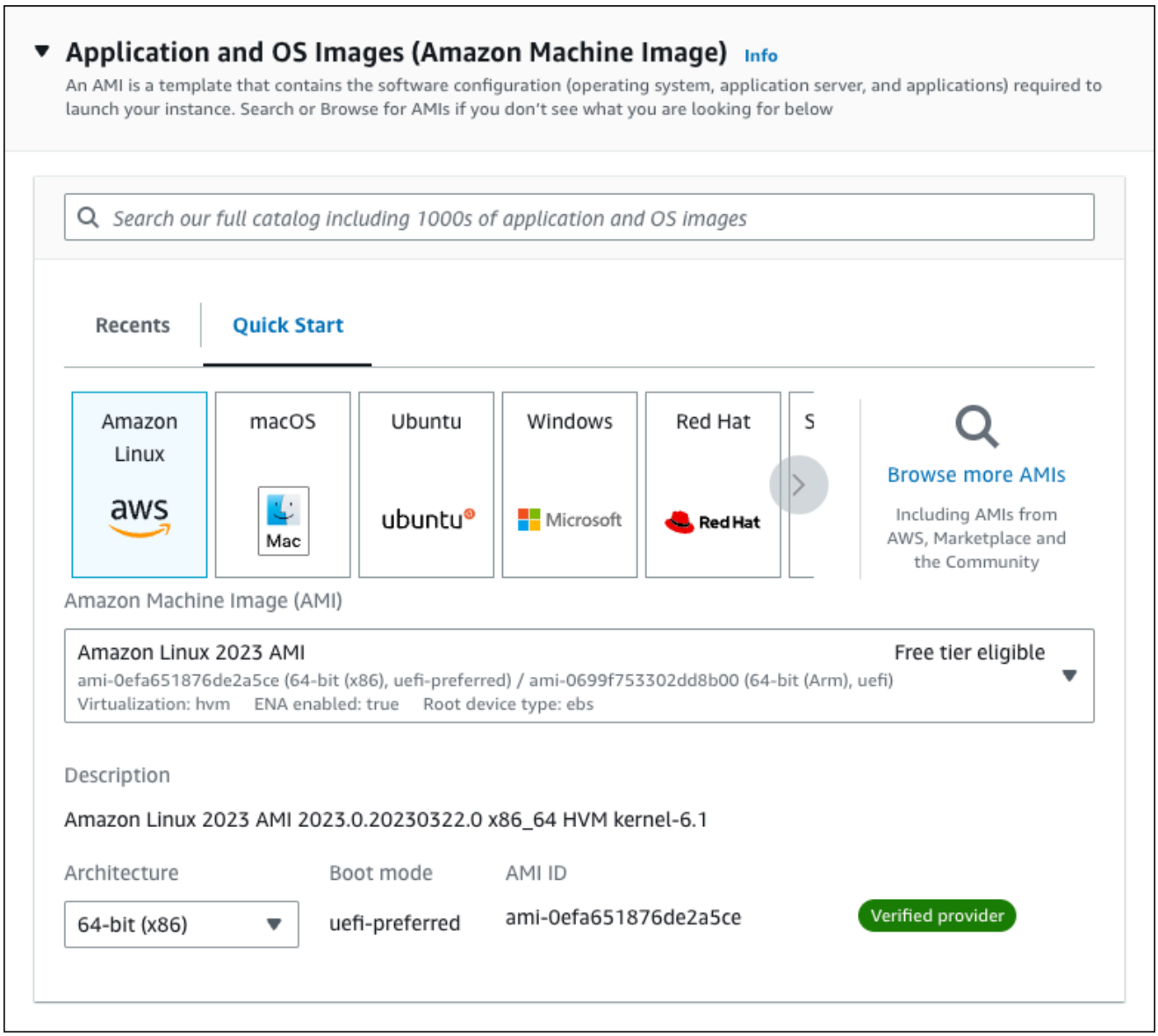
1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der oberen rechten Ecke von den aus AWS Management Console, AWS-Region wo Sie die EC2-Instance erstellen möchten.
3. Wählen Sie EC2-Dashboard und anschließend Instance starten wie im Folgenden gezeigt.



4. Wählen Sie auf der Seite Eine Instance starten die folgenden Einstellungen aus.

   a. Geben Sie unter Name and tags (Name und Tags) als Name den Namen **`tutorial-ec2-instance-web-server`** ein.

   b. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Amazon Linux und dann die Registerkarte Amazon Linux 2023 AMI aus. Übernehmen Sie für alle anderen Einstellungen die Standardwerte.



c. Wählen Sie unter Instance type (Instance-Typ) den Wert t2.micro aus.

d. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) einen Key pair name (Schlüsselpaarname), um ein vorhandenes Schlüsselpaar zu verwenden. Wenn Sie ein neues Schlüsselpaar für die Amazon-EC2-Instance erstellen möchten, wählen Sie Create new key pair (Neues Schlüsselpaar erstellen) aus und erstellen sie das Schlüsselpaar im Fenster Create key pair (Schlüsselpaar erstellen).

   Weitere Informationen zum Erstellen eines neuen Schlüsselpaars finden Sie unter Create a key pair im Amazon EC2 EC2-Benutzerhandbuch.

e. Legen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Werte fest und übernehmen Sie für die anderen Einstellungen die Standardwerte:

- Wählen Sie für Allow SSH traffic from (SSH-Verkehr zulassen von) die Quelle von SSH-Verbindungen mit der EC2-Instance aus.

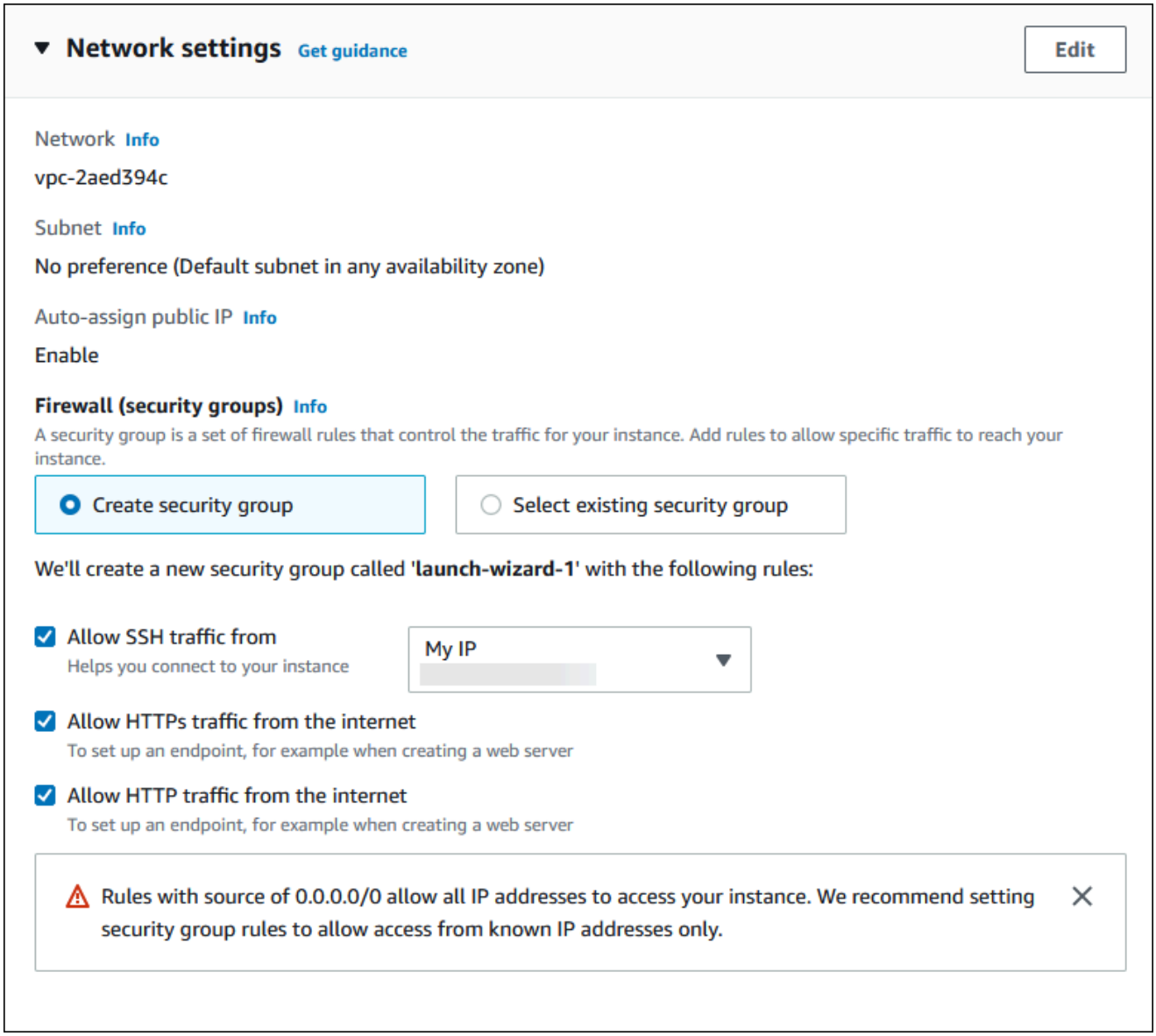
  Sie können My IP (Meine IP) auswählen, wenn die angezeigte IP-Adresse für SSH-Verbindungen korrekt ist.

  Andernfalls können Sie die IP-Adresse, die für die Verbindung mit EC2-Instances in Ihrer VPC verwendet werden soll, mit Secure Shell (SSH) ermitteln. Um Ihre öffentliche IP-Adresse zu ermitteln, können Sie in einem anderen Browserfenster oder einer anderen Registerkarte den Service unter https://checkip.amazonaws.com verwenden. Ein Beispiel für eine IP-Adresse ist `203.0.113.25/32`.

  In vielen Fällen können Sie eine Verbindung über einen Internetdienstanbieter (ISP) oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen. Bestimmen Sie in diesem Fall den Bereich der IP-Adressen, die von Client-Computern verwendet werden.

  > **Warning**
  >
  > Wenn Sie `0.0.0.0/0` für SSH-Zugriff verwenden, ermöglichen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen Instances. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Für die Produktion wird nur eine bestimmte IP-Adresse bzw. ein bestimmter Adressbereich für den Zugriff auf Ihre Instances autorisiert.

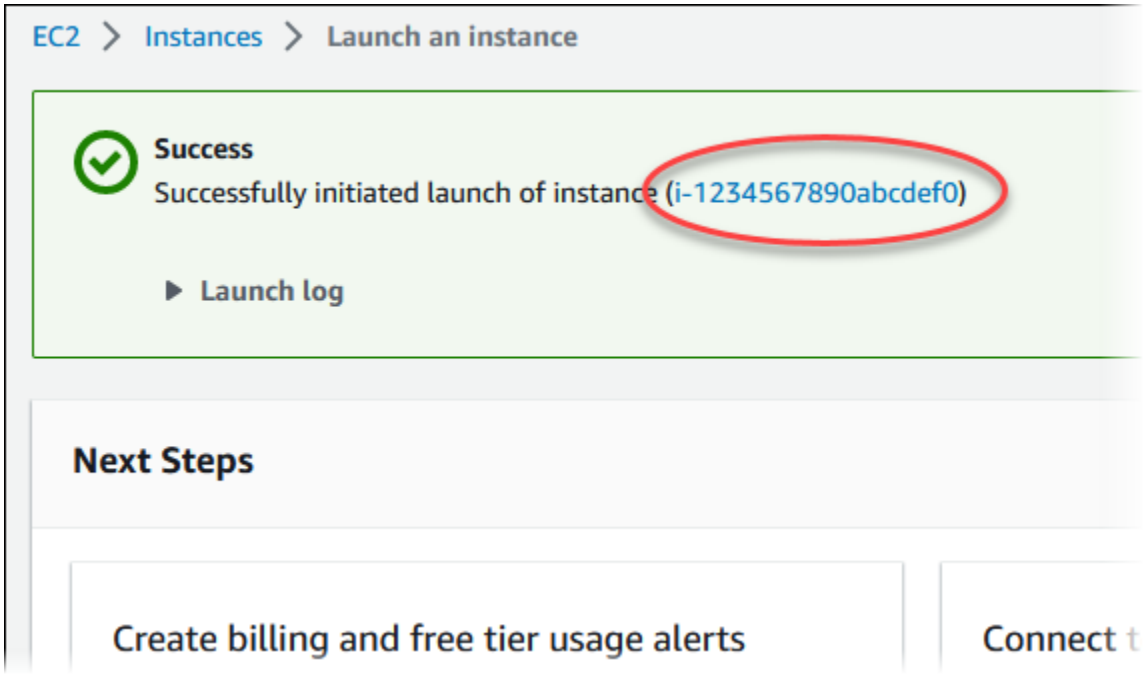
- Aktivieren Sie Allow HTTPs traffic from the internet (HTTPs-Verkehr aus dem Internet zulassen).
- Aktivieren Sie Allow HTTP traffic from the internet (HTTP-Verkehr aus dem Internet zulassen).



f. Übernehmen Sie die Standardwerte für die übrigen Abschnitte.

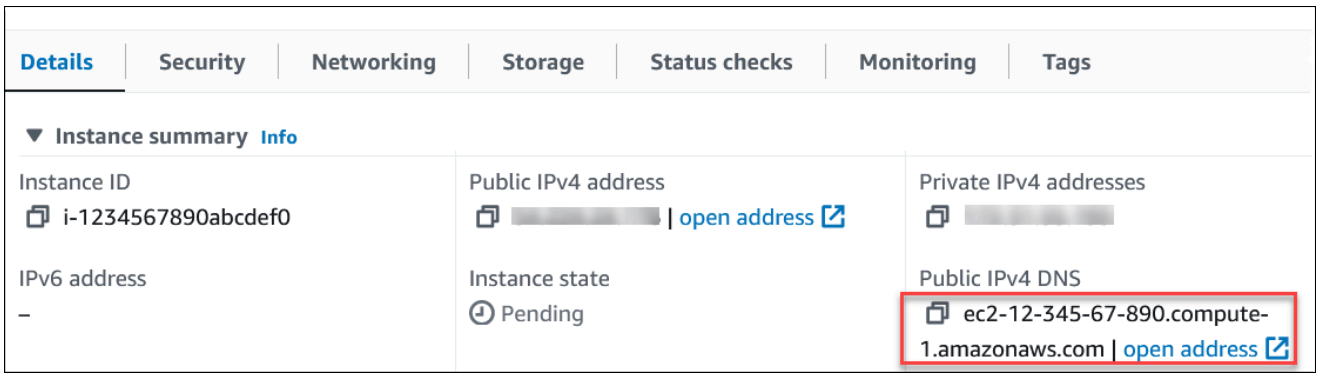
g. Überprüfen Sie Ihre Instance-Konfiguration im Bereich Summary (Übersicht). Wenn alles in Ordnung ist, klicken Sie auf Launch instance (Instance starten).

5. Notieren Sie auf der im Folgenden gezeigten Seite Startstatus die Kennung für die neue EC2-Instance, beispielsweise: `i-1234567890abcdef0`.

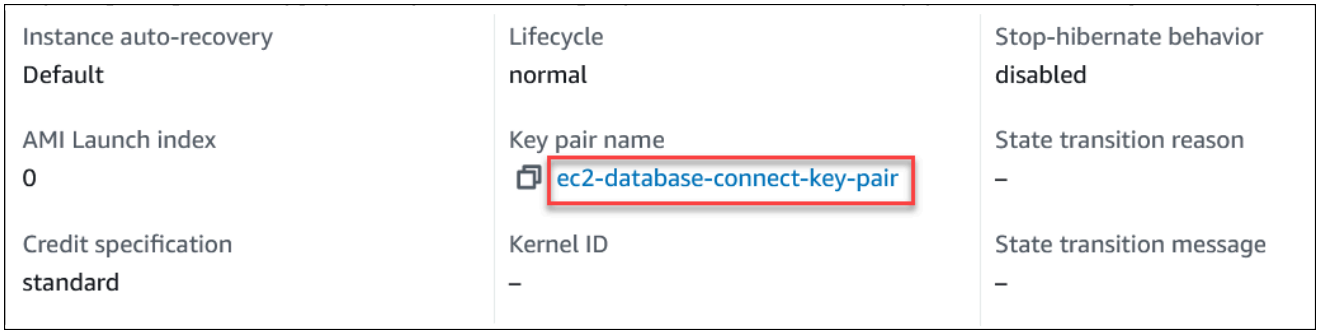


6. Wählen Sie die EC2-Instance-Kennung aus, um die Liste der EC2-Instances zu öffnen. Wählen Sie dann Ihre EC2-Instance aus.
7. Notieren Sie sich die folgenden Werte auf der Registerkarte Details. Diese benötigen Sie, wenn Sie eine Verbindung über SSH herstellen:

   a. Notieren Sie sich unter Instance-Zusammenfassung den Wert für Public IPv4 DNS.



   b. Notieren Sie sich unter Instance-Details den Wert für Schlüsselpaarname.



8. Warten Sie, bis der Instance state (Instance-Status) für Ihre Instance als Running (Wird ausgeführt) angezeigt wird, bevor Sie fortfahren.
9. Schließen Sie Erstellen eines Amazon Aurora-DB-Clusters ab.

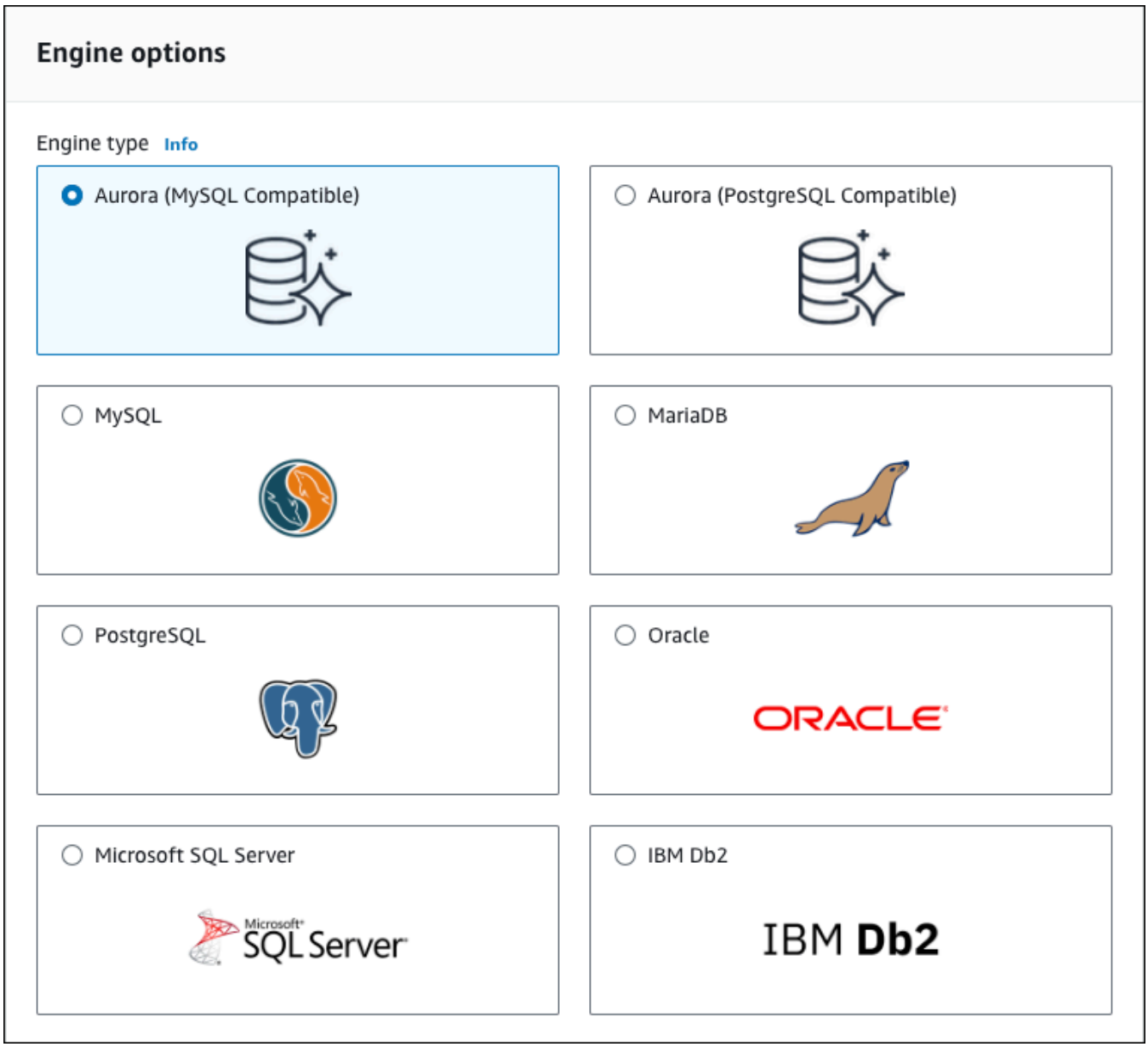
Erstellen eines Amazon Aurora-DB-Clusters

Erstellen eines DB-Clusters von Amazon Aurora MySQL oder Aurora PostgreSQL, der die von einer Webanwendung verwendeten Daten enthält.

Aurora MySQL

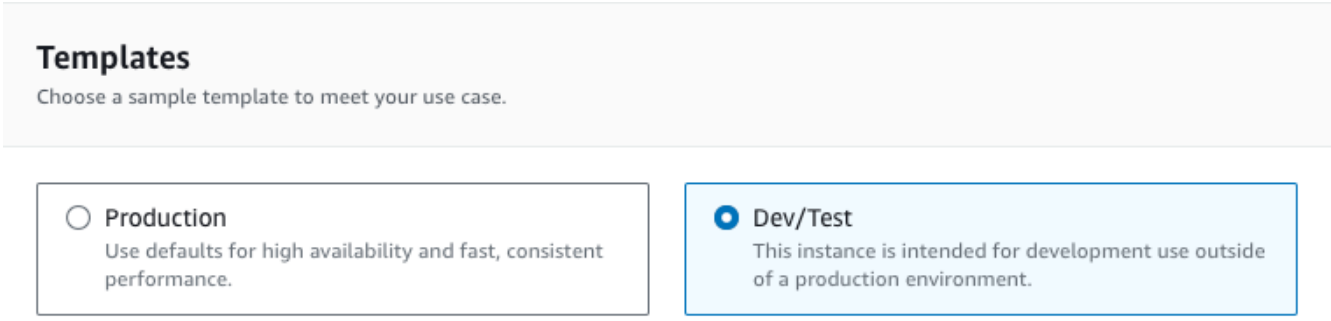
Erstellen eines Aurora MySQL-DB-Clusters

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Vergewissern Sie sich, dass in der oberen rechten Ecke desAWS Management Console derselbe AWS-Region steht wie der, an dem Sie Ihre EC2-Instance erstellt haben.
3. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
4. Wählen Sie Create database (Datenbank erstellen) aus.
5. Wählen Sie auf der Seite Datenbank erstellen die Option Standarderstellung aus.
6. Wählen Sie unter Engine-Optionen die Option Aurora (MySQL-kompatibel) aus.



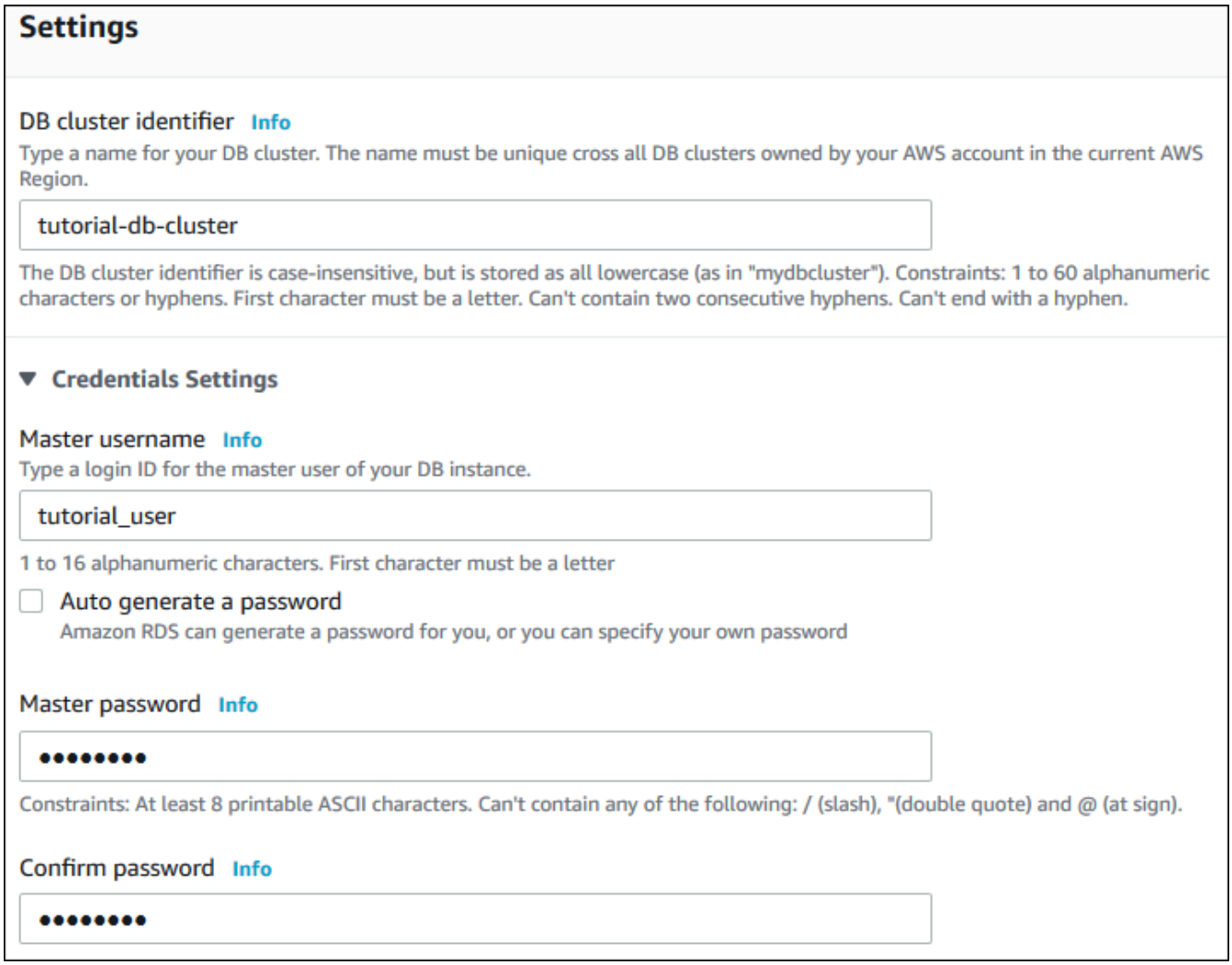
Behalten Sie die Standardwerte für Version und die anderen Engine-Optionen bei.

7. Wählen Sie unter Templates (Vorlagen) die Option Dev/Test (Entwicklung/Testing).



8. Legen Sie im Abschnitt Settings (Einstellungen) die folgenden Werte fest:

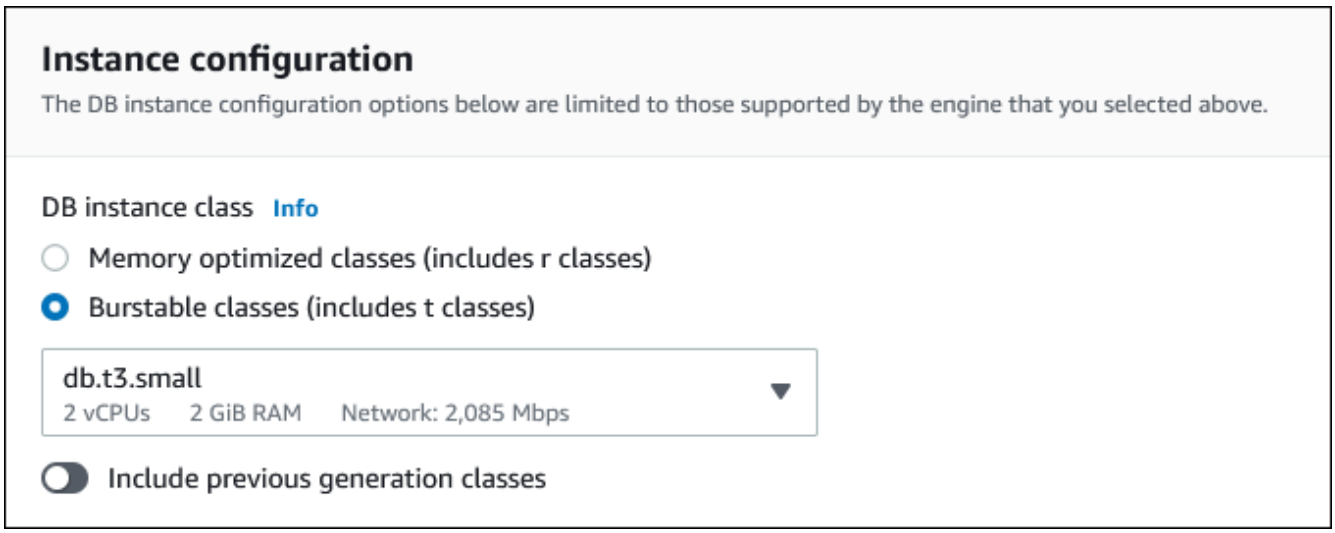
   - DB cluster identifier (DB-Cluster-Kennung) – Geben Sie **`tutorial-db-cluster`** ein.
   - Master username (Masterbenutzername) – Typ **`tutorial_user`**.
   - Automatisch ein Passwort generieren - Lassen Sie die Option ausgeschaltet.
   - Master-Passwort - Geben Sie ein Passwort ein.
   - Confirm password (Passwort bestätigen): Geben Sie das Passwort erneut ein.



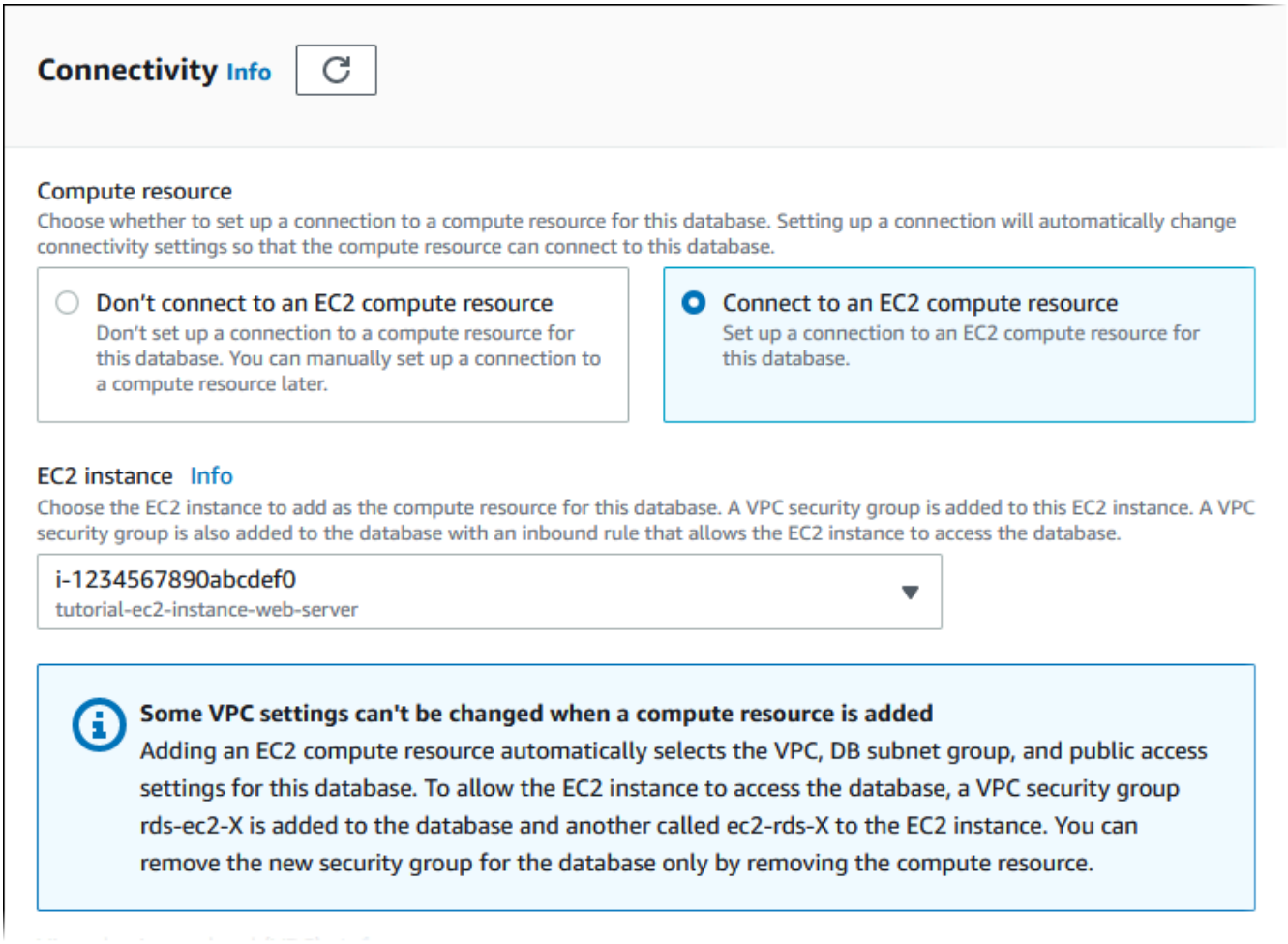
9. Legen Sie im Abschnitt Instance Configuration folgende Werte fest:

   - Burst-fähige Klassen (einschließlich t-Klassen)
   - db.t3.small oder db.t3.medium

> **Note**
>
> Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter DB-Instance-Klassenarten.

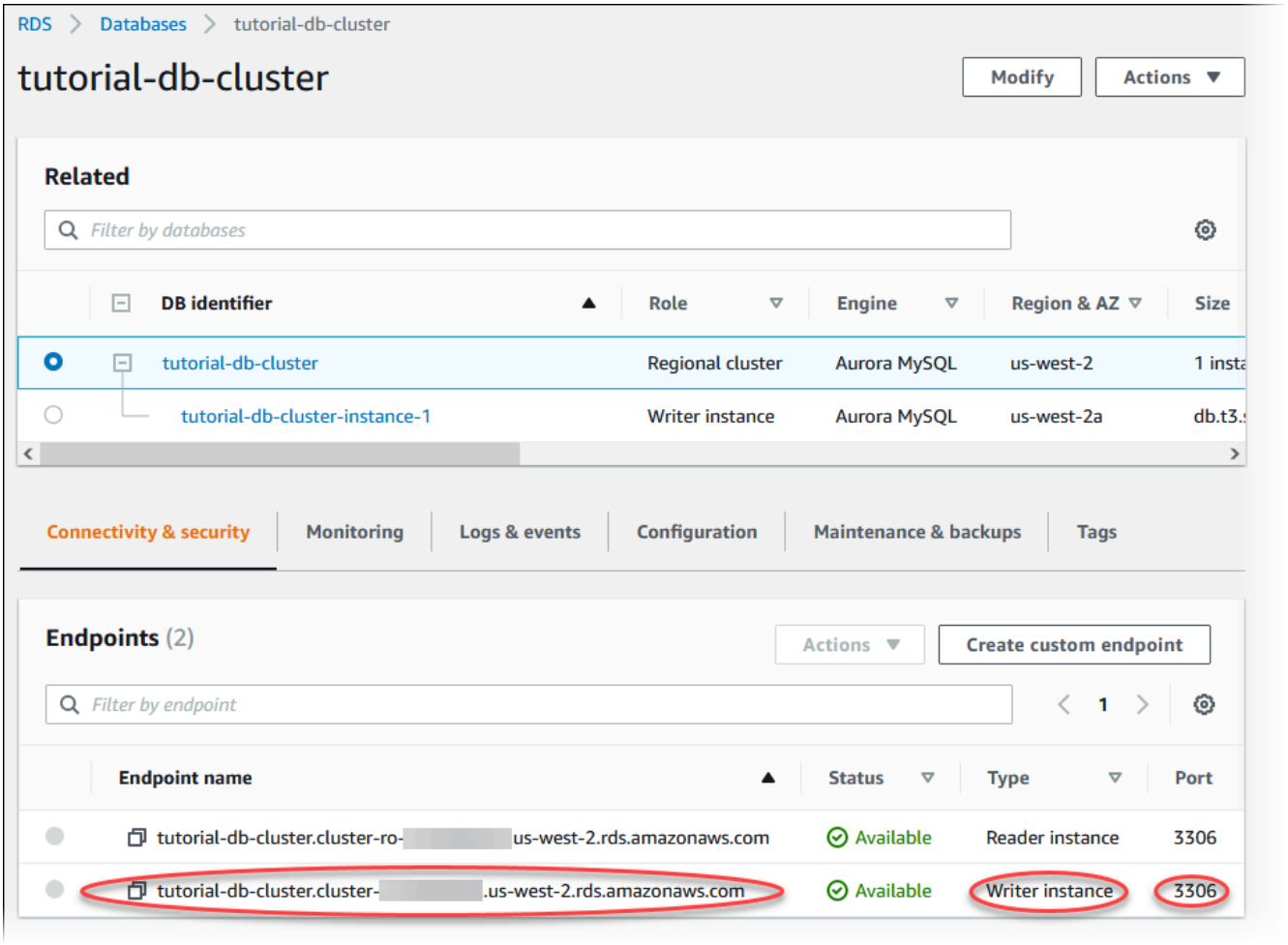


10. Verwenden Sie im Abschnitt Availability and durability (Verfügbarkeit und Beständigkeit) die Standardwerte.
11. Legen Sie im Abschnitt Connectivity (Konnektivität) die folgenden Werte fest und übernehmen Sie für die anderen Einstellungen die Standardwerte:
    - Wählen Sie unter Compute-Ressource die Option Connect to an EC2 compute resource (Verbinden mit einer EC2 Compute-Ressource).
    - Wählen Sie für EC2-Instance die EC2-Instance aus, die Sie zuvor erstellt haben, z. B.tutorial-ec2-instance-web-serveraus.



12. Öffnen Sie den Abschnitt Additional configuration (Zusätzliche Konfiguration) und geben Sie **`sample`** für Initial database name (Erster Datenbankname) ein. Behalten Sie für die anderen Optionen die Standardeinstellungen bei.
13. Zum Erstellen Ihres Aurora MySQL-DB-Clusters wählen Sie Create database (Datenbank erstellen).

    Ihr neuer DB-Cluster wird in der Liste Databases (Datenbanken) mit dem Status Creating (Wird erstellt) angezeigt.
14. Warten Sie, bis der Status Ihres neuen DB-Clusters als Available (Verfügbar) angezeigt wird. Wählen Sie dann den Namen des DB-Clusters aus, um dessen Details anzuzeigen.
15. Zeigen Sie im Abschnitt Connectivity & security (Konnektivität und Sicherheit) den Endpoint (Endpunkt) und den Port der DB-Writer-Instance an.



Notieren Sie den Endpunkt und den Port Ihrer DB-Writer-Instance. Sie verwenden diese Informationen, um Ihren Webserver mit Ihrem DB-Cluster zu verbinden.

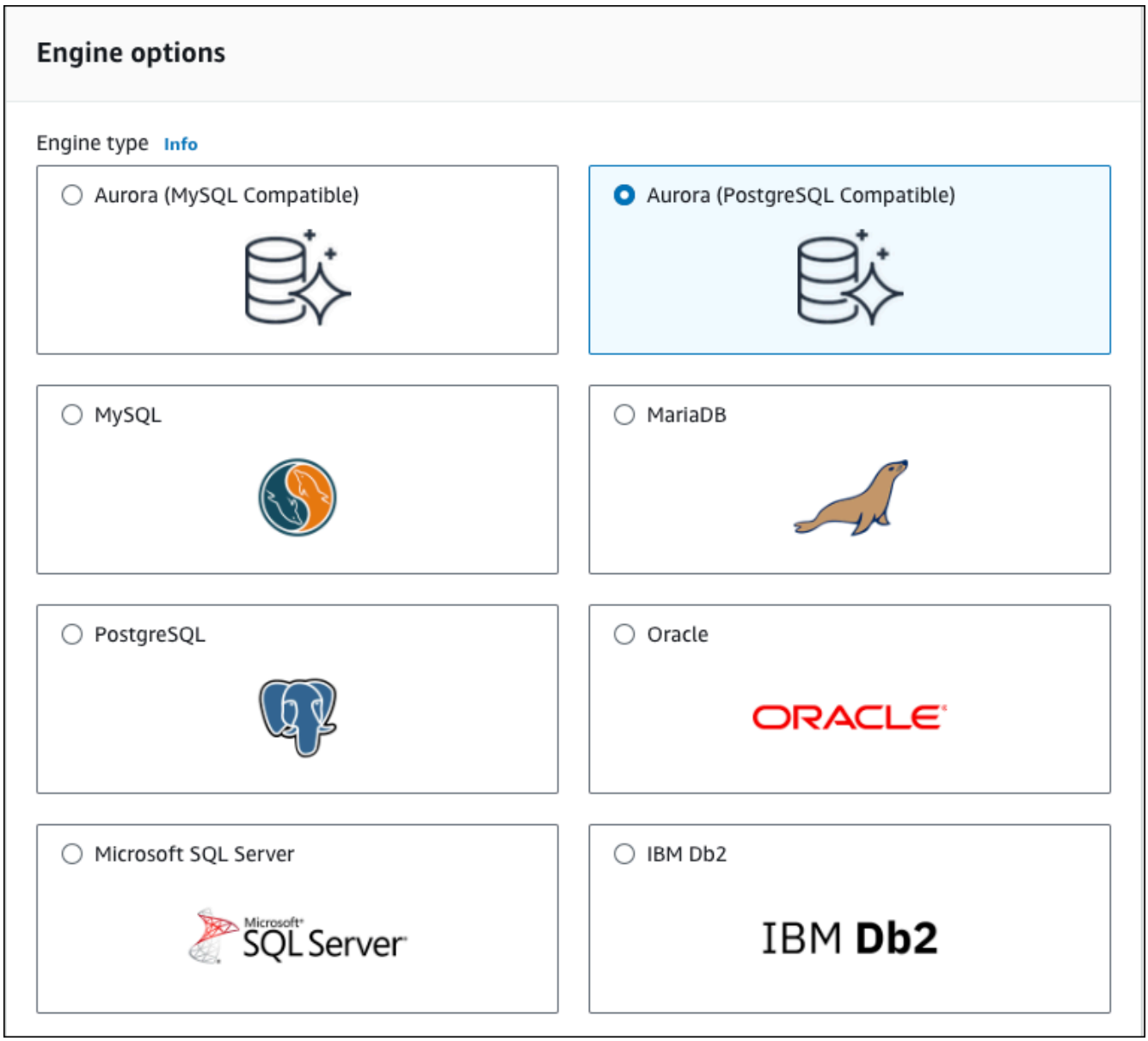
16. Schließen Sie Installieren eines Webservers auf Ihrer EC2-Instance ab.

Aurora PostgreSQL

Erstellen eines Aurora PostgreSQL-DB-Clusters

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Vergewissern Sie sich, dass in der oberen rechten Ecke desAWS Management Console derselbe AWS-Region steht wie der, an dem Sie Ihre EC2-Instance erstellt haben.
3. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
4. Wählen Sie Create database (Datenbank erstellen) aus.

5. Wählen Sie auf der Seite Datenbank erstellen die Option Standarderstellung aus.
6. Wählen Sie unter Engine-Optionen Aurora (PostgreSQL-kompatibel).

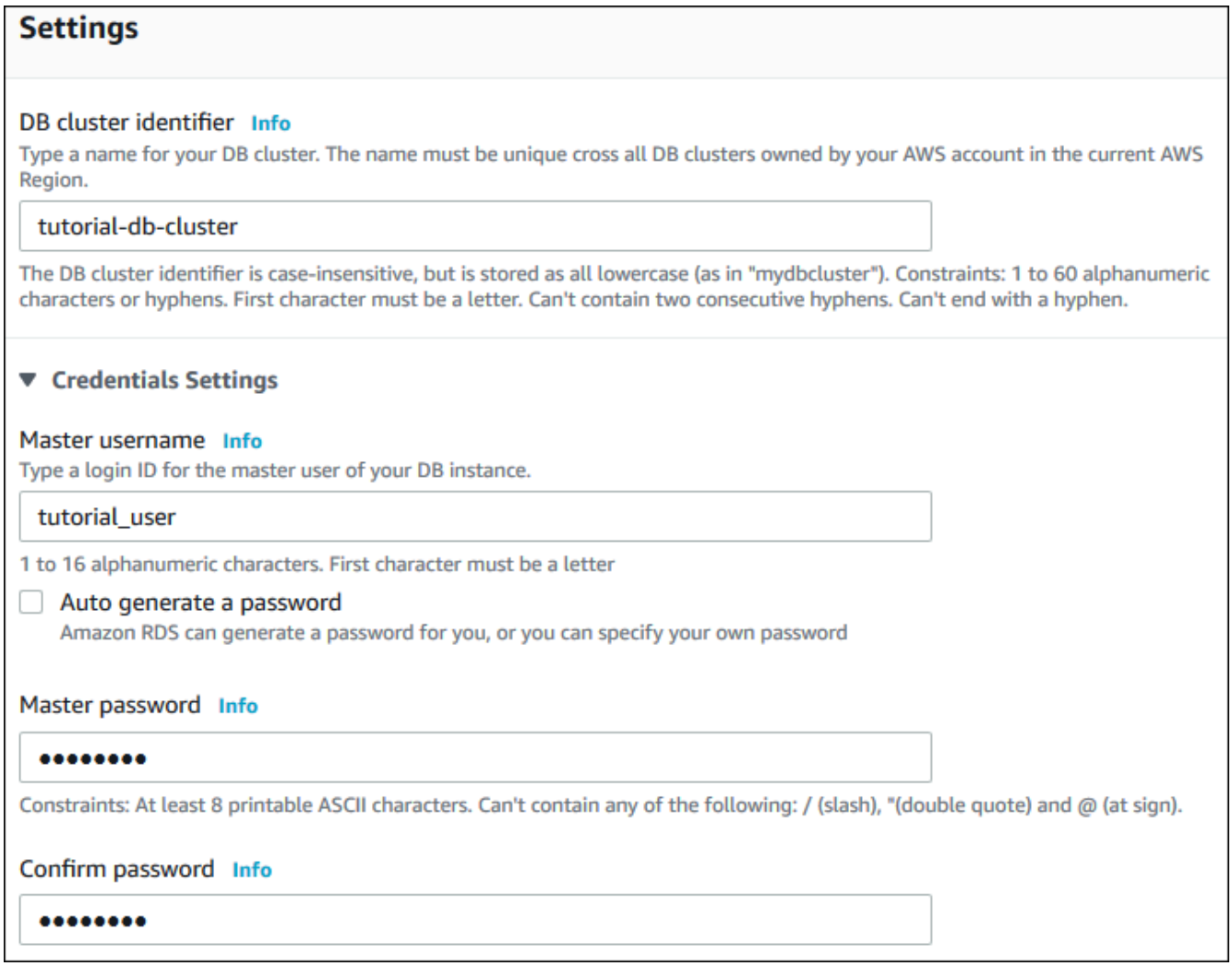


Behalten Sie die Standardwerte für Version und die anderen Engine-Optionen bei.

7. Wählen Sie unter Templates (Vorlagen) die Option Dev/Test (Entwicklung/Testing).

8. Legen Sie im Abschnitt Settings (Einstellungen) die folgenden Werte fest:

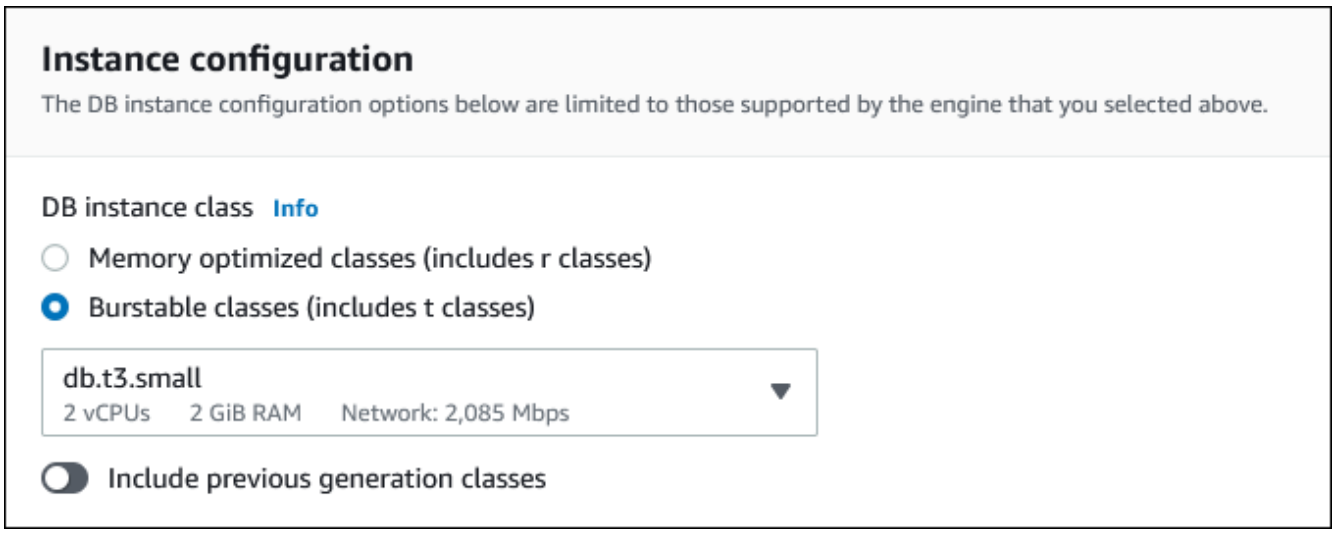
   - DB cluster identifier (DB-Cluster-Kennung) – Geben Sie **`tutorial-db-cluster`** ein.
   - Master username (Masterbenutzername) – Typ **`tutorial_user`**.
   - Automatisch ein Passwort generieren - Lassen Sie die Option ausgeschaltet.
   - Master-Passwort - Geben Sie ein Passwort ein.
   - Confirm password (Passwort bestätigen): Geben Sie das Passwort erneut ein.



9. Legen Sie im Abschnitt Instance Configuration folgende Werte fest:

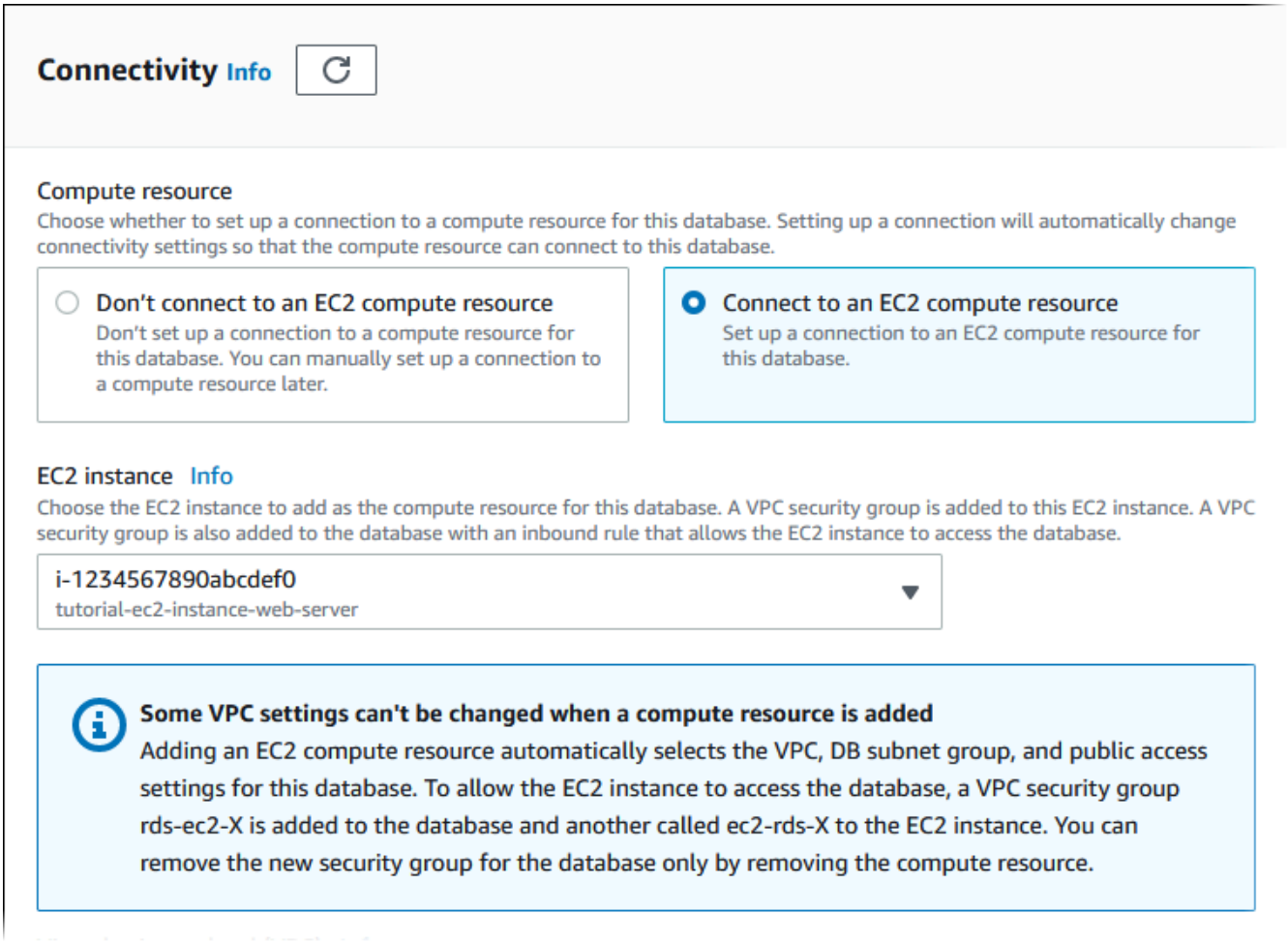
   - Burst-fähige Klassen (einschließlich t-Klassen)
   - db.t3.small oder db.t3.medium

   > **Note**
   >
   > Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter DB-Instance-Klassenarten.



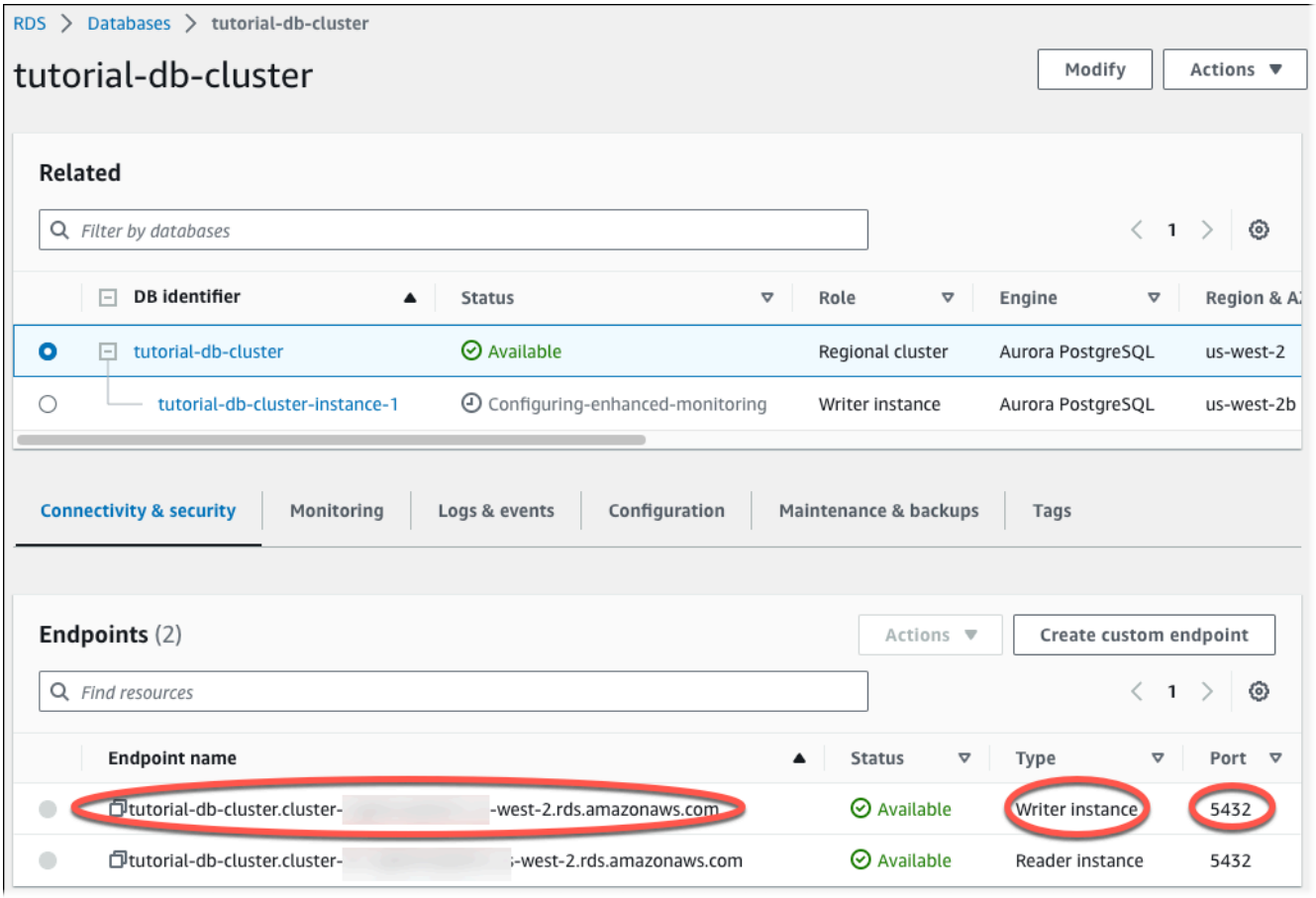
10. Verwenden Sie im Abschnitt Availability and durability (Verfügbarkeit und Beständigkeit) die Standardwerte.
11. Legen Sie im Abschnitt Connectivity (Konnektivität) die folgenden Werte fest und übernehmen Sie für die anderen Einstellungen die Standardwerte:

    - Wählen Sie unter Compute-Ressource die Option Connect to an EC2 compute resource (Verbinden mit einer EC2 Compute-Ressource).
    - Wählen Sie für EC2-Instance die EC2-Instance aus, die Sie zuvor erstellt haben, z. B.tutorial-ec2-instance-web-serveraus.



12. Öffnen Sie den Abschnitt Additional configuration (Zusätzliche Konfiguration) und geben Sie **`sample`** für Initial database name (Erster Datenbankname) ein. Behalten Sie für die anderen Optionen die Standardeinstellungen bei.
13. Zum Erstellen Ihres Aurora PostgreSQL-DB-Clusters wählen Sie Datenbank erstellen.

    Ihr neuer DB-Cluster wird in der Liste Databases (Datenbanken) mit dem Status Creating (Wird erstellt) angezeigt.
14. Warten Sie, bis der Status Ihres neuen DB-Clusters als Available (Verfügbar) angezeigt wird. Wählen Sie dann den Namen des DB-Clusters aus, um dessen Details anzuzeigen.
15. Zeigen Sie im Abschnitt Connectivity & security (Konnektivität und Sicherheit) den Endpoint (Endpunkt) und den Port der DB-Writer-Instance an.



Notieren Sie den Endpunkt und den Port Ihrer DB-Writer-Instance. Sie verwenden diese Informationen, um Ihren Webserver mit Ihrem DB-Cluster zu verbinden.

16. Schließen Sie a Installieren eines Webservers auf Ihrer EC2-Instance.

Installieren eines Webservers auf Ihrer EC2-Instance

Installieren Sie einen Webserver auf der EC2-Instance, die Sie in Starten einer EC2-Instance erstellt haben. Der Webserver verbindet sich mit dem DB-Cluster von Amazon Aurora, den Sie in Erstellen eines Amazon Aurora-DB-Clusters erstellt haben.

Installieren eines Apache-Webservers mit PHP und MariaDB

Stellen Sie eine Verbindung mit Ihrer EC2-Instance her und installieren Sie den Webserver.

So stellen Sie eine Verbindung mit Ihrer EC2-Instance her und installieren den Apache-Webserver mit PHP

1. Stellen Sie eine Verbindung zu der EC2-Instance her, die Sie zuvor erstellt haben, indem Sie den Schritten unter Connect to your Linux Instance im Amazon EC2 EC2-Benutzerhandbuch folgen.

   Wir empfehlen, dass Sie eine Verbindung mit Ihrer EC2-Instance mithilfe von SSH herstellen. Wenn das SSH-Client-Dienstprogramm unter Windows, Linux oder Mac installiert ist, können Sie mit dem folgenden Befehlsformat eine Verbindung mit der Instance herstellen:

   ```
   ssh -i location_of_pem_file ec2-user@ec2-instance-public-dns-name
   ```

   Nehmen wir zum Beispiel an, das `ec2-database-connect-key-pair.pem` in `/dir1` unter Linux gespeichert und das öffentliche IPv4-DNS für Ihre EC2-Instance `ec2-12-345-678-90.compute-1.amazonaws.com` ist. Ihr SSH-Befehl würde wie folgt aussehen:

   ```
   ssh -i /dir1/ec2-database-connect-key-pair.pem ec2-
   user@ec2-12-345-678-90.compute-1.amazonaws.com
   ```

2. Installieren Sie die neuesten Fehlerbehebungen und Sicherheitsupdates, indem Sie die Software auf Ihrer EC2-Instance aktualisieren. Verwenden Sie dazu den folgenden Befehl.

   > **Note**
   >
   > Mit der Option `-y` werden die Updates installiert, ohne um Bestätigung zu bitten. Um Updates vor der Installation zu überprüfen, lassen Sie diese Option aus.

   ```
   sudo dnf update -y
   ```

3. Nachdem die Aktualisierungen abgeschlossen sind, installieren Sie die Software von Apache-Webserver, PHP und MariaDB mit den folgenden Befehlen. Mit diesem Befehl werden gleichzeitig mehrere Softwarepakete und zugehörige Abhängigkeiten installiert.

   MariaDB & MySQL

   ```
   sudo dnf install -y httpd php php-mysqli mariadb105
   ```

PostgreSQL

```
sudo dnf install -y httpd php php-pgsql postgresql15
```

Wenn Sie eine Fehlermeldung erhalten, wurde Ihre Instance wahrscheinlich nicht mit einem Amazon-Linux-2023-AMI gestartet. Stattdessen verwenden Sie möglicherweise das Amazon-Linux-2-AMI. Sie können Ihre Version von Amazon Linux mit dem folgenden Befehl anzeigen.

```
cat /etc/system-release
```

Weitere Informationen finden Sie unter Aktualisieren der Software einer Instance.

4. Starten Sie den Webserver mithilfe des folgenden Befehls.

```
sudo systemctl start httpd
```

Sie können testen, ob Ihr Webserver richtig installiert und gestartet ist. Geben Sie dazu den öffentlichen DNS-Namen (Domain Name System) Ihrer EC2-Instance in die Adressleiste eines Webbrowsers ein, zum Beispiel: `http://ec2-42-8-168-21.us-west-1.compute.amazonaws.com`. Wenn Ihr Webserver ausgeführt wird, wird Ihnen die Apache-Testseite angezeigt.

Wenn Sie die Apache-Testseite nicht sehen, überprüfen Sie die Regeln für eingehenden Datenverkehr für die VPC-Sicherheitsgruppe, die Sie in erstellt habe Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4). Stellen Sie sicher, dass die Regeln für eingehenden Datenverkehr eine Regel enthalten, die den HTTP-Zugriff (Port 80) für die IP-Adresse ermöglicht, um eine Verbindung mit dem Webserver herzustellen.

> **Note**
>
> Die Apache-Testseite wird nur angezeigt, wenn im Dokumentstammverzeichnis `/var/www/html` keine Inhalte vorhanden sind. Wenn Sie dem Dokumentstammverzeichnis Inhalte hinzugefügt haben, werden unter der öffentlichen DNS-Adresse Ihrer EC2-Instance Ihre Inhalte angezeigt. Bis zu diesem Zeitpunkt erscheinen sie auf der Apache-Testseite.

5. Konfigurieren Sie den Webserver so, dass er mit jedem Systemstart gestartet wird. Verwenden Sie hierzu den Befehl `systemctl`.

```
sudo systemctl enable httpd
```

Um für `ec2-user` die Verwaltung von Dateien im Standardstammverzeichnis Ihres Apache-Webservers zuzulassen, ändern Sie die Eigentümerschaft und die Berechtigungen für das Verzeichnis `/var/www`. Es gibt viele Möglichkeiten, um diese Aufgabe zu erfüllen. In diesem Tutorial fügen Sie `ec2-user` zur `apache`-Gruppe hinzu, geben der `apache`-Gruppe Eigentümerschaft über das Verzeichnis `/var/www` und weisen der Gruppe Schreibberechtigungen zu.

So legen Sie Dateiberechtigungen für den Apache-Webserver fest

1. Fügen Sie den Benutzer `ec2-user` zur Gruppe `apache` hinzu.

```
sudo usermod -a -G apache ec2-user
```

2. Melden Sie sich ab, um Ihre Berechtigungen zu aktualisieren und die neue Gruppe `apache` einzufügen.

```
exit
```

3. Melden Sie sich wieder an und überprüfen Sie mit dem Befehl `apache`, ob die Gruppe `groups` vorhanden ist.

```
groups
```

   Die Ausgabe sieht folgendermaßen oder ähnlich aus:

```
ec2-user adm wheel apache systemd-journal
```

4. Ändern Sie die Besitzergruppe für das Verzeichnis `/var/www` und dessen Inhalte in die Gruppe `apache`.

```
sudo chown -R ec2-user:apache /var/www
```

5. Ändern Sie die Verzeichnisberechtigungen von `/var/www` und dessen Unterverzeichnissen, indem Sie Schreibberechtigungen für die Gruppe hinzufügen und die Gruppen-ID für zukünftige Unterverzeichnisse einrichten.

```
sudo chmod 2775 /var/www
find /var/www -type d -exec sudo chmod 2775 {} \;
```

6. Ändern Sie die Dateiberechtigungen für Dateien im Verzeichnis `/var/www` und dessen Unterverzeichnissen rekursiv, um Schreibberechtigungen für die Gruppe hinzuzufügen.

```
find /var/www -type f -exec sudo chmod 0664 {} \;
```

Jetzt kann `ec2-user` (und jedes künftige Mitglied der `apache`-Gruppe) im Dokumentstammverzeichnis von Apache Dateien hinzufügen, löschen und bearbeiten. Damit haben Sie die Möglichkeit, Inhalte hinzuzufügen, z. B. eine statische Website oder eine PHP-Anwendung.

> **Note**
>
> Ein Webserver, auf dem HTTP ausgeführt wird, bietet keine Transportsicherheit für die gesendeten oder empfangenen Daten. Wenn Sie über einen Webbrowser eine Verbindung mit einem HTTP-Server herstellen, sind viele Informationen überall auf dem Netzwerkpfad für Lauscher zugänglich. Zu diesen Informationen gehören die URLs, die Sie aufrufen, die Inhalte von Webseiten, die Sie empfangen, und die Inhalte (einschließlich Passwörtern) von HTML-Formularen.
> Die bewährte Methode, Ihren Webserver abzusichern, besteht darin, Unterstützung für HTTPS (HTTP Secure) zu installieren. Dieses Protokoll schützt Ihre Daten mit SSL-/TLS-Verschlüsselung. Weitere Informationen finden Sie unter Tutorial: SSL/TLS mit dem Amazon Linux AMI konfigurieren im Amazon EC2-Benutzerhandbuch .

Herstellen der Verbindung zwischen Ihrem Apache-Webserver und Ihrem DB-Cluster

Als Nächstes fügen Sie Ihrem Apache-Server, der mit Ihrer /dem Amazon Aurora-DB-Cluster verbunden ist, Inhalte hinzu.

So fügen Sie dem Apache-Server, der mit Ihrer /dem DB-Cluster verbunden ist, Inhalte hinzu

1. Während die Verbindung mit Ihrer EC2-Instance besteht, ändern Sie das Verzeichnis in `/var/www` und erstellen Sie ein neues Unterverzeichnis namens `inc`.

```
cd /var/www
mkdir inc
cd inc
```

2. Erstellen Sie im Verzeichnis `inc` eine neue Datei namens `dbinfo.inc` und bearbeiten Sie anschließend die Datei, indem Sie Nano (oder einen Editor Ihrer Wahl) aufrufen.

```
>dbinfo.inc
nano dbinfo.inc
```

3. Fügen Sie der Datei `dbinfo.inc` die folgenden Inhalte hinzu. In diesem Fall ist *`db_instance_endpoint`* Ihr DB-Cluster-Writer-Endpunkt ohne den Port für Ihre Ihren DB-Cluster.

> **Note**
>
> Es wird empfohlen, die Informationen zu Benutzername und Passwort in einem Ordner abzulegen, der nicht Teil des Dokumentstammverzeichnisses für Ihren Webserver ist. Auf diese Weise wird die Möglichkeit verringert, dass Ihre Sicherheitsinformationen offengelegt werden.
> Stellen Sie sicher, dass Sie `master password` in Ihrer Anwendung in ein geeignetes Passwort ändern.

```
<?php

define('DB_SERVER', 'db_cluster_writer_endpoint');
define('DB_USERNAME', 'tutorial_user');
define('DB_PASSWORD', 'master password');
define('DB_DATABASE', 'sample');
?>
```

4. Speichern und schließen Sie die Datei `dbinfo.inc`. Wenn Sie Nano verwenden, speichern und schließen Sie die Datei mit Strg+S und Strg+X.

5. Ändern Sie das Verzeichnis in `/var/www/html`.

```
cd /var/www/html
```

6. Erstellen Sie im Verzeichnis `html` eine neue Datei namens `SamplePage.php` und bearbeiten Sie anschließend die Datei, indem Sie Nano (oder einen Editor Ihrer Wahl) aufrufen.

```
>SamplePage.php
nano SamplePage.php
```

7. Fügen Sie der Datei `SamplePage.php` die folgenden Inhalte hinzu:

   MariaDB & MySQL

```
<?php include "../inc/dbinfo.inc"; ?>
<html>
<body>
<h1>Sample page</h1>
<?php

  /* Connect to MySQL and select the database. */
  $connection = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD);

  if (mysqli_connect_errno()) echo "Failed to connect to MySQL: " .
 mysqli_connect_error();

  $database = mysqli_select_db($connection, DB_DATABASE);

  /* Ensure that the EMPLOYEES table exists. */
  VerifyEmployeesTable($connection, DB_DATABASE);

  /* If input fields are populated, add a row to the EMPLOYEES table. */
  $employee_name = htmlentities($_POST['NAME']);
  $employee_address = htmlentities($_POST['ADDRESS']);

  if (strlen($employee_name) || strlen($employee_address)) {
    AddEmployee($connection, $employee_name, $employee_address);
  }
?>

<!-- Input form -->
<form action="<?PHP echo $_SERVER['SCRIPT_NAME'] ?>" method="POST">
  <table border="0">
```

```
    <tr>
      <td>NAME</td>
      <td>ADDRESS</td>
    </tr>
    <tr>
      <td>
        <input type="text" name="NAME" maxlength="45" size="30" />
      </td>
      <td>
        <input type="text" name="ADDRESS" maxlength="90" size="60" />
      </td>
      <td>
        <input type="submit" value="Add Data" />
      </td>
    </tr>
  </table>
</form>

<!-- Display table data. -->
<table border="1" cellpadding="2" cellspacing="2">
  <tr>
    <td>ID</td>
    <td>NAME</td>
    <td>ADDRESS</td>
  </tr>

<?php

$result = mysqli_query($connection, "SELECT * FROM EMPLOYEES");

while($query_data = mysqli_fetch_row($result)) {
  echo "<tr>";
  echo "<td>",$query_data[0], "</td>",
       "<td>",$query_data[1], "</td>",
       "<td>",$query_data[2], "</td>";
  echo "</tr>";
}
?>

</table>

<!-- Clean up. -->
<?php
```

```
  mysqli_free_result($result);
  mysqli_close($connection);

?>

</body>
</html>


<?php

/* Add an employee to the table. */
function AddEmployee($connection, $name, $address) {
   $n = mysqli_real_escape_string($connection, $name);
   $a = mysqli_real_escape_string($connection, $address);

   $query = "INSERT INTO EMPLOYEES (NAME, ADDRESS) VALUES ('$n', '$a');";

   if(!mysqli_query($connection, $query)) echo("<p>Error adding employee data.</
p>");
}

/* Check whether the table exists and, if not, create it. */
function VerifyEmployeesTable($connection, $dbName) {
  if(!TableExists("EMPLOYEES", $connection, $dbName))
  {
     $query = "CREATE TABLE EMPLOYEES (
         ID int(11) UNSIGNED AUTO_INCREMENT PRIMARY KEY,
         NAME VARCHAR(45),
         ADDRESS VARCHAR(90)
       )";

     if(!mysqli_query($connection, $query)) echo("<p>Error creating table.</
p>");
  }
}

/* Check for the existence of a table. */
function TableExists($tableName, $connection, $dbName) {
  $t = mysqli_real_escape_string($connection, $tableName);
  $d = mysqli_real_escape_string($connection, $dbName);

  $checktable = mysqli_query($connection,
```

```
      "SELECT TABLE_NAME FROM information_schema.TABLES WHERE TABLE_NAME = '$t'
 AND TABLE_SCHEMA = '$d'");

  if(mysqli_num_rows($checktable) > 0) return true;

  return false;
}
?>
```

PostgreSQL

```
<?php include "../inc/dbinfo.inc"; ?>

<html>
<body>
<h1>Sample page</h1>
<?php

/* Connect to PostgreSQL and select the database. */
$constring = "host=" . DB_SERVER . " dbname=" . DB_DATABASE . " user=" .
 DB_USERNAME . " password=" . DB_PASSWORD ;
$connection = pg_connect($constring);

if (!$connection){
 echo "Failed to connect to PostgreSQL";
 exit;
}

/* Ensure that the EMPLOYEES table exists. */
VerifyEmployeesTable($connection, DB_DATABASE);

/* If input fields are populated, add a row to the EMPLOYEES table. */
$employee_name = htmlentities($_POST['NAME']);
$employee_address = htmlentities($_POST['ADDRESS']);

if (strlen($employee_name) || strlen($employee_address)) {
  AddEmployee($connection, $employee_name, $employee_address);
}

?>

<!-- Input form -->
```

```
<form action="<?PHP echo $_SERVER['SCRIPT_NAME'] ?>" method="POST">
  <table border="0">
    <tr>
      <td>NAME</td>
      <td>ADDRESS</td>
    </tr>
    <tr>
      <td>
    <input type="text" name="NAME" maxlength="45" size="30" />
      </td>
      <td>
    <input type="text" name="ADDRESS" maxlength="90" size="60" />
      </td>
      <td>
    <input type="submit" value="Add Data" />
      </td>
    </tr>
  </table>
</form>
<!-- Display table data. -->
<table border="1" cellpadding="2" cellspacing="2">
  <tr>
    <td>ID</td>
    <td>NAME</td>
    <td>ADDRESS</td>
  </tr>

<?php

$result = pg_query($connection, "SELECT * FROM EMPLOYEES");

while($query_data = pg_fetch_row($result)) {
  echo "<tr>";
  echo "<td>",$query_data[0], "</td>",
       "<td>",$query_data[1], "</td>",
       "<td>",$query_data[2], "</td>";
  echo "</tr>";
}
?>
</table>

<!-- Clean up. -->
<?php
```

```
  pg_free_result($result);
  pg_close($connection);
?>
</body>
</html>


<?php

/* Add an employee to the table. */
function AddEmployee($connection, $name, $address) {
   $n = pg_escape_string($name);
   $a = pg_escape_string($address);
   echo "Forming Query";
   $query = "INSERT INTO EMPLOYEES (NAME, ADDRESS) VALUES ('$n', '$a');";

   if(!pg_query($connection, $query)) echo("<p>Error adding employee data.</
p>");
}

/* Check whether the table exists and, if not, create it. */
function VerifyEmployeesTable($connection, $dbName) {
  if(!TableExists("EMPLOYEES", $connection, $dbName))
  {
     $query = "CREATE TABLE EMPLOYEES (
         ID serial PRIMARY KEY,
         NAME VARCHAR(45),
         ADDRESS VARCHAR(90)
       )";

     if(!pg_query($connection, $query)) echo("<p>Error creating table.</p>");
  }
}
/* Check for the existence of a table. */
function TableExists($tableName, $connection, $dbName) {
  $t = strtolower(pg_escape_string($tableName)); //table name is case sensitive
  $d = pg_escape_string($dbName); //schema is 'public' instead of 'sample' db
 name so not using that

  $query = "SELECT TABLE_NAME FROM information_schema.TABLES WHERE TABLE_NAME =
 '$t';";
  $checktable = pg_query($connection, $query);

  if (pg_num_rows($checktable) >0) return true;
```

```
  return false;

}
?>
```

8. Speichern und schließen Sie die Datei `SamplePage.php`.
9. Überprüfen Sie, ob Ihr Webserver erfolgreich eine Verbindung mit Ihrem DB-Cluster herstellen kann, indem Sie einen Webbrowser öffnen und zu `http://`*`EC2 instance endpoint`*`/SamplePage.php` navigieren, beispielsweise: `http://ec2-12-345-67-890.us-west-2.compute.amazonaws.com/SamplePage.php`.

Sie können `SamplePage.php` verwenden, um Ihrem DB-Cluster Daten hinzuzufügen. Die von Ihnen hinzugefügten Daten werden anschließend auf der Seite angezeigt. Wenn Sie überprüfen möchten, ob die Daten in die Tabelle eingefügt wurden, installieren Sie den MySQL-Client auf der Amazon-EC2-Instance. Stellen Sie dann eine Verbindung mit dem DB-Cluster her und führen Sie eine Abfrage der Tabelle aus.

Informationen zum Herstellen einer Verbindung mit einem DB-Cluster finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

Um sicherzustellen, dass Ihr DB-Cluster so sicher wie möglich ist, müssen Sie sich vergewissern, dass Quellen außerhalb der VPC keine Verbindungen mit Ihrem DB-Cluster herstellen können.

Nachdem Sie Ihren Webserver und Ihre Datenbank getestet haben, sollten Sie Ihren DB-Cluster und Ihre Amazon EC2-Instance löschen.

- Um einen DB-Cluster zu löschen, folgen Sie den Anweisungen in Löschen von Aurora-DB-Clustern und -DB-Instances. Sie müssen keinen abschließenden Snapshot erstellen.
- Um eine Amazon EC2-Instance zu beenden, folgen Sie den Anweisungen in Beenden Ihrer Instance im Amazon EC2-Benutzerhandbuch.

Amazon Aurora Tutorials und Beispiel-Code

Die AWS Dokumentation enthält mehrere Tutorials, die Sie durch gängige Aurora Aurora-Anwendungsfälle führen. Viele dieser Tutorials zeigen Ihnen, wie Sie Aurora mit anderen AWS Diensten verwenden können. Darüber hinaus können Sie in auf den Beispielcode zugreifen GitHub.

> **Note**
>
> Weitere Tutorials finden Sie im AWS -Datenbank-Blog. Informationen zu Schulungen finden Sie unter AWS Training and Certification.

Themen

Tutorials in diesem Handbuch

Die folgenden Tutorials in diesem Handbuch veranschaulichen, wie Sie mit Amazon Aurora gängige Aufgaben durchführen.

- Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4)

  Erfahren Sie, wie Sie einen DB-Cluster in eine Virtual Private Cloud (VPC) aufnehmen, die auf dem Amazon-VPC-Service basiert. In diesem Fall teilt die VPC Daten mit einem Webserver, der auf einer Amazon-EC2-Instance in derselben VPC ausgeführt wird.
- Tutorial: Erstellen einer VPC zur Verwendung mit einer DB–einem DB-Cluster (Dual-Stack-Modus)

  Erfahren Sie, wie Sie einen DB-Cluster in eine Virtual Private Cloud (VPC) aufnehmen, die auf dem Amazon-VPC-Service basiert. In diesem Fall teilt die VPC Daten mit einer Amazon-EC2-

Instance in derselben VPC. In diesem Tutorial erstellen Sie die VPC für dieses Szenario, die mit einer Datenbank arbeitet, die im Dual-Stack-Modus ausgeführt wird.

- Tutorial: Erstellen eines Webservers und einer eines Amazon Aurora-DB-Clusters

  Weitere Informationen darüber, wie Sie einen Apache-Webserver mit PHP installieren und eine MySQL-Datenbank zu erstellen. Der Webserver wird auf einer Amazon EC2-Instance unter Verwendung von Amazon Linux ausgeführt und bei der MySQL-Datenbank handelt es sich um ein Aurora MySQL-DB-Cluster. Sowohl die Amazon EC2-Instance als auch der DB--Cluster läufen in einer Amazon VPC.

- Tutorial: Wiederherstellen eines DB-Clusters von Amazon Aurora aus einem DB-Cluster-Snapshot

  Erfahren Sie, wie Sie einen DB-Cluster aus einem DB-Cluster-Snapshot wiederherstellen.

- Tutorial: Verwenden Sie Tags, um festzulegen, welcher Aurora-DB-Cluster stoppt.

  Erfahren Sie, wie Sie Tags verwenden, um festzulegen, welcher Aurora-DB-Cluster stoppt.

- Tutorial: Statusänderungen der DB-Instance mithilfe von Amazon protokollieren EventBridge

  Erfahren Sie, wie Sie eine Änderung des DB-Instance-Status mithilfe von Amazon EventBridge und protokollieren AWS Lambda.

Tutorials in anderen Leitfäden AWS

Die folgenden Tutorials in anderen AWS Handbüchern zeigen Ihnen, wie Sie allgemeine Aufgaben mit Amazon Aurora ausführen:

> **Note**
>
> Einige der Tutorials verwenden Amazon RDS-DB-Instances, aber sie können angepasst werden, so dass sie Aurora-DB-Cluster verwenden.

- Tutorial: Aurora Serverless in AWS AppSync -Entwicklerhandbuch

  Erfahren Sie, wie Sie AWS AppSync mit aktivierter Daten-API eine Datenquelle für die Ausführung von SQL-Befehlen für Aurora Serverless DB-Cluster bereitstellen können. Sie können AWS AppSync -Resolver nutzen, um SQL-Anweisungen für die Daten-API mit GraphQL-Abfragen, Mutationen und Abonnements auszuführen.

- Tutorial: Ein Geheimnis für eine AWS Datenbank rotieren im AWS Secrets Manager Benutzerhandbuch

  Erfahren Sie, wie Sie ein Geheimnis für eine AWS Datenbank erstellen und das Geheimnis so konfigurieren, dass es nach einem Zeitplan rotiert. Sie lösen eine Rotation manuell aus und bestätigen dann, dass die neue Version des Secrets weiterhin Zugriff bietet.
- Tutorials und Beispiele im AWS Elastic Beanstalk -Entwicklerhandbuch

  Erfahren Sie, wie Sie Anwendungen bereitstellen, die Amazon RDS-Datenbanken verwenden AWS Elastic Beanstalk.
- Verwenden von Daten aus einer Amazon RDS-Datenbank zum Erstellen einer Amazon ML-Datenquelle im Amazon Machine Learning Developer Guide

  Erfahren Sie, wie Sie ein Amazon Machine Learning (Amazon ML)-Datenquellenobjekt aus Daten erstellen, die in einer MySQL-DB-Instance gespeichert sind.
- Manuelles Aktivieren des Zugriffs auf eine Amazon RDS-Instance in einer VPC im QuickSight Amazon-Benutzerhandbuch

  Erfahren Sie, wie Sie den QuickSight Amazon-Zugriff auf eine Amazon RDS-DB-Instance in einer VPC aktivieren.

AWS Portal für Workshop- und Laborinhalte für Amazon Aurora PostgreSQL

Die folgende Sammlung von Workshops und anderen praktischen Inhalten hilft Ihnen, die Funktionen und Möglichkeiten von Amazon Aurora PostgreSQL zu verstehen:

- Erstellen eines Aurora-Clusters

  Erfahren Sie mehr dazu, wie Sie einen Cluster von Amazon Aurora PostgreSQL manuell erstellen.
- Erstellen einer cloudbasierten Cloud9-IDE-Umgebung zur Verbindung mit Ihrer Datenbank

  Erfahren Sie, wie Sie Cloud9 konfigurieren und die PostgreSQL-Datenbank initialisieren.
- Schnelles Klonen

  Erfahren Sie mehr dazu, wie Sie einen schnellen Aurora-Klon erstellen.
- Abfrageplanverwaltung

Erfahren Sie mehr dazu, wie Sie die Ausführungspläne für einen Satz von Anweisungen mithilfe der Abfrageplanverwaltung kontrollieren.

- Cluster-Cache-Verwaltung

  Erfahren Sie mehr über die Cluster-Cache-Verwaltungsfunktion in Aurora PostgreSQL.

- Datenbankaktivitäts-Streaming

  Erfahren Sie mehr dazu, wie Sie mit dieser Funktion Ihre Datenbankaktivitäten überwachen und überprüfen.

- Verwenden von Performance-Insights

  Erfahren Sie, wie Sie Ihre DB-Instance mithilfe von Performance Insights überwachen und optimieren können.

- Leistungsüberwachung mit RDS-Tools

  Erfahren Sie, wie Sie Postgres-Tools (Cloudwatch, Enhanced Monitoring, Slow Query Logs, Performance Insights, PostgreSQL Catalog Views) verwenden AWS , um Leistungsprobleme zu verstehen und Möglichkeiten zur Verbesserung der Leistung Ihrer Datenbank zu finden.

- Auto Scaling von Lesereplikaten

  Erfahren Sie, wie Auto Scaling von Aurora-Lesereplikaten mithilfe eines Lastgeneratorskripts in der Praxis funktioniert.

- Testen der Fehlertoleranz

  Erfahren Sie mehr über die Fehlertoleranz eines DB-Clusters.

- Globale Aurora-Datenbank

  Erfahren Sie mehr über globale Aurora-Datenbanken.

- Verwendung von Machine Learning

  Erfahren Sie mehr über Aurora Machine Learning.

- Aurora Serverless v2

  Erfahren Sie mehr über Aurora Serverless v2.

- Trusted Language Extensions für PostgreSQL

Erfahren Sie, wie Sie Hochleistungserweiterungen erstellen, die sicher auf Aurora PostgreSQL laufen.

AWS Portal für Workshop- und Laborinhalte für Amazon Aurora MySQL

Die folgende Sammlung von Workshops und anderen praktischen Inhalten hilft Ihnen, die Funktionen und Möglichkeiten von Amazon Aurora MySQL zu verstehen:

- Erstellen eines Aurora-Clusters

  Erfahren Sie mehr dazu, wie Sie einen Cluster von Amazon Aurora MySQL manuell erstellen.
- Erstellen einer cloudbasierten Cloud9-IDE-Umgebung zur Verbindung mit Ihrer Datenbank

  Erfahren Sie, wie Sie Cloud9 konfigurieren und die MySQL-Datenbank initialisieren.
- Schnelles Klonen

  Erfahren Sie mehr dazu, wie Sie einen schnellen Aurora-Klon erstellen.
- Rückverfolgen eines Clusters

  Erfahren Sie mehr dazu, wie Sie einen DB-Cluster rückverfolgen.
- Verwenden von Performance-Insights

  Erfahren Sie, wie Sie Ihre DB-Instance mithilfe von Performance Insights überwachen und optimieren können.
- Leistungsüberwachung mit RDS-Tools

  Erfahren Sie, wie Sie SQL-Tools verwenden AWS , um Leistungsprobleme zu verstehen und Möglichkeiten zur Verbesserung der Leistung Ihrer Datenbank zu finden.
- Analysieren der Abfrageleistung

  Erfahren Sie, wie Sie Probleme mit der SQL-Leistung mithilfe verschiedener Tools beheben können.
- Auto Scaling von Lesereplikaten

  Erfahren Sie, wie Auto Scaling von Lesereplikaten funktioniert.

- Testen der Fehlertoleranz

  Erfahren Sie mehr über Hochverfügbarkeits- und Fehlertoleranzfunktionen in Aurora MySQL.

- Globale Aurora-Datenbank

  Erfahren Sie mehr über globale Aurora-Datenbanken.

- Aurora Serverless v2

  Erfahren Sie mehr über Aurora Serverless v2.

- Verwendung von Machine Learning

  Erfahren Sie mehr über Aurora Machine Learning.

Tutorials und Beispielcode in GitHub

Die folgenden Tutorials und der Beispielcode GitHub zeigen Ihnen, wie Sie allgemeine Aufgaben mit Amazon Aurora ausführen:

- Erstellen einer Leihbibliothek von Aurora Serverless v2

  Erfahren Sie, wie Sie eine Leihbibliothekanwendung erstellen, in der Kunden Bücher ausleihen und zurückgeben können. Das Beispiel verwendet Aurora Serverless v2 und AWS SDK for Python (Boto3).

- Erstellen einer Item-Tracker-Anwendung von Amazon Aurora mit einer Spring-REST-API, die Aurora Serverless v2 mithilfe von SDK for Java 2.x abfragt

  Erfahren Sie, wie Sie eine Spring-REST-API erstellen, die Daten von Aurora Serverless v2 abfragt. Sie wird von einer React-Anwendung unter Verwendung von SDK für Java 2.x genutzt.

- Erstellen einer Amazon Aurora Aurora-Artikel-Tracker-Anwendung, die Aurora Serverless v2 Daten abfragt mit AWS SDK for PHP

  Erfahren Sie, wie Sie eine Anwendung erstellen, die den `RdsDataClient` der Daten-API und Aurora Serverless v2 verwendet, um Arbeitselemente zu verfolgen und Berichte darüber zu erstellen. Das Beispiel verwendet AWS SDK for PHP.

- Erstellen einer Item-Tracker-Anwendung von Amazon Aurora, die Aurora Serverless v2 mithilfe von AWS SDK for Python (Boto3) abfragt

Erfahren Sie, wie Sie eine Anwendung erstellen, die den `RdsDataClient` der Daten-API und Aurora Serverless v2 verwendet, um Arbeitselemente zu verfolgen und Berichte darüber zu erstellen. Das Beispiel verwendet AWS SDK for Python (Boto3).

Verwenden dieses Dienstes mit einem AWS SDK

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK for C++	AWS SDK for C++ Codebeispiele
AWS CLI	AWS CLI Codebeispiele
AWS SDK for Go	AWS SDK for Go Codebeispiele
AWS SDK for Java	AWS SDK for Java Codebeispiele
AWS SDK for JavaScript	AWS SDK for JavaScript Codebeispiele
AWS SDK for Kotlin	AWS SDK for Kotlin Codebeispiele
AWS SDK for .NET	AWS SDK for .NET Codebeispiele
AWS SDK for PHP	AWS SDK for PHP Codebeispiele
AWS Tools for PowerShell	Tools für PowerShell Codebeispiele
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) Codebeispiele
AWS SDK for Ruby	AWS SDK for Ruby Codebeispiele
AWS SDK for Rust	AWS SDK for Rust Codebeispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Codebeispiele
AWS SDK for Swift	AWS SDK for Swift Codebeispiele

Weitere Beispiele speziell für diesen Service finden Sie unter Codebeispiele für Aurora mit AWS SDKs.

Beispiel für die Verfügbarkeit

Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Provide feedback (Feedback geben) auswählen.

Konfigurieren Ihres Amazon Aurora-DB-Clusters

In diesem Abschnitt wird erläutert, wie Sie Ihren Aurora-DB-Cluster einrichten. Legen Sie vor dem Erstellen eines Aurora-DB-Clusters fest, welche DB-Instance-Klasse den DB-Cluster ausführen soll. Legen Sie außerdem fest, wo der DB-Cluster ausgeführt wird, indem Sie eine - AWS Region auswählen. Erstellen Sie nun den DB-Cluster. Wenn Sie Daten außerhalb von Aurora haben, können Sie diese in einen Aurora-DB-Cluster migrieren.

Themen

Erstellen eines Amazon Aurora-DB Clusters

Ein Amazon-Aurora-DB-Cluster besteht aus einer DB-Instance, die entweder mit MySQL oder PostgreSQL kompatibel ist, und einem Cluster-Volume, das die Daten für den DB-Cluster enthält und in drei Availability Zones als ein einziges virtuelles Volume kopiert wird. Standardmäßig enthält ein Aurora-DB-Cluster eine primäre DB-Instance, die Lese- und Schreibvorgänge ausführt, und optional bis zu 15 Aurora-Replikate (Reader-DB-Instances). Weitere Informationen zu Aurora-DB-Clustern finden Sie unter Amazon-Aurora-DB-Cluster.

Aurora bietet zwei Haupttypen von DB-Clustern:

- Von Aurora bereitgestellt – Sie wählen die DB-Instance-Klasse für die Writer- und Reader-Instances basierend auf Ihrer erwarteten Workload aus. Weitere Informationen finden Sie unter Aurora DB-Instance-Klassen. Der Typ „von Aurora bereitgestellt“ verfügt über mehrere Optionen, einschließlich globalen Aurora-Datenbanken. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Global Databases.
- Aurora Serverless – Aurora Serverless v1 und Aurora Serverless v2 sind bedarfsabhängige Auto-Scaling-Konfigurationen für Aurora. Die Kapazität wird automatisch basierend auf dem Anwendungsbedarf angepasst. Berechnet werden Ihnen nur die Ressourcen, die Ihr DB-Cluster verbraucht. Diese Automatisierung ist besonders nützlich für Umgebungen mit sehr variablen und unvorhersehbaren Workloads. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Serverless v1 und Verwenden von Aurora Serverless v2.

Im Folgenden erfahren Sie, wie Sie einen Aurora-DB-Cluster erstellen. Lesen Sie zum Einstieg zuerst Voraussetzungen für DB-Cluster.

Anweisungen zum Herstellen von Verbindungen mit Ihrem Aurora-DB-Cluster finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

Inhalt

- Erstellen einer primären (Writer-) DB-Instance
- Einstellungen für Aurora-DB-Cluster
- Einstellungen, die nicht für Amazon-Aurora-DB-Cluster gelten
- Einstellungen, die nicht für Amazon-Aurora-DB-Instances gelten

Voraussetzungen für DB-Cluster

> **Important**
>
> Sie müssen die Schritte im Abschnitt Einrichten Ihrer Umgebung für Amazon Aurora abschließen, bevor Sie einen Aurora-DB-Cluster erstellen können.

Im Folgenden werden die Voraussetzungen vor dem Erstellen eines DB-Clusters aufgeführt.

Themen

- Konfigurieren des Netzwerks für den DB-Cluster
- Zusätzliche Voraussetzungen

Konfigurieren des Netzwerks für den DB-Cluster

Sie können einen Amazon Aurora Aurora-DB-Cluster nur in einer Virtual Private Cloud (VPC) erstellen, die auf dem Amazon VPC-Service basiert und über mindestens zwei Availability Zones verfügt. AWS-Region Die DB-Subnetzgruppe, die Sie für den DB-Cluster wählen, muss mindestens zwei Availability Zones abdecken. Diese Konfiguration stellt sicher, dass Ihr DB-Cluster stets über mindestens eine DB-Instance verfügt, um in dem unwahrscheinlichen Fall, dass eine Availability Zone ausfällt, einen Failover ausführen zu können.

Wenn Sie die Konnektivität zwischen Ihrem neuen DB-Cluster und einer EC2-Instance in derselben VPC einrichten möchten, können Sie dies während der Erstellung des DB-Clusters tun. Wenn Sie von anderen Ressourcen als EC2-Instances in derselben VPC aus eine Verbindung zu Ihrem DB-Cluster herstellen möchten, können Sie die Netzwerkverbindungen manuell konfigurieren.

Themen

- Automatische Netzwerkkonnektivität mit einer EC2-Instance konfigurieren

- Manuelles Konfigurieren des Netzwerks

Automatische Netzwerkkonnektivität mit einer EC2-Instance konfigurieren

Wenn Sie einen Aurora-DB-Cluster erstellen, können Sie den verwenden, AWS Management Console um die Konnektivität zwischen einer Amazon EC2 EC2-Instance und dem neuen DB-Cluster einzurichten. In diesem Fall konfiguriert RDS Ihre VPC- und Netzwerkeinstellungen automatisch. Der DB-Cluster wird in derselben VPC wie die EC2-Instance erstellt, sodass die EC2-Instance auf den DB-Cluster zugreifen kann.

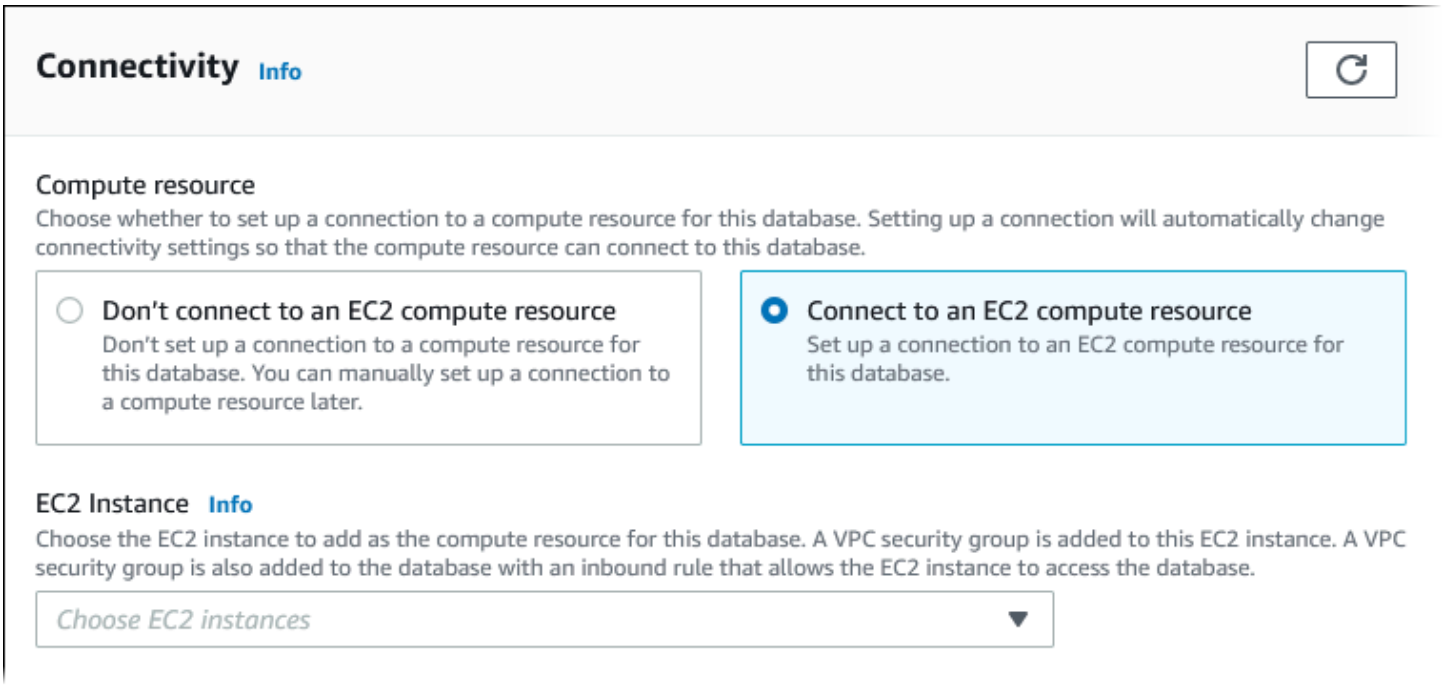
Im Folgenden sind die Anforderungen für die Verbindung einer EC2-Instance mit dem DB-Cluster aufgeführt:

- Die EC2-Instance muss in der vorhanden sein, AWS-Region bevor Sie den DB-Cluster erstellen.

  Wenn in der keine EC2-Instances vorhanden sind AWS-Region, bietet die Konsole einen Link zum Erstellen einer.
- Derzeit kann der DB-Cluster kein DB-Cluster von Aurora Serverless oder Teil einer globalen Aurora-Datenbank sein.
- Der Benutzer, der die DB-Instance erstellt, muss über Berechtigungen zum Ausführen der folgenden Vorgänge verfügen:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSubnet`
  - `ec2:CreateSecurityGroup`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Mit dieser Option wird ein privater DB-Cluster erstellt. Der DB-Cluster verwendet eine DB-Subnetzgruppe mit ausschließlich privaten Subnetzen, um den Zugriff auf Ressourcen innerhalb der VPC einzuschränken.

Um eine EC2-Instance mit dem DB-Cluster zu verbinden, wählen Sie Connect to an EC2 compute resource (Verbindung mit einer EC2-Compute-Ressource herstellen) im Abschnitt Connectivity (Konnektivität) auf der Seite Create database (Datenbank erstellen) aus.



Wenn Sie Verbindung zu einer EC2-Rechenressource herstellen wählen, legt RDS die folgenden Optionen automatisch fest. Sie können diese Einstellungen nur ändern, wenn Sie sich dafür entscheiden, keine Konnektivität mit einer EC2-Instance einzurichten, indem Sie Keine Verbindung zu einer EC2-Rechenressource herstellen wählen.

Konsolenoption	Automatische Einstellung
Netzwerktyp	RDS legt den Netzwerktyp auf IPv4 fest. Derzeit wird der Dual-Stack-Modus nicht unterstützt, wenn Sie eine Verbindung zwischen einer EC2-Instance und dem DB-Cluster einrichten.
Virtual Private Cloud (VPC)	RDS legt die VPC auf die VPC fest, die der EC2-Instance zugeordnet ist.

Konsolenoption	Automatische Einstellung
DB-Subnetzgruppe	RDS erfordert eine DB-Subnetzgruppe mit einem privaten Subnetz in derselben Availability Zone wie die EC2-Insta nce. Wenn eine DB-Subnetzgruppe vorhanden ist, die diese Anforderung erfüllt, dann verwendet RDS die vorhandene DB-Subnetzgruppe. Standardmäßig ist diese Option auf Automatic setup (Automatische Einrichtung) eingestellt. Wenn Sie Automatic setup (Automatische Einrichtung) auswählen und es keine DB-Subnetzgruppe gibt, die diese Anforderung erfüllt, wird die folgende Aktion ausgeführt. RDS verwendet drei verfügbare private Subnetze in drei Availability Zones, wobei eine der Availability Zones mit der AZ der EC2-Instance identisch ist. Wenn kein privates Subnetz in einer Availability Zone verfügbar ist, erstellt RDS ein privates Subnetz in der Availability Zone. Anschließend erstellt RDS die DB-Subnetzgruppe. Wenn ein privates Subnetz verfügbar ist, verwendet RDS die zugehörige Routing-Tabelle und fügt alle Subnetze, die es erstellt, dieser Routing-Tabelle hinzu. Wenn kein privates Subnetz verfügbar ist, erstellt RDS eine Routing-Tabelle ohne Internet-Gateway-Zugriff und fügt die erstellten Subnetze der Routing-Tabelle hinzu. Mit RDS können Sie auch vorhandene DB-Subnetzgruppen verwenden. Wählen Sie Choose existing (Vorhandene wählen) aus, wenn Sie eine vorhandene DB-Subnetzgruppe Ihrer Wahl verwenden möchten.
Öffentlicher Zugriff	RDS wählt Nein, so dass der DB-Cluster nicht öffentlich zugänglich ist. Aus Sicherheitsgründen ist es eine bewährte Methode, die Datenbank privat zu halten und sicherzustellen, dass sie nicht über das Internet zugänglich ist.

Konsolenoption	Automatische Einstellung
VPC-Sicherheitsgruppe (Firewall)	RDS erstellt eine neue Sicherheitsgruppe, die mit dem DB-Cluster verknüpft ist. Die Sicherheitsgruppe heißt `rds-ec2-`*n*, wobei *n* eine Zahl ist. Diese Sicherheitsgruppe enthält eine Regel für eingehenden Datenverkehr mit der EC2 VPC-Siche rheitsgruppe (Firewall) als Quelle. Diese Sicherheitsgruppe, die dem DB-Cluster zugeordnet ist, ermöglicht der EC2-Instance den Zugriff auf den DB-Cluster. RDS erstellt außerdem eine neue Sicherheitsgruppe, die der EC2-Instance zugeordnet ist. Die Sicherheitsgruppe heißt `ec2-rds-`*n*, wobei *n* eine Zahl ist. Diese Sicherheitsgruppe enthält eine ausgehende Regel mit der VPC-Sicherheitsgruppe des DB-Clusters als Quelle. Diese Sicherheitsgruppe ermöglicht es der EC2-Instance, Datenverkehr an den DB-Cluster zu senden. Sie können eine weitere neue Sicherheitsgruppe hinzufügen, indem Sie Neu erstellen wählen und den Namen der neuen Sicherheitsgruppe eingeben. Sie können vorhandene Sicherheitsgruppen hinzufügen, indem Sie Bestehende auswählen und Sicherheitsgruppen auswählen, die hinzugefügt werden sollen.

Konsolenoption	Automatische Einstellung
Availability Zone	Wenn Sie keine Aurora-Replica in Availability & durability (Verfügbarkeit und Haltbarkeit) bei der Erstellung eines DB-Clusters (Single-AZ-Bereitstellung) erstellen, wählt RDS die Availability Zone der EC2-Instance aus. Wenn Sie während der Erstellung eines DB-Clusters ein Aurora Replica erstellen (Multi-AZ-Bereitstellung), wählt RDS die Availability Zone der EC2-Instance für eine DB-Instance im DB-Cluster aus. RDS wählt zufällig eine andere Availability Zone für die andere DB-Instance im DB-Cluster aus. Entweder die primäre DB-Instance oder Aurora-Replica wird in derselben Availability Zone wie die EC2-Instance erstellt. Es besteht die Möglichkeit von Kosten über Availability Zones hinweg, wenn sich die primäre DB-Instance und die EC2-Instance in unterschi edlichen Availability Zones befinden.

Weitere Informationen zu diesen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.

Wenn Sie nach dem Erstellen des DB-Clusters Änderungen an diesen Einstellungen vornehmen, können sich die Änderungen auf die Verbindung zwischen der EC2-Instance und dem DB-Cluster auswirken.

Manuelles Konfigurieren des Netzwerks

Wenn Sie von anderen Ressourcen als EC2-Instances in derselben VPC aus eine Verbindung zu Ihrem DB-Cluster herstellen möchten, können Sie die Netzwerkverbindungen manuell konfigurieren. Wenn Sie die AWS Management Console zum Erstellen Ihres DB-Clusters verwenden, kann Amazon RDS automatisch eine VPC für Sie erstellen. Sie können auch eine bestehende VPC verwenden oder eine neue VPC für Ihren Aurora-DB-Cluster erstellen. Unabhängig davon, welchen Ansatz Sie wählen, muss Ihre VPC mindestens ein Subnetz in jeder von mindestens zwei Availability Zones haben, damit Sie sie mit einem Amazon-Aurora-DB-Cluster verwenden können.

Standardmäßig erstellt Amazon RDS die primäre DB-Instance und das Aurora Replica in den Availability Zones automatisch für Sie. Um eine bestimmte Availability Zone auszuwählen, müssen Sie die Einstellung der Multi-AZ-Bereitstellung Availability & durability (Verfügbarkeit und Haltbarkeit) auf Kein Aurora-Replikat erstellen ändern. Dadurch wird eine Availability Zone-Einstellung,

mit der Sie zwischen den Availability Zones in Ihrer VPC auswählen können, angezeigt. Wir empfehlen jedoch dringend, die Standardeinstellung beizubehalten und Amazon RDS eine Multi-AZ-Bereitstellung erstellen zu lassen und Availability Zones für Sie auszuwählen. Auf diese Weise wird Ihr Aurora-DB-Cluster mit den schnellen Failover- und Hochverfügbarkeitsfunktionen erstellt, die zwei der Hauptvorteile von Aurora sind.

Wenn Sie keine Standard-VPC besitzen oder keine VPC erstellt haben, kann Amazon RDS automatisch eine VPC für Sie erstellen, wenn Sie ein DB-Cluster über die Konsole erstellen. Andernfalls müssen Sie wie folgt vorgehen:

- Erstellen Sie eine VPC mit mindestens einem Subnetz in jeder der mindestens zwei Availability Zones in der Region, AWS-Region in der Sie Ihren DB-Cluster bereitstellen möchten. Weitere Informationen finden Sie unter Arbeiten mit einer DB-Cluster in einer VPC und Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4).
- Legen Sie eine VPC-Sicherheitsgruppe fest, die Verbindungen mit Ihrem DB-Cluster autorisiert. Weitere Informationen finden Sie unter Ermöglichen des Zugriffs auf den DB-Cluster in der VPC durch Erstellen einer Sicherheitsgruppe und Zugriffskontrolle mit Sicherheitsgruppen.
- Legen Sie eine RDS-DB-Subnetzgruppe fest, die mindestens zwei Subnetze in der VPC definiert, die vom DB-Cluster verwendet werden können. Weitere Informationen finden Sie unter Arbeiten mit DB-Subnetzgruppen.

Weitere Informationen zu VPCs finden Sie unter Amazon VPCs und Amazon Aurora. Ein Tutorial, das das Netzwerk für einen privaten DB-Cluster konfiguriert, finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4).

Wenn Sie eine Verbindung mit einer Ressource herstellen möchten, die sich nicht in derselben VPC wie der Aurora-DB-Cluster befindet, sehen Sie sich die entsprechenden Szenarien unter Szenarien für den Zugriff auf eine DB-Cluster in einer VPC an.

Zusätzliche Voraussetzungen

Bevor Sie Ihren DB-Cluster erstellen, sollten Sie die folgenden zusätzlichen Voraussetzungen beachten:

- Wenn Sie eine Verbindung AWS mit AWS Identity and Access Management (IAM-) Anmeldeinformationen herstellen, muss Ihr AWS Konto über IAM-Richtlinien verfügen, die die für die Durchführung von Amazon RDS-Vorgängen erforderlichen Berechtigungen gewähren. Weitere Informationen finden Sie unter Identity and Access Management für Amazon Aurora.

Wenn Sie IAM für den Zugriff auf die Amazon RDS-Konsole verwenden, müssen Sie sich zunächst AWS Management Console mit Ihren Benutzeranmeldedaten bei der anmelden. Öffnen Sie dann die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

- Wenn Sie die Konfigurationsparameter für Ihren DB-Cluster anpassen möchten, müssen Sie eine DB-Cluster-Parametergruppe und eine DB-Parametergruppe mit den erforderlichen Parametereinstellungen festlegen. Weitere Informationen über das Erstellen oder Ändern einer DB-Cluster-Parametergruppe oder DB-Parametergruppe finden Sie unter Arbeiten mit Parametergruppen.
- Bestimmen Sie die TCP/IP-Portnummer, die Sie für Ihr DB-Cluster festlegen werden. Die Firewalls einiger Unternehmen blockieren Verbindungen zu den Standard-Ports (3306 für MySQL, 5432 für PostgreSQL) für Aurora. Wenn die Firewall Ihres Unternehmens den Standard-Port blockiert, wählen Sie einen anderen Port für Ihr DB-Cluster aus. Alle Instances in einem DB-Cluster verwenden denselben Port.
- Wenn die Haupt-Engine-Version für Ihre Datenbank das Ende des Standard-Supports für RDS erreicht hat, müssen Sie die CLI Option Extended Support oder den RDS-API-Parameter verwenden. Weitere Informationen finden Sie unter RDS Extended Support unterEinstellungen für Aurora-DB-Cluster.

Erstellen eines DB-Clusters

Sie können einen Aurora-DB-Cluster mithilfe der AWS Management Console AWS CLI, der oder der RDS-API erstellen.

Konsole

Sie können einen DB-Cluster AWS Management Console mit aktiviertem oder deaktiviertem Easy Create erstellen. Wenn die Option Einfache Erstellung aktiviert ist, geben Sie nur den Engine-Typ, die Größe der Instance und die Kennung der Instance für die DB an. Mit der Option Einfache Erstellung werden für die anderen Konfigurationsoptionen die Standardeinstellungen verwendet. Ist die Option Einfache Erstellung nicht aktiviert, geben Sie bei der Erstellung einer Datenbank weitere Konfigurationsoptionen an, über die Verfügbarkeit, Sicherheit, Backups und Wartung der Datenbank konfiguriert werden.

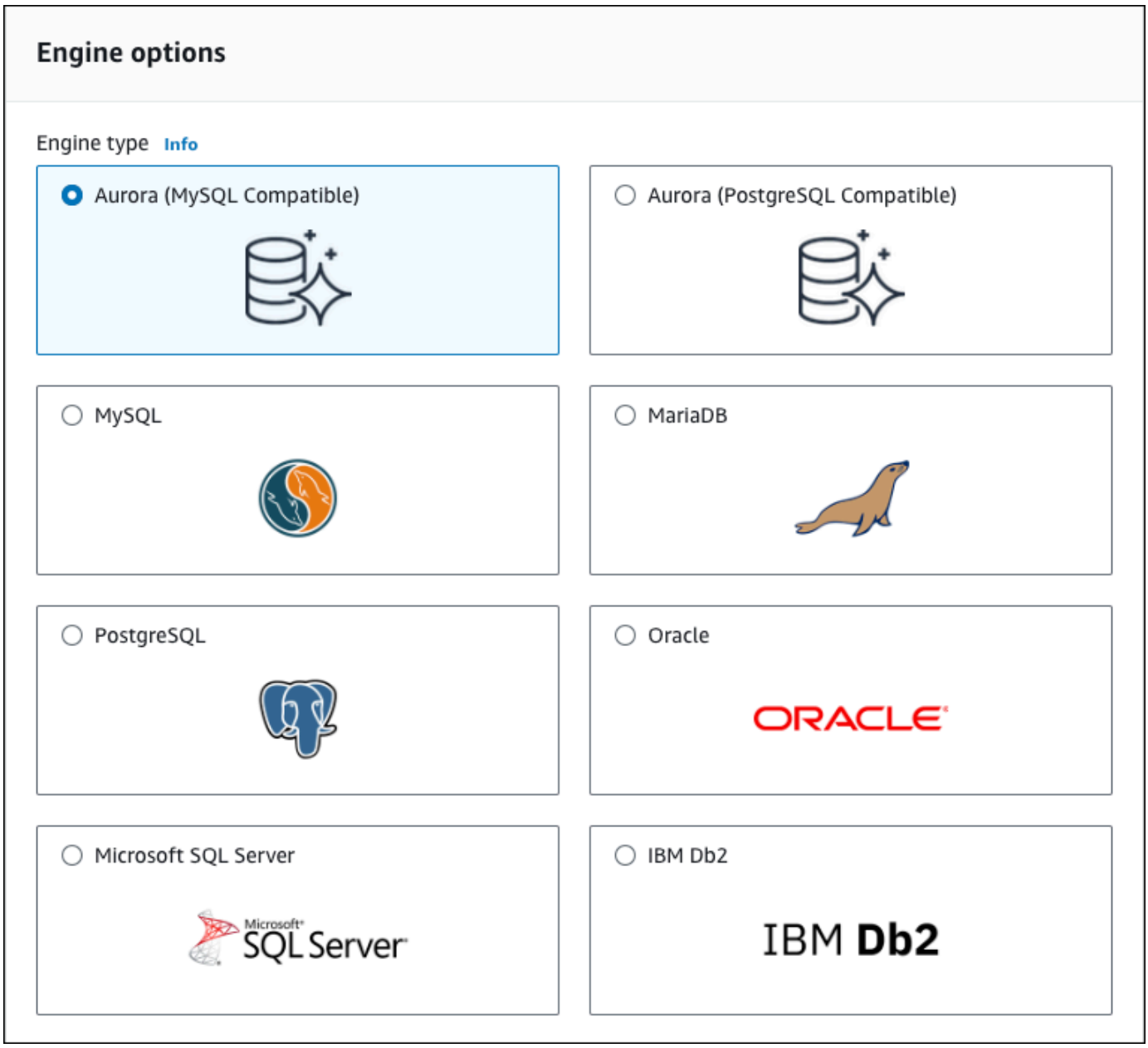
> **Note**
>
> In diesem Beispiel ist Standarderstellung aktiviert und Einfache Erstellung ist nicht aktiviert. Informationen zum Erstellen eines DB-Clusters mit aktiviertem Easy Create finden Sie unterErste Schritte mit Amazon Aurora.

Erstellen Sie einen Aurora-DB-Cluster mithilfe der Konsole wie folgt:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der oberen rechten Ecke von die AWS Region aus AWS Management Console, in der Sie den DB-Cluster erstellen möchten.

   Aurora ist nicht in allen AWS Regionen verfügbar. Eine Liste der AWS Regionen, in denen Aurora verfügbar ist, finden Sie unterVerfügbarkeit in Regionen.
3. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
4. Wählen Sie Datenbank erstellen aus.
5. Wählen Sie unter Auswahl einer Datenbank-Erstellungsmethode Standarderstellung aus.
6. Wählen Sie für Cache-Typ eine der folgenden Optionen aus:

   - Aurora (MySQL-kompatibel)
   - Aurora (PostgreSQL-kompatibel



7. Wählen Sie die Engine-Version.

   Weitere Informationen finden Sie unter Amazon-Aurora-Versionen. Sie können die Filter verwenden, um Versionen auszuwählen, die mit den gewünschten Funktionen kompatibel sind, z. B. Aurora Serverless v2. Weitere Informationen finden Sie unter Verwenden von Aurora Serverless v2.

8. Wählen Sie unter Vorlagen die Vorlage für Ihr Anwendungsszenario aus.

9. Gehen Sie wie folgt vor, um Ihr Masterpasswort einzugeben:

a. Öffnen Sie im Abschnitt Einstellungen die Option Einstellungen zu Anmeldeinformationen.

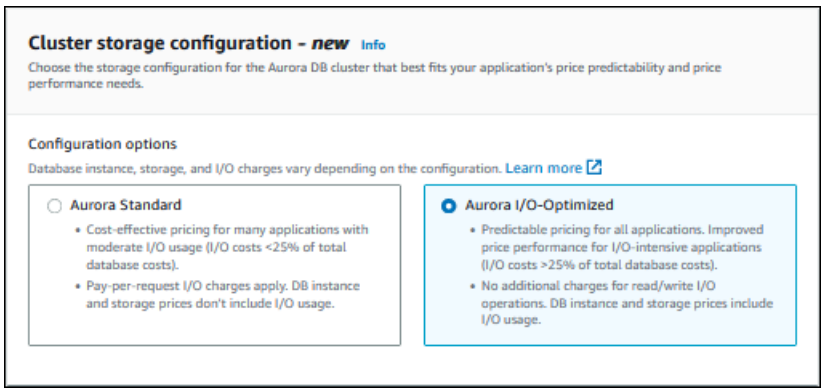
b. Deaktivieren Sie das Kontrollkästchen Ein Passwort automatisch erstellen.

c. (Optional) Ändern Sie den Wert für Hauptbenutzername und geben Sie in Hauptpasswort und Passwort bestätigen dasselbe Passwort ein.

Neu erstellte DB-Instances verwenden standardmäßig automatisch generierte Passwörter für den Hauptbenutzer.

10. Wenn Sie im Abschnitt Konnektivität unter VPC-Sicherheitsgruppe (Firewall) die Option Neu erstellen auswählen, wird eine VPC-Sicherheitsgruppe mit einer Regel für eingehenden Datenverkehr erstellt, die es der IP-Adresse Ihres lokalen Computers ermöglicht, auf die Datenbank zuzugreifen.

11. Wählen Sie für Cluster-Speicherkonfiguration entweder Aurora I/O-Optimized oder Aurora Standard aus. Weitere Informationen finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora.



12. (Optional) Richten Sie eine Verbindung zu einer Rechenressource für diesen DB-Cluster ein.

Sie können die Konnektivität zwischen einer Amazon-EC2-Instance und dem neuen DB-Cluster während der Erstellung eines DB-Clusters konfigurieren. Weitere Informationen finden Sie unter Automatische Netzwerkkonnektivität mit einer EC2-Instance konfigurieren.

13. In den übrigen Abschnitten geben Sie die Einstellungen für Ihren DB-Cluster an. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.

14. Wählen Sie Create database (Datenbank erstellen) aus.

Wenn Sie ein automatisch generiertes Passwort verwenden, wird auf der Seite Databases (Datenbanken) die Schaltfläche View credential details (Details zu Anmeldeinformationen anzeigen) angezeigt.

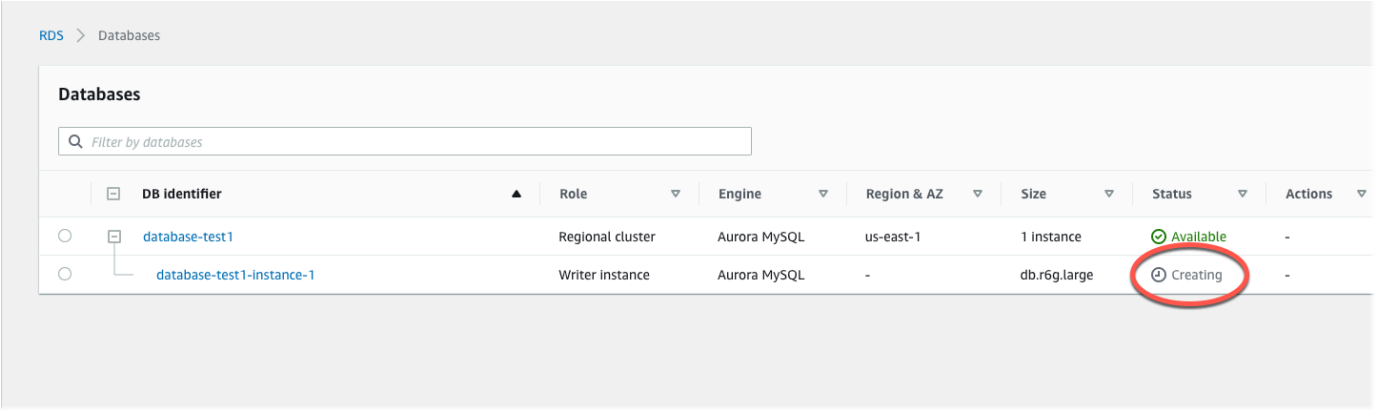
Um den Hauptbenutzernamen und das Passwort für den DB-Cluster anzuzeigen, wählen Sie Anmeldeinformationen anzeigen.

Verwenden Sie den angezeigten Benutzernamen und das angezeigte Passwort, um eine Verbindung zu DB-Instance als Hauptbenutzer herzustellen.

> **Important**
>
> Sie können dieses Passwort für den Hauptbenutzer nicht erneut anzeigen. Wenn Sie es nicht notieren, müssen Sie es möglicherweise ändern. Wenn Sie das Passwort für den Hauptbenutzer ändern müssen, nachdem die DB-Instance verfügbar wurde, können Sie die DB-Instance entsprechend ändern. Weitere Informationen über das Ändern einer DB-Instance finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

15. Wählen Sie unter Datenbanken den Namen des neuen Aurora-DB-Clusters aus.

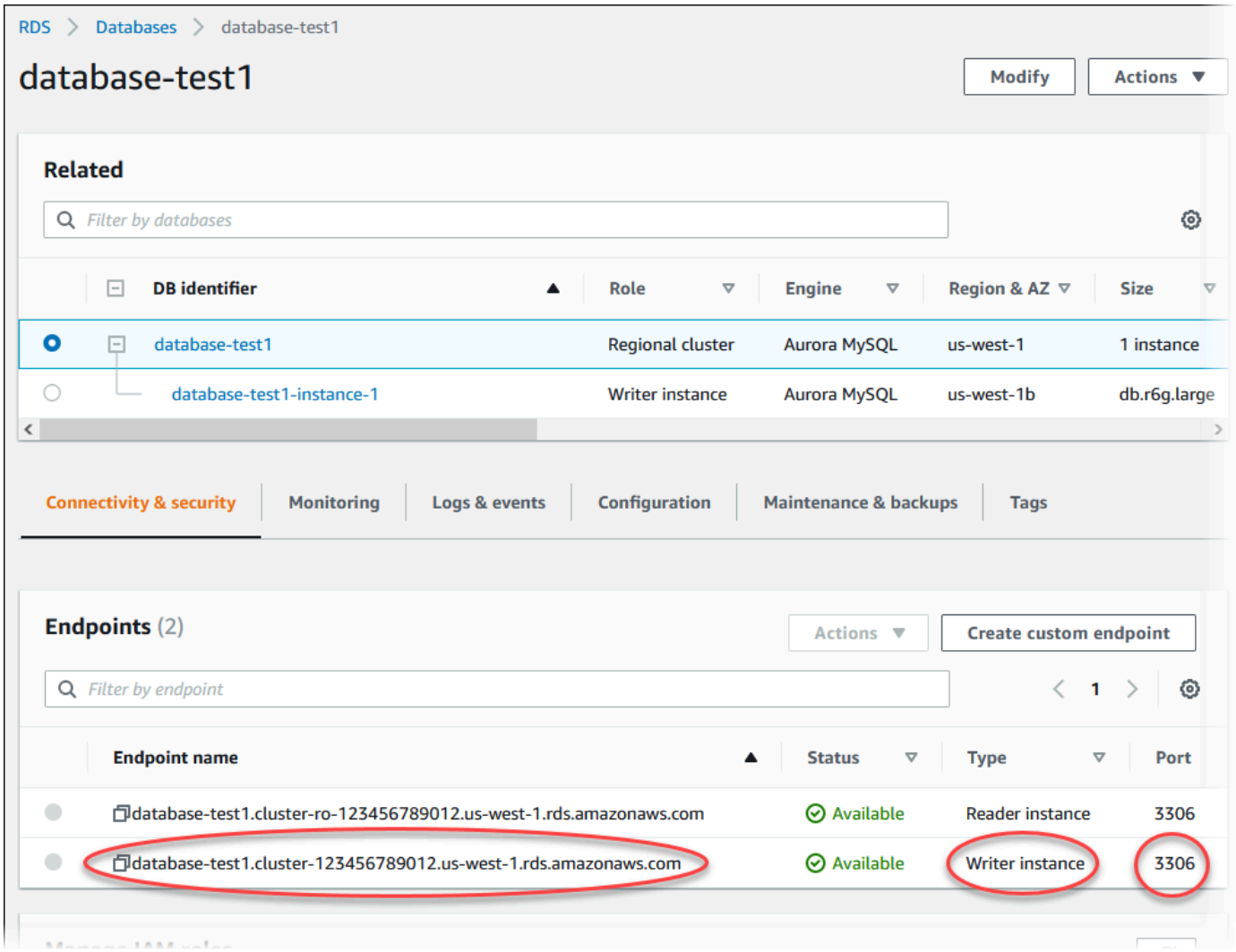
In der RDS-Konsole werden die Details des neuen DB-Clusters angezeigt. Bis der DB-Cluster verwendet werden kann, haben er und seine DB-Instance den Status Wird erstellt.



Wenn der Status zu Verfügbar geändert wird, können Sie eine Verbindung zum DB-Cluster herstellen. Je nach Klasse und Speicherort der DB-Instance kann es bis zu 20 Minuten dauern, bis der neue DB-Cluster verfügbar ist.

Um den neu erstellten Cluster anzuzeigen, wählen Sie Datenbanken im Navigationsbereich der Amazon RDS-Konsole aus. Wählen Sie dann den DB-Cluster aus, um die DB-Cluster-

Details anzuzeigen. Weitere Informationen finden Sie unter Anzeigen eines Amazon Aurora-DB-Clusters.



Notieren Sie sich auf der Registerkarte Konnektivität und Sicherheit den Port und den Endpunkt der Writer-DB-Instance. Verwenden Sie diesen Endpunkt und Port in den JDBC- und ODBC-Verbindungszeichenfolgen aller Anwendungen, die Lese- oder Schreibvorgänge im Cluster ausführen.

AWS CLI

> **Note**
>
> Bevor Sie mit dem einen Aurora-DB-Cluster erstellen können AWS CLI, müssen Sie die erforderlichen Voraussetzungen erfüllen, z. B. das Erstellen einer VPC und einer RDS-DB-Subnetzgruppe. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.

Sie können den verwenden AWS CLI , um einen Aurora MySQL DB-Cluster oder einen Aurora PostgreSQL DB-Cluster zu erstellen.

Um einen Aurora MySQL-DB-Cluster mit dem AWS CLI

Wenn Sie einen mit Aurora MySQL 8.0 oder 5.7 kompatiblen DB-Cluster oder eine DB-Instance erstellen, geben Sie `aurora-mysql` für die Option `--engine` an.

Führen Sie folgende Schritte aus:

1. Identifizieren Sie die DB-Subnetzgruppe und die VPC-Sicherheitsgruppen-ID für Ihren neuen DB-Cluster und rufen Sie dann den create-db-cluster AWS CLI Befehl zum Erstellen des Aurora MySQL-DB-Clusters auf.

   Z. B. erstellt der folgende Befehl ein neues MySQL 8.0-kompatibles DB-Cluster mit dem Namen `sample-cluster`. Der Cluster verwendet die Standard-Engine-Version und den Speichertyp Aurora I/O-Optimized.

   FürLinux, odermacOS: Unix

   ```
   aws rds create-db-cluster --db-cluster-identifier sample-cluster \
       --engine aurora-mysql --engine-version 8.0 \
       --storage-type aurora-iopt1 \
       --master-username user-name --manage-master-user-password \
       --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
   ```

   Windows:

   ```
   aws rds create-db-cluster --db-cluster-identifier sample-cluster ^
       --engine aurora-mysql --engine-version 8.0 ^
       --storage-type aurora-iopt1 ^
   ```

```
    --master-username user-name --manage-master-user-password ^
    --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
```

Der folgende Befehl erstellt ein neues MySQL 5.7-kompatibles DB-Cluster mit dem Namen `sample-cluster`. Der Cluster verwendet die Standard-Engine-Version und den Speichertyp Aurora Standard.

Für LinuxmacOS, oderUnix:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster  \
    --engine aurora-mysql --engine-version 5.7 \
    --storage-type aurora \
    --master-username user-name --manage-master-user-password \
    --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
```

Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster sample-cluster  ^
    --engine aurora-mysql --engine-version 5.7 ^
    --storage-type aurora ^
    --master-username user-name --manage-master-user-password ^
    --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
```

2. Wenn Sie die Konsole für das Erstellen eines DB-Clusters verwenden, erstellt Amazon RDS automatisch die primäre Instance (Writer) für Ihr DB-Cluster. Wenn Sie den verwenden, AWS CLI um einen DB-Cluster zu erstellen, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance. Die DB-Cluster-Endpunkte bleiben im Status `Creating`, bis Sie die primäre DB-Instance erstellen.

   Rufen Sie den create-db-instance AWS CLI Befehl auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Fügen Sie den Namen des DB-Clusters als `--db-cluster-identifier`-Optionswert ein.

   > **Note**
   >
   > Sie können die Option `--storage-type` für DB-Instances nicht festlegen. Sie können sie nur für DB-Cluster festlegen.

Der folgende Befehl erstellt beispielsweise eine neue MySQL 5.7-kompatible oder MySQL 8.0-kompatible DB-Instance namens `sample-instance`.

Für LinuxmacOS, oderUnix:

```
aws rds create-db-instance --db-instance-identifier sample-instance \
     --db-cluster-identifier sample-cluster --engine aurora-mysql --db-instance-
class db.r5.large
```

Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance ^
     --db-cluster-identifier sample-cluster --engine aurora-mysql --db-instance-
class db.r5.large
```

Um einen Aurora PostgreSQL-DB-Cluster mit dem AWS CLI

1. Identifizieren Sie die DB-Subnetzgruppe und die VPC-Sicherheitsgruppen-ID für Ihren neuen DB-Cluster und rufen Sie dann den create-db-cluster AWS CLI Befehl zum Erstellen des Aurora PostgreSQL-DB-Clusters auf.

   Beispielsweise erstellt der folgende Befehl ein neues DB-Cluster mit dem Namen `sample-cluster`. Der Cluster verwendet die Standard-Engine-Version und den Speichertyp Aurora I/O-Optimized.

   FürLinux, oder: macOS Unix

   ```
   aws rds create-db-cluster --db-cluster-identifier sample-cluster \
       --engine aurora-postgresql \
       --storage-type aurora-iopt1 \
       --master-username user-name --manage-master-user-password \
       --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
   ```

   Windows:

   ```
   aws rds create-db-cluster --db-cluster-identifier sample-cluster ^
       --engine aurora-postgresql ^
       --storage-type aurora-iopt1 ^
   ```

```
    --master-username user-name --manage-master-user-password ^
    --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2
```

2. Wenn Sie die Konsole für das Erstellen eines DB-Clusters verwenden, erstellt Amazon RDS automatisch die primäre Instance (Writer) für Ihr DB-Cluster. Wenn Sie den verwenden, AWS CLI um einen DB-Cluster zu erstellen, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance. Die DB-Cluster-Endpunkte bleiben im Status `Creating`, bis Sie die primäre DB-Instance erstellen.

   Rufen Sie den create-db-instance AWS CLI Befehl auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Fügen Sie den Namen des DB-Clusters als `--db-cluster-identifier`-Optionswert ein.

   Für LinuxmacOS, oderUnix:

```
aws rds create-db-instance --db-instance-identifier sample-instance \
     --db-cluster-identifier sample-cluster --engine aurora-postgresql --db-
instance-class db.r5.large
```

   Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance ^
     --db-cluster-identifier sample-cluster --engine aurora-postgresql --db-
instance-class db.r5.large
```

In diesen Beispielen wird die Option `--manage-master-user-password` zum Generieren des Hauptbenutzerpassworts und zum Verwalten dieses Passworts in Secrets Manager angegeben. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager. Alternativ können Sie die Option `--master-password` verwenden, um das Passwort selbst festzulegen und zu verwalten.

RDS-API

> **Note**
>
> Bevor Sie mit dem einen Aurora-DB-Cluster erstellen können AWS CLI, müssen Sie die erforderlichen Voraussetzungen erfüllen, z. B. das Erstellen einer VPC und einer RDS-DB-Subnetzgruppe. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.

Geben Sie die DB-Subnetzgruppe und die VPC-Sicherheitsgruppen-ID für Ihren neuen DB-Cluster an und rufen Sie anschließend die Aktion CreateDBCluster auf, um den DB-Cluster zu erstellen.

Wenn Sie einen DB-Cluster oder eine DB-Instance von Aurora MySQL Version 2 oder 3 geben Sie `aurora-mysql` für den Parameter `Engine` an.

Wenn Sie einen Aurora-PostgreSQL-DB-Cluster oder DB-Instances erstellen, müssen Sie `aurora-postgresql` für den Parameter `Engine` angeben.

Wenn Sie die Konsole für das Erstellen eines DB-Clusters verwenden, erstellt Amazon RDS automatisch die primäre Instance (Writer) für Ihr DB-Cluster. Wenn Sie die RDS-API für das Erstellen eines DB-Clusters verwenden, müssen Sie die primäre Instance für Ihren DB-Cluster mit CreateDBInstance explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance. Die DB-Cluster-Endpunkte bleiben im Status `Creating`, bis Sie die primäre DB-Instance erstellen.

Erstellen einer primären (Writer-) DB-Instance

Wenn Sie den verwenden, AWS Management Console um einen DB-Cluster zu erstellen, erstellt Amazon RDS automatisch die primäre Instance (Writer) für Ihren DB-Cluster. Wenn Sie die AWS CLI oder RDS-API verwenden, um einen DB-Cluster zu erstellen, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance. Die DB-Cluster-Endpunkte bleiben im Status `Creating`, bis Sie die primäre DB-Instance erstellen.

Weitere Informationen finden Sie unter Erstellen eines DB-Clusters.

> **Note**
>
> Wenn Sie einen DB-Cluster ohne Writer-DB-Instance haben, der auch als Headless-Cluster bezeichnet wird, können Sie die Konsole nicht zum Erstellen einer Writer-Instance verwenden. Sie müssen die AWS CLI oder RDS-API verwenden.

Im folgenden Beispiel wird der create-db-instance AWS CLI Befehl verwendet, um eine Writer-Instance für einen Aurora PostgreSQL-DB-Cluster mit dem Namen zu erstellen. `headless-test`

```
aws rds create-db-instance \
    --db-instance-identifier no-longer-headless \
    --db-cluster-identifier headless-test \
```

```
    --engine aurora-postgresql \
    --db-instance-class db.t4g.medium
```

Einstellungen für Aurora-DB-Cluster

Die folgende Tabelle enthält Einzelheiten zu Einstellungen, die Sie beim Erstellen eines Aurora-DB-Clusters wählen können.

> **Note**
>
> Wenn Sie einen Aurora Serverless v1-DB-Cluster erstellen, stehen zusätzliche Einstellungen zur Verfügung. Weitere Informationen zu diesen Einstellungen finden Sie unter Erstellen eines Aurora Serverless v1-DB Clusters. Außerdem sind einige Einstellungen für Aurora Serverless v1 aufgrund von Einschränkungen von Aurora Serverless v1 nicht verfügbar. Weitere Informationen finden Sie unter Einschränkungen von Aurora Serverless v1.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Automatisches Unterversion-Upgrade	Wählen Sie Automatische Aktualisierung von Unterversionen aktivieren aus, wenn Ihr Aurora-DB-Cluster automatisch bevorzugte Upgrades auf Unterversionen erhalten soll, sobald diese verfügbar werden. Die Einstellung Automatisches Unterversion-Upgrade gilt nur für Aurora-PostgreSQL- und Aurora-MySQL-DB-Cluster. Weitere Informationen über Engine-Updates für Aurora PostgreSQL finden Sie unter Amazon Aurora PostgreSQL-Aktualisierungen.	Legen Sie diesen Wert für jede DB-Instance in Ihrem Aurora-Cluster fest. Wenn für eine DB-Instance in Ihrem Cluster diese Einstellung deaktiviert ist, wird der Cluster nicht automatisch aktualisiert. Führen Sie mit dem die AWS CLI Option aus `create-db-instance` und legen Sie sie fest. `--auto-minor-version-upgrade|--no-auto-minor-version-upgrade` Bei Verwendung der RDS API: Rufen Sie `CreateDBInstance` auf und legen Sie den Parameter

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-P arameter
	Weitere Informationen über Engine-Updates für Aurora MySQL finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.	`AutoMinorVersionUpgrade` fest.
AWS KMS key	Nur verfügbar, wenn Verschlüs selung auf Verschlüsselung aktivieren festgelegt ist. Wählen Sie die AWS KMS key , die für die Verschlüsselung dieses DB-Clusters verwendet werden soll. Weitere Informationen finden Sie unter Verschlüsseln von Amazon Aurora-Ressourcen.	Führen Sie mit der die AWS CLI `--kms-key-id` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `KmsKeyId` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Backtrack	Gilt nur für Aurora MySQL. Wählen Sie Enable Backtrack (Rückverfolgung aktivieren) aus, um die Rückverfolgung zu aktivieren, oder Disable Backtrack (Rückverfolgung deaktivieren), um die Rückverfolgung zu deaktivieren. Mit der Rückverfolgung können Sie einen DB-Cluster auf einen bestimmten Zeitpunkt zurückspulen, ohne einen neuen DB-Cluster zu erstellen. Standardmäßig ist die Rückverfolgung deaktiviert. Wenn Sie die Rückverfolgung aktivieren, geben Sie zusätzlich den Zeitraum an, für den die Rückverfolgung des DB-Clusters möglich sein soll (Zielfenster für die Rückverfolgung). Weitere Informationen finden Sie unter Rückverfolgen eines Aurora-DB-Clusters.	Führen Sie mit der die AWS CLI `--backtrack-window` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `BacktrackWindow` fest.
Zertifizierungsstelle	Die Zertifizierungsstelle (CA) für das Serverzertifikat, das von den DB-Instances im DB-Cluster verwendet wird. Weitere Informationen finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .	Führen Sie mit der die AWS CLI `--ca-certificate-identifier` Option aus `create-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBInstance` auf und legen Sie den Parameter `CACertificateIdentifier` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Cluster-Speicherkonfiguration	Der Speichertyp für den DB-Cluster: Aurora I/O-Optimized oder Aurora Standard. Weitere Informationen finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora.	Führen Sie mit der die AWS CLI `--storage-type` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `StorageType` fest.
Tags zu Snapshots kopieren	Wählen Sie diese Option, wenn beim Erstellen eines Snapshots DB-Instance-Tags in den DB-Snapshot kopiert werden sollen. Weitere Informationen finden Sie unter Markieren von Amazon RDS-Ressourcen.	Führen Sie mit der die AWS CLI `--copy-tags-to-snapshot | --no-copy-tags-to-snapshot` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `CopyTagsToSnapshot` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Datenbank-Authentifizierung	Die Datenbank-Authentifizierung, die Sie verwenden möchten. Für MySQL: • Wählen Sie Passwortauthentifizierung aus, um Datenbankbenutzer ausschließlich mit Datenbankpasswörtern zu authentifizieren. • Wählen Sie Passwort- und IAM-Datenbank-Authentifizierung aus, um Datenbankbenutzer mit Datenbankpasswörtern und Benutzeranmeldeinformationen über IAM-Benutzer und -Rollen zu authentifizieren. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung. Für PostgreSQL: • Wählen Sie IAM database authentication (IAM-Datenbank-Authentifizierung) aus, um Datenbankbenutzer mit Datenbankpasswörtern und Benutzeranmeldeinformationen über Benutzer und Rollen zu authentifizieren. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung. • Wählen Sie Kerberos-Authentifizierung zur Authentifizierung	Um die IAM-Datenbankauthentifizierung mit dem zu verwenden AWS CLI, führen Sie die `--enable-iam-database-authentication | --no-enable-iam-database-authentication` Option aus `create-db-cluster` und legen Sie sie fest. Um die IAM-Datenbank-Authentifizierung mit der RDS API zu verwenden, rufen Sie `CreateDBCluster` auf und legen Sie die `EnableIAMDatabaseAuthentication` -Parameter fest. Um die Kerberos-Authentifizierung mit der zu verwenden AWS CLI, führen Sie die Optionen `create-db-cluster` und aus und legen Sie sie fest. `--domain --domain-iam-role-name` Um die Kerberos-Authentifizierung mit der RDS API zu verwenden, rufen Sie `CreateDBCluster` auf und legen Sie die `Domain`- und `DomainIAMRoleName` -Parameter fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
	von Datenbankkennwörtern und Benutzeranmeldeinformationen mit Kerberos-Authentifizierung. Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung mit Aurora PostgreSQL.	
Datenbankport	Geben Sie den Port an, über den Anwendungen und Dienstprogramme auf die Datenbank zugreifen können. Aurora MySQL-DB-Cluster verwenden standardmäßig den MySQL-Standardport 3306. Aurora-PostgreSQL-DB-Cluster verwenden standardmäßig den PostgreSQL-Standardport 5432. Die Firewalls einiger Unternehmen blockieren Verbindungen zu diesen Standard-Ports. Wenn die Firewall Ihres Unternehmens den Standardport blockiert, wählen Sie einen anderen Port für den neuen DB-Cluster aus.	Führen Sie mit den die AWS CLI Option aus `create-db-cluster`und legen Sie sie fest. `--port` Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `Port` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
DB-Cluster-Kennung	Geben Sie einen Namen für Ihren DB-Cluster ein, der für Ihr Konto in der von Ihnen ausgewählten AWS Region eindeutig ist. Dieser Bezeichner wird in der Cluster-Endpunktadresse für den DB-Cluster verwendet. Weitere Informationen zum Cluster-Endpunkt finden Sie unter Amazon Aurora-Verbindungsverwaltung. Für den DB-Cluster-Bezeichner gelten folgende Einschränkungen: • Sie darf 1 bis 63 alphanumerische Zeichen oder Bindestriche enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Er darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten. • Er muss für alle DB-Cluster pro AWS Konto und AWS Region eindeutig sein.	Führen Sie mit dem die AWS CLI `--db-cluster-identifier` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `DBClusterIdentifier` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
DB-Cluster-Parametergruppe	Wählen Sie eine DB-Cluster-Parametergruppe. Aurora verfügt über eine DB-Cluster-Standardparametergruppe, die Sie verwenden können, oder Sie können Ihre eigene DB-Cluster-Parametergruppe erstellen. Weitere Informationen zu DB-Cluster-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.	Führen Sie mit der die AWS CLI `--db-cluster-parameter-group-name` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `DBClusterParameterGroupName` fest.
DB-Instance-Klasse	Gilt nur für den bereitgestellten Kapazitätstyp. Wählen Sie eine DB-Instance-Klasse aus, die die Verarbeitungs- und Speicheranforderungen für jede Instance im DB-Cluster definiert. Weitere Informationen zu DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.	Legen Sie diesen Wert für jede DB-Instance in Ihrem Aurora-Cluster fest. Führen Sie mit der die AWS CLI `--db-instance-class` Option aus `create-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBInstance` auf und legen Sie den Parameter `DBInstanceClass` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
DB-Parametergruppe	Wählen Sie eine Parametergruppe. Aurora verfügt über eine Standardparametergruppe, die Sie verwenden können, oder Sie können Ihre eigene Parametergruppe erstellen. Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.	Legen Sie diesen Wert für jede DB-Instance in Ihrem Aurora-Cluster fest. Führen Sie mit der die AWS CLI `--db-parameter-group-name` Option aus `create-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBInstance` auf und legen Sie den Parameter `DBParameterGroupName` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
DB-Subnetzgruppe	Die DB-Subnetzgruppe, die Sie für den DB-Cluster verwenden möchten. Wählen Sie Choose existing (Vorhandene wählen) aus, um eine vorhandene DB-Subnetzgruppe zu verwenden. Wählen Sie dann die erforderliche Subnetzgruppe aus der Dropdown-Liste Existing DB subnet groups (Vorhandene DB-Subnetzgruppen) aus. Wählen Sie Automatic setup (Automatische Einrichtung) aus, damit RDS eine kompatible DB-Subnetzgruppe auswählen kann. Wenn keine vorhanden ist, erstellt RDS eine neue Subnetzgruppe für Ihren Cluster. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.	Führen Sie mit der die AWS CLI `--db-subnet-group-name` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `DBSubnetGroupName` fest.
Löschschutz aktivieren	Wählen Sie Löschschutz aktivieren aus, um zu verhindern, dass Ihr DB-Cluster gelöscht wird. Wenn Sie einen Produktions-DB-Cluster über die Konsole erstellen, ist der Löschschutz standardmäßig aktiviert.	Führen Sie mit der die AWS CLI `--deletion-protection | --no-deletion-protection` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `DeletionProtection` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Verschlüsselung aktivieren	Wählen Sie `Enable encryption` , um die Verschlüsselung von Daten bei der Speicherung für diesen DB-Cluster zu aktivieren. Weitere Informationen finden Sie unter Verschlüsseln von Amazon Aurora-Ressourcen.	Führen Sie mit der die AWS CLI`--storage-encrypted | --no-storage-encrypted` Option aus `create-db-cluster`und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `StorageEncrypted` fest.
Erweiterte Überwachung aktivieren	Wählen Sie Enable enhanced monitoring (Erweiterte Überwachung aktivieren) aus, um die Erfassung von Metriken in Echtzeit für das Betriebssystem zu aktivieren, in dem Ihr DB-Cluster ausgeführt wird. Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).	Legen Sie diese Werte für jede DB-Instance in Ihrem Aurora-Cluster fest. Verwenden Sie die `--monitoring-role-arn` Optionen AWS CLI, starten Sie `create-db-instance` `--monitoring-interval` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBInstance` auf und legen Sie die Parameter `MonitoringInterval` und `MonitoringRoleArn` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Aktivieren Sie die RDS-Daten-API	Wählen Sie RDS-Daten-API aktivieren, um die RDS-Daten-API (Daten-API) zu aktivieren. Die Daten-API bietet einen sicheren HTTP-Endpunkt für die Ausführung von SQL-Anweisungen, ohne Verbindungen zu verwalten. Weitere Informationen finden Sie unter Verwenden der RDS-Daten-API.	Führen Sie mit dem die AWS CLI `--enable-http-endpoint | --no-enable-http-endpoint` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `EnableHttpEndpoint` fest.
Engine-Typ	Wählen Sie den Namen der Datenbank-Engine aus, die für diesen DB-Cluster verwendet werden soll.	Führen Sie mit der die AWS CLI `--engine` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `Engine` fest.
Engine-Version	Gilt nur für den bereitgestellten Kapazitätstyp. Wählen Sie die Versionsnummer der Datenbank-Engine.	Führen Sie mit der die AWS CLI `--engine-version` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `EngineVersion` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Failover-Priorität	Wählen Sie eine Failover-Priorität für die Instance aus. Wenn Sie keinen Wert auswählen, wird als Standard tier-1 (Tier-1) eingestellt. Diese Priorität bestimmt die Reihenfolge, in der Aurora-Replikate bei der Wiederherstellung nach einem Ausfall der primären Instance hochgestuft werden. Weitere Informationen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.	Legen Sie diesen Wert für jede DB-Instance in Ihrem Aurora-Cluster fest. Führen Sie mit der die AWS CLI `--promotion-tier` Option aus `create-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBInstance` auf und legen Sie den Parameter `PromotionTier` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Anfänglicher Datenbankname	Geben Sie einen Namen für Ihre Standarddatenbank ein. Wenn Sie keinen Namen für einen Aurora MySQL-DB-Cluster angeben, erstellt Amazon RDS nicht automatisch eine Datenbank im neuen DB-Cluster. Wenn Sie keinen Namen für einen Aurora PostgreSQL-DB-Cluster angeben, erstellt Amazon RDS eine Datenbank mit dem Namen `postgres`. Für Aurora MySQL hat der Standarddatenbankname diese Einschränkungen: • Er muss 1–64 alphanumerische Zeichen enthalten. • Es darf kein von der Datenbank-Engine reserviertes Wort sein. Für Aurora PostgreSQL hat der Standarddatenbankname diese Einschränkungen: • Er muss 1–63 alphanumerische Zeichen enthalten. • Er muss mit einem Buchstaben beginnen. Nachfolgende Zeichen können Buchstaben, Unterstriche oder Ziffern sein (0–9).	Führen Sie mit der die AWS CLI `--database-name` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `DatabaseName` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
	• Es darf kein von der Datenbank-Engine reserviertes Wort sein. Verbinden Sie sich mit dem DB-Cluster und verwenden Sie den SQL-Befehl CREATE DATABASE, um zusätzliche Datenbanken zu erstellen. Weitere Informationen zum Herstellen einer Verbindung mit dem DB-Cluster finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.	
Protokollexporte	Wählen Sie im Abschnitt Protokollexporte die Protokolle aus, die Sie auf Amazon CloudWatch Logs veröffentlichen möchten. Weitere Informationen zum Veröffentlichen von Aurora MySQL-Protokollen in CloudWatch Logs finden Sie unterVeröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs. Weitere Informationen zum Veröffentlichen von Aurora PostgreSQL-Protokollen in Logs finden Sie CloudWatch unter. Veröffentlichen von Aurora-PostgreSQL-Protokollen in Amazon CloudWatch Logs	Führen Sie mit dem die AWS CLI Option aus `create-db-cluster`und legen Sie sie fest. `--enable-cloudwatch-logs-exports` Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `EnableCloudwatchLogsExports` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Wartungsfenster	Wählen Sie Fenster auswählen aus und geben Sie den wöchentlichen Zeitraum an, in dem Systemwartungen durchgeführt werden können. Oder wählen Sie für Amazon RDS Keine Präferenz aus, um zufällig einen Zeitraum zuzuordnen.	Führen Sie mit der die AWS CLI `--preferred-maintenance-window` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `PreferredMaintenanceWindow` fest.
Hauptanmeldedaten verwalten in AWS Secrets Manager	Wählen Sie Master-Anmeldeinformationen verwalten in AWS Secrets Manager aus, um das Hauptbenutzerpasswort in Secrets Manager geheim zu verwalten. Wählen Sie optional einen KMS-Schlüssel zum Schutz des Secrets aus. Wählen Sie aus den KMS-Schlüsseln in Ihrem Konto oder geben Sie den Schlüssel eines anderen Kontos ein. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager.	Verwenden Sie die AWS CLI, führen Sie die `--master-user-secret-kms-key-id` Optionen `create-db-cluster`und aus `--manage-master-user-password | --no-manage-master-user-password` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie die Parameter `ManageMasterUserPassword` und `MasterUserSecretKmsKeyId` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Hauptpasswort	Geben Sie ein Passwort ein, um sich an Ihrem DB-Cluster anzumelden: • Für Aurora MySQL muss das Passwort 8–41 druckbare ASCII-Zeichen enthalten. • Für Aurora PostgreSQL muss es 8–99 druckbare ASCII-Zeichen enthalten. • Es darf weder `/`, `"`, `@` noch ein Leerzeichen enthalten.	Führen Sie mit den die AWS CLI `--master-user-password` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `MasterUserPassword` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Master-Benutzername	Geben Sie einen Namen ein, der als Master-Benutzername für die Anmeldung an Ihrem DB-Cluster verwendet werden soll: • Für Aurora MySQL muss der Name 1–16 alphanumerische Zeichen enthalten. • Für Aurora PostgreSQL muss er 1–63 alphanumerische Zeichen enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Der Name darf kein von der Datenbank-Engine reserviertes Wort sein. Sie können den Master-Benutzernamen nicht ändern, nachdem der DB-Cluster erstellt wurde.	Führen Sie mit der die AWS CLI `--master-username` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `MasterUsername` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Multi-AZ-Bereitstellung	Gilt nur für den bereitgestellten Kapazitätstyp. Legen Sie fest, ob Aurora-Replikate in anderen Availability Zones zur Failover-Unterstützung erstellt werden sollen. Wenn Sie Create Replica in Different Zone (Replica in anderer Zone erstellen) auswählen, erstellt Amazon RDS in Ihrem DB-Cluster eine Aurora-Replica in einer anderen Availability Zone als der, in dem sich die primäre Instance Ihres DB-Clusters befindet. Weitere Informationen über die Multi-AZ-Bereitstellung finden Sie unter Regionen und Availability Zones.	Führen Sie mit der die AWS CLI `--availability-zones` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `AvailabilityZones` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Netzwerktyp	Die vom DB-Cluster unterstützten IP-Adressierungsprotokolle. IPv4, um anzugeben, dass Ressourcen mit dem DB-Cluster nur über das IPv4-Adressierungsprotokoll kommunizieren können. Dual-Stack-Modus, um anzugeben, dass Ressourcen mit dem DB-Cluster über IPv4, IPv6 oder beiden kommunizieren können. Verwenden Sie den Dual-Stack-Modus, wenn Sie über Ressourcen verfügen, die über das IPv6-Adressierungsprotokoll mit Ihrem DB-Cluster kommunizieren müssen. Wenn Sie den Dual-Stack-Modus verwenden möchten, stellen Sie sicher, dass mindestens zwei Subnetze über zwei Availability Zones verteilt sind die sowohl das IPv4- als auch das IPv6-Netzwerkprotokoll unterstützen. Stellen Sie außerdem sicher, dass Sie einen IPv6-CIDR-Block mit allen Subnetzen in der von Ihnen angegebenen DB-Subnetzgruppe verknüpfen. Weitere Informationen finden Sie unter Amazon-Aurora-IP-Adressierung.	Führen Sie mit der die AWS CLI-`network-type` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `NetworkType` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Öffentlicher Zugriff	Wählen Sie Publicly accessible (Öffentlich zugänglich), um dem DB-Cluster eine öffentliche IP-Adresse zu geben, oder wählen Sie Not publicly accessible (Nicht öffentlich zugänglich). Die Instances in Ihrem DB-Cluster können eine Mischung aus öffentlichen und privaten DB-Instances sein. Weitere Informationen darüber, wie Sie den öffentlichen Zugriff für Instances deaktivieren, finden Sie unter Ausblenden einer DB-Clusters in einer VPC vor dem Internet. Um eine Verbindung zu einer DB-Instance von außerhalb ihrer Amazon VPC herzustellen, muss die DB-Instance öffentlich zugänglich sein und der Zugriff muss unter Anwendung der Regeln für den eingehenden Datenverkehr der Sicherheitsgruppe der DB-Instance gewährt werden. Darüber hinaus müssen weitere Anforderungen erfüllt werden. Weitere Informationen finden Sie unter Verbindung zur Amazon RDS-DB-Instance kann nicht hergestellt werden. Wenn Ihre DB-Instance nicht öffentlich zugänglich ist, können	Legen Sie diesen Wert für jede DB-Instance in Ihrem Aurora-Cluster fest. Führen Sie mit dem die AWS CLI Option aus `create-db-instance` und legen Sie sie fest. `--publicly-accessible | --no-publicly-accessible` Bei Verwendung der RDS API: Rufen Sie `CreateDBInstance` auf und legen Sie den Parameter `PubliclyAccessible` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
	Sie auch eine AWS Site-to-Site-VPN-Verbindung oder eine AWS Direct Connect Verbindung verwenden, um von einem privaten Netzwerk aus darauf zuzugreifen. Weitere Informationen finden Sie unter Richtlinie für den Datenverkehr zwischen Netzwerken.	
Erweiterter RDS-Support	Wählen Sie Enable RDS Extended Support aus, damit unterstützte Engine-Hauptversionen auch nach Ablauf des Standard-Supportdatums von Aurora weiter ausgeführt werden können. Wenn Sie einen DB-Cluster erstellen, verwendet Amazon Aurora standardmäßig RDS Extended Support. Um die Erstellung eines neuen DB-Clusters nach Ablauf des Standard-Supports in Aurora zu verhindern und Gebühren für RDS Extended Support zu vermeiden, deaktivieren Sie diese Einstellung. Für Ihre vorhandenen DB-Cluster fallen bis zum Startdatum der Preise für RDS Extended Support keine Gebühren an. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Extended Support.	Führen Sie mit dem AWS CLI die `--engine-lifecycle-support` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `EngineLifecycleSupport` fest.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
RDS-Proxy	Wählen Sie Create an RDS Proxy (RDS-Proxy erstellen) aus, um einen Proxy für Ihren DB-Cluster zu erstellen. Amazon RDS erstellt automatisch eine IAM-Rolle und ein Secrets-Manager-Secret für den Proxy. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.	Nicht verfügbar beim Erstellen eines DB-Clusters
Aufbewahrungszeitraum	Wählen Sie den Aufbewahrungszeitraum (1 bis 35 Tage) für Sicherungskopien der Datenbank in Aurora aus. Sicherungskopien können sekundengenau für point-in-time Wiederherstellungen (PITR) Ihrer Datenbank verwendet werden.	Führen Sie mit dem AWS CLI die `--backup-retention-period` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `BackupRetentionPeriod` fest.
Schalte DevOps Guru ein	Wählen Sie Turn on DevOps Guru, um Amazon DevOps Guru für Ihre Aurora-Datenbank zu aktivieren. Damit DevOps Guru for RDS eine detaillierte Analyse von Leistungsanomalien bereitstellen kann, muss Performance Insights aktiviert sein. Weitere Informationen finden Sie unter DevOpsGuru für RDS einrichten.	Sie können DevOps Guru for RDS von der RDS-Konsole aus aktivieren, jedoch nicht mithilfe der RDS-API oder CLI. Weitere Informationen zum Aktivieren von DevOps Guru finden Sie im Amazon DevOps Guru-Benutzerhandbuch.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
Performance Insights aktivieren	Klicken Sie auf Performance Insights aktivieren, um Erkenntnisse zur Amazon-RDS-Leistung zu aktivieren. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .	Legen Sie diese Werte für jede DB-Instance in Ihrem Aurora-Cluster fest. Bei Verwendung der AWS CLI: Führen Sie `create-db-instance` aus und legen Sie die Optionen `--enable-performance-insights | --no-enable-performance-insights` , `--performance-insights-kms-key-id` und `--performance-insights-retention-period` fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBInstance` auf und legen Sie die Parameter `EnablePerformanceInsights` , `PerformanceInsightsKMSKeyId` und `PerformanceInsightsRetentionPeriod` fest.
Virtual Private Cloud (VPC)	Wählen Sie die VPC zum Hosten des DB-Clusters aus. Wählen Sie Create a new VPC (Neue VPC erstellen) aus, damit Amazon RDS eine VPC für Sie erstellt. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.	Für die AWS CLI AND-API geben Sie die VPC-Sicherheitsgruppen-IDs an.

Konsoleneinstellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter
VPC-Sicherheitsgruppe (Firewall)	Wählen Sie Neu erstellen aus, damit Amazon RDS eine VPC-Sicherheitsgruppe für Sie erstellt. Oder wählen Sie Vorhandene auswählen aus und geben Sie eine oder mehrere VPC-Sicherheitsgruppen an, um den Netzwerkzugriff auf den DB-Cluster zu sichern. Wenn Sie in der RDS-Konsole die Option Neu erstellen auswählen, wird eine Sicherheitsgruppe mit einer Regel für eingehenden Datenverkehr erstellt, die den Zugriff auf die DB-Instance von der im Browser erkannten IP-Adresse aus gestattet. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.	Führen Sie mithilfe von AWS CLI die `--vpc-security-group-ids` Option aus `create-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `CreateDBCluster` auf und legen Sie den Parameter `VpcSecurityGroupIds` fest.

Einstellungen, die nicht für Amazon-Aurora-DB-Cluster gelten

Die folgenden Einstellungen im AWS CLI Befehl `create-db-cluster` und im RDS-API-Vorgang `CreateDBCluster` gelten nicht für Amazon Aurora Aurora-DB-Cluster.

> **Note**
>
> Diese Einstellungen für Aurora-DB-Cluster werden AWS Management Console nicht angezeigt.

AWS CLI Einstellung	RDS-API-Einstellung
`--allocated-storage`	`AllocatedStorage`
`--auto-minor-version-upgrade | --no-auto-minor-version-upgrade`	`AutoMinorVersionUpgrade`
`--db-cluster-instance-class`	`DBClusterInstanceClass`
`--enable-performance-insights | --no-enable-performance-insights`	`EnablePerformanceInsights`
`--iops`	`Iops`
`--monitoring-interval`	`MonitoringInterval`
`--monitoring-role-arn`	`MonitoringRoleArn`
`--option-group-name`	`OptionGroupName`
`--performance-insights-kms-key-id`	`PerformanceInsightsKMSKeyId`
`--performance-insights-retention-period`	`PerformanceInsightsRetentionPeriod`
`--publicly-accessible | --no-publicly-accessible`	`PubliclyAccessible`

Einstellungen, die nicht für Amazon-Aurora-DB-Instances gelten

Die folgenden Einstellungen im AWS CLI Befehl `create-db-instance` und im RDS-API-Vorgang gelten `CreateDBInstance` nicht für DB-Instances — Amazon Aurora DB-Cluster.

> **Note**
>
> Diese Einstellungen für Aurora-DB-Instances werden AWS Management Console nicht angezeigt.

AWS CLI Einstellung	RDS-API-Einstellung
`--allocated-storage`	`AllocatedStorage`
`--availability-zone`	`AvailabilityZone`
`--backup-retention-period`	`BackupRetentionPeriod`
`--backup-target`	`BackupTarget`
`--character-set-name`	`CharacterSetName`
`--character-set-name`	`CharacterSetName`
`--custom-iam-instance-profile`	`CustomIamInstanceProfile`
`--db-security-groups`	`DBSecurityGroups`
`--deletion-protection | --no-deletion-protection`	`DeletionProtection`
`--domain`	`Domain`
`--domain-iam-role-name`	`DomainIAMRoleName`
`--enable-cloudwatch-logs-exports`	`EnableCloudwatchLogsExports`
`--enable-customer-owned-ip | --no-enable-customer-owned-ip`	`EnableCustomerOwnedIp`
`--enable-iam-database-authentication | --no-enable-iam-database-authentication`	`EnableIAMDatabaseAuthentication`
`--engine-version`	`EngineVersion`
`--iops`	`Iops`
`--kms-key-id`	`KmsKeyId`
`--master-username`	`MasterUsername`

AWS CLI Einstellung	RDS-API-Einstellung
`--master-user-password`	`MasterUserPassword`
`--max-allocated-storage`	`MaxAllocatedStorage`
`--multi-az | --no-multi-az`	`MultiAZ`
`--nchar-character-set-name`	`NcharCharacterSetName`
`--network-type`	`NetworkType`
`--option-group-name`	`OptionGroupName`
`--preferred-backup-window`	`PreferredBackupWindow`
`--processor-features`	`ProcessorFeatures`
`--storage-encrypted | --no-storage-encrypted`	`StorageEncrypted`
`--storage-type`	`StorageType`
`--tde-credential-arn`	`TdeCredentialArn`
`--tde-credential-password`	`TdeCredentialPassword`
`--timezone`	`Timezone`
`--vpc-security-group-ids`	`VpcSecurityGroupIds`

Amazon-Aurora-Ressourcen erstellen mit AWS CloudFormation

Amazon Aurora ist in AWS CloudFormation integriert, welches ein Service ist, der Ihnen hilft, Ihre AWS-Ressourcen zu modellieren und einzurichten, damit Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen können. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt (wie DB-Cluster und DB-Cluster-Parametergruppen), AWS CloudFormation und diese Ressourcen für Sie bereitstellt und konfiguriert.

Wenn Sie AWS CloudFormation verwenden, können Sie Ihre Vorlage wiederverwenden, um Ihre Aurora-Ressourcen konsistent und wiederholt einzurichten. Sie beschreiben Ihre Ressourcen dann einmal und können die gleichen Ressourcen dann in mehreren AWS-Konten und -Regionen immer wieder bereitstellen.

Aurora und AWS CloudFormation-Vorlagen

Um Ressourcen für Aurora und zugehörige Dienste bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation-Vorlagen verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer verwenden, der den Einstieg in die Arbeit mit AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

Aurora unterstützt das Erstellen von Ressourcen in AWS CloudFormation. Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für diese Ressourcen, finden Sie in der Referenz zum RDS-Ressourcentyp im AWS CloudFormation-Benutzerhandbuch.

Weitere Informationen zu AWS CloudFormation

Weitere Informationen zu AWS CloudFormation finden Sie in den folgenden Ressourcen.

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation API Referenz
- AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle

Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster

Sie können mit denselben Tools eine Verbindung zu einer DB-Instance in einem Aurora-DB-Cluster einrichten, die Sie UCH für die Verbindung mit einer MySQL- oder PostgreSQL-Datenbank verwenden. Sie geben eine Verbindungszeichenfolge mit einem beliebigen Skript, einem Hilfsprogramm oder einer Anwendung an, das/die sich mit einer MySQL- oder PostgreSQL-DB-Instance verbindet. Hierbei können Sie den gleichen öffentlichen Schlüssel für Secure Sockets Layer (SSL)-Verbindungen nutzen.

In der Verbindungszeichenfolge verwenden Sie typischerweise die Host- und Port-Informationen von besonderen mit dem DB-Cluster verbundenen Endpunkten. Mit diesen Endpunkten können Sie dieselben Verbindungsparameter verwenden, unabhängig davon, wie viele DB-Instances sich in dem Cluster befinden. Sie können die Host- und Port-Informationen aus einer spezifischen DB-Instance in Ihrem Aurora-DB_Cluster für spezielle Aufgaben wie die Fehlerbehebung verwenden.

> **Note**
>
> Bei Aurora Serverless-DB-Clustern stellen Sie eine Verbindung zum Datenbank-Endpunkt statt mit der DB-Instance her. Sie finden den Datenbank-Endpunkt für einen Aurora Serverless-DB-Cluster auf der Registerkarte Connectivity & security (Konnektivität und Sicherheit) von AWS Management Console. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Serverless v1.

Unabhängig von der Aurora-DB-Engine und spezifischen Tools, die Sie für die Arbeit mit dem DB-Cluster oder der Instance verwenden, muss der Endpunkt zugänglich sein. Ein Aurora-DB-Cluster kann nur in einer Virtual Private Cloud (VPC) erstellt werden, die auf dem Amazon VPC-Service basiert. Das bedeutet, dass Sie mit einem der folgenden Ansätze entweder innerhalb der VPC oder außerhalb der VPC auf den Endpunkt zugreifen.

- Zugriff auf den Aurora-DB-Cluster innerhalb der VPC — Aktivieren Sie den Zugriff auf den Aurora-DB-Cluster über die VPC. Sie tun dies, indem Sie die Inbound-Regeln der Sicherheitsgruppe für die VPC bearbeiten, um den Zugriff auf Ihren spezifischen Aurora-DB-Cluster zu ermöglichen. Weitere Informationen, einschließlich der Konfiguration Ihrer VPC für verschiedene Aurora-DB-Cluster-Szenarien, finden Sie unter Amazon Virtual Private Cloud VPCs und Amazon Aurora.
- Zugriff auf den Aurora-DB-Cluster außerhalb der VPC — Um von außerhalb der VPC auf einen Aurora-DB-Cluster zuzugreifen, verwenden Sie die öffentliche Endpunktadresse des DB-Clusters.

Weitere Informationen finden Sie unter Behebung von Aurora-Verbindungsfehlern.

Inhalt

Mit den AWS Treibern eine Verbindung zu Aurora-DB-Clustern herstellen

Die AWS Treibersuite wurde so konzipiert, dass sie schnellere Switchover- und Failover-Zeiten sowie Authentifizierung mit AWS Secrets Manager, AWS Identity and Access Management (IAM) und Federated Identity unterstützt. Die AWS Treiber sind darauf angewiesen, den Status des DB-Clusters zu überwachen und die Clustertopologie zu kennen, um den neuen Writer zu ermitteln. Dieser Ansatz reduziert die Switchover- und Failover-Zeiten auf einstellige Sekunden, im Vergleich zu mehreren zehn Sekunden bei Open-Source-Treibern.

In der folgenden Tabelle sind die Funktionen aufgeführt, die für die einzelnen Treiber unterstützt werden. Im Zuge der Einführung neuer Servicefunktionen besteht das Ziel der AWS Treibersuite darin, eine integrierte Unterstützung für diese Servicefunktionen zu bieten.

Funktion	AWS JDBC-Treiber	AWS Python-Treiber
Failover-Unterstützung	Ja	Ja
Verbesserte Failover-Überwachung	Ja	Ja
Aufteilung von Lese-/Schreibvorgängen	Ja	Ja
Aurora-Verbindungs-Tracker	Ja	Ja
Verbindung mit Treiber-Metadaten	Ja	N/A
Telemetrie	Ja	Ja
Secrets Manager	Ja	Ja
IAM-Authentifizierung	Ja	Ja
Föderierte Identität (AD FS)	Ja	Ja
Föderierte Identität (Okta)	Ja	Nein

Weitere Informationen zu den AWS Treibern finden Sie im entsprechenden Sprachtreiber für Ihren Aurora MySQL- oder Aurora PostgreSQL-DB-Cluster.

Herstellen einer Verbindung mit einem Amazon Aurora MySQL-DB-Cluster

Um sich bei Ihrem Aurora MySQL-DB-Cluster zu authentifizieren, können Sie entweder die MySQL-Authentifizierung mit Benutzername und Passwort oder die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung verwenden. Weitere Informationen über die Verwendung der MySQL-Benutzernamen- und Passwort-Authentifizierung finden Sie unter Access Control and Account Management in der MySQL-Dokumentation. Weitere Informationen zur Verwendung der IAM-Datenbankauthentifizierung finden Sie unter IAM-Datenbankauthentifizierung.

Wenn Sie eine Verbindung mit Ihrem Amazon-Aurora-DB-Cluster mit MySQL 8.0-Kompatibilität hergestellt haben, können Sie SQL-Befehle ausführen, die mit MySQL 8.0 kompatibel sind. Die

minimale kompatible Version ist MySQL 8.0.23. Weitere Informationen zur MySQL 8.0-SQL-Syntax finden Sie im MySQL 8.0-Referenzhandbuch. Informationen zu Einschränkungen für Aurora-MySQL-Version 3 finden Sie unter Vergleich von Aurora-MySQL-Version 3 und MySQL 8.0 Community Edition.

Wenn Sie eine Verbindung mit Ihrem Amazon-Aurora-DB-Cluster mit MySQL 5.7-Kompatibilität hergestellt haben, können Sie SQL-Befehle ausführen, die mit MySQL 5.7 kompatibel sind. Weitere Informationen zur MySQL 5.7-SQL-Syntax finden Sie im MySQL 5.7-Referenzhandbuch. Informationen zu Einschränkungen für Aurora MySQL 5.7 finden Sie unter Aurora-MySQL-Version 2, kompatibel mit MySQL 5.7.

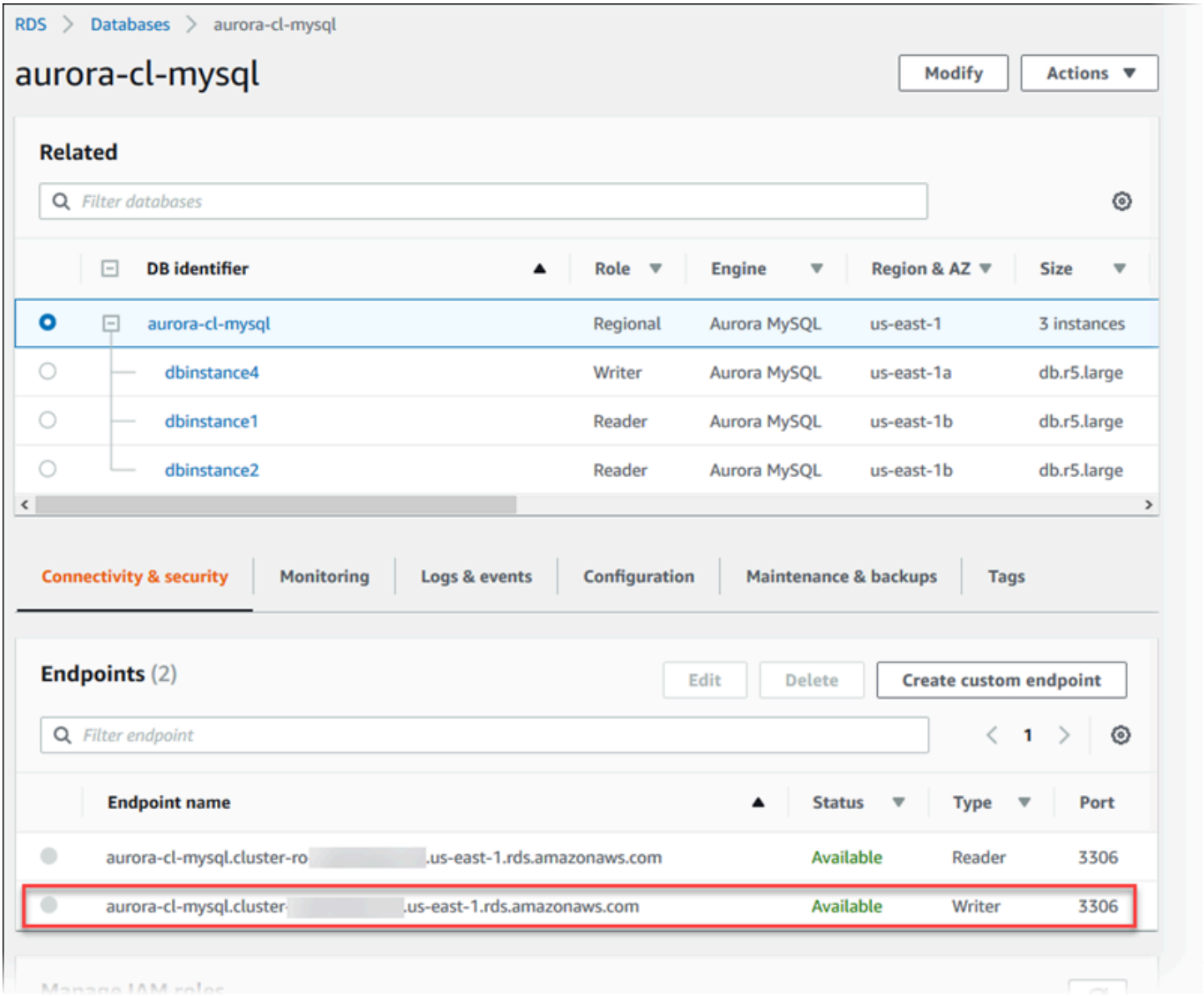
> **Note**
>
> Eine nützliche und detaillierte Anleitung für die Herstellung von Verbindungen mit einem Amazon Aurora MySQL-DB-Cluster finden Sie im Handbuch für das Aurora-Verbindungsmanagement.

In der Detailansicht für Ihren DB-Cluster finden Sie den Cluster-Endpunkt, den Sie in Ihrer MySQL-Verbindungszeichenfolge verwenden können. Der Endpunkt besteht aus dem Domänenamen und dem Port für Ihr DB-Cluster. Wenn beispielsweise ein Endpunktwert `mycluster.cluster-123456789012.us-east-1.rds.amazonaws.com:3306` lautet, sollten Sie die folgenden Werte in einer MySQL-Verbindungszeichenfolge angeben:

- Geben Sie als Host oder Host-Namen, an `mycluster.cluster-123456789012.us-east-1.rds.amazonaws.com`
- Geben Sie für Port `3306` oder den Port-Wert an, den Sie beim Erstellen des DB-Clusters verwendet haben

Der Cluster-Endpunkt verbindet Sie mit der primären Instance für das DB-Cluster. Sie können sowohl Lese- als auch Schreiboperationen mithilfe des Cluster-Endpunkts durchführen. Ihr DB-Cluster kann darüber hinaus bis zu 15 Aurora-Replicas besitzen, die einen schreibgeschützten Zugriff auf die Daten im DB-Cluster unterstützen. Die primäre Instance und jede Aurora-Replica haben jeweils einen eindeutigen Endpunkt, der unabhängig vom Cluster-Endpunkt ist, und Ihnen ermöglicht sich mit einer bestimmten DB-Instance im Cluster direkt zu verbinden. Der Cluster-Endpunkt verweist immer auf die primäre Instance. Falls die primäre Instance ausfällt und ersetzt wird, verweist der Cluster-Endpunkt auf die neue primäre Instance.

Um den Cluster-Endpunkt (Writer-Endpunkt) anzuzeigen, wählen Sie Databases (Datenbanken) in der Amazon RDS-Konsole und anschließend den Namen des DB-Clusters aus, um die Details des DB-Clusters anzuzeigen.



Themen

- Hilfsprogramme für die Herstellung von Verbindungen für Aurora MySQL
- Mit dem MySQL-Hilfsprogramm eine Verbindung zu Aurora MySQL herstellen
- Mit dem Amazon Web Services (AWS) JDBC-Treiber eine Verbindung zu Aurora MySQL herstellen
- Mit dem Amazon Web Services (AWS) Python-Treiber eine Verbindung zu Aurora MySQL herstellen
- Mit SSL eine Verbindung zu Aurora MySQL herstellen

Hilfsprogramme für die Herstellung von Verbindungen für Aurora MySQL

Unter anderem können Sie dazu die folgenden Verbindungsdienstprogramme verwenden:

- Befehlszeile – Sie können mittels Tools wie dem MySQL-Befehlszeilen-Hilfsprogramm Verbindungen mit einem Amazon-Aurora-DB-Cluster herstellen: Weitere Informationen zur Verwendung des MySQL-Hilfsprogramms finden Sie unter mysql – The MySQL Command Line Tool in der MySQL-Dokumentation.
- GUI – Sie können das Hilfsprogramm MySQL Workbench verwenden, um eine Verbindung über eine Benutzeroberfläche herzustellen. Weitere Informationen finden Sie auf der Seite Download MySQL Workbench.
- AWS Treiber:
  - Mit dem Amazon Web Services (AWS) JDBC-Treiber eine Verbindung zu Aurora MySQL herstellen
  - Mit dem Amazon Web Services (AWS) Python-Treiber eine Verbindung zu Aurora MySQL herstellen

Mit dem MySQL-Hilfsprogramm eine Verbindung zu Aurora MySQL herstellen

Gehen Sie wie folgt vor: Es wird davon ausgegangen, dass Sie Ihren DB-Cluster in einem privaten Subnetz der VPC konfiguriert haben. Sie stellen eine Verbindung mit einer Amazon-EC2-Instance her, die Sie gemäß den Tutorials in Tutorial: Erstellen eines Webservers und einer eines Amazon Aurora-DB-Clusters konfiguriert haben.

> **Note**
>
> Für dieses Verfahren ist die Installation des Webservers im Tutorial nicht nötig, erfordert jedoch die Installation von MariaDB 10.5.

So stellen Sie eine Verbindung mit einem DB-Cluster mit dem MySQL-Dienstprogramm her

1. Melden Sie sich bei der EC2-Instance an, die Sie verwenden, um eine Verbindung mit Ihrem DB-Cluster herzustellen.

   Die Ausgabe sollte in etwa wie folgt aussehen:

   ```
   Last login: Thu Jun 23 13:32:52 2022 from xxx.xxx.xxx.xxx
   ```

```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-xxx.xxx ~]$
```

2. Geben Sie den folgenden Befehl in die Befehlszeile ein, um eine Verbindung mit der primären DB-Instance Ihres DB-Clusters herzustellen.

   Ersetzen Sie für den `-h`-Parameter den Endpunkt-DNS-Namen für Ihre primäre Instance. Ersetzen Sie den `-u`-Parameter durch die Benutzer-ID eines Datenbankbenutzerkontos.

   ```
   mysql -h primary-instance-endpoint.AWS_account.AWS_Region.rds.amazonaws.com -P 3306
    -u database_user -p
   ```

   Beispiel:

   ```
   mysql -h my-aurora-cluster-instance.c1xy5example.123456789012.eu-
   central-1.rds.amazonaws.com -P 3306 -u admin -p
   ```

3. Geben Sie das Passwort für den Datenbankbenutzer ein.

   Die Ausgabe sollte in etwa wie folgt aussehen:

   ```
   Welcome to the MariaDB monitor.  Commands end with ; or \g.
   Your MySQL connection id is 1770
   Server version: 8.0.23 Source distribution

   Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

   Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

   MySQL [(none)]>
   ```

4. Geben Sie Ihre SQL-Befehle ein.

Mit dem Amazon Web Services (AWS) JDBC-Treiber eine Verbindung zu Aurora MySQL herstellen

Der Amazon Web Services (AWS) JDBC-Treiber ist als fortschrittlicher JDBC-Wrapper konzipiert. Dieser Wrapper ergänzt und erweitert die Funktionalität eines vorhandenen JDBC-Treibers, sodass Anwendungen die Funktionen von Cluster-Datenbanken wie Aurora MySQL nutzen können. Der Treiber ist Drop-In-kompatibel mit dem Community-Treiber MySQL Connector/J und dem Community-Treiber MariaDB Connector/J.

Um den AWS JDBC-Treiber zu installieren, hängen Sie die JAR-Datei des JDBC-Treibers an (befindet sich in der Anwendung) und AWS behalten Sie die Verweise auf den jeweiligen Community-Treiber bei. `CLASSPATH` Aktualisieren Sie das jeweilige Verbindungs-URL-Präfix wie folgt:

- `jdbc:mysql://` auf `jdbc:aws-wrapper:mysql://`
- `jdbc:mariadb://` auf `jdbc:aws-wrapper:mariadb://`

Weitere Informationen zum AWS JDBC-Treiber und vollständige Anweisungen zu seiner Verwendung finden Sie im Amazon Web Services (AWS) JDBC-Treiber-Repository. GitHub

> **Note**
>
> Version 3.0.3 des Dienstprogramms MariaDB Connector/J stellt die Unterstützung für Aurora-DB-Cluster ein. Wir empfehlen daher dringend, zum JDBC-Treiber zu wechseln. AWS

Mit dem Amazon Web Services (AWS) Python-Treiber eine Verbindung zu Aurora MySQL herstellen

Der Amazon Web Services (AWS) Python-Treiber ist als fortschrittlicher Python-Wrapper konzipiert. Dieser Wrapper ergänzt den Open-Source-Treiber Psycopg und erweitert dessen Funktionalität. Der AWS Python-Treiber unterstützt Python-Versionen 3.8 und höher. Sie können das `aws-advanced-python-wrapper` Paket zusammen mit den `psycopg` Open-Source-Paketen mit dem `pip` Befehl installieren.

Weitere Informationen zum AWS Python-Treiber und vollständige Anweisungen zu seiner Verwendung finden Sie im GitHub Python-Treiber-Repository von Amazon Web Services (AWS).

Mit SSL eine Verbindung zu Aurora MySQL herstellen

Sie können SSL-Verschlüsselung für Verbindungen mit einer Aurora MySQL DB-Instance verwenden. Weitere Informationen finden Sie unter Verwenden von TLS mit DB-Clustern von Aurora MySQL.

Verwenden Sie das MySQL-Hilfsprogramm wie im folgenden Vorgang beschrieben, um eine Verbindung per SSL herzustellen. Wenn Sie die IAM-Datenbank-Authentifizierung nutzen, müssen Sie eine SSL-Verbindung verwenden. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung.

> **Note**
>
> Damit Sie sich mit dem Cluster-Endpunkt unter Verwendung von SSL verbinden können, muss Ihr Client-Verbindungshilfsprogramm Subject Alternative Names (SAN) unterstützen. Wenn Ihr Client-Verbindungshilfsprogramm kein SAN unterstützt, können Sie sich nicht direkt mit den Instances in Ihrem Aurora-DB-Cluster verbinden. Weitere Informationen zu Aurora-Endpunkten finden Sie unter Amazon Aurora-Verbindungsverwaltung.

So stellen Sie eine SSL-Verbindung mit einem DB-Cluster mittels des MySQL-Hilfsprogramms her:

1. Laden Sie den öffentlichen Schlüssel für das Amazon RDS-Signaturzertifikat herunter.

   Informationen zum Herunterladen von Zertifikaten finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .
2. Geben Sie den folgenden Befehl in die Befehlszeile ein, um sich mit der primären Instance eines DB-Clusters per SSL mithilfe des MySQL-Hilfsprogramms zu verbinden. Ersetzen Sie für den `-h`-Parameter den Endpunkt-DNS-Namen für Ihre primäre Instance. Ersetzen Sie den `-u`-Parameter durch die Benutzer-ID eines Datenbankbenutzerkontos. Ersetzen Sie entsprechend den SSL-Zertifikatsnamen für den Parameter `--ssl-ca`. Geben Sie das Hauptbenutzerpasswort ein, falls Sie aufgefordert werden.

   ```
   mysql -h mycluster-primary.123456789012.us-east-1.rds.amazonaws.com -u admin_user -p --ssl-ca=[full path]global-bundle.pem --ssl-verify-server-cert
   ```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
```

```
Your MySQL connection id is 350
Server version: 8.0.26-log MySQL Community Server (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Allgemeine Anweisungen zum Konstruieren von RDS for MySQL-Verbindungszeichenfolgen und zum Auffinden des öffentlichen Schlüssels für SSL-Verbindungen finden Sie unter Verbinden mit einer DB-Instance auf einer MySQL-Datenbank-Engine.

Herstellen einer Verbindung mit einem Amazon-Aurora-PostgreSQL-DB-Cluster

Sie können sich mit einer DB-Instance in Ihrem Amazon Aurora PostgreSQL-DB-Cluster mit denselben Tools verbinden, die Sie für die Verbindung mit einer PostgreSQL-Datenbank verwendet haben. Hierbei können Sie den gleichen öffentlichen Schlüssel für Secure Sockets Layer (SSL)-Verbindungen nutzen. Sie können die Endpunkt- und Portinformationen der primären Instance oder der Aurora-Replicas in Ihrem Aurora-PostgreSQL-DB-Cluster in der Verbindungszeichenfolge aller Skripts, Hilfsprogramme oder Anwendungen verwenden, die Verbindungen mit einer PostgreSQL-DB-Instance herstellen. Geben Sie in der Verbindungszeichenfolge die DNS-Adresse aus der primären Instance oder dem Endpunkt der Aurora-Replica als Host-Parameter an. Geben Sie die Portnummer aus dem Endpunkt als Portparameter an.

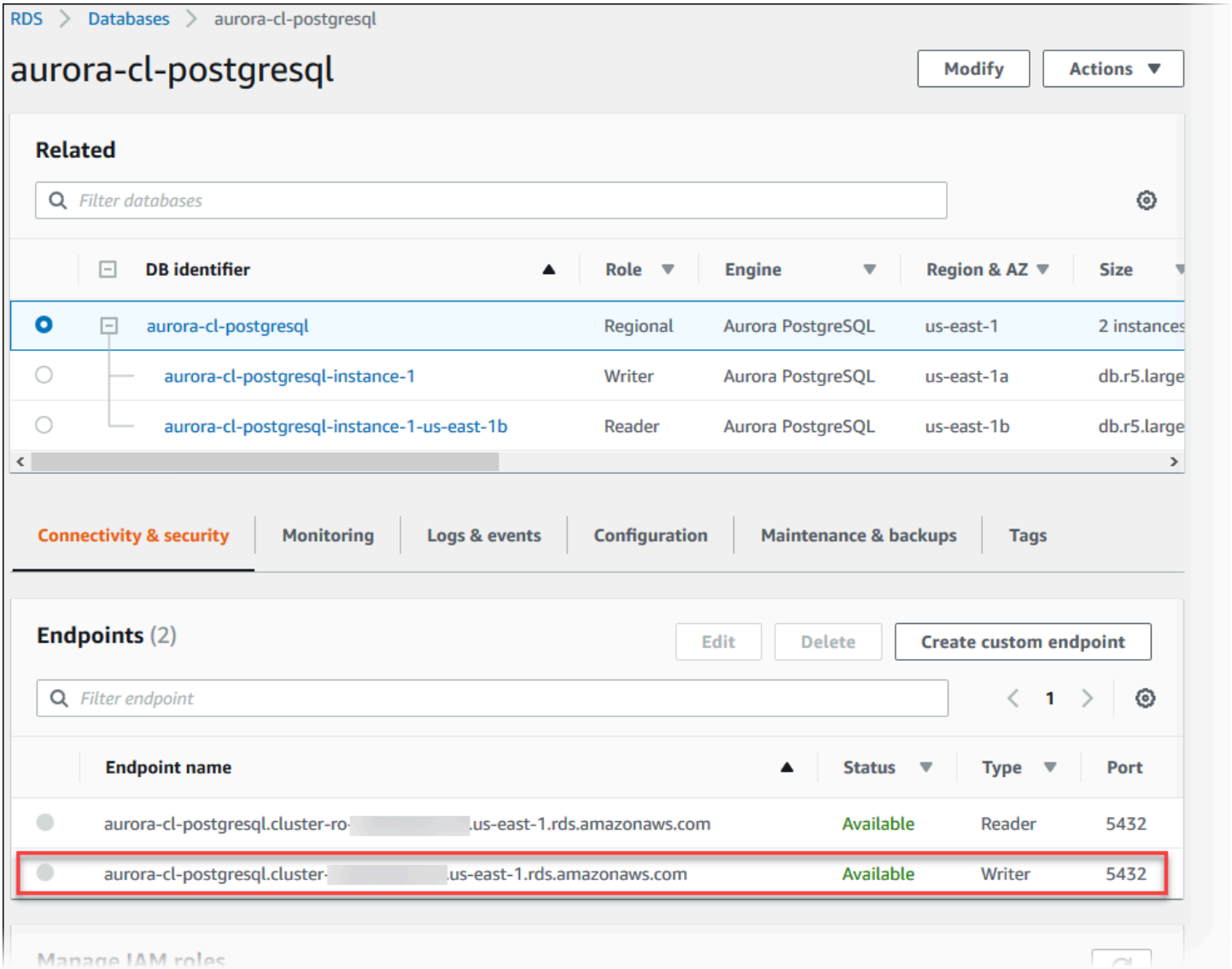
Sobald Sie eine Verbindung zu einer DB-Instance in Ihrem Amazon-Aurora-PostgreSQL-DB-Cluster hergestellt haben, können Sie einen beliebigen SQL-Befehl ausführen, der mit PostgreSQL kompatibel ist.

In der Detailansicht Ihres Aurora-PostgreSQL-DB-Clusters finden Sie den Cluster-Endpunktnamen, den Status, den Typ und die Portnummer. Sie verwenden den Endpunkt und die Portnummer in Ihrer PostgreSQL-Verbindungszeichenfolge. Wenn beispielsweise der Endpunktwert `mycluster.cluster-123456789012.us-east-1.rds.amazonaws.com` lautet, geben Sie die folgenden Werte in der PostgreSQL-Verbindungszeichenfolge an:

- Geben Sie als Host oder Host-Namen, an `mycluster.cluster-123456789012.us-east-1.rds.amazonaws.com`
- Geben Sie für Port `5432` oder den Port-Wert an, den Sie beim Erstellen des DB-Clusters verwendet haben

Der Cluster-Endpunkt verbindet Sie mit der primären Instance für das DB-Cluster. Sie können sowohl Lese- als auch Schreiboperationen mithilfe des Cluster-Endpunkts durchführen. Ihr DB-Cluster kann darüber hinaus bis zu 15 Aurora-Replicas besitzen, die einen schreibgeschützten Zugriff auf die Daten im DB-Cluster unterstützen. Jede DB-Instance im Aurora-Cluster (d. h. die primäre Instance und alle Aurora-Replicas) besitzt einen eindeutigen Endpunkt, der vom Cluster-Endpunkt unabhängig ist. Über diesen eindeutigen Endpunkt können Sie eine direkte Verbindung zu einer bestimmten DB-Instance im Cluster herstellen. Der Cluster-Endpunkt verweist immer auf die primäre Instance. Falls die primäre Instance ausfällt und ersetzt wird, verweist der Cluster-Endpunkt auf die neue primäre Instance.

Um den Cluster-Endpunkt (Writer-Endpunkt) anzuzeigen, wählen Sie Databases (Datenbanken) in der Amazon RDS-Konsole und anschließend den Namen des DB-Clusters aus, um die Details des DB-Clusters anzuzeigen.



Hilfsprogramme für die Herstellung von Verbindungen für Aurora PostgreSQL

Unter anderen können Sie dazu die folgenden Verbindungsdienstprogramme verwenden:

- Befehlszeile: Sie können mittels Tools wie dem interaktiven PostgreSQL-Terminal psql Verbindungen mit DB-Clustern von Aurora PostgreSQL herstellen. Weitere Informationen über die Verwendung des interaktiven PostgreSQL-Terminals finden Sie unter psql in der PostgreSQL-Dokumentation.
- GUI: Sie können das Dienstprogramm pgAdmin verwenden, um über eine Benutzeroberfläche Verbindungen mit DB-Clustern von Aurora PostgreSQL herzustellen. Weitere Informationen finden Sie auf der Seite Download der pgAdmin-Website.
- AWS Treiber:
  - Mit dem Amazon Web Services (AWS) JDBC-Treiber eine Verbindung zu Aurora PostgreSQL herstellen
  - Herstellen einer Verbindung zu Aurora PostgreSQL mit dem Amazon Web Services (AWS) Python-Treiber

Mit dem Amazon Web Services (AWS) JDBC-Treiber eine Verbindung zu Aurora PostgreSQL herstellen

Der Amazon Web Services (AWS) JDBC-Treiber ist als fortschrittlicher JDBC-Wrapper konzipiert. Dieser Wrapper ergänzt und erweitert die Funktionalität eines vorhandenen JDBC-Treibers, sodass Anwendungen die Funktionen von Cluster-Datenbanken wie Aurora PostgreSQL nutzen können. Der Treiber ist Drop-In-kompatibel mit dem Community-Treiber PGJDBC.

Um den AWS JDBC-Treiber zu installieren, hängen Sie die JAR-Datei des AWS JDBC-Treibers an (befindet sich in der Anwendung`CLASSPATH`) und behalten Sie die Verweise auf den PGJDBC-Community-Treiber bei. Aktualisieren Sie `jdbc:postgresql://` `jdbc:aws-wrapper:postgresql://` das Verbindungs-URL-Präfix von bis.

Weitere Informationen zum AWS JDBC-Treiber und vollständige Anweisungen zu seiner Verwendung finden Sie im Amazon Web Services (AWS) JDBC-Treiber-Repository. GitHub

Herstellen einer Verbindung zu Aurora PostgreSQL mit dem Amazon Web Services (AWS) Python-Treiber

Der Amazon Web Services (AWS) Python-Treiber ist als fortschrittlicher Python-Wrapper konzipiert. Dieser Wrapper ergänzt den Open-Source-Treiber Psycopg und erweitert dessen Funktionalität. Der

AWS Python-Treiber unterstützt Python-Versionen 3.8 und höher. Sie können das `aws-advanced-python-wrapper` Paket zusammen mit den `psycopg` Open-Source-Paketen mit dem `pip` Befehl installieren.

Weitere Informationen zum AWS Python-Treiber und vollständige Anweisungen zu seiner Verwendung finden Sie im GitHub Python-Treiber-Repository von Amazon Web Services (AWS).

Behebung von Aurora-Verbindungsfehlern

Häufige Ursachen für Verbindungsfehler mit einem neuen Aurora-DB-Cluster umfassen Folgende:

- Die Sicherheitsgruppe in der VPC erlaubt keinen Zugriff – Ihre VPC muss Verbindungen von Ihrem Gerät oder von einer Amazon-EC2-Instance durch ordnungsgemäße Konfiguration der Sicherheitsgruppe in der VPC zulassen. Um dies zu beheben, ändern Sie die Inbound-Regeln der Sicherheitsgruppe Ihrer VPC, um Verbindungen zuzulassen. Ein Beispiel finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4).
- Port durch Firewallregeln blockiert – Überprüfen Sie den Wert des für Ihren Aurora-DB-Cluster konfigurierten Ports. Wenn eine Firewallregel diesen Port blockiert, können Sie die Instance mithilfe eines anderen Ports neu erstellen.
- Unvollständige oder falsche IAM Konfiguration – Wenn Sie Ihre Aurora-DB-Instance für die Verwendung von IAM–basierter Authentifizierung erstellt haben, stellen Sie sicher, dass sie ordnungsgemäß konfiguriert ist. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung.

Weitere Informationen zur Fehlerbehebung von Aurora DB-Verbindungsproblemen finden Sie unter Verbindung zur Amazon RDS-DB-Instance kann nicht hergestellt werden.

Arbeiten mit Parametergruppen

Database parameters (Datenbankparameter) – geben Sie an, wie die Datenbank konfiguriert wird. Datenbankparameter können z. B. die Menge der Ressourcen angeben, die einer Datenbank zugewiesen werden sollen, wie etwa den Speicher.

Sie verwalten Ihre Datenbankkonfiguration, indem Sie Ihre DB-Instances und Aurora-DB-Cluster mit Parametergruppen zuordnen. Aurora definiert Parametergruppen mit Standardeinstellungen. Sie können auch eigene Parametergruppen mit angepassten Einstellungen definieren.

Themen

Übersicht über Parametergruppen

Eine DB-Cluster-Parametergruppe dient als Container für Engine-Konfigurationswerte, die für jede DB-Instance in einem Aurora-DB-Cluster gelten. Das freigegebene Aurora-Speichermodell erfordert, dass jede DB-Instance in einem Aurora-Cluster dieselbe Einstellung für Parameter wie verwende `innodb_file_per_table`. Daher sind Parameter, die sich auf das Layout des physischen Speichers auswirken, Teil der Cluster-Parametergruppe. Die DB-Cluster-Parametergruppe enthält auch Standardwerte für alle Parameter auf Instance-Ebene.

Eine DB-Parametergruppe dient als Container für Engine-Konfigurationswerte, die auf eine oder mehrere DB-Instances angewendet werden. DB-Parametergruppen gelten für DB-Instances in Amazon RDS und Aurora. Diese Konfigurationseinstellungen gelten für Eigenschaften, die je nach DB-Instances in einem Aurora-Cluster unterschiedlich sein können, z. B. Größe der Speicherpuffer.

Themen

- Zeichensatzparameter
- Unterstützte Parameter und Parameterwerte

Standard- und benutzerdefinierte Parametergruppen

Wenn Sie eine DB-Instance ohne Angabe einer DB-Parametergruppe erstellen, verwendet die DB-Instance eine Standard-DB-Parametergruppe. Beim Erstellen eines Aurora-DB-Clusters ohne Angabe einer DB-Cluster-Parametergruppe verwendet der DB-Cluster ebenso eine Standard-DB-Cluster-Parametergruppe. Jede Standard-Parametergruppe enthält Standardeinstellungen für die Datenbank-Engine und das Amazon RDS-System, die auf der Engine, der Datenverarbeitungsklasse und dem zugeordneten Speicher der Instance basieren.

Sie können die Parametereinstellungen für eine Standard-Parametergruppe nicht ändern. Stattdessen können Sie Folgendes tun:

1. Neue Parametergruppe erstellen.
2. Ändern Sie die Einstellungen Ihrer gewünschten Parameter. In einer Parametergruppe können nicht alle DB-Engine-Parameter geändert werden.
3. Ändern Sie Ihre DB-Instance oder Ihren DB-Cluster, um die neue Parametergruppe zuzuordnen.

   Informationen zum Ändern eines DB-Clusters oder einer DB-Instance finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

   > **Note**
   >
   > Wenn Sie Ihre DB-Instance so geändert haben, dass sie eine benutzerdefinierte Parametergruppe verwendet, und Sie die DB-Instance starten, startet RDS die DB-Instance im Rahmen des Startvorgangs automatisch neu.

RDS wendet die geänderten statischen und dynamischen Parameter in einer neu zugeordneten Parametergruppe erst an, nachdem die DB-Instance neu gestartet wurde. Wenn Sie jedoch dynamische Parameter in der DB-Parametergruppe ändern, nachdem Sie sie der DB-Instance zugeordnet haben, werden diese Änderungen sofort ohne Neustart angewendet. Weitere Informationen zum Ändern der DB-Parametergruppe finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Wenn Sie Parameter innerhalb einer DB-Parametergruppe aktualisieren, gelten die Änderungen für alle DB-Instances, die dieser Parametergruppe zugeordnet sind. Wenn Sie Parameter innerhalb einer Parametergruppe eines Aurora-DB-Clusters aktualisieren, gelten die Änderungen ebenso für alle Aurora-DB-Cluster, die dieser DB-Cluster-Parametergruppe zugeordnet sind.

Wenn Sie keine Parametergruppe von Grund auf neu erstellen möchten, können Sie eine vorhandene Parametergruppe mit dem AWS CLI copy-db-parameter-group Befehl oder dem Befehl copy-db-cluster-parameter-group kopieren. Das Kopieren einer Parametergruppe kann sich in einigen Fällen als nützlich erweisen. Wenn Sie beispielsweise die am häufigsten verwendeten benutzerdefinierten Parameter und Werte einer vorhandenen -Parametergruppe in eine neue -Parametergruppe aufnehmen möchten.

Statische und dynamische DB-Cluster-Parameter

Die DB-Cluster-Parameter sind entweder statisch oder dynamisch. Sie unterscheiden sich in den folgenden Punkten:

- Wenn Sie einen statischen Parameter ändern und die DB-Cluster-Parametergruppe speichern, wird die Änderung des Parameters nach einem manuellen Neustart der DB-Instances in jedem zugeordneten DB-Cluster wirksam. Wenn Sie die verwenden AWS Management Console , um statische DB-Cluster-Parameterwerte zu ändern, wird immer `pending-reboot` für die verwendet`ApplyMethod`.
- Wenn Sie einen dynamischen Parameter ändern, wird die Parameteränderung standardmäßig sofort wirksam, ohne dass ein Neustart erforderlich ist. Wenn Sie die Konsole verwenden, wird immer `immediate` als `ApplyMethod` verwendet. Um die Parameteränderung aufschieben, bis Sie die DB-Instances in einem zugeordneten DB-Cluster neu gestartet haben, verwenden Sie die AWS CLI oder RDS-API. Legen Sie die `ApplyMethod` für die Parameteränderung auf `pending-reboot` fest.

Weitere Informationen zur Verwendung der AWS CLI zum Ändern eines Parameterwerts finden Sie unter modify-db-cluster-parameter-group. Weitere Informationen zur Verwendung der RDS-API zum Ändern eines Parameterwerts finden Sie unter ModifyDBClusterParameterGroup.

Wenn Sie die DB-Cluster-Parametergruppe geändert haben, die einem DB-Cluster zugeordnet ist, starten Sie die DB-Instances im DB-Cluster neu. Durch den Neustart werden die Änderungen auf alle DB-Instances im DB-Cluster angewendet. Um zu ermitteln, ob die DB-Instances eines DB-Clusters zum Übernehmen von Änderungen neu gestartet werden muss, führen Sie den folgenden AWS CLI -Befehl aus.

```
aws rds describe-db-clusters --db-cluster-identifier db_cluster_identifier
```

Überprüfen Sie den Wert `DBClusterParameterGroupStatus` für die primäre DB-Instance in der Ausgabe. Wenn der Wert `pending-reboot` lautet, starten Sie die DB-Instances des DB-Clusters neu.

Statische und dynamische DB-Instance-Parameter

Die DB-Instance-Parameter sind entweder statisch oder dynamisch. Sie weisen folgende Unterschiede auf:

- Wenn Sie einen statischen Parameter ändern und eine DB-Parametergruppe speichern, wird die Änderung des Parameters nach einem manuellen Neustart der zugeordneten DB-Instances angewendet. Bei statischen Parametern verwendet die Konsole immer `pending-reboot` als `ApplyMethod`.
- Wenn Sie einen dynamischen Parameter ändern, wird die Parameteränderung standardmäßig sofort wirksam, ohne dass ein Neustart erforderlich ist. Wenn Sie die verwenden, AWS Management Console um DB-Instance-Parameterwerte zu ändern, wird immer `immediate` für die `ApplyMethod` für dynamische Parameter verwendet. Um die Parameteränderung aufschieben, bis Sie eine zugeordnete DB-Instance neu gestartet haben, verwenden Sie die AWS CLI oder RDS-API. Legen Sie die `ApplyMethod` für die Parameteränderung auf `pending-reboot` fest.

Weitere Informationen zur Verwendung der AWS CLI zum Ändern eines Parameterwerts finden Sie unter modify-db-parameter-group. Weitere Informationen zur Verwendung der RDS-API zum Ändern eines Parameterwerts finden Sie unter ModifyDBParameterGroup.

Wenn auf der DB-Instance noch nicht die neuesten Änderungen der zugeordneten DB-Parametergruppe übernommen wurden, gibt die Konsole für die DB-Parametergruppe den Status pending-reboot an. Dieser Status führt während des nächsten Wartungsfensters nicht zu einem automatischen Neustart. Damit die neuesten Parameteränderungen für diese DB-Instance übernommen werden, starten Sie die DB-Instance manuell neu.

Zeichensatzparameter

Bevor Sie einen Cluster erstellen, legen Sie alle Parameter für den Zeichensatz oder die Datenbanksortierung in Ihrer Parametergruppe fest. Führen Sie diesen Schritt auch aus, bevor Sie darin eine Datenbank erstellen. Dadurch stellen Sie sicher, dass die Standard-Datenbank und neue Datenbanken den Zeichensatz und die Sortierungswerte verwenden, die Sie angeben. Wenn Sie

einen Zeichensatz oder eine Sammlung von Parametern ändern, werden die Parameteränderungen nicht in Ihren bestehenden Datenbanken angewandt.

Bei einigen DB-Engines können Sie den Zeichensatz oder die Sortierreihenfolge für eine bestehende Datenbank ändern, indem Sie z. B. den Befehl `ALTER DATABASE` verwenden:

```
ALTER DATABASE database_name CHARACTER SET character_set_name COLLATE collation;
```

Weitere Informationen zum Ändern des Zeichensatzes oder der Sortierreihenfolge für eine Datenbank finden Sie in der Dokumentation zu Ihrer DB-Engine.

Unterstützte Parameter und Parameterwerte

Wenn Sie die unterstützten Parameter für Ihre DB-Engine ermitteln möchten, zeigen Sie die Parameter in der DB-Parametergruppe und in der DB-Cluster-Parametergruppe an, die vom DB-Cluster oder von der DB-Instance verwendet werden. Weitere Informationen finden Sie unter Anzeigen von Parameterwerten für eine DB-Parametergruppe und Anzeigen der Parameterwerte für eine DB-Cluster-Parametergruppe.

In vielen Fällen können Sie Ganzzahl- und Boolesche Parameter mithilfe von Ausdrücken, Formeln und Funktionen angeben. Funktionen können einen mathematischen "log"-Ausdruck enthalten. Nicht alle Parameter unterstützen jedoch Ausdrücke, Formeln und Funktionen für Parameterwerte. Weitere Informationen finden Sie unter Festlegen von DB-Parametern.

Für eine globale Aurora-Datenbank können Sie verschiedene Konfigurationseinstellungen für die einzelnen Aurora-Cluster festlegen. Wenn Sie einen sekundären Cluster zum primären Cluster hochstufen, müssen die Einstellungen in ausreichendem Umfang ähnlich sein, um ein einheitliches Verhalten zu erzeugen. Verwenden Sie beispielsweise die gleichen Einstellungen für Zeitzonen und Zeichensätze für alle Cluster einer globalen Aurora-Datenbank.

Werden die Parameter in einer Parametergruppe unpassend eingestellt, kann dies unbeabsichtigte unerwünschte Auswirkungen haben, einschließlich verminderter Leistung und Systeminstabilität. Gehen Sie immer mit Bedacht vor, wenn Sie Datenbankparameter ändern, und sichern Sie Ihre Daten, bevor Sie eine Parametergruppe ändern. Führen Sie Änderungen an einer Parametergruppe immer zuerst auf einer Test-DB-Instance oder einem DB-Cluster aus, bevor Sie diese Änderungen für eine Produktions-DB-Instance oder einen -DB-Cluster übernehmen.

Arbeiten mit DB-Cluster-Parametergruppen

Amazon-Aurora-DB-Cluster verwenden DB-Cluster-Parametergruppen. Die folgenden Abschnitte beschreiben das Konfigurieren und Verwalten von DB-Cluster-Parametergruppen.

Themen

Amazon Aurora-DB-Cluster und DB-Instance-Parameter

Aurora verwendet ein Zwei-Level-System von Konfigurationseinstellungen:

- Parameter in einer DB-Cluster-Parametergruppe werden auf jede DB-Instance in einem DB-Cluster angewandt. Ihre Daten werden im freigegebenen Aurora-Speicher-Subsystem gespeichert. Daher müssen alle Parameter, die sich auf das physische Layout von Tabellendaten beziehen, bei allen DB-Instances in einem Aurora-Cluster gleich sein. Da Aurora-DB-Instances durch Replikation verbunden sind, müssen alle Parameter für Replikationseinstellungen innerhalb eines Aurora-Clusters ebenfalls identisch sein.
- Parameter in einer DB-Parametergruppe werden auf eine einzelne DB-Instance in einem Aurora-DB-Cluster angewandt. Diese Parameter beziehen sich auf Aspekte wie die Speichernutzung, die Sie über die DB-Instances in demselben Aurora-Cluster hinweg unterschiedlich einstellen können. Ein Cluster enthält beispielsweise oft DB-Instances mit verschiedenen AWS -Instance-Klassen.

Jeder Aurora-Cluster ist einer DB-Cluster-Parametergruppe zugeordnet. Diese Parametergruppe weist jedem Konfigurationswert Standardwerte für die entsprechende DB-Engine zu. Die Cluster-Parametergruppe enthält auch Standardwerte für Parameter sowohl auf Cluster- als auch auf

Instance-Ebene. Jede DB-Instance innerhalb eines bereitgestellten oder eines Aurora Serverless v2-Clusters erbt die Einstellungen von dieser DB-Cluster-Parametergruppe.

Jede DB-Instance wird außerdem einer DB-Parametergruppe zugeordnet. Die Werte in der DB-Parametergruppe können Standardwerte aus der Cluster-Parametergruppe außer Kraft setzen. Wenn beispielsweise bei einer Instance in einem Cluster Probleme auftraten, können Sie dieser Instance eine benutzerdefinierte DB-Parametergruppe zuweisen. Die benutzerdefinierte Parametergruppe hat möglicherweise spezifische Einstellungen für Parameter im Hinblick auf Debuggen oder Leistungsoptimierung.

Wenn Sie einen Cluster oder eine neue DB-Instance erstellen, weist Aurora Parametergruppen basierend auf der angegebenen Datenbank-Engine und -Version zu. Sie können stattdessen eine benutzerdefinierte Parametergruppe angeben. Sie erstellen diese Parametergruppen selbst und können die Parameterwerte bearbeiten. Diese benutzerdefinierten Parametergruppen geben Sie bei der Erstellung an. Sie können auch einen DB-Cluster oder eine Instance später ändern, um eine benutzerdefinierte Parametergruppe zu verwenden.

Bei bereitgestellten und Aurora Serverless v2-Instances überschreiben alle Konfigurationswerte, die Sie in der DB-Cluster-Parametergruppe ändern, die Standardwerte in der DB-Parametergruppe. Wenn Sie die entsprechenden Werte in der DB-Parametergruppe bearbeiten, überschreiben diese Werte die Einstellungen aus der DB-Cluster-Parametergruppe.

Alle von Ihnen geänderten DB-Parameter-Einstellungen haben Vorrang vor den Werten der DB-Cluster-Parametergruppe. Dies gilt selbst dann, wenn Sie die Konfigurationsparameter wieder auf deren Standardwerte zurücksetzen. Mit dem AWS CLI Befehl describe-db-parameters oder dem RDS-API-Vorgang DescribeDBParameters können Sie sehen, welche Parameter überschrieben werden. Das Feld `Source` enthält den Wert `user`, wenn Sie diesen Parameter geändert haben. Um einen oder mehrere Parameter zurückzusetzen, sodass der Wert aus der DB-Cluster-Parametergruppe Vorrang hat, verwenden Sie den Befehl reset-db-parameter-group oder den RDS-API-Vorgang ResetDB. AWS CLI ParameterGroup

Die Parameter des DB-Clusters und der DB-Instance, die Ihnen in Aurora zur Verfügung stehen, variieren je nach Kompatibilität der Datenbank-Engine.

Datenbank-Engine	Parameter
Aurora MySQL	Siehe Aurora MySQL Konfigurationsparameter.

Datenbank-Engine	Parameter
	Für Aurora Serverless-Cluster finden Sie weitere Einzelheiten unter Arbeiten mit Parametergruppen für Aurora Serverless v2 und Parametergruppen für Aurora Serverless v1.
Aurora PostgreSQL	Siehe Amazon-Aurora-PostgreSQL-Parameter. Für Aurora Serverless-Cluster finden Sie weitere Einzelheiten unter Arbeiten mit Parametergruppen für Aurora Serverless v2 und Parametergruppen für Aurora Serverless v1.

> **Note**
>
> Aurora Serverless v1-Cluster verfügen nur über zugehörige DB-Cluster-Parametergruppen und nicht über DB-Parametergruppen. Für Aurora Serverless v2-Cluster nehmen Sie alle Ihre Änderungen an benutzerdefinierten Parametern in der DB-Cluster-Parametergruppe vor. Aurora Serverless v2 verwendet sowohl DB-Cluster-Parametergruppen als auch DB-Parametergruppen. Mit Aurora Serverless v2 können Sie fast alle Konfigurationsparameter ändern. Aurora Serverless v2 überschreibt die Einstellungen einiger kapazitätsbezogener Konfigurationsparameter, sodass Ihre Workload nicht unterbrochen wird, wenn Aurora Serverless v2-Instances herunterskalieren.
> Weitere Informationen zu Aurora Serverless-Konfigurationseinstellungen und dazu, welche Einstellungen Sie ändern können, finden Sie unter Arbeiten mit Parametergruppen für Aurora Serverless v2 und Parametergruppen für Aurora Serverless v1.

Erstellen einer DB-Cluster-Parametergruppe

Sie können eine neue DB-Cluster-Parametergruppe mithilfe der, der oder der RDS-API erstellen. AWS Management Console AWS CLI

Nachdem Sie eine DB-Cluster-Parametergruppe erstellt haben, sollten Sie mindestens fünf Minuten warten, bevor Sie einen DB-Cluster erstellen, der diese DB-Cluster-Parametergruppe verwendet. Auf diese Weise kann Amazon RDS die Parametergruppe vollständig erstellen, bevor sie vom neuen DB-Cluster verwendet wird. Mithilfe der Option Parameter Groups (Parametergruppen) in der Amazon-RDS-Konsole oder mithilfe des Befehls describe-db-cluster-parameters können Sie überprüfen, ob Ihre DB-Cluster-Parametergruppe erstellt wurde.

Die folgenden Einschränkungen gelten für den Namen der DB-Cluster-Parametergruppe:

- Der Name muss zwischen 1 und 255 Buchstaben, Zahlen oder Bindestriche enthalten.

  Standardnamen für Parametergruppen können einen Punkt enthalten, z. B. `default.aurora-mysql5.7`. Namen von benutzerdefinierten Parametergruppen dürfen jedoch keinen Punkt enthalten.
- Das erste Zeichen muss ein Buchstabe sein.
- Der Name darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.

Konsole

So erstellen Sie eine DB-Cluster-Parametergruppe

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie Create parameter group (Parametergruppe erstellen).

   Das Fenster Create parameter group (Parametergruppe erstellen) wird angezeigt.
4. Wählen Sie in der Liste Parameter group family (Parametergruppenfamilie) eine DB-Parametergruppenfamilie aus.
5. Wählen Sie in der Typliste die DB-Cluster-Parametergruppe aus.
6. Geben Sie im Feld Group name (Gruppenname) den Namen der neuen DB-Cluster-Parametergruppe ein.
7. Geben Sie im Feld Description (Beschreibung) eine Beschreibung für die neue DB-Cluster-Parametergruppe ein.
8. Wählen Sie Create (Erstellen) aus.

AWS CLI

Verwenden Sie den AWS CLI `create-db-cluster-parameter-group`Befehl, um eine DB-Cluster-Parametergruppe zu erstellen.

Im folgenden Beispiel wird eine DB-Cluster-Parametergruppe mit dem Namen mydbclusterparametergroup für Aurora MySQL Version 5.7 und der Beschreibung „My new cluster parameter group“ erstellt.

Nutzen Sie die folgenden erforderlichen Parameter:

- `--db-cluster-parameter-group-name`
- `--db-parameter-group-family`
- `--description`

Um alle verfügbaren Parametergruppenfamilien aufzulisten, führen Sie den folgenden Befehl aus:

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

> **Note**
>
> Die Ausgabe enthält Duplikate.

Example

Für LinuxmacOS, oderUnix:

```
aws rds create-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup \
    --db-parameter-group-family aurora-mysql5.7 \
    --description "My new cluster parameter group"
```

Windows:

```
aws rds create-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbclusterparametergroup ^
    --db-parameter-group-family aurora-mysql5.7 ^
    --description "My new cluster parameter group"
```

Die Ausgabe dieses Befehls sieht etwa so aus:

```
{
```

```
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "mydbclusterparametergroup",
        "DBParameterGroupFamily": "aurora-mysql5.7",
        "Description": "My new cluster parameter group",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:mydbclusterparametergroup"
    }
}
```

RDS-API

Um eine DB-Cluster-Parametergruppe zu erstellen, verwenden Sie die RDS-API-Aktion `CreateDBClusterParameterGroup`.

Nutzen Sie die folgenden erforderlichen Parameter:

- `DBClusterParameterGroupName`
- `DBParameterGroupFamily`
- `Description`

Zuordnen einer DB-Cluster-Parametergruppe zu einem DB-Cluster

Sie können Ihre eigenen DB-Cluster-Parametergruppen mit benutzerdefinierten Einstellungen erstellen. Sie können eine DB-Cluster-Parametergruppe mit einem DB-Cluster verknüpfen, indem Sie die AWS Management Console AWS CLI, oder die RDS-API verwenden. Das können Sie tun, wenn Sie einen DB-Cluster erstellen oder ändern.

Informationen über das Erstellen einer DB-Cluster-Parametergruppe finden Sie unter Erstellen einer DB-Cluster-Parametergruppe. Informationen zum Erstellen eines DB-Clusters finden Sie unter Erstellen eines Amazon Aurora-DB Clusters. Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

> **Note**
>
> Wenn Sie für Aurora PostgreSQL 15.2, 14.7, 13.10, 12.14 und alle 11 Versionen die mit einem DB-Cluster verknüpfte DB-Cluster-Parametergruppe ändern, starten Sie jede Replikatinstanz neu, um die Änderungen zu übernehmen.
> Führen Sie den folgenden Befehl aus, um festzustellen, ob die primäre DB-Instance eines DB-Clusters neu gestartet werden muss, um die Änderungen zu übernehmen: AWS CLI

```
aws rds describe-db-clusters --db-cluster-identifier
db_cluster_identifier
```

Überprüfen Sie den Wert `DBClusterParameterGroupStatus` für die primäre DB-Instance in der Ausgabe. Wenn der Wert `pending-reboot` lautet, starten Sie die primäre DB-Instance des DB-Clusters neu.

Konsole

So ordnen Sie eine DB-Cluster-Parametergruppe zu einem DB-Cluster zu

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann den zu ändernden DB-Cluster aus.
3. Wählen Sie Ändern aus. Die Seite Modify DB cluster (DB-Cluster ändern) wird angezeigt.
4. Ändern Sie die Einstellung für DB-Cluster-Parametergruppen.
5. Klicken Sie auf Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.

   Die Änderung wird unabhängig von der Einstellung Einplanung von Änderungen sofort angewendet.
6. Überprüfen Sie auf der Bestätigungsseite Ihre Änderungen. Wenn sie korrekt sind, wählen Sie Modify cluster (Cluster ändern) aus, um Ihre Änderungen zu speichern.

   Klicken Sie anderenfalls auf Zurück, um Ihre Änderungen zu bearbeiten, oder klicken Sie auf Abbrechen, um Ihre Änderungen zu verwerfen.

AWS CLI

Um eine DB-Cluster-Parametergruppe einem DB-Cluster zuzuordnen, verwenden Sie den AWS CLI `modify-db-cluster`Befehl mit den folgenden Optionen:

- `--db-cluster-name`
- `--db-cluster-parameter-group-name`

Im folgenden Beispiel wird die `mydbclpg`-DB-Parametergruppe zum `mydbcluster`-DB-Cluster zugeordnet.

Example

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --db-cluster-parameter-group-name mydbclpg
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --db-cluster-parameter-group-name mydbclpg
```

RDS-API

Um eine DB-Cluster-Parametergruppe einem DB-Cluster zuzuordnen, verwenden Sie die RDS-API-Operation `ModifyDBCluster` mit den folgenden Parametern:

- `DBClusterIdentifier`
- `DBClusterParameterGroupName`

Ändern von Parametern in einer DB-Cluster-Parametergruppe

Sie können Parameterwerte in einer vom Kunden erstellten DB-Clusterparametergruppe ändern. Sie können die Parameterwerte in einer Standard-DB-Clusterparametergruppe nicht ändern. Änderungen an Parametern in einer benutzerdefinierten DB-Cluster-Parametergruppe gelten für alle DB-Cluster, die dieser DB-Cluster-Parametergruppe zugeordnet sind.

Konsole

So ändern Sie eine DB-Cluster-Parametergruppe

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie in der Liste die zu ändernde Parametergruppe.
4. Wählen Sie für Parameter group actions (Parametergruppenaktionen) die Option Bearbeiten.

5. Ändern Sie die Werte der Parameter, die Sie ändern möchten. Sie können durch die Parameter scrollen, in dem Sie die Pfeiltasten oben rechts im Dialogfeld verwenden.

   Die Werte in einer Standardparametergruppe können Sie nicht ändern.
6. Wählen Sie Save Changes.
7. Starten Sie die primäre (Writer-) DB-Instance im Cluster neu, um die Änderungen darauf anzuwenden.
8. Starten Sie anschließend die Reader-DB-Instances neu, um die Änderungen auf sie anzuwenden.

AWS CLI

Um eine DB-Cluster-Parametergruppe zu ändern, verwenden Sie den AWS CLI `modify-db-cluster-parameter-group`Befehl mit den folgenden erforderlichen Parametern:

- `--db-cluster-parameter-group-name`
- `--parameters`

Im folgenden Beispiel werden die Werte `server_audit_logging` und `server_audit_logs_upload` in der DB-Cluster-Parametergruppe mydbclusterparametergroup geändert.

Example

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup \
    --parameters
 "ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" \

 "ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbclusterparametergroup ^
    --parameters
 "ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" ^
```

```
"ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

Die Ausgabe des Befehls ähnelt der Folgenden:

```
DBCLUSTERPARAMETERGROUP  mydbclusterparametergroup
```

RDS-API

Um eine DB-Cluster-Parametergruppe zu ändern, verwenden Sie den RDS-API-Befehl `ModifyDBClusterParameterGroup` mit den folgenden erforderlichen Parametern:

- `DBClusterParameterGroupName`
- `Parameters`

Zurücksetzen von Parametern in einer DB-Cluster-Parametergruppe

Sie können Parameter in einer vom Kunden erstellten DB-Clusterparametergruppe auf ihre Standardwerte zurücksetzen. Änderungen an Parametern in einer benutzerdefinierten DB-Cluster-Parametergruppe gelten für alle DB-Cluster, die dieser DB-Cluster-Parametergruppe zugeordnet sind.

> **Note**
>
> In einer Standardparametergruppe des DB-Clusters werden die Parameter immer auf ihre Standardwerte eingestellt.

Konsole

So setzen Sie Parameter in einer DB-Cluster-Parametergruppe auf ihre Standardwerte zurück

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie in der Liste die Parametergruppe aus.
4. Wählen Sie für Parameter group actions (Parametergruppenaktionen) die Option Bearbeiten.

5. Wählen Sie die Parameter aus, die Sie auf ihre Standardwerte zurücksetzen möchten. Sie können durch die Parameter scrollen, in dem Sie die Pfeiltasten oben rechts im Dialogfeld verwenden.

   Sie können die Werte in einer Standardparametergruppe nicht zurücksetzen.
6. Wählen Sie Reset (Zurücksetzen) und bestätigen Sie dann mit Reset parameters (Parameter zurücksetzen).
7. Starten Sie die primäre DB-Instance im DB-Cluster neu, um die Änderungen auf alle DB-Instances im DB-Cluster anzuwenden.

AWS CLI

Um Parameter in einer DB-Cluster-Parametergruppe auf ihre Standardwerte zurückzusetzen, verwenden Sie den AWS CLI `reset-db-cluster-parameter-group`Befehl mit der folgenden erforderlichen Option:`--db-cluster-parameter-group-name`.

Um alle Parameter in der Parametergruppe des DB-Clusters zurückzusetzen, wählen Sie die Option `--reset-all-parameters`. Um bestimmte Parameter zurückzusetzen, geben Sie die Option `--parameters` an.

Im folgenden Beispiel werden alle Parameter in der DB-Parametergruppe namens mydbparametergroup auf ihre Standardwerte zurückgesetzt.

Example

Für LinuxmacOS, oderUnix:

```
aws rds reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbparametergroup \
    --reset-all-parameters
```

Windows:

```
aws rds reset-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbparametergroup ^
    --reset-all-parameters
```

Im folgenden Beispiel werden die Werte `server_audit_logging` und `server_audit_logs_upload` in der DB-Cluster-Parametergruppe mydbclusterparametergroup auf ihre Standardwerte zurückgesetzt.

Example

Für LinuxmacOS, oderUnix:

```
aws rds reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup \
    --parameters "ParameterName=server_audit_logging,ApplyMethod=immediate" \
                 "ParameterName=server_audit_logs_upload,ApplyMethod=immediate"
```

Windows:

```
aws rds reset-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbclusterparametergroup ^
    --parameters
 "ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" ^

 "ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

Die Ausgabe des Befehls ähnelt der Folgenden:

```
DBClusterParameterGroupName  mydbclusterparametergroup
```

RDS-API

Um Parameter in einer DB-Cluster-Parametergruppe auf ihre Standardwerte zurückzusetzen, verwenden Sie den `ResetDBClusterParameterGroup`-RDS-API-Befehl mit dem folgenden erforderlichen Parameter: `DBClusterParameterGroupName`.

Um alle Parameter in der Parametergruppe des DB-Clusters zurückzusetzen, legen Sie den Parameter `ResetAllParameters` auf `true` fest. Um bestimmte Parameter zurückzusetzen, geben Sie den Parameter `Parameters` an.

Kopieren einer DB-Cluster-Parametergruppe

Sie können die von Ihnen erstellten benutzerdefinierten DB-Cluster-Parametergruppen kopieren. Das Kopieren einer Parametergruppe ist eine praktische Lösung, wenn Sie bereits eine DB-Cluster-Parametergruppe erstellt haben und die am häufigsten verwendeten Parameter und Werte aus dieser Gruppe in eine neuen DB-Cluster-Parametergruppe übernehmen möchten. Sie können eine DB-Cluster-Parametergruppe kopieren, indem Sie den Befehl AWS CLIcopy-db-cluster-parameter-group oder den RDS-API-Vorgang CopyDB Group verwenden. ClusterParameter

Nachdem Sie eine DB-Cluster-Parametergruppe kopiert haben, warten Sie mindestens fünf Minuten, bevor Sie einen DB-Cluster erstellen, der diese DB-Cluster-Parametergruppe verwendet. Auf diese Weise kann Amazon RDS die Parametergruppe vollständig kopieren, bevor sie vom neuen DB-Cluster verwendet wird. Mithilfe der Option Parameter Groups (Parametergruppen) in der Amazon-RDS-Konsole oder mithilfe des Befehls describe-db-cluster-parameters können Sie überprüfen, ob Ihre DB-Cluster-Parametergruppe erstellt wurde.

> **Note**
>
> Standardparametergruppen können nicht kopiert werden. Sie können jedoch eine neue Parametergruppe erstellen, die auf einer Standardparametergruppe basiert.
> Sie können eine DB-Cluster-Parametergruppe nicht in eine andere oder kopieren. AWS-Konto AWS-Region

Konsole

So kopieren Sie eine DB-Cluster-Parametergruppe

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie in der Liste die zu kopierende benutzerdefinierte Parametergruppe.
4. Wählen Sie für Parameter group actions (Parametergruppenaktionen) die Option Kopieren.
5. Geben Sie unter New DB parameter group identifier (Neue DB-Parametergruppenkennung) einen Namen für die neue Parametergruppe ein.
6. Geben Sie unter Beschreibung eine Beschreibung für die neue Parametergruppe ein.
7. Wählen Sie die Option Copy aus.

AWS CLI

Um eine DB-Cluster-Parametergruppe zu kopieren, verwenden Sie den AWS CLI `copy-db-cluster-parameter-group`Befehl mit den folgenden erforderlichen Parametern:

- `--source-db-cluster-parameter-group-identifier`
- `--target-db-cluster-parameter-group-identifier`

- `--target-db-cluster-parameter-group-description`

Im folgenden Beispiel wird eine neue DB-Cluster-Parametergruppe mit dem Namen `mygroup2` als Kopie der DB-Cluster-Parametergruppe `mygroup1` erstellt.

Example

Für LinuxmacOS, oderUnix:

```
aws rds copy-db-cluster-parameter-group \
    --source-db-cluster-parameter-group-identifier mygroup1 \
    --target-db-cluster-parameter-group-identifier mygroup2 \
    --target-db-cluster-parameter-group-description "DB parameter group 2"
```

Windows:

```
aws rds copy-db-cluster-parameter-group ^
    --source-db-cluster-parameter-group-identifier mygroup1 ^
    --target-db-cluster-parameter-group-identifier mygroup2 ^
    --target-db-cluster-parameter-group-description "DB parameter group 2"
```

RDS-API

Um eine DB-Cluster-Parametergruppe zu kopieren, verwenden Sie die RDS-API-Operation `CopyDBClusterParameterGroup` mit den folgenden erforderlichen Parametern:

- `SourceDBClusterParameterGroupIdentifier`
- `TargetDBClusterParameterGroupIdentifier`
- `TargetDBClusterParameterGroupDescription`

Auflisten von DB-Cluster-Parametergruppen

Sie können die DB-Cluster-Parametergruppen auflisten, die Sie für Ihr AWS Konto erstellt haben.

> **Note**
>
> Standardparametergruppen werden automatisch aus einer Standardparametervorlage generiert, wenn Sie ein DB-Cluster für eine bestimmte DB-Engine und -Version erstellen. Diese Standardparametergruppen enthalten bevorzugte Parametereinstellungen und können

nicht geändert werden. Wenn Sie eine benutzerdefinierte Parametergruppe erstellen, können Sie Parametereinstellungen ändern.

Konsole

Um alle DB-Cluster-Parametergruppen für ein AWS Konto aufzulisten

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   Die DB-Cluster-Parametergruppen erscheinen in der Liste mit DB cluster parameter group (DB-Cluster-Parametergruppe) als Type (Typ).

AWS CLI

Verwenden Sie den AWS CLI `describe-db-cluster-parameter-groups`Befehl, um alle DB-Cluster-Parametergruppen für ein AWS Konto aufzulisten.

Example

Im folgenden Beispiel werden alle verfügbaren DB-Cluster-Parametergruppen für ein AWS -Konto aufgelistet.

```
aws rds describe-db-cluster-parameter-groups
```

Im folgenden Beispiel wird die Parametergruppe mydbclusterparametergroup beschrieben.

Für LinuxmacOS, oderUnix:

```
aws rds describe-db-cluster-parameter-groups \
    --db-cluster-parameter-group-name mydbclusterparametergroup
```

Windows:

```
aws rds describe-db-cluster-parameter-groups ^
    --db-cluster-parameter-group-name mydbclusterparametergroup
```

Die Ausgabe des Befehls ähnelt der Folgenden:

```
{
    "DBClusterParameterGroups": [
        {
            "DBClusterParameterGroupName": "mydbclusterparametergroup",
            "DBParameterGroupFamily": "aurora-mysql5.7",
            "Description": "My new cluster parameter group",
            "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:mydbclusterparametergroup"
        }
    ]
}
```

RDS-API

Verwenden Sie die DescribeDBClusterParameterGroupsRDS-API-Aktion, um alle DB-Cluster-Parametergruppen für ein AWS Konto aufzulisten.

Anzeigen der Parameterwerte für eine DB-Cluster-Parametergruppe

Sie können alle Parameter in einer DB-Cluster-Parametergruppe mit ihren Werten in einer Liste anzeigen.

Konsole

So zeigen Sie die Parameterwerte für eine DB-Cluster-Parametergruppe an

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   Die DB-Cluster-Parametergruppen erscheinen in der Liste mit DB cluster parameter group (DB-Cluster-Parametergruppe) als Type (Typ).
3. Wählen Sie den Namen der DB-Cluster-Parametergruppe, um deren Parameterliste anzuzeigen.

AWS CLI

Um die Parameterwerte für eine DB-Cluster-Parametergruppe anzuzeigen, verwenden Sie den AWS CLI describe-db-cluster-parametersBefehl mit dem folgenden erforderlichen Parameter.

- `--db-cluster-parameter-group-name`

Example

Das folgende Beispiel listet die Parameter und Parameterwerte für eine DB-Cluster-Parametergruppe namens mydbclusterparametergroup im JSON-Format auf.

Die Ausgabe des Befehls ähnelt der Folgenden:

```
aws rds describe-db-cluster-parameters --db-cluster-parameter-group-
name mydbclusterparametergroup
```

```
{
    "Parameters": [
        {
            "ParameterName": "allow-suspicious-udfs",
            "Description": "Controls whether user-defined functions that have only an
 xxx symbol for the main function can be loaded",
            "Source": "engine-default",
            "ApplyType": "static",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": false,
            "ApplyMethod": "pending-reboot",
            "SupportedEngineModes": [
                "provisioned"
            ]
        },
        {
            "ParameterName": "aurora_binlog_read_buffer_size",
            "ParameterValue": "5242880",
            "Description": "Read buffer size used by master dump thread when the switch
 aurora_binlog_use_large_read_buffer is ON.",
            "Source": "engine-default",
            "ApplyType": "dynamic",
            "DataType": "integer",
            "AllowedValues": "8192-536870912",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot",
            "SupportedEngineModes": [
                "provisioned"
            ]
        },

...
```

RDS-API

Um die Parameterwerte für eine DB-Cluster-Parametergruppe anzuzeigen, verwenden Sie den RDS-API-Befehl `DescribeDBClusterParameters` mit dem folgenden erforderlichen Parameter.

- `DBClusterParameterGroupName`

In einigen Fällen werden die zulässigen Werte für einen Parameter nicht angezeigt. Es handelt sich dabei immer um Parameter, bei denen die Quelle die Standardeinstellung der Datenbank-Engine ist.

Um die Werte dieser Parameter anzuzeigen, können Sie die folgenden SQL-Anweisungen ausführen:

- MySQL:

```
-- Show the value of a particular parameter
mysql$ SHOW VARIABLES LIKE '%parameter_name%';

-- Show the values of all parameters
mysql$ SHOW VARIABLES;
```

- PostgreSQL:

```
-- Show the value of a particular parameter
postgresql=> SHOW parameter_name;

-- Show the values of all parameters
postgresql=> SHOW ALL;
```

Löschen einer DB-Cluster-Parametergruppe

Sie können eine DB-Cluster-Parametergruppe mithilfe der AWS Management Console AWS CLI, oder RDS-API löschen. Eine Parametergruppe für eine DB-Cluster-Parametergruppe kann nur gelöscht werden, wenn sie keinem DB-Cluster zugeordnet ist.

Konsole

Um Parametergruppen zu löschen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   Die Parametergruppen werden in einer Liste angezeigt.
3. Wählen Sie den Namen der DB-Cluster-Parametergruppen, die gelöscht werden sollen.
4. Wählen Sie Aktionen und dann Löschen.
5. Überprüfen Sie die Namen der Parametergruppen und wählen Sie dann Löschen.

AWS CLI

Um eine DB-Cluster-Parametergruppe zu löschen, verwenden Sie den AWS CLI `delete-db-cluster-parameter-group`Befehl mit dem folgenden erforderlichen Parameter.

- `--db-parameter-group-name`

Example

Im folgenden Beispiel wird eine DB-Cluster-Parametergruppe mit dem Namen mydbparametergroup gelöscht.

```
aws rds delete-db-cluster-parameter-group --db-parameter-group-name mydbparametergroup
```

RDS-API

Um eine DB-Cluster-Parametergruppe zu löschen, verwenden Sie den `DeleteDBClusterParameterGroup`RDS-API-Befehl mit dem folgenden erforderlichen Parameter.

- `DBParameterGroupName`

Arbeiten mit DB-Parametergruppen in einer DB-Instance

DB-Instances verwenden DB-Parametergruppen. Die folgenden Abschnitte beschreiben das Konfigurieren und Verwalten von DB-Instance-Parametergruppen.

Themen

- Erstellen einer DB-Parametergruppe
- Verknüpfen einer DB-Parametergruppe mit einer DB-Instance

- Ändern von Parametern in einer DB-Parametergruppe
- Zurücksetzen von Parametern in einer DB-Parametergruppe auf ihre Standardwerte
- Kopieren einer DB-Parametergruppe
- Auflisten von DB-Parametergruppen
- Anzeigen von Parameterwerten für eine DB-Parametergruppe
- Löschen einer DB-Parametergruppe

Erstellen einer DB-Parametergruppe

Sie können eine neue DB-Parametergruppe mithilfe der AWS Management Console AWS CLI, der oder der RDS-API erstellen.

Die folgenden Einschränkungen gelten für den Namen der DB-Parametergruppe:

- Der Name muss zwischen 1 und 255 Buchstaben, Zahlen oder Bindestriche enthalten.

  Standardnamen für Parametergruppen können einen Punkt enthalten, z. B. `default.mysql8.0`. Namen von benutzerdefinierten Parametergruppen dürfen jedoch keinen Punkt enthalten.
- Das erste Zeichen muss ein Buchstabe sein.
- Der Name darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.

Konsole

So erstellen Sie eine DB-Parametergruppe:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie Create parameter group (Parametergruppe erstellen).
4. Geben Sie unter Parametergruppenname den Namen Ihrer neuen DB-Parametergruppe ein.
5. Geben Sie unter Beschreibung eine Beschreibung für Ihre neue DB-Parametergruppe ein.
6. Wählen Sie als Engine-Typ Ihre DB-Engine aus.
7. Wählen Sie für Parametergruppenfamilie eine DB-Parametergruppenfamilie aus.

8. Wählen Sie für Typ, falls zutreffend, DB-Parametergruppe aus.
9. Wählen Sie Create (Erstellen) aus.

AWS CLI

Verwenden Sie den AWS CLI `create-db-parameter-group`Befehl, um eine DB-Parametergruppe zu erstellen. Im folgenden Beispiel wird eine DB-Parametergruppe mit dem Namen mydbparametergroup für MySQL Version 8.0 und der Beschreibung „My new parameter group“ erstellt.

Nutzen Sie die folgenden erforderlichen Parameter:

- `--db-parameter-group-name`
- `--db-parameter-group-family`
- `--description`

Um alle verfügbaren Parametergruppenfamilien aufzulisten, führen Sie den folgenden Befehl aus:

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

> **Note**
>
> Die Ausgabe enthält Duplikate.

Example

Für LinuxmacOS, oderUnix:

```
aws rds create-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --db-parameter-group-family aurora-mysql5.7 \
    --description "My new parameter group"
```

Windows:

```
aws rds create-db-parameter-group ^
```

```
    --db-parameter-group-name mydbparametergroup ^
    --db-parameter-group-family aurora-mysql5.7 ^
    --description "My new parameter group"
```

Die Ausgabe dieses Befehls sieht etwa so aus:

```
DBPARAMETERGROUP  mydbparametergroup  aurora-mysql5.7  My new parameter group
```

RDS-API

Um eine DB-Parametergruppe zu erstellen, verwenden Sie die RDS-API-Operation `CreateDBParameterGroup`.

Nutzen Sie die folgenden erforderlichen Parameter:

- `DBParameterGroupName`
- `DBParameterGroupFamily`
- `Description`

Verknüpfen einer DB-Parametergruppe mit einer DB-Instance

Sie können Ihre eigenen DB-Parametergruppen mit benutzerdefinierten Einstellungen erstellen. Sie können einer DB-Instance mithilfe der AWS Management Console, der oder der RDS-API eine DB-Parametergruppe zuordnen. AWS CLI Das können Sie tun, wenn Sie eine DB-Instance erstellen oder ändern.

Informationen über das Erstellen einer Parametergruppe finden Sie unter Erstellen einer DB-Parametergruppe. Informationen zum Ändern einer DB-Instance finden Sie unter Ändern einer DB-Instance in einem DB-Cluster.

> **Note**
>
> Wenn Sie eine neue DB-Parametergruppe einer DB-Instance zuordnen, werden die geänderten statischen und dynamischen Parameter erst nach Neustart der DB-Instance angewendet. Wenn Sie jedoch dynamische Parameter in der DB-Parametergruppe ändern, nachdem Sie sie der DB-Instance zugeordnet haben, werden diese Änderungen sofort ohne Neustart angewendet.

Konsole

So verknüpfen Sie eine DB-Parametergruppe mit einer DB-Instance

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die DB-Instance, die Sie ändern möchten.
3. Wählen Sie Modify aus. Die Seite Modify DB instance (DB-Instance ändern) wird angezeigt.
4. Ändern Sie die Einstellung für DB-Parametergruppen .
5. Klicken Sie auf Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.
6. (Optional) Klicken Sie auf Apply immediately (Sofort anwenden), um die Änderungen direkt zu übernehmen. Die Auswahl dieser Option kann in einigen Fällen einen Ausfall verursachen.
7. Überprüfen Sie auf der Bestätigungsseite Ihre Änderungen. Wenn sie korrekt sind, wählen Sie Modify DB Instance (DB-Instance ändern) aus, um Ihre Änderungen zu speichern.

   Oder klicken Sie auf Zurück, um Ihre Änderungen zu bearbeiten, oder auf Abbrechen, um Ihre Änderungen zu verwerfen.

AWS CLI

Um eine DB-Parametergruppe mit einer DB-Instance zu verknüpfen, verwenden Sie den AWS CLI `modify-db-instance`Befehl mit den folgenden Optionen:

- `--db-instance-identifier`
- `--db-parameter-group-name`

Im folgenden Beispiel wird die `mydbpg`-DB-Parametergruppe mit der `database-1`-DB-Instance verknüpft. Die Änderungen werden mit sofort übernomme `--apply-immediately`. Verwenden Sie `--no-apply-immediately`, um Änderungen im nächsten Wartungszeitraum anzuwenden.

Example

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-instance \
```

```
    --db-instance-identifier database-1 \
    --db-parameter-group-name mydbpg \
    --apply-immediately
```

Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier database-1 ^
    --db-parameter-group-name mydbpg ^
    --apply-immediately
```

RDS-API

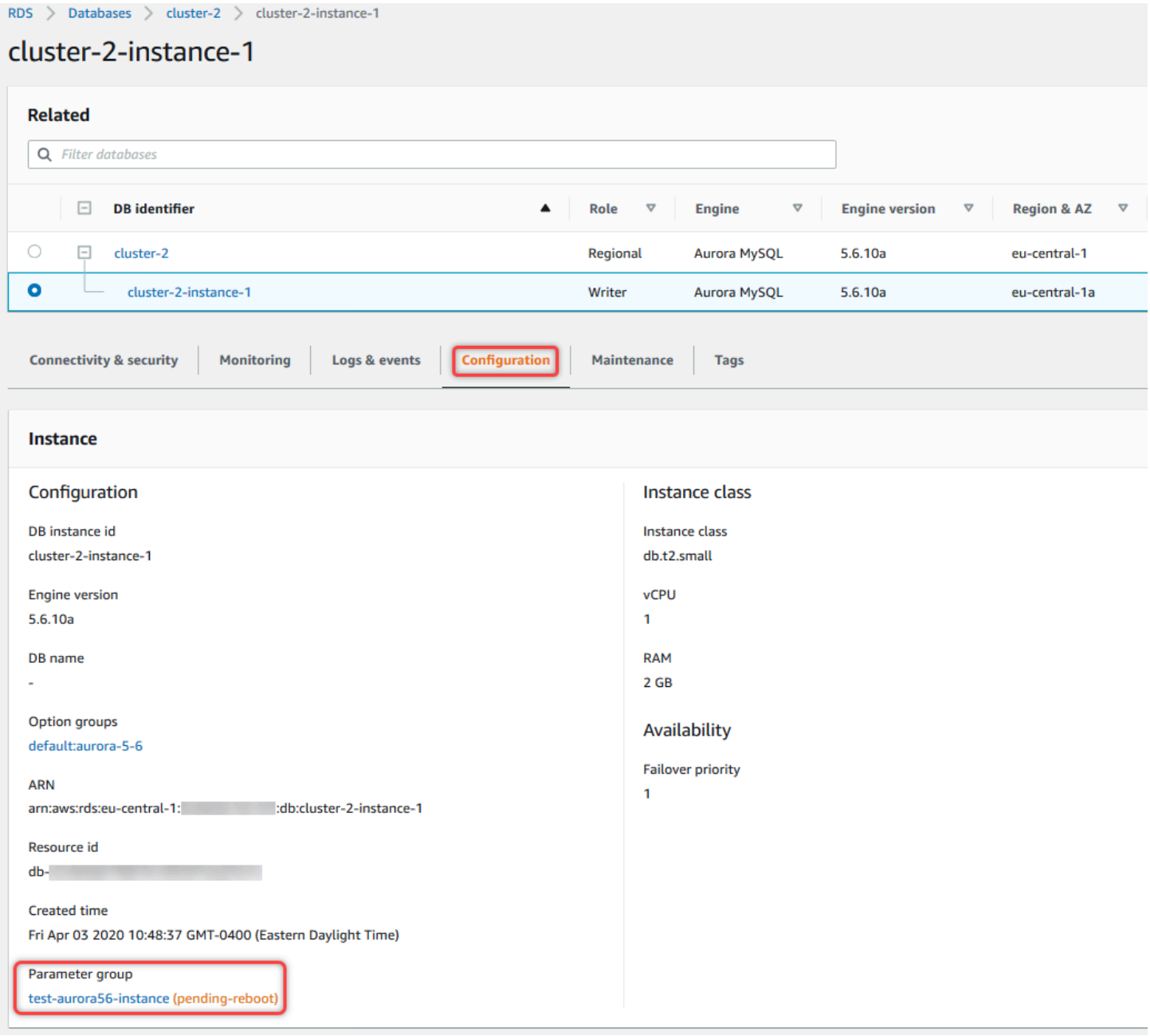
Um eine DB-Parametergruppe zu einer DB-Instance zuzuordnen, verwenden Sie die RDS-API-Operation `ModifyDBInstance` mit den folgenden Parametern:

- `DBInstanceName`
- `DBParameterGroupName`

Ändern von Parametern in einer DB-Parametergruppe

Sie können die Parameterwerte in einer benutzerdefinierten DB-Parametergruppe ändern. Die Parameterwerte in einer Standard-DB-Parametergruppe können nicht geändert werden. Änderungen bei Parametern in einer benutzerdefinierten DB-Parametergruppe werden auf alle DB-Instances angewandt, die dieser DB-Parametergruppe zugeteilt sind.

Änderungen an einigen Parametern werden sofort ohne Neustart auf die DB-Instance angewendet. Änderungen an anderen Parametern werden erst angewendet, nachdem die DB-Instance neu gestartet wurde. In der RDS-Konsole wird der Status einer DB-Parametergruppe, die einer DB-Instance zugeordnet ist, auf der Registerkarte Konfiguration angezeigt. Nehmen wir beispielsweise an, dass auf der DB-Instance die neuesten Änderungen an der zugeordneten DB-Parametergruppe noch nicht übernommen wurden. In diesem Fall gibt die RDS-Konsole für die DB-Parametergruppe den Status pending-reboot an. Damit die neuesten Parameteränderungen für diese DB-Instance übernommen werden, starten Sie die DB-Instance manuell neu.



Konsole

Um die Parameter in einer DB-Parametergruppe zu ändern

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie in der Liste den Namen der Parametergruppe aus, die Sie ändern möchten.
4. Wählen Sie für Parameter group actions (Parametergruppenaktionen) die Option Bearbeiten.

5. Ändern Sie wie gewünscht die Werte der Parameter. Sie können durch die Parameter scrollen, in dem Sie die Pfeiltasten oben rechts im Dialogfeld verwenden.

   Die Werte in einer Standardparametergruppe können Sie nicht ändern.

6. Wählen Sie Save Changes.

AWS CLI

Um eine DB-Parametergruppe zu ändern, verwenden Sie den AWS CLI `modify-db-parameter-group`Befehl mit den folgenden erforderlichen Optionen:

- `--db-parameter-group-name`
- `--parameters`

Im folgenden Beispiel werden die Werte `max_connections` und `max_allowed_packet` in der DB-Parametergruppe mydbparametergroup geändert.

Example

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --parameters
 "ParameterName=max_connections,ParameterValue=250,ApplyMethod=immediate" \

 "ParameterName=max_allowed_packet,ParameterValue=1024,ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-parameter-group ^
    --db-parameter-group-name mydbparametergroup ^
    --parameters
 "ParameterName=max_connections,ParameterValue=250,ApplyMethod=immediate" ^

 "ParameterName=max_allowed_packet,ParameterValue=1024,ApplyMethod=immediate"
```

Die Ausgabe des Befehls ähnelt der Folgenden:

```
DBPARAMETERGROUP  mydbparametergroup
```

RDS-API

Zum Ändern einer DB-Parametergruppe verwenden Sie die RDS-API-Operation `ModifyDBParameterGroup` mit den folgenden erforderlichen Parametern:

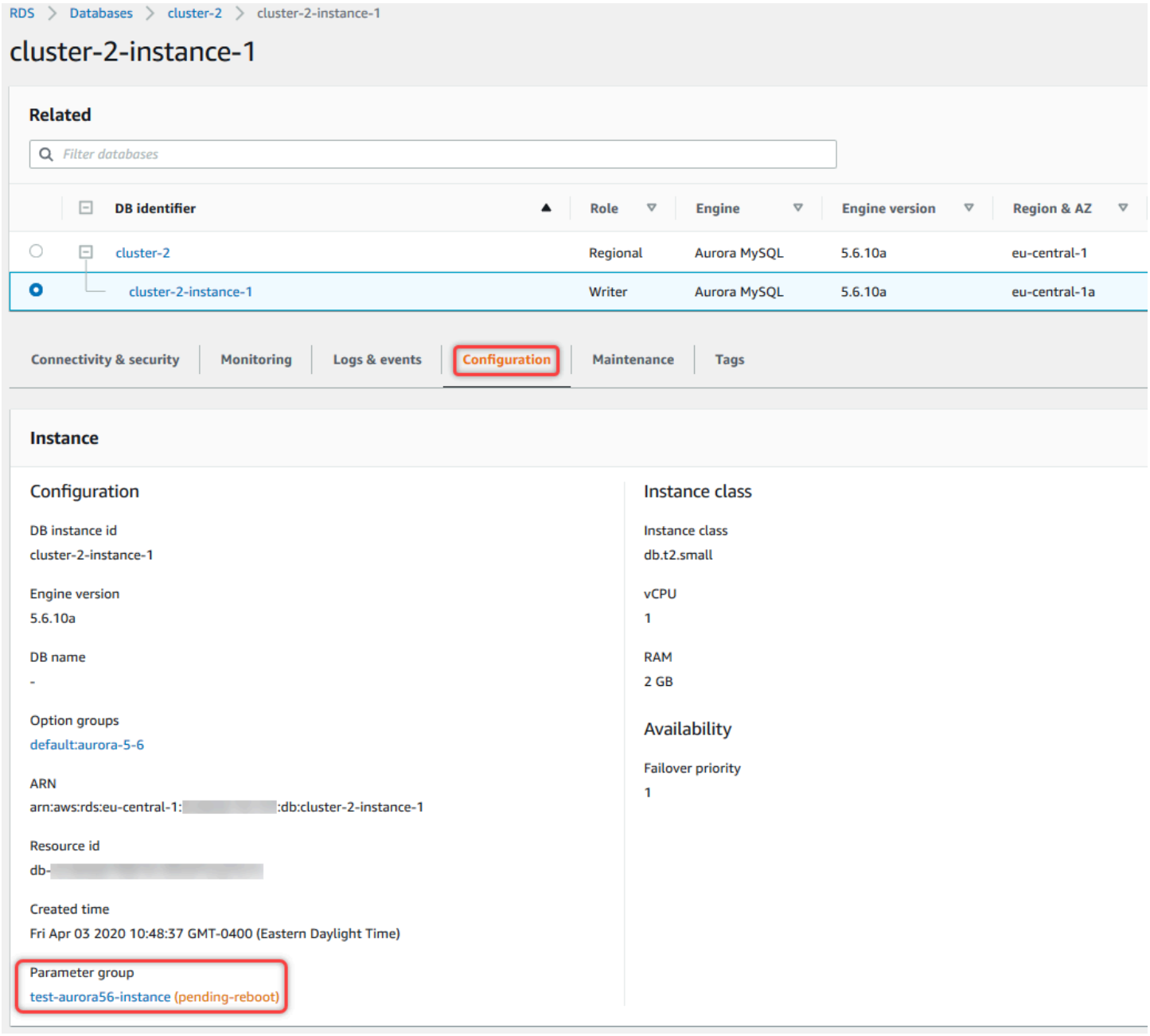
- `DBParameterGroupName`
- `Parameters`

Zurücksetzen von Parametern in einer DB-Parametergruppe auf ihre Standardwerte

Sie können Parameterwerte in einer vom Kunden erstellten DB-Parametergruppe auf ihre Standardwerte zurücksetzen. Änderungen bei Parametern in einer benutzerdefinierten DB-Parametergruppe werden auf alle DB-Instances angewandt, die dieser DB-Parametergruppe zugeteilt sind.

Wenn Sie die Konsole verwenden, können Sie bestimmte Parameter auf ihre Standardwerte zurücksetzen. Sie können jedoch nicht einfach alle Parameter in der DB-Parametergruppe auf einmal zurücksetzen. Wenn Sie die AWS CLI oder die RDS-API verwenden, können Sie bestimmte Parameter auf ihre Standardwerte zurücksetzen. Sie können auch alle Parameter in der DB-Parametergruppe auf einmal zurücksetzen.

Änderungen an einigen Parametern werden sofort ohne Neustart auf die DB-Instance angewendet. Änderungen an anderen Parametern werden erst angewendet, nachdem die DB-Instance neu gestartet wurde. In der RDS-Konsole wird der Status einer DB-Parametergruppe, die einer DB-Instance zugeordnet ist, auf der Registerkarte Konfiguration angezeigt. Nehmen wir beispielsweise an, dass auf der DB-Instance die neuesten Änderungen an der zugeordneten DB-Parametergruppe noch nicht übernommen wurden. In diesem Fall gibt die RDS-Konsole für die DB-Parametergruppe den Status pending-reboot an. Damit die neuesten Parameteränderungen für diese DB-Instance übernommen werden, starten Sie die DB-Instance manuell neu.



> **Note**
>
> In einer Standard-DB-Parametergruppe werden Parameter immer auf ihre Standardwerte festgelegt.

Konsole

So setzen Sie Parameter in einer DB-Parametergruppe auf ihre Standardwerte zurück

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie in der Liste die Parametergruppe aus.
4. Wählen Sie für Parameter group actions (Parametergruppenaktionen) die Option Bearbeiten.
5. Wählen Sie die Parameter aus, die Sie auf ihre Standardwerte zurücksetzen möchten. Sie können durch die Parameter scrollen, in dem Sie die Pfeiltasten oben rechts im Dialogfeld verwenden.

   Sie können die Werte in einer Standardparametergruppe nicht zurücksetzen.
6. Wählen Sie Reset (Zurücksetzen) und bestätigen Sie dann mit Reset parameters (Parameter zurücksetzen).

AWS CLI

Um einige oder alle Parameter in einer DB-Parametergruppe zurückzusetzen, verwenden Sie den AWS CLI `reset-db-parameter-group`Befehl mit der folgenden erforderlichen Option:`--db-parameter-group-name`.

Um alle Parameter in der DB-Parametergruppe zurückzusetzen, geben Sie die Option `--reset-all-parameters` an. Um bestimmte Parameter zurückzusetzen, geben Sie die Option `--parameters` an.

Im folgenden Beispiel werden alle Parameter in der DB-Parametergruppe namens mydbparametergroup auf ihre Standardwerte zurückgesetzt.

Example

Für LinuxmacOS, oderUnix:

```
aws rds reset-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --reset-all-parameters
```

Windows:

```
aws rds reset-db-parameter-group ^
    --db-parameter-group-name mydbparametergroup ^
    --reset-all-parameters
```

Im folgenden Beispiel werden die Optionen `max_connections` und `max_allowed_packet` in der DB-Parametergruppe namens mydbparametergroup auf ihre Standardwerte zurückgesetzt.

Example

Für LinuxmacOS, oderUnix:

```
aws rds reset-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --parameters "ParameterName=max_connections,ApplyMethod=immediate" \
                 "ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

Windows:

```
aws rds reset-db-parameter-group ^
    --db-parameter-group-name mydbparametergroup ^
    --parameters "ParameterName=max_connections,ApplyMethod=immediate" ^
                 "ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

Die Ausgabe des Befehls ähnelt der Folgenden:

```
DBParameterGroupName  mydbparametergroup
```

RDS-API

Um Parameter in einer DB-Parametergruppe auf ihre Standardwerte zurückzusetzen, verwenden Sie den RDS-API-Befehl `ResetDBParameterGroup` mit dem folgenden erforderlichen Parameter: `DBParameterGroupName`.

Um alle Parameter in der DB-Parametergruppe zurückzusetzen, setzen Sie den Parameter `ResetAllParameters` auf `true`. Um bestimmte Parameter zurückzusetzen, geben Sie den Parameter `Parameters` an.

Kopieren einer DB-Parametergruppe

Sie können benutzerdefinierte DB-Parametergruppen, die Sie erstellt haben, kopieren. Das Kopieren einer Parametergruppe kann eine bequeme Lösung sein. Ein Beispiel ist, wenn Sie eine DB-

Parametergruppe erstellt haben und die am häufigsten verwendeten Parameter und Werte in einer neuen DB-Parametergruppe aufnehmen möchten. Sie können eine DB-Parametergruppe kopieren, indem Sie den verwenden AWS Management Console. Sie können auch den AWS CLI copy-db-parameter-groupBefehl oder den ParameterGroupCopyDB-Vorgang der RDS-API verwenden.

Nachdem Sie eine DB-Parametergruppe kopiert haben, warten Sie mindestens fünf Minuten, bevor Sie die erste DB-Instance erstellen, die diese DB-Parametergruppe als Standardparametergruppe verwendet. So kann die Kopieraktion in Amazon RDS abgeschlossen werden, bevor die Parametergruppe verwendet wird. Dies ist insbesondere für Parameter wichtig, die beim Erstellen der Standarddatenbank für eine DB-Instance wichtig sind. Ein Beispiel ist der Zeichensatz für die mit dem Parameter `character_set_database` definierte Standarddatenbank. Verwenden Sie die Option Parameter Groups der Amazon RDS-Konsole oder den describe-db-parametersBefehl, um zu überprüfen, ob Ihre DB-Parametergruppe erstellt wurde.

> **Note**
>
> Standardparametergruppen können nicht kopiert werden. Sie können jedoch eine neue Parametergruppe erstellen, die auf einer Standardparametergruppe basiert.
> Sie können eine DB-Parametergruppe nicht in eine andere AWS-Konto oder kopieren AWS-Region.

Konsole

So kopieren Sie eine DB-Parametergruppe

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie in der Liste die zu kopierende benutzerdefinierte Parametergruppe.
4. Wählen Sie für Parameter group actions (Parametergruppenaktionen) die Option Kopieren.
5. Geben Sie unter New DB parameter group identifier (Neue DB-Parametergruppenkennung) einen Namen für die neue Parametergruppe ein.
6. Geben Sie unter Beschreibung eine Beschreibung für die neue Parametergruppe ein.
7. Wählen Sie die Option Copy aus.

AWS CLI

Um eine DB-Parametergruppe zu kopieren, verwenden Sie den AWS CLI `copy-db-parameter-group`Befehl mit den folgenden erforderlichen Optionen:

- `--source-db-parameter-group-identifier`
- `--target-db-parameter-group-identifier`
- `--target-db-parameter-group-description`

Im folgenden Beispiel wird eine neue DB-Parametergruppe mit dem Namen `mygroup2 that is a copy of the DB parameter group mygroup1` erstellt.

Example

Für LinuxmacOS, oderUnix:

```
aws rds copy-db-parameter-group \
    --source-db-parameter-group-identifier mygroup1 \
    --target-db-parameter-group-identifier mygroup2 \
    --target-db-parameter-group-description "DB parameter group 2"
```

Windows:

```
aws rds copy-db-parameter-group ^
    --source-db-parameter-group-identifier mygroup1 ^
    --target-db-parameter-group-identifier mygroup2 ^
    --target-db-parameter-group-description "DB parameter group 2"
```

RDS-API

Zum Kopieren einer DB-Parametergruppe verwenden Sie die RDS-API-Aktion `CopyDBParameterGroup` mit den folgenden erforderlichen Parametern:

- `SourceDBParameterGroupIdentifier`
- `TargetDBParameterGroupIdentifier`
- `TargetDBParameterGroupDescription`

Auflisten von DB-Parametergruppen

Sie können die DB-Parametergruppen auflisten, die Sie für Ihr AWS Konto erstellt haben.

> **Note**
>
> Standard-Parametergruppen werden automatisch aus einer Vorlage für Standard-Parameter erstellt, wenn Sie eine DB-Instance für eine bestimmte DB-Engine und -Version erstellen. Diese Standardparametergruppen enthalten bevorzugte Parametereinstellungen und können nicht geändert werden. Wenn Sie eine benutzerdefinierte Parametergruppe erstellen, können Sie Parametereinstellungen ändern.

Konsole

Um alle DB-Parametergruppen für ein AWS Konto aufzulisten

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   Die verfügbaren DB-Parametergruppen erscheinen in einer Liste.

AWS CLI

Verwenden Sie den AWS CLI `describe-db-parameter-groups`Befehl, um alle DB-Parametergruppen für ein AWS Konto aufzulisten.

Example

Im folgenden Beispiel werden alle verfügbaren DB-Parametergruppen für ein AWS -Konto aufgelistet.

```
aws rds describe-db-parameter-groups
```

Die Ausgabe des Befehls ähnelt der Folgenden:

```
DBPARAMETERGROUP  default.mysql8.0     mysql8.0  Default parameter group for MySQL8.0
DBPARAMETERGROUP  mydbparametergroup   mysql8.0  My new parameter group
```

Im folgenden Beispiel wird die Parametergruppe mydbparamgroup1 beschrieben.

Für LinuxmacOS, oderUnix:

```
aws rds describe-db-parameter-groups \
    --db-parameter-group-name mydbparamgroup1
```

Windows:

```
aws rds describe-db-parameter-groups ^
    --db-parameter-group-name mydbparamgroup1
```

Die Ausgabe des Befehls ähnelt der Folgenden:

```
DBPARAMETERGROUP  mydbparametergroup1  mysql8.0  My new parameter group
```

RDS-API

Verwenden Sie den DescribeDBParameterGroupsRDS-API-Vorgang, um alle DB-Parametergruppen für ein AWS Konto aufzulisten.

Anzeigen von Parameterwerten für eine DB-Parametergruppe

Sie können eine Liste aller Parameter in einer DB-Parametergruppe und ihren Werten erhalten.

Konsole

So können Sie die Parameterwerte für eine DB-Parametergruppe ansehen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   Die verfügbaren DB-Parametergruppen erscheinen in einer Liste.
3. Wählen Sie den Namen der Parametergruppe, um deren Parameterliste anzuzeigen.

AWS CLI

Um die Parameterwerte für eine DB-Parametergruppe anzuzeigen, verwenden Sie den AWS CLI describe-db-parametersBefehl mit dem folgenden erforderlichen Parameter.

- `--db-parameter-group-name`

Example

Im folgenden Beispiel werden die Parameter und Parameterwerte für eine DB-Parametergruppe mit dem Namen mydbparametergroup. aufgelistet.

```
aws rds describe-db-parameters --db-parameter-group-name mydbparametergroup
```

Die Ausgabe des Befehls ähnelt der Folgenden:

```
DBPARAMETER  Parameter Name            Parameter Value  Source           Data Type
 Apply Type  Is Modifiable
DBPARAMETER  allow-suspicious-udfs                      engine-default   boolean
 static      false
DBPARAMETER  auto_increment_increment                   engine-default   integer
 dynamic     true
DBPARAMETER  auto_increment_offset                      engine-default   integer
 dynamic     true
DBPARAMETER  binlog_cache_size         32768            system           integer
 dynamic     true
DBPARAMETER  socket                    /tmp/mysql.sock  system           string
 static      false
```

RDS-API

Um die Parameterwerte für eine DB-Parametergruppe anzuzeigen, verwenden Sie den RDS-API-Befehl `DescribeDBParameters` mit dem folgenden erforderlichen Parameter.

- `DBParameterGroupName`

Löschen einer DB-Parametergruppe

Sie können eine DB-Parametergruppe mithilfe der AWS Management Console AWS CLI, oder RDS-API löschen. Eine Parametergruppe kann nur gelöscht werden, wenn sie keiner DB-Instance zugeordnet ist.

Konsole

Um eine DB-Parametergruppe zu löschen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.

   Die verfügbaren DB-Parametergruppen erscheinen in einer Liste.
3. Wählen Sie den Namen der Parametergruppen, die gelöscht werden sollen.
4. Wählen Sie Aktionen und dann Löschen.
5. Überprüfen Sie die Namen der Parametergruppen und wählen Sie dann Löschen.

AWS CLI

Um eine DB-Parametergruppe zu löschen, verwenden Sie den AWS CLI `delete-db-parameter-group`Befehl mit dem folgenden erforderlichen Parameter.

- `--db-parameter-group-name`

Example

Im folgenden Beispiel wird eine DB-Parametergruppe mit dem Namen mydbparametergroup gelöscht.

```
aws rds delete-db-parameter-group --db-parameter-group-name mydbparametergroup
```

RDS-API

Um eine DB-Parametergruppe zu löschen, verwenden Sie den `DeleteDBParameterGroup`RDS-API-Befehl mit dem folgenden erforderlichen Parameter.

- `DBParameterGroupName`

Vergleichen von DB-Parametergruppen

Sie können die verwenden AWS Management Console , um die Unterschiede zwischen zwei DB-Parametergruppen anzuzeigen.

Die angegebenen Parametergruppen müssen beide DB-Parametergruppen oder DB-Cluster-Parametergruppen sein. Dies gilt, auch wenn die DB-Engine und die Version identisch sind. Sie können beispielsweise eine -DB-Parametergruppe `aurora-mysql8.0` (Aurora MySQL Version 3) nicht mit einer -`aurora-mysql8.0`DB-Cluster-Parametergruppe vergleichen.

Sie können DB-Parametergruppen von Aurora MySQL und RDS für MySQL vergleichen, auch für verschiedene Versionen. Im Gegensatz dazu können Sie DB-Parametergruppen von Aurora PostgreSQL und RDS für PostgreSQL jedoch nicht vergleichen.

So vergleichen Sie zwei DB-Parametergruppen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie in der Liste die beiden zu vergleichenden Parametergruppen.

   > **Note**
   >
   > Um eine Standardparametergruppe mit einer benutzerdefinierten Parametergruppe zu vergleichen, wählen Sie zuerst die Standardparametergruppe auf der Registerkarte Standard und dann die benutzerdefinierte Parametergruppe auf der Registerkarte Benutzerdefiniert aus.

4. Wählen Sie unter Aktionen die Option Vergleichen aus.

Festlegen von DB-Parametern

Zu den DB-Parametertypen gehören die folgenden:

- Ganzzahl
- Boolesch
- String
- Long
- Double
- Zeitstempel
- Objekt anderer definierter Datentypen
- Array von Werten vom Typ Ganzzahlwert, Boolesch, String, Long, Double, Zeitstempel oder Objekt

Sie können auch Ganzzahl- und Boolesche Parameter mit Ausdrücken, Formeln und Funktionen angeben.

Inhalt

DB-Parameter-Formeln

Eine DB-Parameterformel ist ein Ausdruck, der in einen Ganzzahlwert oder einen booleschen Wert aufgelöst wird. Sie schließen den Ausdruck in Klammern ein: {}. Sie können eine Formel entweder für einen DB-Parameterwert oder als Argument für eine DB-Parameterfunktion verwenden.

Syntax

```
{FormulaVariable}
{FormulaVariable*Integer}
{FormulaVariable*Integer/Integer}
{FormulaVariable/Integer}
```

DB-Parameter-Formel-Variablen

Jede Formelvariable gibt einen Ganzzahlwert oder einen booleschen Wert zurück. Bei den Namen aller Variablen muss die Groß- und Kleinschreibung beachtet werden.

AllocatedStorage

Gibt einen Ganzzahlwert zurück, der die Größe des Datenvolumens in Byte darstellt.

DB InstanceClassMemory

Gibt eine Ganzzahl für die Anzahl der Speicherbytes zurück, die für den Datenbankprozess verfügbar sind. Diese Zahl wird intern berechnet, indem mit der Gesamtspeichermenge für die DB-Instance-Klasse begonnen wird. Hiervon wird bei der Berechnung der Speicher subtrahiert, der für das Betriebssystem und die RDS-Prozesse reserviert ist, die die Instance verwalten. Daher ist die Zahl immer etwas niedriger als die Speicherzahlen, die in den Instance-Klassentabellen unter Aurora DB-Instance-Klassen genannt werden. Der genaue Wert hängt von

einer Kombination von Faktoren ab. Dazu gehören Instance-Klasse, DB-Engine und die Frage, ob der Wert für eine RDS-Instance oder eine Instance gilt, die Teil eines Aurora-Clusters ist.

EndPointPort

Gibt eine Ganzzahl zurück, die den beim Herstellen einer Verbindung mit der DB-Instance verwendeten Port darstellt.

TrueIfReplica

Gibt 1 zurück, wenn es sich bei der DB-Instance um ein Lesereplikat handelt, und `0`, wenn dies nicht der Fall ist. Dies ist der Standardwert für den Parameter `read_only` in Aurora MySQL.

DB-Parameter-Formel-Operatoren

DB-Parameter-Formeln unterstützen zwei Operatoren: Division und Multiplikation.

Divisions-Operator: /

Dividiert den Dividend durch den Divisor, gibt einen Quotienten als Ganzzahl zurück. Dezimalzahlen in einem Quotienten werden gekürzt und nicht gerundet.

Syntax

```
dividend / divisor
```

Die Dividend- und Divisor-Argumente müssen Ausdrücke mit Ganzzahlen sein.

Multiplikations-Operator: *

Multipliziert die Ausdrücke und gibt das Produkt der Ausdrücke zurück. Dezimalstellen in Ausdrücken werden gekürzt (und nicht gerundet).

Syntax

```
expression * expression
```

Beide Ausdrücke müssen Ganzzahlen sein.

DB-Parameter-Funktionen

Sie geben die Argumente von DB-Parameter-Funktionen entweder als Ganzzahlen oder Formeln an. Jede Funktion muss mindestens ein Argument haben. Geben Sie mehrere

Argumente als kommagetrennte Liste an. Die Liste darf keine leeren Elemente aufweisen, z. B. argument1,,argument3. Bei Funktionsnamen wird zwischen Groß- und Kleinschreibung unterschieden.

IF

Gibt ein Argument zurück.

Syntax

```
IF(argument1, argument2, argument3)
```

Gibt das zweite Argument zurück, wenn das erste Argument als wahr ausgewertet wird. Gibt andernfalls das dritte Argument zurück.

GREATEST

Gibt den größten Wert aus einer Liste von Ganzzahlen oder Parameter-Formeln zurück.

Syntax

```
GREATEST(argument1, argument2,...argumentn)
```

Gibt eine Ganzzahl zurück.

LEAST

Gibt den kleinsten Wert aus einer Liste von Ganzzahlen oder Parameter-Formeln zurück.

Syntax

```
LEAST(argument1, argument2,...argumentn)
```

Gibt eine Ganzzahl zurück.

SUM

Addiert die Werte der festgelegten Ganzzahlen oder Parameter-Formeln.

Syntax

```
SUM(argument1, argument2,...argumentn)
```

Gibt eine Ganzzahl zurück.

Protokollausdrücke von DB-Parametern

Sie können einen DB-Parameterwert, der eine Ganzzahl ist, auf einen Protokollausdruck festlegen. Sie schließen den Ausdruck in Klammern ein: {}. Zum Beispiel:

```
{log(DBInstanceClassMemory/8187281418)*1000}
```

Die `log`-Funktion repräsentiert die Protokollbasis 2. In diesem Beispiel wird auch die `DBInstanceClassMemory`-Formelvariable verwendet. Siehe DB-Parameter-Formel-Variablen.

Beispiele für DB-Parameterwerte

Diese Beispiele zeigen die Verwendung von Formeln, Funktionen und Ausdrücken für die Werte von DB-Parametern.

> **Warning**
>
> Wenn die Parameter in einer DB-Parametergruppe unpassend eingestellt werden, kann dies unbeabsichtigte unerwünschte Auswirkungen haben. Dies kann eine gestörte Leistung und Systeminstabilität umfassen. Gehen Sie mit Bedacht vor, wenn Sie Datenbank-Parameter ändern und sichern Sie Ihre Daten bevor Sie Ihre DB-Parametergruppe ändern. Testen Sie Parametergruppenänderungen an einer Test-DB-Instance, die mit, erstellt wurde point-in-time-restores, bevor Sie diese Änderungen an den Parametergruppen auf Ihre Produktions-DB-Instances anwenden.

Example Verwenden der DB-Parameter-Funktion LEAST

Sie können die `LEAST`-Funktion in einem Aurora MySQL `table_definition_cache`-Parameter-Wert angeben. Verwenden Sie es, um die Anzahl der Tabellendefinitionen, die im Definitionscache gespeichert werden können, auf den kleineren Wert von `DBInstanceClassMemory` geteilt durch 393040 oder 20 000 festzulegen.

```
LEAST({DBInstanceClassMemory/393040}, 20000)
```

Migrieren von Daten zu einem Amazon Aurora-DB-Cluster

Sie haben mehrere Möglichkeiten, Daten von einer vorhandenen Datenbank in einen Amazon Aurora-DB-Cluster zu migrieren, abhängig von der Datenbank-Engine-Kompatibilität. Die verfügbaren Migrationsoptionen sind auch von der Quelldatenbank und der Menge der zu migrierenden Daten abhängig.

Migrieren von Daten zu einem Amazon Aurora MySQL-DB-Cluster

Sie können Daten von einer der folgenden Quellen in einen Amazon Aurora MySQL-DB-Cluster migrieren.

- Eine RDS für MySQL-DB-Instance
- einer MySQL-Datenbank außerhalb von Amazon RDS
- einer Datenbank, die nicht MySQL-kompatibel ist

Weitere Informationen finden Sie unter Migrieren von Daten zu einem Amazon Aurora MySQL-DB-Cluster.

Migrieren von Daten zu einem Amazon Aurora PostgreSQL-DB-Cluster

Sie können Daten von einer der folgenden Quellen in einen Amazon Aurora PostgreSQL-DB-Cluster migrieren.

- Amazon RDS-PostgreSQL-DB-Instance
- Einer Datenbank, die nicht PostgreSQL-kompatibel ist

Weitere Informationen finden Sie unter Migrieren von Daten nach Amazon Aurora mit PostgreSQL-Kompatibilität.

Erstellen eines Amazon- ElastiCache Caches mit den Amazon-DB-Cluster-DB-Instance-Einstellungen von Aurora

ElastiCache ist ein vollständig verwalteter In-Memory-Caching-Service, der Lese- und Schreiblatenzen in Mikrosekunden bereitstellt, die flexible Anwendungsfälle in Echtzeit unterstützen. ElastiCache kann Ihnen helfen, die Anwendungs- und Datenbankleistung zu beschleunigen.
Sie können ElastiCache als primären Datenspeicher für Anwendungsfälle verwenden, die keine Datenbeständigkeit erfordern, z. B. Gaming-Bestenlisten, Streaming und Datenanalysen. ElastiCache helps beseitigen die Komplexität, die mit der Bereitstellung und Verwaltung einer verteilten Computing-Umgebung verbunden ist. Weitere Informationen finden Sie unter Häufige ElastiCache Anwendungsfälle und wie für Memcached helfen ElastiCache kann und Häufige ElastiCache Anwendungsfälle und wie für Redis helfen ElastiCache kann. Sie können die Amazon-RDS-Konsole zum Erstellen eines ElastiCache Cache verwenden.

Sie können Amazon ElastiCache in zwei Formaten betreiben. Sie können mit einem Serverless-Cache beginnen oder einen eigenen Cache-Cluster entwerfen. Wenn Sie Ihren eigenen Cache-Cluster entwerfen möchten, ElastiCache funktioniert sowohl mit den Redis- als auch mit den Memcached-Engines. Wenn Sie sich nicht sicher sind, welche Engine Sie verwenden möchten, finden Sie weitere Informationen unter Memcached und Redis im Vergleich. Weitere Informationen zu Amazon ElastiCachefinden Sie im Amazon- ElastiCache Benutzerhandbuch.

Themen

- Übersicht über die ElastiCache Cache-Erstellung mit RDS-DB-Cluster-Einstellungen
- Erstellen eines - ElastiCache Cache mit Einstellungen aus einer Aurora-DB-Cluster

Übersicht über die ElastiCache Cache-Erstellung mit RDS-DB-Cluster-Einstellungen

Sie können einen - ElastiCache Cache aus Amazon RDS mit denselben Konfigurationseinstellungen wie ein neu erstellter oder vorhandener Aurora-DB-Cluster erstellen.

Einige Anwendungsfälle zum Zuordnen eines - ElastiCache Cache zu Ihrem DB-ClusterIhrer DB-

- Sie können Kosten sparen und Ihre Leistung verbessern, indem Sie ElastiCache mit RDS verwenden, anstatt nur auf RDS zu laufen.

- Sie können den ElastiCache Cache als primären Datenspeicher für Anwendungen verwenden, für die keine Datenbeständigkeit erforderlich ist. Ihre Anwendungen, die Redis oder Memcached verwenden, können ElastiCache fast ohne Änderungen verwenden.

Wenn Sie einen ElastiCache Cache aus RDS erstellen, erbt der ElastiCache Cache die folgenden Einstellungen von der zugehörigen Aurora-DB-Cluster:

- ElastiCache -Konnektivitätseinstellungen
- ElastiCache -Sicherheitseinstellungen

Sie können die Cache-Konfigurationseinstellungen auch entsprechend Ihren Anforderungen festlegen.

Einrichten von ElastiCache in Ihren Anwendungen

Ihre Anwendungen müssen so eingerichtet sein, dass sie den ElastiCache Cache verwenden. Sie können die Cache-Leistung auch optimieren und verbessern, indem Sie Ihre Anwendungen so einrichten, dass sie je nach Ihren Anforderungen Caching-Strategien verwenden.

- Informationen zum Zugriff auf Ihren ElastiCache Cache und zu den ersten Schritten finden Sie unter Erste Schritte mit Amazon ElastiCache für Redis und Erste Schritte mit Amazon ElastiCache für Memcached.
- Weitere Informationen zu Caching-Strategien finden Sie unter Caching-Strategien und bewährte Methoden für Memcached und Caching-Strategien und bewährte Methoden für Redis.
- Weitere Informationen zur Hochverfügbarkeit in ElastiCache für Redis-Cluster finden Sie unter Hochverfügbarkeit mithilfe von Replikationsgruppen.
- Es können Kosten für Backup-Speicher, Datenübertragung innerhalb oder zwischen Regionen oder die Verwendung von anfallen AWS Outposts. Einzelheiten zu den Preisen finden Sie unter Amazon- ElastiCache Preise.

Erstellen eines - ElastiCache Cache mit Einstellungen aus einer Aurora-DB-Cluster

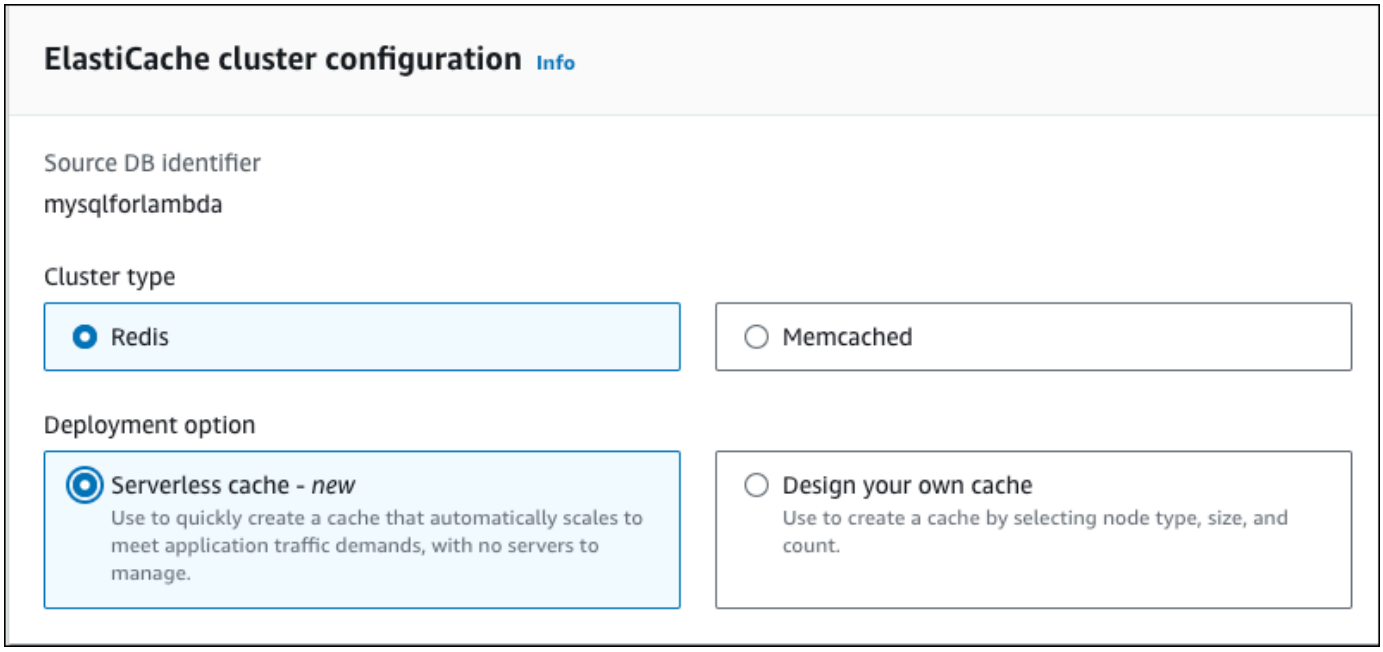
Sie können einen - ElastiCache Cache für Ihre Aurora-DB-Cluster RDS-DB-Instances mit Einstellungen für erstellen, die von der DB-Cluster geerbt wurden.

Erstellen eines - ElastiCache Cache mit Einstellungen aus einer DB-Cluster-

1. Befolgen Sie die Anweisungen unter , um einen DB-Cluster zu erstelle Erstellen eines Amazon Aurora-DB Clusters.
2. Nach dem Erstellen eines Aurora-DB-Clusters einer zeigt die Konsole das Fenster Empfohlene Add-Ons an. Wählen Sie Erstellen eines - ElastiCache Clusters aus RDS mit Ihren DB-Einstellungen aus.

   Wählen Sie für eine vorhandene Datenbank auf der Seite Datenbanken die erforderliche DB-Cluster-. Wählen Sie im Dropdown-Menü Aktionen die Option ElastiCache Cluster erstellen aus, um einen ElastiCache Cache in RDS zu erstellen, der dieselben Einstellungen wie Ihre vorhandene Aurora-DB-Cluster hat.

   Im ElastiCache Konfigurationsabschnitt zeigt die Quell-DB-Kennung an, von welcher DB-Cluster- der ElastiCache Cache Einstellungen erbt.
3. Wählen Sie aus, ob Sie einen Redis- oder Memcached-Cluster erstellen möchten. Weitere Informationen finden Sie unter Memcached und Redis im Vergleich.



4. Wählen Sie danach aus, ob Sie einen Serverless-Cache erstellen oder Ihren eigenen Cache entwerfen möchten. Weitere Informationen finden Sie unter Auswählen zwischen Bereitstellungsoptionen.

   Wenn Sie Serverless-Cache wählen:

   a. Geben Sie unter Cache-Einstellungen Werte für Name und Beschreibung ein.

b. Behalten Sie unter Standardeinstellungen anzeigen die Standardeinstellungen bei, um die Verbindung zwischen Ihrem Cache und der DB-Cluster herzustellen.

c. Sie können die Standardeinstellungen auch bearbeiten, indem Sie Standardeinstellungen anpassen auswählen. Wählen Sie die ElastiCache Konnektivitätseinstellungen , ElastiCache Sicherheitseinstellungen und Maximale Nutzungslimits aus.

5. Wenn Sie Eigenen Cache entwerfen wählen:

a. Wenn Sie Redis-Cluster ausgewählt haben, wählen Sie aus, ob der Clustermodus aktiviert oder deaktiviert bleiben soll. Weitere Informationen finden Sie unter Replikation: Redis (Cluster-Modus deaktiviert) im Vergleich zu Redis (Cluster-Modus aktiviert).

b. Geben Sie Werte für Name, Beschreibung und Engine-Version ein.

   Für Engine-Version wird als Standardwert die neueste Engine-Version empfohlen. Sie können auch eine Engine-Version für den ElastiCache Cache auswählen, die Ihren Anforderungen am besten entspricht.

c. Wählen Sie den Knotentyp in der Option Knotentyp aus. Weitere Informationen finden Sie unter Verwalten von Knoten.

   Wenn Sie einen Redis-Cluster erstellen möchten, dessen Cluster-Modus auf Aktiviert festgelegt ist, geben Sie die Anzahl der Shards (Partitionen/Knotengruppen) für die Option Anzahl der Shards ein.

   Geben Sie im Feld Anzahl der Replikate die Zahl der Replikate jedes Shards ein.

   > **Note**
   >
   > Der ausgewählte Knotentyp, die Anzahl der Shards und die Anzahl der Replikate wirken sich alle auf Ihre Cache-Leistung und Ihre Ressourcenkosten aus. Stellen Sie sicher, dass diese Einstellungen Ihren Datenbankanforderungen entsprechen. Preisinformationen finden Sie unter Amazon- ElastiCache Preise.

d. Wählen Sie die ElastiCache Konnektivitäts- und ElastiCache Sicherheitseinstellungen aus. Sie können die Standardeinstellungen beibehalten oder diese Einstellungen an Ihre Anforderungen anpassen.

6. Überprüfen Sie die Standard- und geerbten Einstellungen Ihres ElastiCache Cache. Einige Einstellungen können nach der Erstellung nicht geändert werden.

> **Note**
>
> RDS passt möglicherweise das Backup-Fenster Ihres ElastiCache Cache an, um die Mindestfensteranforderung von 60 Minuten zu erfüllen. Das Backup-Fenster Ihrer Quelldatenbank bleibt gleich.

7. Wenn Sie bereit sind, wählen Sie ElastiCache Cache erstellen aus.

Die Konsole zeigt ein Bestätigungsbanner für die ElastiCache Cache-Erstellung an. Folgen Sie dem Link im Banner zur ElastiCache Konsole, um die Cache-Details anzuzeigen. Die ElastiCache Konsole zeigt den neu erstellten ElastiCache Cache an.

Verwalten eines Amazon Aurora-DB-Clusters

In diesem Abschnitt erfahren Sie, wie Sie Ihren Aurora-DB-Cluster verwalten. Aurora umfasst Cluster von Datenbankservern, die mittels Replikationstopologie verbunden sind. Daher beinhaltet die Verwaltung von Aurora häufig das Bereitstellen von Änderungen auf mehreren Servern und das Sicherstellen, dass alle Aurora-Replicas mit dem Master-Server Schritt halten. Da Aurora den zugrunde liegenden Speicher bei wachsender Datenmenge transparent skaliert, erfordert die Verwaltung von Aurora relativ wenig Verwaltung von Festplattenspeicher. Ähnlich gilt: Da Aurora automatisch fortlaufend Sicherungen durchführt, erfordert ein Aurora-Cluster keine umfangreichen Planungen oder Ausfallzeiten für die Durchführung von Sicherungen.

Themen

Stoppen und Starten eines Amazon Aurora-DB-Clusters

Mithilfe des Stoppens und Startens von Amazon Aurora-Clustern können Sie die Kosten für Entwicklungs- und Testumgebungen verwalten. Sie können vorübergehend alle DB-Instances in Ihrem Cluster stoppen, anstatt alle DB-Instances jedes Mal, wenn Sie den Cluster verwenden, einzurichten und zu entfernen.

Themen

Übersicht über das Stoppen und Starten eines Aurora-DB-Clusters

In Zeiten, in denen Sie keinen Aurora-Cluster benötigen, können Sie alle Instances in dem betreffenden Cluster gleichzeitig stoppen. Bei Bedarf können Sie den Cluster jederzeit erneut starten. Durch das Starten und Stoppen werden die Einrichtungs- und Entfernungsvorgänge für Cluster erleichtert, die in der Entwicklung, für Tests oder ähnliche Aktivitäten verwendet werden, die keine kontinuierliche Verfügbarkeit erfordern. Unabhängig davon, wie viele Instances in dem Cluster enthalten sind, können Sie alle beteiligten AWS Management Console-Prozeduren mit einer einzigen Aktion ausführen.

Solange Ihr DB-Cluster gestoppt ist, werden Ihnen nur Gebühren für Cluster-Speicherspeicherplatz, manuelle Snapshots und automatisierten Sicherungsspeicher innerhalb des von Ihnen festgelegten Aufbewahrungsfensters berechnet. Für DB-Instance-Stunden werden Ihnen keine Gebühren berechnet.

> **Important**
>
> Sie können einen DB-Cluster für bis zu sieben Tage anhalten. Wenn Sie Ihren DB-Cluster nach sieben Tagen nicht manuell starten, wird der Cluster automatisch gestartet, damit dieser in Bezug auf erforderliche Wartungsupdates nicht in Verzug gerät.

Um die Gebühren für einen Aurora-Cluster mit geringer Auslastung zu minimieren, können Sie den Cluster stoppen, anstatt alle seine Aurora-Replicas zu löschen. Bei Clustern mit mehr als nur ein oder zwei Instances ist ein häufiges Löschen und Neuerstellen der DB-Instances nur über die AWS CLI oder die Amazon-RDS-API praktikabel. Es kann auch schwierig sein, bei der Ausführung einer solchen Folge von Operationen die richtige Reihenfolge einzuhalten, also beispielsweise vor dem Löschen der primären Instance alle Aurora-Replicas zu löschen, um eine Aktivierung des Failover-Mechanismus zu vermeiden.

Verwenden Sie die Funktion zum Starten und Stoppen nicht, wenn Ihr DB-Cluster aktiv bleiben muss, jedoch überschüssige Kapazitäten hat. Wenn Ihr Cluster zu teuer oder zu wenig ausgelastet ist, löschen Sie eine oder mehrere DB-Instances oder ändern Sie alle Ihre DB-Instances und ordnen Sie sie einer Small-Instance-Klasse zu. Es ist nicht möglich, eine einzelne Aurora-DB-Instance zu stoppen.

Einschränkungen für das Stoppen und Starten eines Aurora-DB-Clusters

Einige Aurora-Cluster können nicht gestoppt und wieder gestartet werden:

- Cluster, die Teil einer globalen Aurora-Datenbank sind, können nicht gestoppt und wieder gestartet werden.
- Sie können einen Cluster, der über ein regionsübergreifendes Lesereplikat verfügt, nicht anhalten und starten.
- Sie können einen Cluster, der Teil einer Blau/Grün-Bereitstellung ist, nicht anhalten und starten.
- Für einen Cluster, der die Funktion Aurora Parallel Query verwendet, ist die Aurora MySQL-Mindestversion 2.09.0.
- Sie können einen Aurora Serverless v1-Cluster nicht stoppen und starten. Mit Aurora Serverless v2 können Sie einen Cluster stoppen und starten.

Wenn ein vorhandener Cluster nicht gestoppt und gestartet werden kann, ist die Aktion Stoppen nicht im Menü Aktionen auf der Seite Datenbanken oder auf der Detailseite verfügbar.

Stoppen eines Aurora-DB-Clusters

Für die Verwendung eines Aurora-DB-Clusters oder die Durchführung von administrativen Aufgaben beginnen Sie immer mit einem aktiven Aurora-DB-Cluster, stoppen diesen und starten ihn anschließend erneut. Während Ihr Cluster gestoppt ist, werden Ihnen Cluster-Speicherplatz,

manuelle Snapshots und automatisierter Sicherungsspeicher innerhalb des von Ihnen festgelegten Aufbewahrungsfensters in Rechnung gestellt, nicht jedoch DB-Instance-Stunden.

Beim Stoppvorgang werden zuerst die Aurora-Replica-Instances und dann die primäre Instance gestoppt, damit der Failover-Mechanismus nicht aktiviert wird.

Ein DB-Cluster, der das Replikationsziel für Daten aus einem anderen DB-Cluster bildet oder als Replikationsmaster fungiert und Daten an einen anderen Cluster überträgt, kann nicht angehalten werden.

Bestimmte besondere Arten von Clustern können nicht angehalten werden. Cluster, die Teil einer globalen Aurora-Datenbank sind, können nicht angehalten und wieder gestartet werden.

Konsole

So stoppen Sie einen Aurora-Cluster:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Databases (Datenbanken) und anschließend einen Cluster aus. Sie können den Stoppvorgang von dieser Seite ausführen oder zur Detailseite für den zu stoppenden DB-Cluster navigieren.
3. Wählen Sie für Actions (Aktionen) die Option Stop temporarily (Temporär anhalten) aus.

   Wenn ein DB-Cluster nicht gestoppt und gestartet werden kann, ist die Aktion Stop temporarily (Temporär anhalten) im Menü Actions (Aktionen) auf der Seite Databases (Datenbanken) oder auf der Detailseite nicht verfügbar. Informationen zu den Arten von Clustern, die Sie nicht starten und stoppen können, finden Sie unter Einschränkungen für das Stoppen und Starten eines Aurora-DB-Clusters.
4. Wählen Sie im Fenster Stop DB cluster temporarily (DB-Cluster vorübergehend anhalten) die Bestätigung aus, dass der DB-Cluster nach 7 Tagen automatisch neu gestartet wird.
5. Klicken Sie auf Stop temporarily (Temporär anhalten), um den DB-Cluster anzuhalten, oder auf Cancel (Abbrechen), wenn Sie den Vorgang abbrechen möchten.

AWS CLI

Um eine DB-Instance mithilfe der anzuhaltenAWS CLI, rufen Sie den stop-db-cluster Befehl mit den folgenden Parametern auf:

- `--db-cluster-identifier` – Der Name des Aurora-Clusters.

Example

```
aws rds stop-db-cluster --db-cluster-identifier mydbcluster
```

RDS-API

Zum Anhalten einer DB-Instance über die Amazon RDS-API rufen Sie die Aktion StopDBCluster mit dem folgenden Parameter auf:

- `DBClusterIdentifier` – Der Name des Aurora-Clusters.

Mögliche Operationen, während ein Aurora-DB-Cluster gestoppt ist

Während ein Aurora-Cluster gestoppt ist, können Sie eine point-in-time Wiederherstellung auf einen beliebigen Punkt innerhalb des von Ihnen angegebenen Zeitfensters für die Aufbewahrung automatisierter Backups durchführen. Weitere Informationen zum Durchführen einer point-in-time Wiederherstellung finden Sie unter Wiederherstellen von Daten.

Die Konfiguration des Aurora-DB-Clusters oder seiner DB-Instances kann nicht geändert werden, solange der Cluster gestoppt ist. Es ist auch nicht möglich, DB-Instances zu dem Cluster hinzuzufügen oder daraus zu entfernen oder den Cluster zu löschen, wenn ihm noch DB-Instances zugeordnet sind. Vor solchen administrativen Aktionen müssen Sie den Cluster starten.

Das Stoppen eines DB-Clusters entfernt ausstehende Aktionen, mit Ausnahme der DB-Cluster-Parametergruppe oder der DB-Parametergruppen der DB-Cluster-Instances.

Aurora wendet alle geplanten Wartungen auf Ihren gestoppten Cluster an, nachdem dieser wieder gestartet wurde. Denken Sie daran: Nach sieben Tagen startet Aurora gestoppte Cluster automatisch, damit diese in Bezug auf ihren Wartungsstatus nicht zu weit zurückfallen.

Aurora führt auch keine automatischen Sicherungen durch, da sich die zugrunde liegenden Daten nicht ändern können, solange der Cluster gestoppt ist. Aurora verlängert den Aufbewahrungszeitraum für Backups für den DB-Cluster nicht, während dieser gestoppt ist.

Starten eines Aurora-DB-Clusters

Ausgangspunkt für den Start eines Aurora-DB-Clusters ist immer ein bereits im gestoppten Zustand befindlicher Aurora-Cluster. Wenn Sie den Cluster starten, werden alle seine DB-Instances wieder verfügbar. Der Cluster behält seine Konfigurationseinstellungen, wie z. B. Endpunkte, Parametergruppen und VPC-Sicherheitsgruppen, bei.

Der Neustart eines DB-Clusters dauert in der Regel mehrere Minuten.

Konsole

So starten Sie einen Aurora-Cluster:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Databases (Datenbanken) und anschließend einen Cluster aus. Sie können den Startvorgang von dieser Seite ausführen oder zur Detailseite für den zu startenden DB-Cluster navigieren.
3. Wählen Sie für Actions (Aktionen) die Option Start.

AWS CLI

Um einen DB-Cluster mit der zu startenAWS CLI, rufen Sie den start-db-cluster Befehl mit den folgenden Parametern auf:

- `--db-cluster-identifier` – Der Name des Aurora-Clusters. Bei diesem Namen handelt es sich entweder um eine bestimmte Clusterkennung, die Sie beim Erstellen des Clusters ausgewählt haben, oder um die von Ihnen ausgewählte DB-Instance-Kennung mit dem Anhang `-cluster`.

Example

```
aws rds start-db-cluster --db-cluster-identifier mydbcluster
```

RDS-API

Zum Starten eines Aurora-DB-Clusters über die Amazon RDS-API, rufen Sie die Aktion StartDBCluster mit dem folgenden Parameter auf:

- `DBCluster` – Der Name des Aurora-Clusters. Bei diesem Namen handelt es sich entweder um eine bestimmte Clusterkennung, die Sie beim Erstellen des Clusters ausgewählt haben, oder um die von Ihnen ausgewählte DB-Instance-Kennung mit dem Anhang `-cluster`.

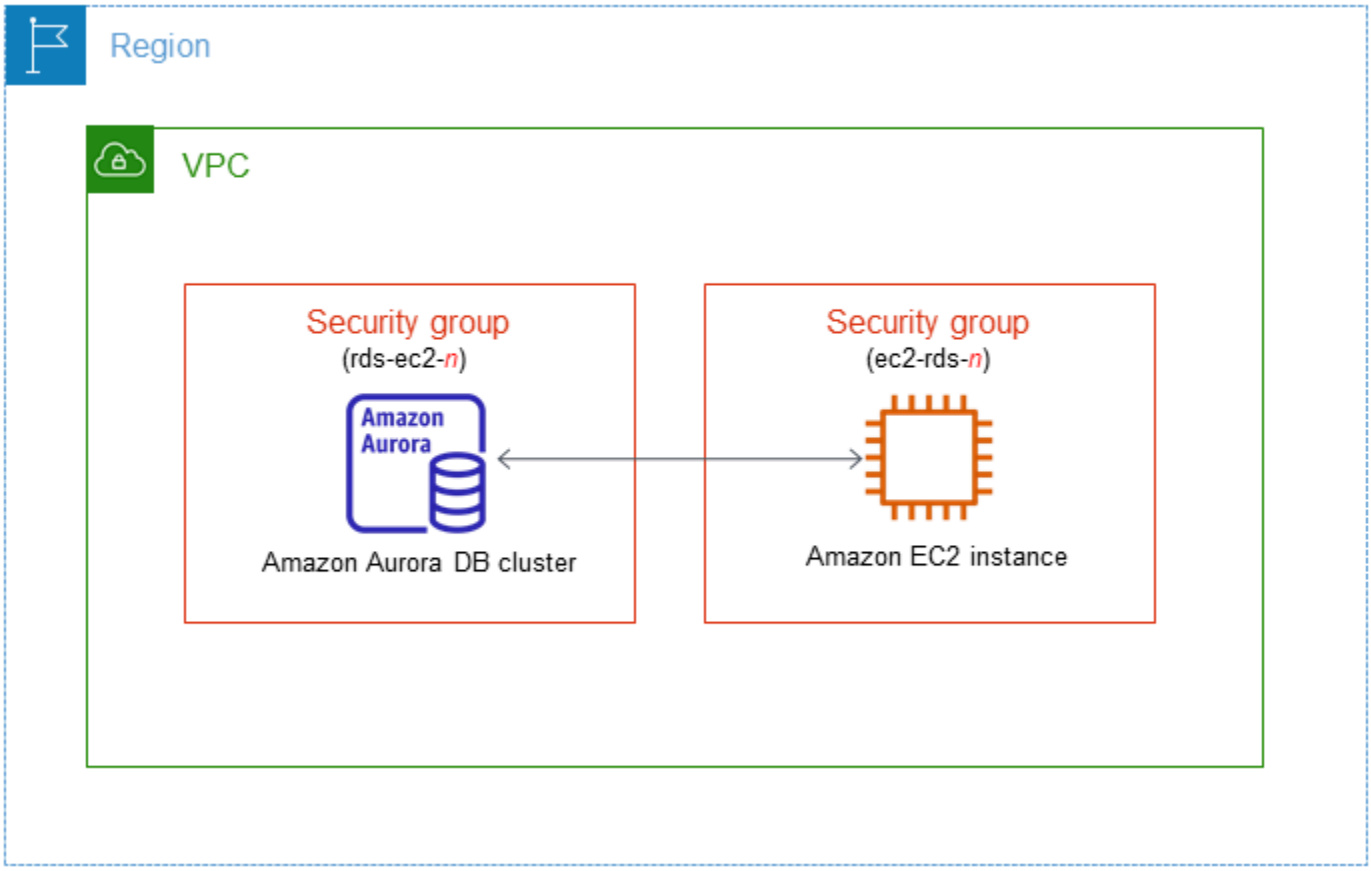
Automatisches Verbinden einer AWS-Rechenressource und einen Aurora-DB-Cluster

Sie können einen Aurora-DB-Cluster und AWS-Rechenressourcen wie Amazon Elastic Compute Cloud (Amazon EC2)-Instances und Funktionen von AWS Lambda automatisch verbinden.

Themen

Automatisches Verbinden einer EC2-Instance mit einem Aurora-DB-Cluster

Sie können die Amazon-RDS-Konsole verwenden, um das Einrichten einer Verbindung zwischen einer Amazon Elastic Compute Cloud (Amazon-EC2)-Instance und einer DB–Instance zu vereinfachen. Häufig befindet sich Ihr DB-Cluster in einem privaten Subnetz und Ihre EC2-Instance in einem öffentlichen Subnetz innerhalb einer VPC. Sie können einen SQL-Client auf Ihrer EC2-Instance verwenden, um eine Verbindung mit Ihrem DB-Cluster herzustellen. Die EC2-Instance kann auch Webserver oder Anwendungen ausführen, die auf Ihren privaten DB-Cluster zugreifen.



Wenn Sie eine Verbindung mit einer EC2-Instance herstellen möchten, die sich nicht in derselben VPC wie der Aurora-DB-Cluster befindet, sehen Sie sich die entsprechenden Szenarien unter Szenarien für den Zugriff auf eine DB-Cluster in einer VPC an.

Themen

- Übersicht über die automatische Verbindung mit einer EC2-Instance
- Automatisches Verbinden einer EC2-Instance und einem Aurora-DB-Cluster
- Anzeigen verbundener Rechenressourcen
- Herstellen einer Verbindung mit einer DB-Instance, die eine bestimmte DB-Engine ausführt

Übersicht über die automatische Verbindung mit einer EC2-Instance

Wenn Sie eine Verbindung zwischen einer EC2-Instance und einer/m einem Aurora-DB-Cluster einrichten, konfiguriert Amazon RDS automatisch die VPC-Sicherheitsgruppe für Ihre EC2-Instance und für Ihre Ihren DB-Cluster.

Im Folgenden sind Anforderungen für die Verbindung einer EC2-Instance mit einer einem Aurora-DB-Cluster aufgeführt:

- Die EC2-Instance muss sich in derselben VPC wie der DB-Cluster befinden.

  Wenn keine EC2-Instances in derselben VPC vorhanden sind, dann bietet die Konsole einen Link zum Erstellen einer solchen Instance.
- Derzeit kann der DB-Cluster kein DB-Cluster von Aurora Serverless oder Teil einer globalen Aurora-Datenbank sein.
- Der Benutzer, der die Verbindung einrichtet, muss über Berechtigungen zum Ausführen der folgenden Amazon-EC2-Vorgänge verfügen:
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateSecurityGroup`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeSecurityGroups`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Auf Ihrem Konto fallen ggf. Kosten über Availability Zones hinweg an, wenn sich die DB-Instance und die EC2-Instance in unterschiedlichen Availability Zones befinden.

Wenn Sie eine Verbindung mit einer EC2-Instance einrichten, führt Amazon RDS eine Aktion aus, die auf der aktuellen Konfiguration der Sicherheitsgruppen basiert, die dem DB-Cluster und der EC2-Instance zugeordnet sind, wie in der folgenden Tabelle beschrieben.

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	RDS-Aktion
Dem DB-Cluster sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rds-ec2-`*n* entspricht (wobei *n*	Der EC2-Instance sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `ec2-rds-`*n* entspricht (wobei *n*	RDS führt keine Aktion aus. Es wurde bereits automatisch eine Verbindung zwischen der EC2-Instance und dem DB-Cluster konfiguriert. Da bereits

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	RDS-Aktion
für eine Zahl steht). Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle.	für eine Zahl steht). Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters als Quelle.	eine Verbindung zwischen der EC2-Instance und der RDS-Datenbank besteht, werden die Sicherheitsgruppen nicht geändert.

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	RDS-Aktion
Es gilt eine der folgenden Bedingungen: • Dem DB-Cluster sind keine Sicherheitsgruppen zugeordnet, deren Name dem Muster `rds-ec2-`*n* entspricht. • Dem DB-Cluster sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rds-ec2-`*n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit der EC2-Instance verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn sie keine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde. Beispiele für Änderungen sind das Hinzufügen einer Regel oder das Ändern des Ports einer vorhandenen Regel.	Es gilt eine der folgenden Bedingungen: • Der EC2-Instance ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `ec2-rds-`*n* entspricht. • Der EC2-Instance sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `ec2-rds-`*n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit dem DB-Cluster verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn diese keine Regel für ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters als Quelle enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	RDS action: create new security groups

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	RDS-Aktion
Dem DB-Cluster sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rds-ec2-`*n* entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle.	Der EC2-Instance sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `ec2-rds-`*n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit dem DB-Cluster verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn diese keine Regel für ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters als Quelle enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	RDS action: create new security groups
Dem DB-Cluster sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rds-ec2-`*n* entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle.	Eine gültige EC2-Sicherheitsgruppe für die Verbindung ist vorhanden, jedoch nicht mit der EC2-Instance verknüpft. Die Sicherheitsgruppe trägt einen Namen, der dem Muster `ec2-rds-`*n* entspricht. Sie wurde nicht geändert. Sie enthält nur eine Regel für ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters als Quelle.	RDS action: associate EC2 security group

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle EC2-Sicherheitsgruppenkonfiguration	RDS-Aktion
Es gilt eine der folgenden Bedingungen: • Dem DB-Cluster sind keine Sicherheitsgruppen zugeordnet, deren Name dem Muster `rds-ec2-`*n* entspricht. • Dem DB-Cluster sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rds-ec2-`*n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit der EC2-Instance verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn sie keine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle enthält. Amazon RDS kann außerdem keine Sicherheitsgruppe verwenden, die geändert wurde.	Der EC2-Instance sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `ec2-rds-`*n* entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters als Quelle.	RDS action: create new security groups

RDS-Aktion : neue Sicherheitsgruppen erstellen

Amazon RDS führt die folgenden Aktionen durch:

- Erstellt eine neue Sicherheitsgruppe, die dem Muster `rds-ec2-`*n* entspricht. Diese Sicherheitsgruppe enthält eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der EC2-Instance als Quelle. Diese Sicherheitsgruppe ist dem DB-Cluster zugeordnet und ermöglicht der EC2-Instance den Zugriff auf den DB-Cluster.
- Erstellt eine neue Sicherheitsgruppe, die dem Muster `ec2-rds-`*n* entspricht. Diese Sicherheitsgruppe hat eine ausgehende Regel mit der VPC-Sicherheitsgruppe des als Ziel. Diese Sicherheitsgruppe ist der EC2-Instance zugeordnet und ermöglicht es der EC2-Instance, Datenverkehr an den DB-Cluster zu senden.

RDS-Aktion : EC2-Sicherheitsgruppe zuordnen

Amazon RDS ordnet die gültige, vorhandene EC2-Sicherheitsgruppe der EC2-Instance zu. Diese Sicherheitsgruppe ermöglicht es der EC2-Instance, Datenverkehr an den DB-Cluster zu senden.

Automatisches Verbinden einer EC2-Instance und einem Aurora-DB-Cluster

Bevor Sie eine Verbindung zwischen einer EC2-Instance und einem Aurora-DB-Cluster einrichten, stellen Sie sicher, dass Sie die unter Übersicht über die automatische Verbindung mit einer EC2-Instance beschriebenen Anforderungen erfüllen.

Wenn Sie nach dem Konfigurieren der Verbindung Änderungen an diesen Sicherheitsgruppen vornehmen, können sich die Änderungen auf die Verbindung zwischen der EC2-Instance und dem Aurora-DB-Cluster auswirken.

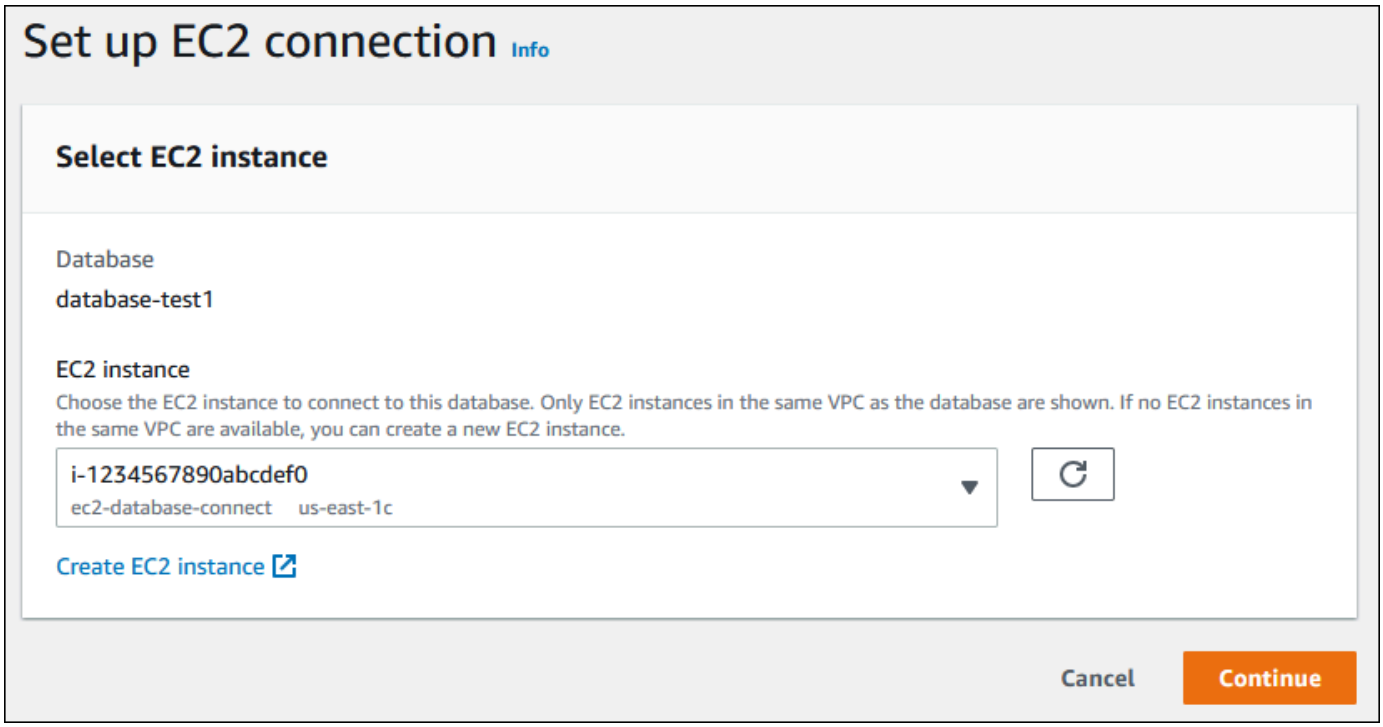
> **Note**
>
> Sie können eine Verbindung zwischen einer EC2-Instance und einem Aurora-DB-Cluster nur automatisch einrichten, indem Sie die AWS Management Console verwenden. Sie können keine automatische Verbindung mit der AWS CLI oder der RDS-API einrichten.

So verbinden Sie eine EC2-Instance und einen Aurora-DB-Cluster automatisch

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die RDS-Datenbank aus.
3. Wählen Sie für Aktionen die Option EC2-Verbindung einrichten aus.

Die Seite Set up EC2 connection (EC2-Verbindung einrichten) wird angezeigt.

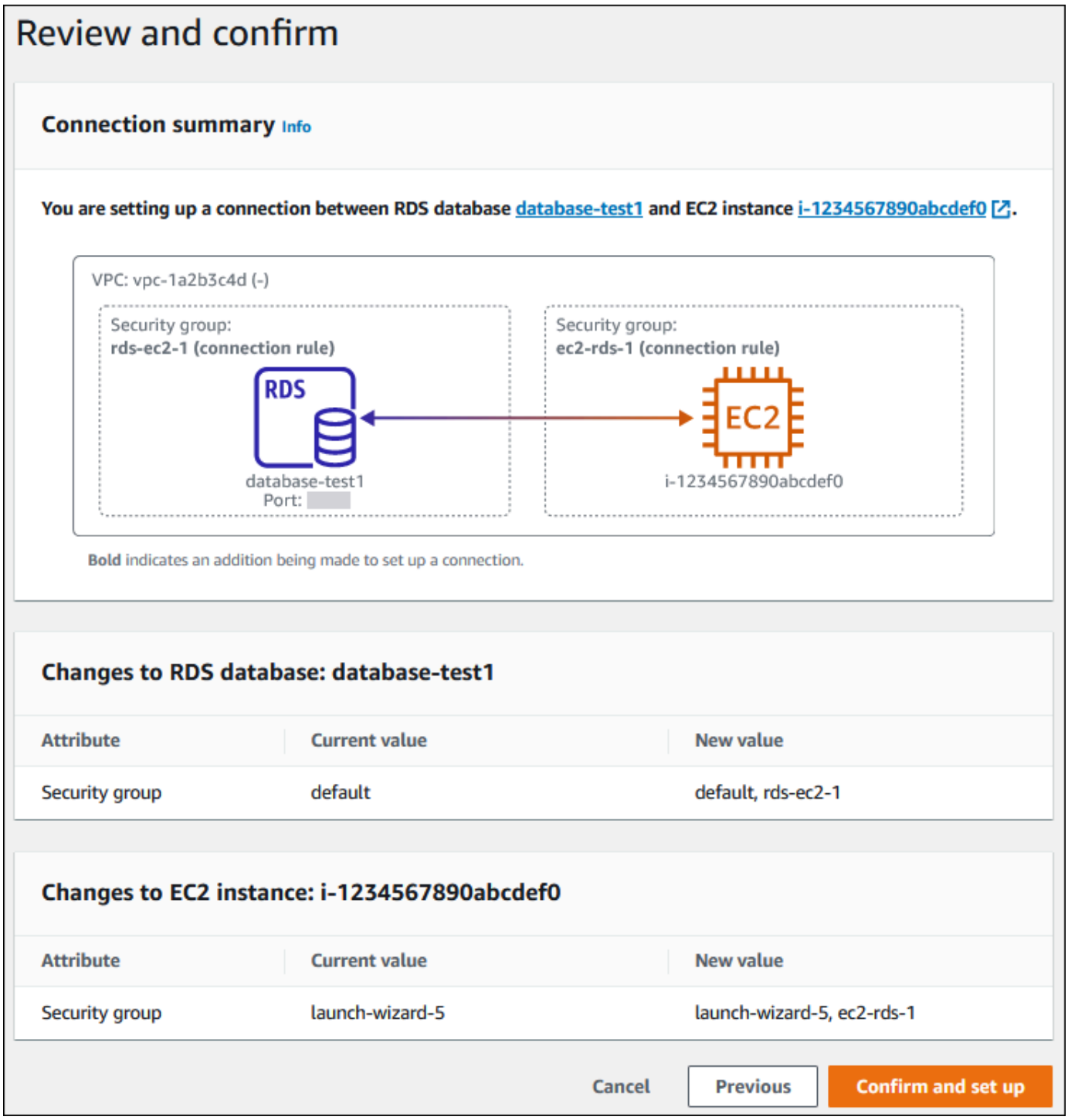
4. Wählen Sie auf der Seite Set up EC2 connection (EC2-Verbindung einrichten) die EC2-Instance aus.



Wenn keine EC2-Instances in derselben VPC vorhanden sind, wählen Sie Create EC2 instance (EC2-Instance erstellen) aus, um eine solche Instance zu erstellen. Stellen Sie in diesem Fall sicher, dass sich die neue EC2-Instance in derselben VPC wie der DB-Cluster befindet.

5. Klicken Sie auf Weiter.

Die Seite Review and confirm (Überprüfen und bestätigen) wird angezeigt.



6. Sehen Sie sich auf der Seite Review and confirm (Überprüfen und bestätigen) die Änderungen an, die RDS beim Einrichten der Verbindung mit der EC2-Instance vornehmen wird.

   Wenn die Änderungen korrekt sind, wählen Sie Bestätigen und einrichten.

   Sind die Änderungen nicht korrekt, wählen Sie Previous (Zurück) oder Cancel (Abbrechen) aus.

Anzeigen verbundener Rechenressourcen

Sie können den verwenden AWS Management Console , um die Rechenressourcen anzuzeigen, die mit einem Aurora DB-Cluster mit einer verbunden sind. Zu den angezeigten Ressourcen gehören Rechenressourcenverbindungen, die automatisch eingerichtet wurden. Sie können die Konnektivität mit Rechenressourcen auf folgende Weise automatisch einrichten:

- Sie können die Rechenressource auswählen, wenn Sie die Datenbank erstellen.

  Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.
- Sie können die Konnektivität zwischen einer vorhandenen Datenbank und einer Rechenressource einrichten.

  Weitere Informationen finden Sie unter Automatisches Verbinden einer EC2-Instance und einem Aurora-DB-Cluster.

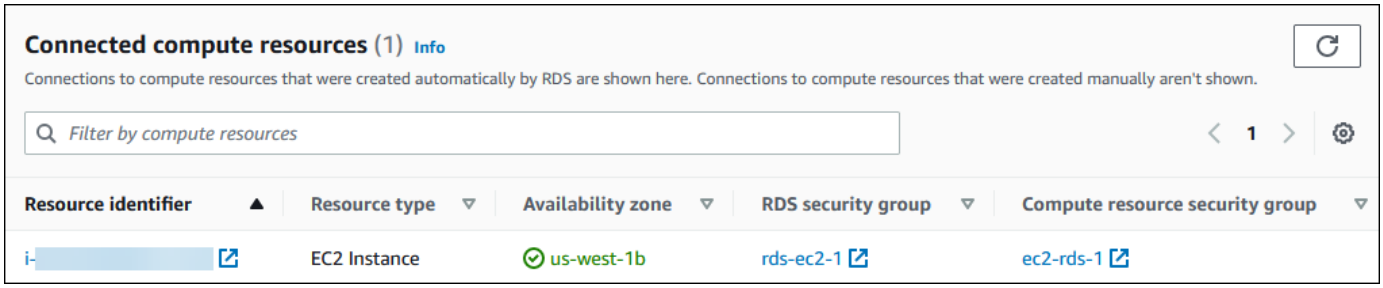
Die aufgelisteten Rechenressourcen enthalten keine Ressourcen, die manuell mit der Datenbank verbunden wurden. Sie können beispielsweise einer Rechenressource den manuellen Zugriff auf eine Datenbank erlauben, indem Sie der VPC-Sicherheitsgruppe, die der Datenbank zugeordnet ist, eine Regel hinzufügen.

Für die Auflistung einer Rechenressource müssen die folgenden Bedingungen erfüllt sei:

- Der Name der Sicherheitsgruppe, die der Rechenressource zugeordnet ist, entspricht dem Muster `ec2-rds-`*n* (wobei *n* für eine Zahl steht).
- Die Sicherheitsgruppe, die der Rechenressource zugeordnet ist, hat eine Regel für ausgehenden Datenverkehr, wobei der Portbereich auf den Port festgelegt ist, den der DB-Cluster verwendet.
- Die Sicherheitsgruppe, die der Rechenressource zugeordnet ist, hat eine Regel für ausgehenden Datenverkehr, wobei die Quelle auf eine Sicherheitsgruppe festgelegt ist, die dem DB-Cluster zugeordnet ist.
- Der Name der Sicherheitsgruppe, die dem DB-Cluster zugeordnet ist, entspricht dem Muster `rds-ec2-`*n* entspricht (wobei *n* für eine Zahl steht).
- Die Sicherheitsgruppe, die dem DB-Cluster zugeordnet ist, hat eine Regel für eingehenden Datenverkehr, wobei der Portbereich auf den Port festgelegt ist, den der DB-Cluster verwendet.
- Die Sicherheitsgruppe, die dem DB-Cluster zugeordnet ist, hat eine Regel für eingehenden Datenverkehr, wobei die Quelle auf eine Sicherheitsgruppe festgelegt ist, die der Rechenressource zugeordnet ist.

So zeigen Sie Rechenressourcen an, die mit einem Aurora-DB-Cluster verbunden sind

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann den Namen der RDS-Datenbank aus.
3. Sehen Sie sich auf der Registerkarte Connectivity & security (Konnektivität und Sicherheit) die Rechenressourcen unter Verbundene Rechenressourcen an.



Herstellen einer Verbindung mit einer DB-Instance, die eine bestimmte DB-Engine ausführt

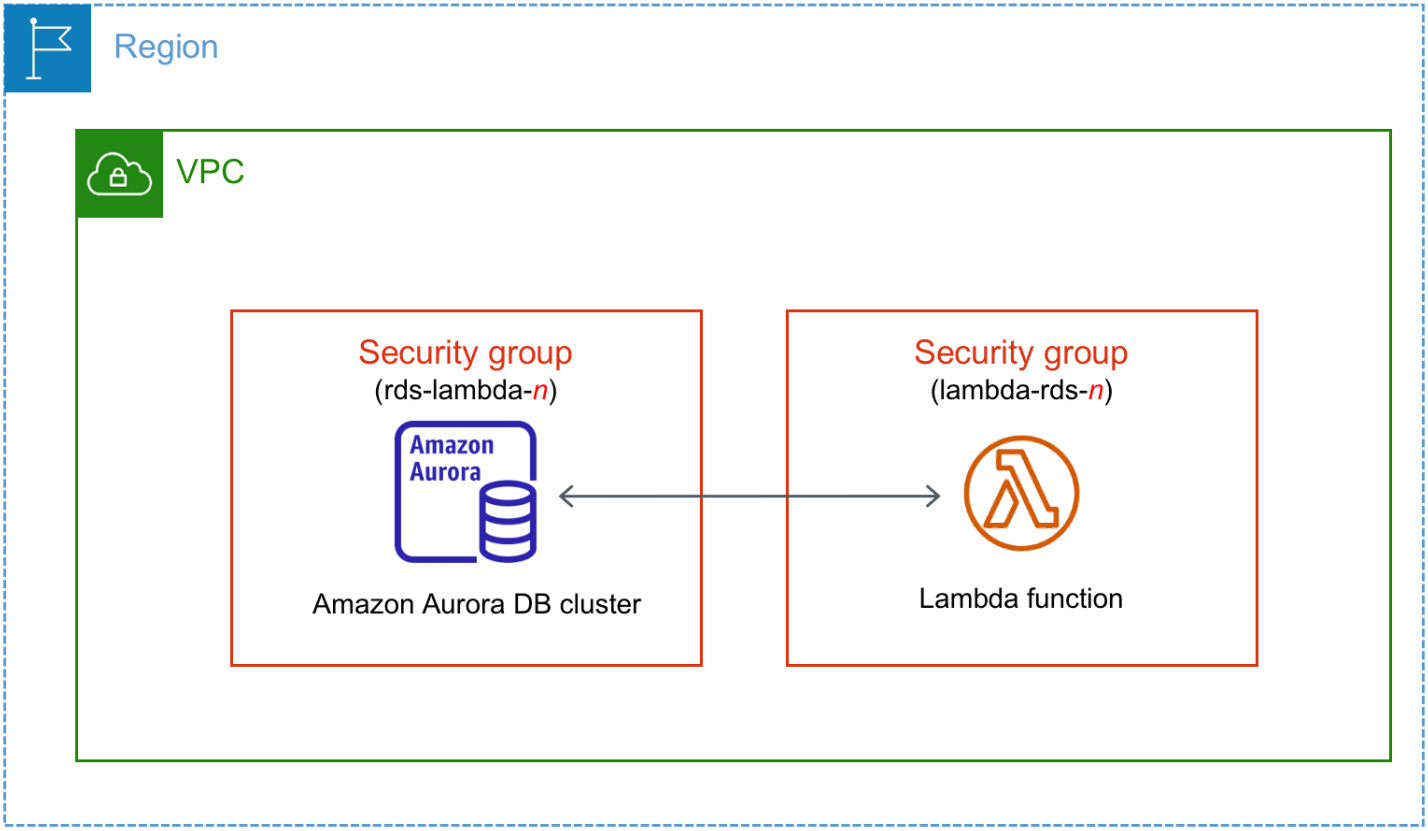
Informationen zum Herstellen einer Verbindung mit einer DB-Instance, die eine bestimmte DB-Engine ausführt, finden Sie in den Anweisungen für Ihre DB-Engine:

- Herstellen einer Verbindung mit einem Amazon Aurora MySQL-DB-Cluster
- Herstellen einer Verbindung mit einem Amazon-Aurora-PostgreSQL-DB-Cluster

Automatisches Verbinden einer Lambda-Funktion mit einem Aurora-DB-Cluster

Sie können die Amazon-RDS-Konsole verwenden, um das Einrichten einer Verbindung zwischen einer Lambda-Funktion und einer DB-Instance zu vereinfachen. Häufig befindet sich Ihr DB-Cluster in einem privaten Subnetz innerhalb einer VPC. Die Lambda-Funktion kann von Anwendungen verwendet werden, um auf Ihren privaten DB-Cluster zuzugreifen.

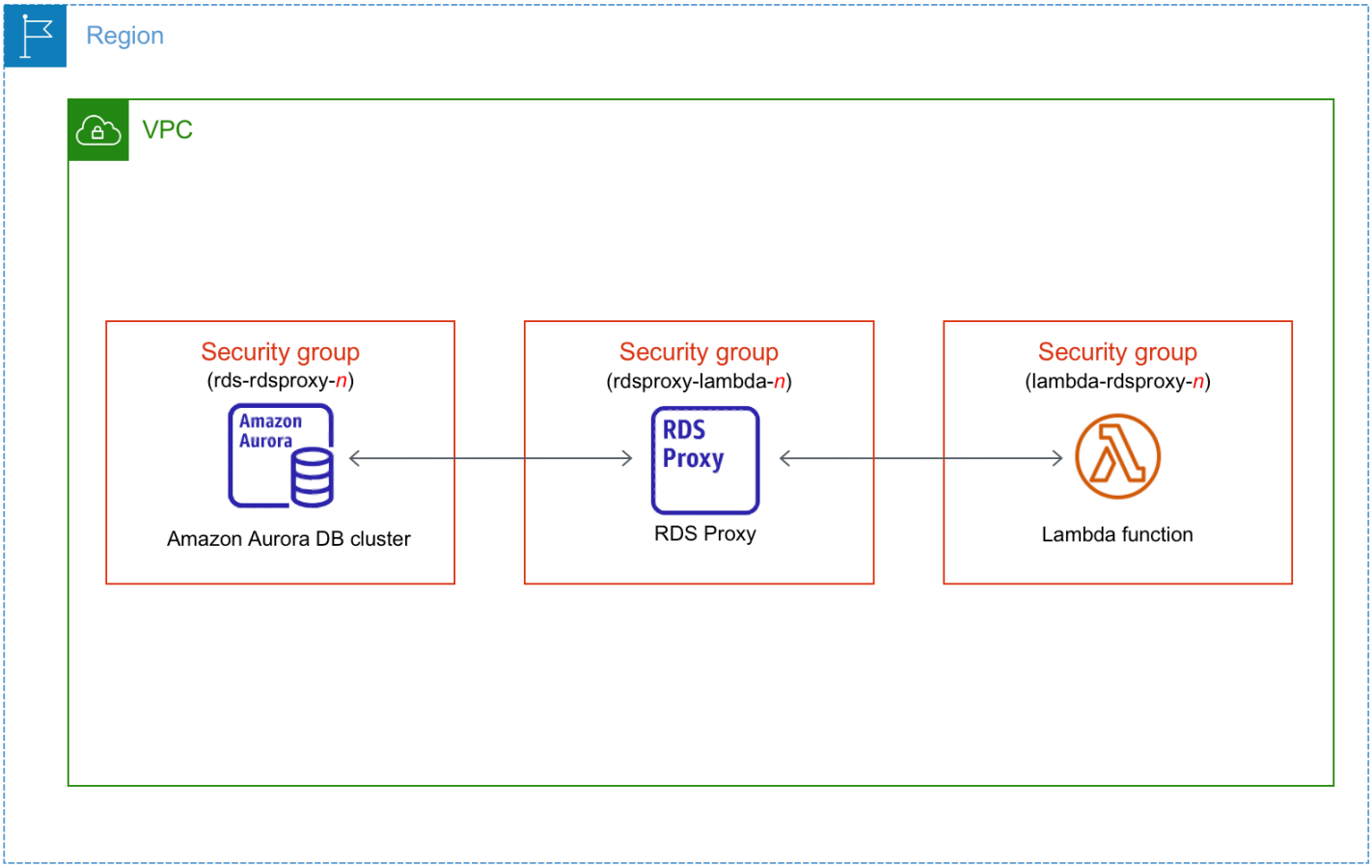
Das folgende Bild zeigt eine direkte Verbindung zwischen Ihrem DB-Cluster und Ihrer Lambda-Funktion.



Sie können die Verbindung zwischen Ihrer Lambda-Funktion und Ihrem DB-Cluster über RDS-Proxy einrichten, um die Leistung und Stabilität Ihrer Datenbank zu verbessern. Oft stellen Lambda-Funktionen häufige, kurze Datenbankverbindungen her, die von dem von RDS Proxy angebotenen Verbindungspooling profitieren. Sie können alle AWS Identity and Access Management (IAM)-Authentifizierungen nutzen, die Sie bereits für Lambda-Funktionen haben, anstatt Datenbankanmeldeinformationen im Lambda-Anwendungscode zu verwalten. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

Wenn Sie die Konsole verwenden, um eine Verbindung mit einem vorhandenen Proxy herzustellen, aktualisiert Amazon RDS die Proxy-Sicherheitsgruppe, um Verbindungen von Ihrem DB-Cluster und der Lambda-Funktion zuzulassen.

Sie können auf dieser Konsolenseite auch einen neuen Proxy erstellen. Wenn Sie in der Konsole einen Proxy erstellen, um auf den DB-Cluster zuzugreifen, müssen Sie Ihre Datenbankanmeldeinformationen eingeben oder ein Secret von AWS Secrets Manager auswählen.



Themen

- Überblick über die automatische Konnektivität mit einer Lambda-Funktion
- Automatisches Verbinden einer Lambda-Funktion und eines Aurora-DB-Clusters
- Anzeigen verbundener Rechenressourcen

Überblick über die automatische Konnektivität mit einer Lambda-Funktion

Im Folgenden sind Anforderungen für die Verbindung einer Lambda-Funktion mit einem Aurora-DB-Cluster aufgeführt:

- Die Lambda-Funktion muss sich in derselben VPC befinden wie der DB-Cluster.
- Derzeit kann der DB-Cluster kein DB-Cluster von Aurora Serverless oder Teil einer globalen Aurora-Datenbank sein.
- Der Benutzer, der die Verbindung einrichtet, muss über Berechtigungen zum Ausführen der folgenden Vorgänge von Amazon RDS, Amazon EC2, Lambda, Secrets Manager und IAM verfügen:

- Amazon RDS
  - `rds:CreateDBProxies`
  - `rds:DescribeDBClusters`
  - `rds:DescribeDBProxies`
  - `rds:ModifyDBCluster`
  - `rds:ModifyDBProxy`
  - `rds:RegisterProxyTargets`
- Amazon EC2
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateSecurityGroup`
  - `ec2:DeleteSecurityGroup`
  - `ec2:DescribeSecurityGroups`
  - `ec2:RevokeSecurityGroupEgress`
  - `ec2:RevokeSecurityGroupIngress`
- Lambda
  - `lambda:CreateFunctions`
  - `lambda:ListFunctions`
  - `lambda:UpdateFunctionConfiguration`
- Secrets Manager
  - `secretsmanager:CreateSecret`
  - `secretsmanager:DescribeSecret`
- IAM
  - `iam:AttachPolicy`
  - `iam:CreateRole`
  - `iam:CreatePolicy`
- AWS KMS
  - `kms:describeKey`

> **Note**
>
> Wenn sich der DB-Cluster und die Lambda-Funktion in unterschiedlichen Availability Zones befinden, fallen auf Ihrem Konto ggf. Kosten über Availability Zones hinweg an.

Wenn Sie eine Verbindung zwischen einer Lambda-Funktion und einem Aurora-DB-Cluster einrichten, konfiguriert Amazon RDS die VPC-Sicherheitsgruppe für Ihre Funktion und für Ihren DB-Cluster automatisch. Wenn Sie RDS-Proxy verwenden, konfiguriert Amazon RDS auch die VPC-Sicherheitsgruppe für den Proxy. Amazon RDS handelt gemäß der aktuellen Konfiguration der Sicherheitsgruppen, die dem DB-Cluster, der Lambda-Funktion und dem Proxy zugeordnet sind, wie in der folgenden Tabelle beschrieben.

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Es gibt eine oder mehrere Sicherheitsgruppen, die dem DB-Cluster mit einem Namen zugeordnet sind, der dem Muster `rds-lambda-` *n* entspricht. Wenn bereits ein Proxy mit Ihrem DB-Cluster verbunden ist, prüft RDS, ob `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. Eine Sicherheitsgruppe, die dem Muster entspricht,	Der Lambda-Funktion sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `lambda-rds-` *n* oder `lambda-rdsproxy-` *n* entspricht (wobei *n* für eine Zahl steht). Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe hat nur eine Regel für ausgehenden Datenverkehr,	Dem Proxy sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rdsproxy-lambda-` *n* entspricht (wobei *n* für eine Zahl steht). Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe verfügt über Regeln für ein- und ausgehenden Datenverkehr mit den VPC-Sicherheitsgru	Amazon RDS führt keine Aktion aus. Es wurde bereits automatisch eine Verbindung zwischen der Lambda-Funktion, dem Proxy (optional) und dem DB-Cluster konfiguriert. Da bereits eine Verbindung zwischen der Funktion, dem Proxy und der Datenbank besteht, werden die Sicherheitsgruppen nicht geändert.

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der Lambda-Funktion oder dem Proxy als Quelle.	wobei entweder die VPC-Sicherheitsgruppe des DB-Clusters oder der Proxy das Ziel ist.	ppen der Lambda-Funktion und des DB-Clusters.	

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Es gilt eine der folgenden Bedingungen: • Dem DB-Cluster ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `rds-lambda-` *n* entspricht, oder wenn `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. • Eine oder mehrere Sicherheitsgruppen sind dem DB-Cluster zugeordnet, deren Name dem Muster `rds-lambda-` *n* entspricht, oder wenn `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. Keine dieser Sicherheitsgruppen kann jedoch für die Verbindung mit der	Es gilt eine der folgenden Bedingungen: • Der Lambda-Funktion ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `lambda-rds-` *n* oder `lambda-rdsproxy-` *n* entspricht. • Der Lambda-Funktion sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `lambda-rds-` *n* oder `lambda-rdsproxy-` *n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit dem DB-Cluster verwenden.	Es gilt eine der folgenden Bedingungen: • Dem Proxy ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `rdsproxy-lambda-` *n* entspricht. • Dem Proxy sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rdsproxy-lambda-` *n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit dem DB-Cluster oder der Lambda-Funktion verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn	RDS action: create new security groups

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Lambda-Funktion verwendet werden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn sie keine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der Lambda-Funktion oder dem Proxy als Quelle enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde. Beispiele für Änderungen sind das Hinzufügen einer Regel oder das Ändern des Ports einer vorhandenen Regel.	Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn diese keine Regel für ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters als Ziel enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	diese keine Regel für ein- und ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters oder der Lambda-Funktion enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Eine oder mehrere Sicherheitsgruppen sind dem DB-Cluster zugeordnet, deren Name dem Muster `rds-lambda-` *n* entspricht, oder wenn `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der Lambda-Funktion oder dem Proxy als Quelle.	Der Lambda-Funktion sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `lambda-rds-` *n* oder `lambda-rdsproxy-` *n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit dem DB-Cluster verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn diese keine Regel für ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters als Ziel enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	Dem Proxy sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rdsproxy-lambda-` *n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit dem DB-Cluster oder der Lambda-Funktion verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn diese keine Regel für ein- und ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters oder der Lambda-Funktion enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	RDS action: create new security groups

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Eine oder mehrere Sicherheitsgruppen sind dem DB-Cluster zugeordnet, deren Name dem Muster `rds-lambda-` *n* entspricht, oder wenn `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der Lambda-Funktion oder dem Proxy als Quelle.	Eine gültige Lambda-Sicherheitsgruppe für die Verbindung ist vorhanden, jedoch nicht mit der Lambda-Funktion verknüpft. Die Sicherheitsgruppe hat einen Namen, der dem Muster `lambda-rds-` *n* oder `lambda-rdsproxy-` *n* entspricht. Sie wurde nicht geändert. Sie hat nur eine Regel für ausgehenden Datenverkehr, wobei die VPC-Sicherheitsgruppe des DB-Clusters oder der Proxy das Ziel ist.	Eine gültige Proxy-Sicherheitsgruppe für die Verbindung ist vorhanden, jedoch nicht mit dem Proxy verknüpft. Die Sicherheitsgruppe trägt einen Namen, der dem Muster `rdsproxy-lambda-` *n* entspricht. Sie wurde nicht geändert. Sie verfügt über Regeln für ein- und ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters und der Lambda-Funktion.	RDS action: associate Lambda security group

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Es gilt eine der folgenden Bedingungen: • Dem DB-Cluster ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `rds-lambda-` *n* entspricht, oder wenn `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. • Eine oder mehrere Sicherheitsgruppen sind dem DB-Cluster zugeordnet, deren Name dem Muster `rds-lambda-` *n* entspricht, oder wenn `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit der Lambda-	Der Lambda-Funktion sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `lambda-rds-` *n* oder `lambda-rdsproxy-` *n* entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe enthält nur eine Regel für ausgehenden Datenverkehr, wobei entweder die VPC-Sicherheitsgruppe des DB-Clusters oder der Proxy das Ziel ist.	Dem Proxy sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rdsproxy-lambda-` *n* entspricht. Eine Sicherheitsgruppe, die dem Muster entspricht, wurde nicht geändert. Diese Sicherheitsgruppe verfügt über Regeln für ein- und ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters und der Lambda-Funktion.	RDS action: create new security groups

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Funktion oder dem Proxy verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn sie keine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der Lambda-Funktion oder dem Proxy als Quelle enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.			

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Es gilt eine der folgenden Bedingungen: • Dem DB-Cluster ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `rds-lambda-` *n* entspricht, oder wenn `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. • Eine oder mehrere Sicherheitsgruppen sind dem DB-Cluster zugeordnet, deren Name dem Muster `rds-lambda-` *n* entspricht, oder wenn `TargetHealth` eines zugehörigen Proxys `AVAILABLE` ist. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit der Lambda-	Es gilt eine der folgenden Bedingungen: • Der Lambda-Funktion ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `lambda-rds-` *n* oder `lambda-rdsproxy-` *n* entspricht. • Der Lambda-Funktion sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `lambda-rds-` *n* oder `lambda-rdsproxy-` *n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit dem DB-Cluster verwenden.	Es gilt eine der folgenden Bedingungen: • Dem Proxy ist keine Sicherheitsgruppe zugeordnet, deren Name dem Muster `rdsproxy-lambda-` *n* entspricht. • Dem Proxy sind eine oder mehrere Sicherheitsgruppen zugeordnet, deren Name dem Muster `rdsproxy-lambda-` *n* entspricht. Amazon RDS kann jedoch keine dieser Sicherheitsgruppen für die Verbindung mit dem DB-Cluster oder der Lambda-Funktion verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn	RDS action: create new security groups

Aktuelle RDS-Sicherheitsgruppenkonfiguration	Aktuelle Konfiguration der Lambda-Sicherheitsgruppe	Aktuelle Konfiguration der Proxy-Sicherheitsgruppe	RDS-Aktion
Funktion oder dem Proxy verwenden. Amazon RDS kann eine Sicherheitsgruppe nicht verwenden, wenn sie keine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der Lambda-Funktion oder dem Proxy als Quelle enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	Eine Sicherheitsgruppe kann nicht verwendet werden, wenn sie keine Regel für ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters oder dem Proxy als Quelle enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	diese keine Regel für ein- und ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters oder der Lambda-Funktion enthält. Amazon RDS kann auch keine Sicherheitsgruppe verwenden, die geändert wurde.	

RDS-Aktion : neue Sicherheitsgruppen erstellen

Amazon RDS führt die folgenden Aktionen durch:

- Erstellt eine neue Sicherheitsgruppe, die dem Muster `rds-lambda-`*n* oder `rds-rdsproxy-`*n* entspricht (wenn Sie RDS Proxy verwenden). Diese Sicherheitsgruppe enthält eine Regel für eingehenden Datenverkehr mit der VPC-Sicherheitsgruppe der Lambda-Funktion oder dem Proxy als Quelle. Diese Sicherheitsgruppe ist dem DB-Cluster zugeordnet und ermöglicht der Funktion oder dem Proxy den Zugriff auf den DB-Cluster.
- Erstellt eine neue Sicherheitsgruppe, die dem Muster `lambda-rds-`*n* oder `lambda-rdsproxy-`*n* entspricht. Diese Sicherheitsgruppe enthält eine Regel für ausgehenden Datenverkehr, wobei entweder die VPC-Sicherheitsgruppe des DB-Clusters oder der Proxy das

Ziel ist. Diese Sicherheitsgruppe ist der Lambda-Funktion zugeordnet und ermöglicht es der Funktion, Datenverkehr an den DB-Cluster zu senden oder Datenverkehr über einen Proxy zu senden.

- Erstellt eine neue Sicherheitsgruppe, die dem Muster `rdsproxy-lambda-`*n* entspricht. Diese Sicherheitsgruppe verfügt über Regeln für ein- und ausgehenden Datenverkehr mit der VPC-Sicherheitsgruppe des DB-Clusters und der Lambda-Funktion.

RDS-Aktion : Lambda-Sicherheitsgruppe zuordnen

Amazon RDS ordnet die gültige, vorhandene Lambda-Sicherheitsgruppe der Lambda-Funktion zu. Diese Sicherheitsgruppe ermöglicht es der Funktion, Datenverkehr an den DB-Cluster zu senden oder Datenverkehr über einen Proxy zu senden.

Automatisches Verbinden einer Lambda-Funktion und eines Aurora-DB-Clusters

Sie können die Amazon-RDS-Konsole verwenden, um eine Lambda-Funktion automatisch mit Ihrem DB-Cluster zu verbinden. Dies vereinfacht das Einrichten einer Verbindung zwischen diesen Ressourcen.

Sie können den RDS-Proxy auch verwenden, um einen Proxy in Ihre Verbindung aufzunehmen. Lambda-Funktionen stellen häufige, kurze Datenbankverbindungen her, die von dem von RDS Proxy angebotenen Verbindungspooling profitieren. Sie können auch eine IAM-Authentifizierung nutzen, die Sie bereits für Lambda-Funktionen eingerichtet haben, anstatt Datenbankanmeldeinformationen im Lambda-Anwendungscode zu verwalten.

Sie können einen vorhandenen DB-Cluster mit neuen oder bestehenden Lambda-Funktionen unter Verwendung der Seite Lambda-Verbindung einrichtenverbinden. Beim Einrichtungsvorgang werden automatisch die erforderlichen Sicherheitsgruppen für Sie eingerichtet.

Vor dem Einrichten einer Verbindung zwischen einer Lambda-Funktion und einem DB-Cluster stellen Sie Folgendes sicher:

- Ihre Lambda-Funktion und Ihr DB-Cluster befinden sich in derselben VPC.
- Sie verfügen über die richtigen Berechtigungen für Ihr Benutzerkonto. Weitere Informationen zu den Anforderungen finden Sie unter Überblick über die automatische Konnektivität mit einer Lambda-Funktion.

Wenn Sie Sicherheitsgruppen nach dem Konfigurieren der Verbindung ändern, können sich die Änderungen auf die Verbindung zwischen der Lambda-Funktion und dem DB-Cluster auswirken.

> **Note**
>
> Sie können eine Verbindung zwischen einem DB-Cluster und einer Lambda-Funktion nur in der AWS Management Console automatisch einrichten. Zum Herstellen einer Verbindung mit einer Lambda-Funktion müssen sich alle Instances im DB-Cluster im Status Verfügbar befinden.

So verbinden Sie eine Lambda-Funktion automatisch mit einem DB-Cluster

<result>

Nachdem Sie die Einrichtung bestätigt haben, beginnt Amazon RDS mit dem Herstellen der Verbindung Ihrer Lambda-Funktion, Ihres RDS-Proxys (falls Sie einen Proxy verwendet haben) und Ihres DB-Clusters. Die Konsole zeigt das Dialogfeld Verbindungsdetails an, in dem die Änderungen der Sicherheitsgruppe aufgeführt sind, die Verbindungen zwischen Ihren Ressourcen ermöglichen.
</result>

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken und dann den DB-Cluster zum Verbinden mit einer Lambda-Funktion aus.
3. Wählen Sie für Aktionen die Option Lambda-Verbindung einrichten aus.
4. Führen Sie auf der Seite Lambda-Verbindung einrichten unter Lambda-Funktion auswählen einen der folgenden Schritte aus:
   - Wenn eine Lambda-Funktion in derselben VPC wie Ihr DB-Cluster vorhanden ist, wählen Sie Vorhandene Funktion auswählen aus und wählen Sie dann die Funktion aus.
   - Wenn Sie keine Lambda-Funktion in derselben VPC vorhanden ist, wählen Sie Neue Funktion erstellen aus und geben Sie dann einen Namen im Feld Funktionsname ein. Die Standard-Laufzeit ist auf Nodejs.18 festgelegt. Sie können die Einstellungen für Ihre neue Lambda-Funktion in der Lambda-Konsole ändern, nachdem Sie die Verbindungseinrichtung abgeschlossen haben.

5. (Optional) Wählen Sie unter RDS Proxy die Option Über RDS Proxy verbinden aus und führen Sie dann einen der folgenden Schritte aus:
   - Wenn Sie einen vorhandenen Proxy haben, den Sie verwenden möchten, klicken Sie auf Vorhandenen Proxy auswählen und wählen Sie dann den Proxy aus.
   - Wenn Sie keinen Proxy haben und möchten, dass Amazon RDS automatisch einen für Sie erstellt, wählen Sie Neuen Proxy erstellen aus. Führen Sie dann für Datenbankanmeldeinformationen einen der folgenden Schritte aus:

     a. Wählen Sie Datenbankbenutzername und Passwort aus und geben Sie dann den Benutzernamen und das Passwort für Ihren DB-Cluster ein.

     b. Wählen Sie Secrets-Manager-Secret aus. Wählen Sie dann unter Secret auswählen ein Secret von AWS Secrets Manager aus. Wenn Sie kein Secrets-Manager-Secret haben, wählen Sie Neues Secrets-Manager-Secret erstellen aus, um ein neues Secret zu erstellen. Nachdem Sie das Secret erstellt haben, wählen Sie das neue Secret unter Secret auswählen aus.

     Nachdem Sie den neuen Proxy erstellt haben, wählen Sie Vorhandenen Proxy auswählen aus und wählen Sie dann den Proxy aus. Beachten Sie, dass es einige Zeit dauern kann, bis Ihr Proxy für die Verbindung verfügbar ist.
6. (Optional) Erweitern Sie die Verbindungsübersicht und überprüfen Sie die hervorgehobenen Updates für Ihre Ressourcen.
7. Wählen Sie Set up (Festlegen).

Anzeigen verbundener Rechenressourcen

Sie können die AWS Management Console verwenden, um die Lambda-Funktionen anzuzeigen, die mit Ihrem DB-Cluster verbunden sind. Zu den angezeigten Ressourcen gehören Rechenressourcenverbindungen, die von Amazon RDS automatisch eingerichtet wurden.

Die aufgelisteten Rechenressourcen umfassen keine Ressourcen, die manuell mit dem DB-Cluster verbunden sind. Sie können beispielsweise einer Rechenressource den manuellen Zugriff auf Ihren DB-Cluster erlauben, indem Sie der VPC-Sicherheitsgruppe, die der Datenbank zugeordnet ist, eine Regel hinzufügen.

Damit die Konsole eine Lambda-Funktion auflistet, müssen die folgenden Bedingungen gelten:

- Der Name der Sicherheitsgruppe, die der Rechenressource zugeordnet ist, entspricht dem Muster `lambda-rds-`*n* oder `lambda-rdsproxy-`*n* (wobei *n* für eine Zahl steht).
- Die Sicherheitsgruppe, die der Rechenressource zugeordnet ist, hat eine Regel für ausgehenden Datenverkehr, wobei der Portbereich auf den Port des DB-Clusters oder einen zugeordneten Proxy festgelegt ist. Das Ziel für die Regel für ausgehende Nachrichten muss auf eine dem DB-Cluster zugeordneten Sicherheitsgruppe oder auf einen zugeordneten Proxy festgelegt werden.
- Wenn die Konfiguration einen Proxy enthält, entspricht der Name der Sicherheitsgruppe, die an den mit Ihrer Datenbank verknüpften Proxy angefügt ist, dem Muster `rdsproxy-lambda-`*n* (wobei *n* für eine Zahl steht).
- Die Sicherheitsgruppe, die der Funktion zugeordnet ist, hat eine Regel für ausgehenden Datenverkehr, wobei der Port auf den Port festgelegt ist, den der DB-Cluster oder ein zugeordneter Proxy verwendet. Das Ziel muss auf eine dem DB-Cluster zugeordneten Sicherheitsgruppe oder auf einen zugeordneten Proxy festgelegt werden.

So zeigen Sie Rechenressourcen an, die automatisch mit einem DB-Cluster verbunden sind

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken und dann den DB-Cluster aus.
3. Sehen Sie sich auf der Registerkarte Konnektivität und Sicherheit die Rechenressourcen unter Verbundene Rechenressourcen an.

Ändern eines Amazon Aurora-DB-Clusters

Sie können die Einstellungen eines DB-Clusters ändern, um Aufgaben durchzuführen, beispielsweise das Ändern des Aufbewahrungszeitraums für Backups oder des Datenbankports. Außerdem können Sie DB-Instances in einem DB-Cluster ändern, um Aufgaben durchzuführen, beispielsweise das Ändern der DB-Instance-Klasse oder das Aktivieren von Performance-Insights für diese. Dieses Thema führt Sie durch die Schritte zum Ändern eines Aurora-DB-Instance-Clusters und seiner DB-Instances und beschreibt die jeweiligen Einstellungen.

Wir empfehlen, alle Änderungen auf einem Test-DB-Cluster oder einer Test-DB-Instance zu testen, bevor Sie einen Produktions-DB-Cluster oder eine Produktions-DB-Instance ändern, damit Sie die Auswirkungen jeder Änderung detailliert nachvollziehen können. Dies ist besonders bei Upgrades der Datenbankversionen wichtig.

Themen

Ändern des DB-Clusters über die Konsole, die CLI und die API

Sie können einen DB-Cluster mithilfe der AWS Management Console AWS CLI, der oder der RDS-API ändern.

> **Note**
>
> Die meisten Änderungen können sofort oder während des nächsten Wartungszeitraums angewendet werden. Einige Änderungen, z. B. das Aktivieren des Löschschutzes, werden sofort umgesetzt – unabhängig davon, wann Sie sie anwenden.
> Das Ändern des Master-Passworts in der AWS Management Console wird immer sofort übernommen. Wenn Sie jedoch die AWS CLI oder die RDS-API verwenden, können Sie wählen, ob Sie diese Änderung sofort oder während des nächsten geplanten Wartungsfensters anwenden möchten.

Wenn Sie SSL-Endpunkte verwenden und die DB-Cluster-ID ändern, beenden Sie den DB-Cluster und starten Sie ihn neu, um die SSL-Endpunkte zu aktualisieren. Weitere Informationen finden Sie unter Stoppen und Starten eines Amazon Aurora-DB-Clusters.

Konsole

So ändern Sie einen DB-Cluster:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann den zu ändernden DB-Cluster aus.
3. Wählen Sie Ändern aus. Die Seite DB-Cluster ändern wird angezeigt.
4. Ändern Sie alle Einstellungen nach Bedarf. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Amazon Aurora.

   > **Note**
   >
   > In der AWS Management Console gelten einige Änderungen auf Instance-Ebene nur für die aktuelle DB-Instance, während andere für den gesamten DB-Cluster gelten. Informationen dazu, wann eine Einstellung auf die DB-Instance oder das DB-Cluster angewendet wird, finden Sie im Abschnitt zum Geltungsbereich der Einstellung in Einstellungen für Amazon Aurora. Um eine Einstellung zu ändern, die den gesamten DB-Cluster auf Instanzebene in ändert AWS Management Console, folgen Sie den Anweisungen unter. Ändern einer DB-Instance in einem DB-Cluster

5. Nachdem Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.
6. Klicken Sie auf Apply immediately, um die Änderungen sofort anzuwenden.
7. Überprüfen Sie auf der Bestätigungsseite Ihre Änderungen. Wenn sie korrekt sind, wählen Sie Modify cluster (Cluster ändern) aus, um Ihre Änderungen zu speichern.

   Klicken Sie anderenfalls auf Zurück, um Ihre Änderungen zu bearbeiten, oder klicken Sie auf Abbrechen, um Ihre Änderungen zu verwerfen.

AWS CLI

Um einen DB-Cluster mit dem zu ändern AWS CLI, rufen Sie den Befehl modify-db-cluster auf. Geben Sie die DB-Cluster-Kennung und die Werte für die Einstellungen an, die geändert werden sollen. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Amazon Aurora.

> **Note**
>
> Einige Einstellungen werden nur auf DB-Instances angewendet. Um diese Einstellungen zu ändern, folgen Sie den Anweisungen in Ändern einer DB-Instance in einem DB-Cluster.

Example

Der folgende Befehl ändert `mydbcluster`, indem der Aufbewahrungszeitraum für Backups auf 1 Woche (7 Tage) festgelegt wird.

Für, oder: Linux macOS Unix

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --backup-retention-period 7
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --backup-retention-period 7
```

RDS-API

Um einen DB-Cluster über die Amazon RDS-API zu ändern, rufen Sie die Aktion ModifyDBCluster auf. Geben Sie die DB-Cluster-Kennung und die Werte für die Einstellungen an, die geändert werden sollen. Weitere Informationen zu den einzelnen Parametern finden Sie unter Einstellungen für Amazon Aurora.

> **Note**
>
> Einige Einstellungen werden nur auf DB-Instances angewendet. Um diese Einstellungen zu ändern, folgen Sie den Anweisungen in Ändern einer DB-Instance in einem DB-Cluster.

Ändern einer DB-Instance in einem DB-Cluster

Sie können eine DB-Instance in einem DB-Cluster mithilfe der AWS Management Console AWS CLI, der oder der RDS-API ändern.

Wenn Sie eine DB-Instance ändern, können Sie die Änderungen sofort anwenden. Um Änderungen sofort anzuwenden, wählen Sie die Option Sofort anwenden in AWS Management Console, Sie verwenden den `--apply-immediately` Parameter beim Aufrufen von AWS CLI, oder Sie setzen den `ApplyImmediately` Parameter auf, `true` wenn Sie die Amazon RDS-API verwenden.

Wenn Sie sich nicht dafür entscheiden, Änderungen sofort anzuwenden, werden die Änderungen auf das nächste Wartungsfenster verschoben. Während des nächsten Wartungsfensters werden alle diese verzögerten Änderungen angewendet. Wenn Sie Änderungen sofort anwenden, werden Ihre neuen Änderungen und alle zuvor verzögerten Änderungen angewendet.

Um die Änderungen zu sehen, die für das nächste Wartungsfenster noch ausstehen, verwenden Sie den AWS CLI Befehl describe-db-clusters und überprüfen Sie das Feld. `PendingModifiedValues`

> **Important**
>
> Wenn ausstehende Änderungen eine Ausfallzeit erfordern, kann die Auswahl von Apply immediately einen unerwarteten Ausfall für die DB-Instance verursachen. Es gibt keine Ausfallzeiten für die anderen DB-Instances im DB-Cluster.
> Änderungen, die Sie verschieben, sind in der Ausgabe des `describe-pending-maintenance-actions`-CLI-Befehls nicht aufgeführt. Wartungsmaßnahmen umfassen nur System-Upgrades, die Sie für das nächste Wartungsfenster planen.

Konsole

So ändern Sie eine DB-Instance in einem DB-Cluster:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die zu ändernde DB-Instance aus.
3. Wählen Sie für Actions (Aktionen) die Option Modify (Ändern) aus. Die Seite DB-Instance ändern wird angezeigt.
4. Ändern Sie alle Einstellungen nach Bedarf. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Amazon Aurora.

   > **Note**
   >
   > Einige Einstellungen gelten für das gesamte DB-Cluster und müssen auf Cluster-Ebene geändert werden. Um diese Einstellungen zu ändern, folgen Sie den Anweisungen in Ändern des DB-Clusters über die Konsole, die CLI und die API.
   > In der AWS Management Console gelten einige Änderungen auf Instance-Ebene nur für die aktuelle DB-Instance, während andere für den gesamten DB-Cluster gelten. Informationen dazu, wann eine Einstellung auf die DB-Instance oder das DB-Cluster angewendet wird, finden Sie im Abschnitt zum Geltungsbereich der Einstellung in Einstellungen für Amazon Aurora.
5. Nachdem Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.
6. Klicken Sie auf Apply immediately, um die Änderungen sofort anzuwenden.
7. Überprüfen Sie auf der Bestätigungsseite Ihre Änderungen. Wenn sie korrekt sind, wählen Sie Modify DB Instance (DB-Instance ändern) aus, um Ihre Änderungen zu speichern.

   Klicken Sie anderenfalls auf Zurück, um Ihre Änderungen zu bearbeiten, oder klicken Sie auf Abbrechen, um Ihre Änderungen zu verwerfen.

AWS CLI

Um eine DB-Instance in einem DB-Cluster mithilfe von zu ändern AWS CLI, rufen Sie den Befehl modify-db-instance auf. Geben Sie die DB-Instance-Kennung und die Werte für die Einstellungen an,

die geändert werden sollen. Weitere Informationen zu den einzelnen Parametern finden Sie unter Einstellungen für Amazon Aurora.

> **Note**
>
> Einige Einstellungen werden auf das gesamte DB-Cluster angewendet. Um diese Einstellungen zu ändern, folgen Sie den Anweisungen in Ändern des DB-Clusters über die Konsole, die CLI und die API.

Example

Der folgende Code ändert `mydbinstance`, indem die Klasse der DB-Instance in `db.r4.xlarge` geändert wird. Die Änderungen werden während des nächsten Wartungsfensters (mit) übernomme `--no-apply-immediately`. Verwenden Sie `--apply-immediately`, damit Änderungen sofort angewendet werden.

Für, oder: Linux macOS Unix

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --db-instance-class db.r4.xlarge \
    --no-apply-immediately
```

Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --db-instance-class db.r4.xlarge ^
    --no-apply-immediately
```

RDS-API

Rufen Sie die Operation ModifyDBInstance auf, um eine DB-Instance mithilfe der Amazon RDS-API zu ändern. Geben Sie die DB-Instance-Kennung und die Werte für die Einstellungen an, die geändert werden sollen. Weitere Informationen zu den einzelnen Parametern finden Sie unter Einstellungen für Amazon Aurora.

> **Note**
>
> Einige Einstellungen werden auf das gesamte DB-Cluster angewendet. Um diese Einstellungen zu ändern, folgen Sie den Anweisungen in Ändern des DB-Clusters über die Konsole, die CLI und die API.

Das Passwort für den Datenbank-Masterbenutzer ändern

Sie können das AWS Management Console oder das verwenden AWS CLI , um das Masterbenutzerpasswort zu ändern.

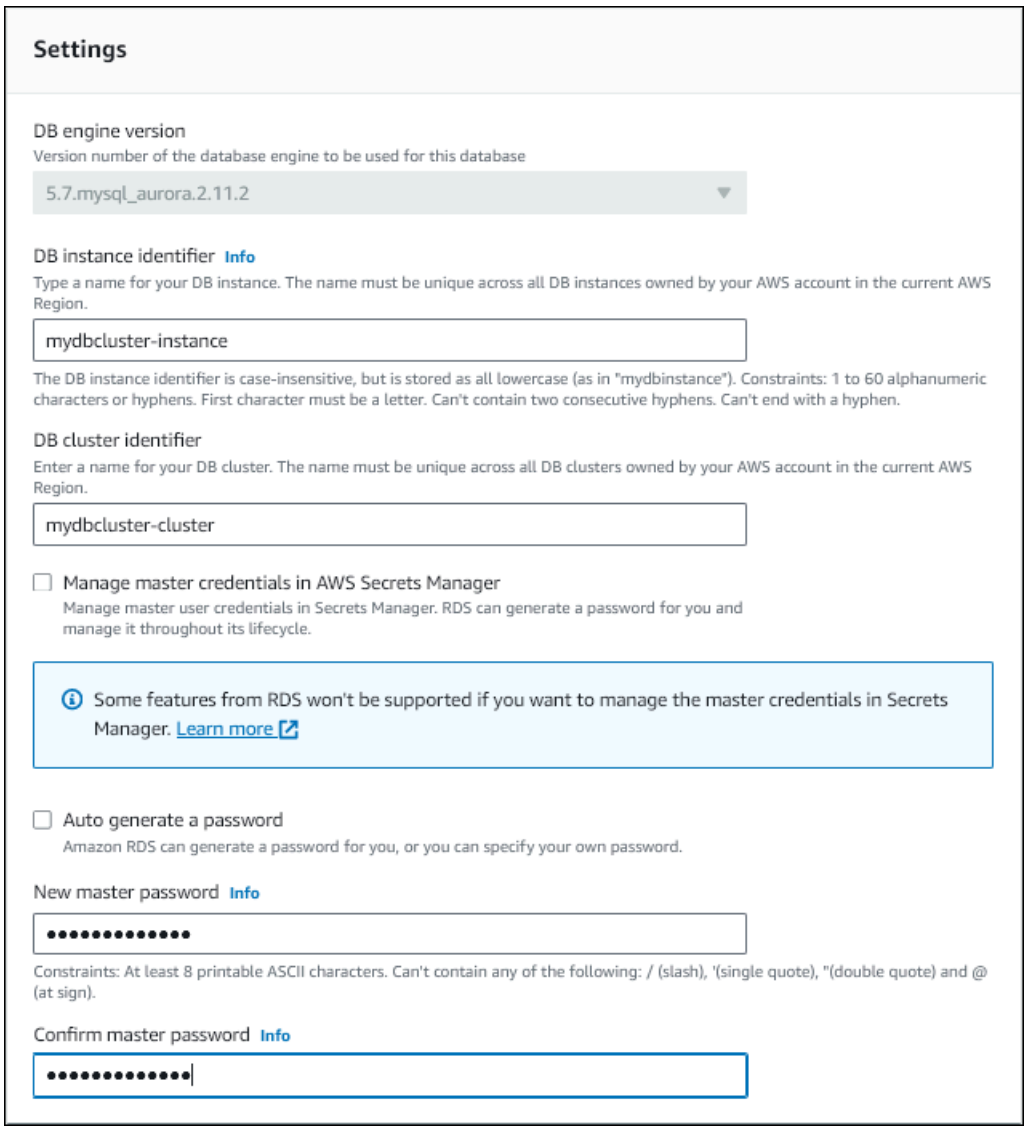
Konsole

Sie ändern die Writer-DB-Instance, um das Masterbenutzerkennwort zu ändern, indem Sie den verwenden AWS Management Console.

Um das Masterbenutzer-Passwort zu ändern

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die zu ändernde DB-Instance aus.
3. Wählen Sie für Actions (Aktionen) die Option Modify (Ändern) aus.

   Die Seite DB-Instance ändern wird angezeigt.
4. Geben Sie ein neues Master-Passwort ein.
5. Geben Sie unter Master-Passwort bestätigen dasselbe neue Passwort ein.



6. Klicken Sie auf Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.

> **Note**
>
> Passwortänderungen werden immer sofort übernommen.

7. Klicken Sie auf der Bestätigungsseite auf Modify DB instance (DB-Instance ändern).

CLI

Sie rufen den Befehl modify-db-cluster auf, um das Masterbenutzerkennwort mit dem zu ändern. AWS CLI Geben Sie die DB-Cluster-ID und das neue Passwort an, wie in den folgenden Beispielen gezeigt.

Sie müssen dies nicht angeben`--apply-immediately|--no-apply-immediately`, da Kennwortänderungen immer sofort übernommen werden.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --master-user-password mynewpassword
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --master-user-password mynewpassword
```

Einstellungen für Amazon Aurora

Die folgende Tabelle enthält Details dazu, welche Einstellungen Sie ändern können, zu den Methoden, mit denen Einstellungen geändert werden, und zum Geltungsbereich der jeweiligen Einstellungen. Der Geltungsumfang legt fest, ob die Einstellung auf den gesamten DB-Cluster angewendet wird oder nur für spezifische DB-Instances festgelegt werden kann.

> **Note**
>
> Wenn Sie einen DB-Cluster von Aurora Serverless v1 oder Aurora Serverless v2 bearbeiten, stehen zusätzliche Einstellungen zur Verfügung. Weitere Informationen zu diesen Einstellungen finden Sie unter Ändern eines Aurora Serverless v1-DB-Clusters und Verwaltung von Aurora Serverless v2 DB-Clustern.
> Außerdem sind einige Einstellungen für Aurora Serverless v1 und Aurora Serverless v2 aufgrund ihrer Einschränkungen nicht verfügbar. Weitere Informationen finden Sie unter Einschränkungen von Aurora Serverless v1 und Anforderungen und Einschränkungen für Aurora Serverless v2.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Automatischer kleiner Version-Upgrade Ob Sie möchten, dass die DB-Instance automatisch Upgrades auf bevorzugte Engine-Unterversionen erhält, wenn sie verfügbar werden. Upgrades werden nur während Ihres geplanten Wartungsfensters installiert. Weitere Informationen über Engine-Updates für finden Sie unter Amazon Aurora PostgreSQL-Aktualisierungen und Datenbank-Engine-Updates für Amazon Aurora MySQL. Weitere Informationen zur Einstellung für automatische Nebenversions-Upgrades für Aurora MySQL finden Sie unter Aktivieren von automatischen Upgrades zwischen	Note Diese Einstellung ist standardmäßig aktiviert. Wählen Sie für jeden neuen Cluster den entsprechenden Wert für diese Einstellung basierend auf der Wichtigkeit, der erwarteten Lebensdauer und dem Umfang der Verifizierungstests, die Sie nach jedem Upgrade durchführen. Wenn Sie diese Einstellung ändern, führen Sie diese Änderung für jede DB-Instance in Ihrem	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall. Wenn Aurora automatische Upgrades durchführt, treten bei zukünftigen Wartungsfenstern Ausfälle auf.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Aurora MySQL-Nebenversionen.	Aurora-Cluster durch. Wenn für eine DB-Instance in Ihrem Cluster diese Einstellung deaktiviert ist, wird der Cluster nicht automatisch aktualisiert. Mit dem AWS Management Console,Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI`--auto-minor-version-upgrade|--no-auto-minor-version-upgrade` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `AutoMinor`		

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
	`VersionUpgrade` fest.		
Aufbewahrungszeitraum für Backups Die Anzahl der Tage, für die automatische Sicherungen aufbewahrt werden. Der Mindestwert ist 1. Weitere Informationen finden Sie unter Backups.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--backup-retention-period` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `BackupRetentionPeriod` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Sicherungsfenster (Startzeit) Der Zeitraum, in dem automatisierte Sicherungen der Datenbank erstellt wird. Das Sicherungsfenster wird mit einer Startzeit (in koordinierter Weltzeit (UTC)) und einer Dauer (in Stunden) angegeben. Aurora Backups sind kontinuierlich und inkrementell. Das Backup-Fenster wird aber verwendet, um eine tägliche Systemsicherung zu erstellen, die innerhalb des Aufbewahrungszeitraums für Backups gespeichert wird. Sie können es kopieren, um es außerhalb des Aufbewahrungszeitraums zu behalten. Das Wartungsfenster und das Sicherungsfenster für den DB-	Mit dem AWS Management Console,Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI`--preferred-backup-window` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `PreferredBackupWindow` fest.	Gesamter DB-Cluster.	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Cluster können sich nicht überschneiden. Weitere Informationen finden Sie unter Backup-Fenster.			
Kapazitätseinstellungen Die Skalierungseigenschaften eines DB-Clusters von Aurora Serverless v1. Sie können die Skalierungseigenschaften für DB-Cluster nur im `serverless` DB-Engine-Modus skalieren. Weitere Informationen zu Aurora Serverless v1 finden Sie unter Verwenden von Amazon Aurora Serverless v1.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--scaling-configuration` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `ScalingConfiguration` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall. Die Änderung wird sofort übernommen. Diese Einstellung ignoriert die Einstellung „Apply Immediately (Sofort Anwenden)“.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Zertifizierungsstelle Die Zertifizierungsstelle (CA) für das Serverzertifikat, das von der DB-Instance verwendet wird.	Mit dem AWS Management Console,Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI`--ca-certificate-identifier` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `CACertificateIdentifier` fest.	Nur die angegebene DB-Instance	Ein Ausfall tritt nur auf, wenn die DB-Engine keine Rotation ohne Neustart unterstützt. Sie können den describe-db-engine-versions AWS CLI Befehl verwenden, um festzustellen, ob die DB-Engine die Rotation ohne Neustart unterstützt.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Cluster-Speicherkonfiguration Der Speichertyp für den DB-Cluster: Aurora I/O-Optimized oder Aurora Standard. Weitere Informationen finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--storage-type` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `StorageType` fest.	Gesamter DB-Cluster	Das Ändern des Speichertyps eines Aurora PostgreSQL-DB-Clusters mit Optimized Reads-Instance-Klassen führt zu einem Ausfall. Dies tritt nicht auf, wenn Speichertypen für Cluster mit anderen Instance-Klassentypen geändert werden. Weitere Informationen zu den DB-Instance-Klassentypen finden Sie unterDB-Instance-Klassenarten.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Tags zu Snapshots kopieren Wählen Sie dies Option, um festzulegen, dass die für diesen DB-Cluster definierten Tags in DB-Snapshots kopiert werden sollen, die von diesem DB-Cluster erstellt wurden. Weitere Informationen finden Sie unter Markieren von Amazon RDS-Ressourcen.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit der AWS CLI `--no-copy-tags-to-snapshot` Option `--copy-tags-to-snapshot` oder die Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `CopyTagsToSnapshot` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Daten-API Sie können Aurora Serverless v1 mit auf Webdienst en basierenden Anwendungen, einschließlich AWS Lambda und, darauf zugreifen. AWS AppSync Diese Einstellung gilt nur für Aurora Serverless v1-DB-Clu ster. Weitere Informati onen finden Sie unter Verwenden der RDS-Daten-API.	Mit dem, AWS Management Console. Ändern des DB-Clusters über die Konsole, die CLI und die API Führen Sie mit dem die AWS CLI `--enable-http-endpoint` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `EnableHttpEndpoint` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Datenbank-Authentifizierung Die Datenbank-Authentifizierung, die Sie verwenden möchten. Für MySQL: • Wählen Sie Passwortauthentifizierung aus, um Datenbankbenutzer ausschließlich mit Datenbankpasswörtern zu authentifizieren. • Wählen Sie Passwort- und IAM-Datenbank-Authentifizierung aus, um Datenbankbenutzer mit Datenbankpasswörtern und Benutzeranmeldeinformationen über IAM-Benutzer und -Rollen zu authentifizieren. Weitere Informationen finden Sie unter IAM-Daten	Mit dem AWS Management Console,Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI folgenden Optionen aus modify-db-clusterund legen Sie sie fest: • Stellen Sie für die IAM-Authentifizierung die `--enable-iam-database-authentication`|`--no-enable-iam-database-authentication` -Option ein. • Für die Kerberos-Authentifizierung stellen Sie die `--domain`- und `--domain-iam-role-name` -Optionen ein.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
bankauthentifizierung. Für PostgreSQL: • Wählen Sie IAM database authentication (IAM-Datenbank-Authentifizierung) aus, um Datenbankbenutzer mit Datenbankpasswörtern und Benutzeranmeldeinformationen über Benutzer und Rollen zu authentifizieren. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung. • Wählen Sie Kerberos-Authentifizierung zur Authentifizierung von Datenbankkennwörtern und Benutzeranmeldeinformationen mit Kerberos-Authentifizierung. Weitere Informationen	Rufen Sie über die RDS-API ModifyDBCluster auf und setzen Sie die folgenden Parameter: • Stellen Sie für die IAM-Authentifizierung den `EnableIAMDatabaseAuthentication` -Parameter ein. • Für die Kerberos-Authentifizierung legen Sie den `Domain`- und `DomainIAMRoleName` -Parameter fest.		

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
finden Sie unter Verwenden der Kerberos-Authentifizierung mit Aurora PostgreSQL.			
Datenbankport Der Port, den Sie für den Zugriff auf das DB-Cluster verwenden möchten.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--port` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `Port` fest.	Gesamter DB-Cluster	Diese Änderung verursacht einen Ausfall. Alle DB-Instances im DB-Cluster werden sofort neu gestartet.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
DB-Cluster-Kennung Die DB-Cluster-ID. Dieser Wert wird als Zeichenfolge in Kleinbuchstaben gespeichert. Wenn Sie die DB-Cluster-ID ändern, werden die DB-Cluster-Endpunkte geändert. Die Endpunkte der DB-Instances im DB-Cluster bleiben unverändert.	Mit dem AWS Management Console,Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI`--new-db-cluster-identifier` Option aus `modify-db-cluster`und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `NewDBClusterIdentifier` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
DB-Cluster-Parametergruppe Die DB-Clusterparametergruppe, die Sie mit dem DB-Cluster verknüpfen möchten. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--db-cluster-parameter-group-name` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `DBClusterParameterGroupName` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall. Wenn Sie die Parametergruppe ändern, werden die Änderungen an einigen Parametern ohne Neustart sofort auf die DB-Instances im DB-Cluster angewendet. Änderungen an anderen Parametern werden erst angewendet, nachdem die DB-Instances im DB-Cluster neu gestartet wurden.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
DB-Instance-Klasse Die zu verwendende DB-Instance-Klasse. Weitere Informationen finden Sie unter Aurora DB-Instance-Klassen.	Mit dem AWS Management Console, Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI `--db-instance-class` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `DBInstanceClass` fest.	Nur die angegebene DB-Instance	Diese Änderung verursacht einen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
DB-Instance-Kennung Die DB-Instance-Kennung. Dieser Wert wird als Zeichenfolge in Kleinbuchstaben gespeichert.	Mit dem AWS Management Console,Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI`--new-db-instance-identifier` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `NewDBInstanceIdentifier` fest.	Nur die angegebene DB-Instance	Während dieser Änderung treten Ausfallzeiten auf. RDS startet die DB-Instance neu, um Folgendes zu aktualisieren: • Aurora MySQL — `SERVER_ID` Spalte in der `information_schema.replica_host_status` Tabelle • Aurora PostgreSQL — `server_id` Spalte in der Funktion `aurora_replica_status()`

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
DB-Parametergruppe Die DB-Parametergruppe, die Sie mit der DB-Instance verknüpfen möchten. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen.	Mit dem, AWS Management Console. Ändern einer DB-Instance in einem DB-Cluster Führen Sie mit dem die AWS CLI `--db-parameter-group-name` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `DBParameterGroupName` fest.	Nur die angegebene DB-Instance	Diese Änderung verursacht keinen Ausfall. Wenn Sie eine neue DB-Parametergruppe mit einer DB-Instance verknüpfen, werden die geänderten statischen und dynamischen Parameter erst nach Neustart der DB-Instance angewendet. Wenn Sie jedoch dynamische Parameter in der DB-Parametergruppe ändern, nachdem Sie sie der DB-Instance zugeordnet haben, werden diese Änderungen sofort ohne Neustart angewendet. Weitere Informationen erhalten Sie unter Arbeiten mit Parametergruppen und Neustart eines Amazon Aurora DB-Clusters oder einer

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
			Amazon Aurora DB-Instance.
Löschschutz Um zu verhindern, dass Ihr DB-Cluster gelöscht wird, können Sie die Option Löschschutz aktivieren aktivieren. Weitere Informationen finden Sie unter Löschschutz für Aurora-DB-Cluster.	Mit dem AWS Management Console,Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI`--deletion-protection|--no-deletion-protection` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `DeletionProtection` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Engine-Version Die Versionsnummer der DB-Engine, die Sie verwenden möchten. Bevor Sie ein Upgrade für Ihr Produktions-DB-Cluster ausführen, sollten Sie den Upgrade-Prozess auf einer DB-Test-Instance testen, um die Dauer zu prüfen und Ihre Anwendungen zu validieren.	Mit dem AWS Management Console,Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI`--engine-version` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `EngineVersion` fest.	Gesamter DB-Cluster	Diese Änderung verursacht einen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
„Enhanced Monitoring“ (Verbesserte Überwachung Wählen Sie Erweiterte Überwachung aktivieren, um Metriken in Echtzeit für das Betriebssystem zu erhalten, in dem Ihre DB-Instance ausgeführt wird. Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).	Mit dem AWS Management Console,Ändern einer DB-Instance in einem DB-Cluster. Verwenden Sie die Optionen AWS CLI, führen Sie die `--monitoring-interval` Optionen `modify-db-instance` und aus `--monitoring-role-arn` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie die Parameter `MonitoringRoleArn` und `MonitoringInterval` fest.	Nur die angegebene DB-Instance	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Protokollexporte Wählen Sie die Protokolltypen aus, die in Amazon CloudWatch Logs veröffentlicht werden sollen. Weitere Informationen finden Sie unter Aurora-MySQL-Datenbank-Protokolldateien.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--cloudwatch-logs-export-configuration` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `CloudwatchLogsExportConfiguration` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Wartungsfenster Der Zeitraum, in dem die Systemwartung durchgeführt wird. Die Systemwartung umfasst auch Upgrades (sofern verfügbar). Das Wartungsfenster wird mit einer Startzeit (in koordinierter Weltzeit (UTC)) und einer Dauer (in Stunden) angegeben. Falls Sie das Fenster auf die aktuelle Zeit einstellen, müssen mindestens 30 Minuten zwischen der aktuellen Zeit und der Endzeit des Fensters liegen, um sicherzustellen, dass alle ausstehenden Änderungen übernommen werden. Sie können die Wartungsfenster für das DB-Cluster und die einzelnen DB-Instances im DB-	Um das Wartungsfenster für den DB-Cluster mithilfe von AWS Management Console, zu ändernÄndern des DB-Clusters über die Konsole, die CLI und die API. Um das Wartungsfenster für eine DB-Instance mit dem AWS Management Console, zu ändernÄndern einer DB-Instance in einem DB-Cluster. Um das Wartungsfenster für den DB-Cluster mithilfe von zu ändern AWS CLI, führen Sie die `--preferred-maintenance-window` Option aus `modify-db-cluster`und legen Sie sie fest. Um das Wartungsfenster für eine DB-Instance mithilfe	Das gesamte DB-Cluster oder eine einzelne DB-Instance	Wenn eine oder mehrere ausstehende Aktionen einen Ausfall verursachen und das Wartungsfenster auf die aktuelle Zeit geändert wird, werden die ausstehenden Aktionen sofort angewendet und es kommt zu einem Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Cluster unabhängig voneinander festlegen. Wenn eine Änderung das gesamte DB-Cluster betrifft, wird die Änderung während des Wartungsfensters für das DB-Cluster ausgeführt. Wenn eine Änderung eine einzelne DB-Instance betrifft, wird die Änderung während des Wartungsfensters für diese DB-Instance ausgeführt. Das Wartungsfenster und das Sicherungsfenster für den DB-Cluster können sich nicht überschneiden. Weitere Informationen finden Sie unter Das Amazon RDS-Wartungsfenster.	von zu ändern AWS CLI, führen Sie die `--preferred-maintenance-window` Option aus `modify-db-instance` und legen Sie sie fest. Bei Änderung des Wartungsfensters für das DB-Cluster über die RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `PreferredMaintenanceWindow` fest. Bei Änderung des Wartungsfensters für eine DB-Instance über die RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `PreferredMaintenanceWindow` fest.		

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Hauptanmeldedaten verwalten in AWS Secrets Manager Wählen Sie Master-Anmeldeinformationen verwalten in AWS Secrets Manager aus, um das Hauptbenutzerpasswort in Secrets Manager geheim zu verwalten. Wählen Sie optional einen KMS-Schlüssel zum Schutz des Secrets aus. Wählen Sie aus den KMS-Schlüsseln in Ihrem Konto oder geben Sie den Schlüssel eines anderen Kontos ein. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager. Wenn Aurora bereits das Hauptbenutzerpasswort für den DB-Cluster verwaltet	Mit dem AWS Management Console,Ändern einer DB-Instance in einem DB-Cluster. Verwenden Sie die Optionen AWS CLI, führen Sie die `--master-user-secret-kms-key-id` Optionen `modify-db-cluster`und aus `--manage-master-user-password | --no-manage-master-user-password` und legen Sie sie fest. Legen Sie die Option `--rotate-master-user-password` fest, um das Hauptbenutzerpasswort sofort zu rotieren. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie die Parameter `ManageMasterUserPa`	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
, können Sie dieses Passwort mit der Option Rotate secret immediately (Sofortige Secret-Drehung) rotieren. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager.	`ssword` und `MasterUserSecretKmsKeyId` fest. Legen Sie den Parameter `RotateMasterUserPassword` auf `true` fest, um das Hauptbenutzerpasswort sofort zu rotieren.		

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Netzwerktyp Die vom DB-Cluster unterstützten IP-Adressierungsprotokolle. IPv4, um anzugeben, dass Ressourcen mit dem DB-Cluster nur über das IPv4-Adressierungsprotokoll kommunizieren können. Dual-Stack-Modus, um anzugeben, dass Ressourcen mit dem DB-Cluster über IPv4, IPv6 oder beiden kommunizieren können. Verwenden Sie den Dual-Stack-Modus, wenn Sie über Ressourcen verfügen, die über das IPv6-Adressierungsprotokoll mit Ihrem DB-Cluster kommunizieren müssen. Wenn Sie den Dual-Stack-Modus verwenden möchten, stellen Sie sicher, dass	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--network-type` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `NetworkType` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
mindestens zwei Subnetze über zwei Availability Zones verteilt sind die sowohl das IPv4- als auch das IPv6-Netzwerkprotokoll unterstützen. Stellen Sie außerdem sicher, dass Sie einen IPv6-CIDR-Block mit allen Subnetzen in der von Ihnen angegebenen DB-Subnetzgruppe verknüpfen. Weitere Informati onen finden Sie unter Amazon-Aurora-IP-Adressierung.			

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Neues Master-Passwort Das Passwort für den Hauptbenutzer. • Für Aurora MySQL muss das Passwort 8–41 druckbare ASCII-Zeichen enthalten. • Für Aurora PostgreSQL muss es 8–99 druckbare ASCII-Zeichen enthalten. • Es darf weder /, ", @ noch ein Leerzeichen enthalten.	Mit dem AWS Management Console, Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI `--master-user-password` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `MasterUserPassword` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Performance Insights Ob Performance-Insights aktiviert werden soll; dabei handelt es sich um ein Tool, das den Workload Ihrer DB-Instance überwacht , sodass Sie die Leistung Ihrer Datenbank analysieren und korrigieren können. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .	Mit dem AWS Management Console,Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI`--enable-performance-insights|--no-enable-performance-insights` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `EnablePerformanceInsights` fest.	Nur die angegebene DB-Instance	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Performance Insights AWS KMS key Die AWS KMS key Kennung für die Verschlüsselung von Performance Insights Insights-Daten. Der KMS-Schlüsselbezeichner ist der Amazon Resource Name (ARN), der Schlüsselbezeichner oder der Schlüsselalias für den KMS-Schlüssel. Weitere Informationen finden Sie unter Performance Insights für Aurora ein- und ausschalten.	Mit dem AWS Management Console, Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI `--performance-insights-kms-key-id` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `PerformanceInsightsKMSKeyId` fest.	Nur die angegebene DB-Instance	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Performance Insights-Aufbewahrungszeitraum Der Zeitraum in Tagen, über den Performance Insights-Daten aufbewahrt werden sollen. Die Aufbewahrungseinstellung im kostenlosen Kontingent ist Standard (7 Tage). Um Ihre Leistungsdaten länger aufzubewahren, geben Sie 1–24 Monate an. Weitere Informationen zum Aufbewahrungszeitraum finden Sie unter Preisgestaltung und Datenaufbewahrung für Performance-Insights. Weitere Informationen finden Sie unter Performance Insights für Aurora ein- und ausschalten.	Mit dem AWS Management Console, Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI `--performance-insights-retention-period` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `PerformanceInsightsRetentionPeriod` fest.	Nur die angegebene DB-Instance	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Erhebungsstufe Ein Wert, der die Reihenfolge angibt, in der eine Aurora Replica zur primären Instance in einem DB-Cluster hochgestu ft wird, wenn die vorhandene primäre Instance ausfällt. Weitere Informati onen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.	Mit dem AWS Management Console,Ändern einer DB-Instance in einem DB-Cluster. Führen Sie mit dem die AWS CLI`--promotion-tier` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `PromotionTier` fest.	Nur die angegebene DB-Instance	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Öffentlicher Zugriff Publicly accessible (Öffentlich zugänglich), um der DB-Instance eine öffentliche IP-Adresse zuzuweisen (was bedeutet, dass sie von außerhalb der VPC aus zugänglich ist). Damit der öffentliche Zugriff für eine DB-Instance möglich ist, muss sie sich auch in einem öffentlichen Subnetz der VPC befinden. Not publicly accessible (Nicht öffentlich zugänglich), um die DB-Instance nur innerhalb der VPC zugänglich zu machen. Weitere Informationen finden Sie unter Ausblenden einer DB-Clusters in einer VPC vor dem Internet. Um eine Verbindung zu einer DB-Instance von außerhalb	Mit dem,. AWS Management ConsoleÄndern einer DB-Instance in einem DB-Cluster Führen Sie mit dem die AWS CLI`--publicly-accessible|--no-publicly-accessible` Option aus `modify-db-instance` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBInstance` auf und legen Sie den Parameter `PubliclyAccessible` fest.	Nur die angegebene DB-Instance	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
ihrer Amazon VPC herzustellen, muss die DB-Instance öffentlich zugänglich sein und der Zugriff muss unter Anwendung der Regeln für den eingehenden Datenverkehr der Sicherheitsgruppe der DB-Instance gewährt werden. Darüber hinaus müssen weitere Anforderungen erfüllt werden. Weitere Informationen finden Sie unter Verbindung zur Amazon RDS-DB-Instance kann nicht hergestellt werden. Wenn Ihre DB-Instance nicht öffentlich zugänglich ist, können Sie auch eine AWS Site-to-Site-VPN-Verbindung oder eine AWS Direct Connect Verbindung verwenden, um von einem privaten Netzwerk aus darauf zuzugreifen. Weitere			

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Informationen finden Sie unter Richtlinie für den Datenverkehr zwischen Netzwerken.			
Kapazitätseinstellungen von Serverless v2 Die in Aurora Capacity Units (ACUs) gemessene Datenbankkapazität eines DB-Clusters von Aurora Serverless v2. Weitere Informationen finden Sie unter Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--serverless-v2-scaling-configuration` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `ServerlessV2ScalingConfiguration` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall. Die Änderung wird sofort übernommen. Diese Einstellung ignoriert die Einstellung „Apply Immediately (Sofort Anwenden)“.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Sicherheitsgruppe Die Sicherheitsgruppe, die Sie mit dem DB-Cluster verknüpfen möchten. Weitere Informationen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen.	Mit dem AWS Management Console, Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI `--vpc-security-group-ids` Option aus `modify-db-cluster` und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `VpcSecurityGroupIds` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellung und Beschreibung	Art	Scope	Hinweise zur Ausfallzeit
Backtrack-Zielfenster Der Zeitraum in Sekunden, über den Sie Ihr DB-Cluster zurückverfolgen möchten. Diese Einstellung ist nur für Aurora MySQL verfügbar und nur dann, wenn während der Erstellung des DB-Clusters die Rückverfolgung aktiviert wurde.	Mit dem AWS Management Console,Ändern des DB-Clusters über die Konsole, die CLI und die API. Führen Sie mit dem die AWS CLI`--backtrack-window` Option aus `modify-db-cluster`und legen Sie sie fest. Bei Verwendung der RDS API: Rufen Sie `ModifyDBCluster` auf und legen Sie den Parameter `BacktrackWindow` fest.	Gesamter DB-Cluster	Diese Änderung verursacht keinen Ausfall.

Einstellungen, die nicht für Amazon-Aurora-DB-Cluster gelten

Die folgenden Einstellungen im AWS CLI Befehl `modify-db-cluster`und im RDS-API-Vorgang gelten `ModifyDBCluster`nicht für Amazon Aurora Aurora-DB-Cluster.

> **Note**
>
> Sie können das nicht verwenden AWS Management Console , um diese Einstellungen für Aurora-DB-Cluster zu ändern.

AWS CLI Einstellung	RDS-API-Einstellung
`--allocated-storage`	`AllocatedStorage`
`--auto-minor-version-upgrade | --no-auto-minor-version-upgrade`	`AutoMinorVersionUpgrade`
`--db-cluster-instance-class`	`DBClusterInstanceClass`
`--enable-performance-insights | --no-enable-performance-insights`	`EnablePerformanceInsights`
`--iops`	`Iops`
`--monitoring-interval`	`MonitoringInterval`
`--monitoring-role-arn`	`MonitoringRoleArn`
`--option-group-name`	`OptionGroupName`
`--performance-insights-kms-key-id`	`PerformanceInsightsKMSKeyId`
`--performance-insights-retention-period`	`PerformanceInsightsRetentionPeriod`

Einstellungen, die nicht für Amazon-Aurora-DB-Instances gelten

Die folgenden Einstellungen im AWS CLI Befehl `modify-db-instance` und im RDS-API-Vorgang gelten `ModifyDBInstance` nicht für Amazon Aurora Aurora-DB-Instances.

> **Note**
>
> Sie können die nicht verwenden AWS Management Console , um diese Einstellungen für Aurora-DB-Instances zu ändern.

AWS CLI Einstellung	RDS-API-Einstellung
`--allocated-storage`	`AllocatedStorage`
`--allow-major-version-upgrade|--no-allow-major-version-upgrade`	`AllowMajorVersionUpgrade`
`--copy-tags-to-snapshot|--no-copy-tags-to-snapshot`	`CopyTagsToSnapshot`
`--domain`	`Domain`
`--db-security-groups`	`DBSecurityGroups`
`--db-subnet-group-name`	`DBSubnetGroupName`
`--domain-iam-role-name`	`DomainIAMRoleName`
`--multi-az|--no-multi-az`	`MultiAZ`
`--iops`	`Iops`
`--license-model`	`LicenseModel`
`--network-type`	`NetworkType`
`--option-group-name`	`OptionGroupName`
`--processor-features`	`ProcessorFeatures`
`--storage-type`	`StorageType`
`--tde-credential-arn`	`TdeCredentialArn`
`--tde-credential-password`	`TdeCredentialPassword`
`--use-default-processor-features|--no-use-default-processor-features`	`UseDefaultProcessorFeatures`

Hinzufügen von Aurora-Replicas zu einem DB-Cluster

Ein Aurora-DB-Cluster mit Replikation hat eine primäre DB-Instance und bis zu 15 Aurora-Replicas. Die primäre DB-Instance Unterstützt Lese- und Schreiboperationen und führt alle Datenänderungen im Cluster-Volume durch. Aurora-Replicas stellen eine Verbindung zu demselben Speichervolume wie die primäre DB-Instance her, aber unterstützen nur Lesevorgänge. Sie nutzen Aurora-Replicas, um schreibgeschützte Workloads von der primären DB-Instance auszulagern. Informationen finden Sie unter Aurora-Replikate.

Amazon Aurora Replicas haben die folgenden Einschränkungen:

- Sie können keine Aurora Replica für einen Aurora Serverless v1-DB-Cluster erstellen. Aurora Serverless v1 verfügt über eine einzelne DB-Instance, die automatisch nach oben und unten skaliert wird, um alle Lese- und Schreibvorgänge der Datenbank zu unterstützen.

  Sie können jedoch Aurora Serverless v2-DB-Clustern Reader-Instances hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Aurora Serverless v2-Readers.

Wir empfehlen Ihnen, die primäre Instance und die Aurora-Replicas Ihres DB-Clusters über mehrere Availability Zones zu verteilen, um die Verfügbarkeit Ihres DB-Clusters zu verbessern. Weitere Informationen finden Sie unter Verfügbarkeit in Regionen.

Zum Entfernen einer Aurora Replica aus einem Aurora-DB-Cluster löschen Sie die Aurora Replica anhand der Anweisungen in Löschen einer DB-Instance aus einem Aurora-DB-Cluster.

> **Note**
>
> Amazon Aurora unterstützt auch die Replikation mit einer externen Datenbank wie einer RDS-DB-Instance. Die RDS-DB-Instance muss sich in derselben AWS-Region befinden wie Amazon Aurora. Weitere Informationen finden Sie unter Replikation mit Amazon Aurora.

Sie können Aurora Replicas über die AWS Management Console, die AWS CLI oder die RDS-API zu einem DB-Cluster hinzufügen.

Konsole

So fügen Sie eine Aurora Replica zu einem DB-Cluster hinzu:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus. Wählen Sie dann den DB-Cluster aus, in dem Sie die neue DB-Instance hinzufügen möchten.
3. Stellen Sie sicher, dass sowohl der Cluster als auch die primäre Instance den Status Verfügbar aufweisen. Wenn sich der DB-Cluster oder die primäre Instance in einem Übergangszustand wie Erstellen befindet, können Sie kein Replikat hinzufügen.

   Wenn der Cluster keine primäre Instance hat, erstellen Sie eine mit dem create-db-instance AWS CLI Befehl . Diese Situation kann auftreten, wenn Sie die CLI verwendet haben, um einen DB-Cluster-Snapshot wiederherzustellen und dann den Cluster in anzeige AWS Management Console.
4. Wählen Sie für Actions (Aktionen) Add reader (Reader hinzufügen) aus.

   Die Seite Add reader (Reader hinzufügen) wird angezeigt.
5. Geben Sie auf der Seite Add reader (Reader hinzufügen) Optionen für Ihr Aurora-Replica an. In der folgenden Tabelle werden die Einstellungen für ein Aurora Replica angezeigt.

Option	Vorgehensweise
Availability Zone	Legen Sie fest, ob Sie eine bestimmte Availability Zone angeben möchten. Die Liste beinhaltet nur jene Availability Zones, die der DB-Subnetzgruppe zugeordnet sind, die Sie beim Erstellen des DB-Cluste rs ausgewählt haben. Weitere Informationen über Availability Zones finden Sie unter Regionen und Availability Zones.
Öffentlich zugänglich	Wählen Sie Yes aus, um der Aurora-Replica eine öffentliche IP-Adresse zuzuweisen. Wählen Sie andernfalls No aus. Weitere Informationen darüber, wie Sie den öffentlichen Zugriff für Aurora-Replicas

Option	Vorgehensweise
	deaktivieren, finden Sie unter Ausblenden einer DB-Clusters in einer VPC vor dem Internet.
Verschlüsselung	Klicken Sie auf `Enable encryption` , um die Verschlüsselung im Ruhezustand für diese Aurora-Replica zu aktivieren. Weitere Informationen finden Sie unter Verschlüsseln von Amazon Aurora-Ressourcen.
DB-Instance-Klasse	Wählen Sie eine DB-Instance-Klasse aus, die die Verarbeitungs- und Speicheranforderungen für das Aurora Replica definiert. Weitere Informationen zu den Optionen für DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.
Aurora-Replikatquelle	Wählen Sie eine Kennung für die primäre Instance aus, für die Sie ein Aurora Replica erstellen möchten.
DB-Instance-Kennung	Geben Sie einen Namen für die Instance ein, der eindeutig für Ihr Konto in der ausgewählten AWS-Region ist. Sie können den Namen aussagekräftiger machen, indem Sie Angaben wie AWS-Region und DB-Engine hinzufügen, z. B. **`aurora-read-instance1`** .
Priorität	Wählen Sie eine Failover-Priorität für die Instance aus. Wenn Sie keinen Wert auswählen, wird als Standard tier-1 eingestellt. Diese Priorität bestimmt die Reihenfolge, in der Aurora-Replikate bei der Wiederherstellung nach einem Ausfall der primären Instance hochgestuft werden. Weitere Informationen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.
Datenbankport	Der Port für ein Aurora Replica ist derselbe wie der für das DB-Cluster.

Option	Vorgehensweise
DB-Parametergruppe	Wählen Sie eine Parametergruppe aus. Aurora verfügt über eine Standardparametergruppe, die Sie verwenden können, oder Sie können Ihre eigene Parametergruppe erstellen. Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.
Performance Insights	Das Kontrollkästchen Performance Insights aktivieren ist standardmäßig aktiviert. Der Wert wird nicht von der Writer-Instance geerbt. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .
Verbesserte Überwachung	Wählen Sie Erweiterte Überwachung aktivieren aus, um die Erfassung von Metriken in Echtzeit für das Betriebssystem zu aktivieren, in dem Ihr DB-Cluster ausgeführt wird. Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).
Überwachungsrolle	Nur verfügbar, wenn Verbesserte Überwachung auf Erweiterte Überwachung aktivieren gesetzt ist. Wählen Sie die IAM-Rolle aus, die Sie erstellt haben, um Amazon RDS die Kommunikation mit Amazon CloudWatch Logs für Sie zu ermöglichen, oder wählen Sie Standard aus, damit RDS eine Rolle mit dem Namen für Sie erstellt`rds-monitoring-role` . Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).
Granularität	Nur verfügbar, wenn Verbesserte Überwachung auf Erweiterte Überwachung aktivieren gesetzt ist. Mit ihr können Sie die Zeitspanne zwischen den Erfassung en der Kennzahlen des DB-Clusters in Sekunden festlegen.

Option	Vorgehensweise
Kleinere Versions-Upgrades automatisch aktivieren	Wählen Sie Kleinere Versions-Upgrades automatisch aktivieren aus, wenn Ihr Aurora-DB-Cluster automatisch Upgrades der DB-Engine-Unterversion erhalten soll, sobald diese verfügbar sind. Die Einstellung Automatisches Unterversion-Upgrade gilt nur für Aurora-PostgreSQL- und Aurora-MySQL-DB-Cluster. Bei Clustern von Aurora MySQL 2.x werden mit dieser Einstellung die Cluster auf eine maximale Version von 2.07.2 aktualisiert. Weitere Informationen über Engine-Updates für Aurora PostgreSQL finden Sie unter Amazon Aurora PostgreSQL-Aktualisierungen. Weitere Informationen über Engine-Updates für Aurora MySQL finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.

6. Wählen Sie Add reader (Reader hinzufügen) aus, um das Aurora Replica zu erstellen.

AWS CLI

Führen Sie den create-db-instance AWS CLI Befehl aus, um eine Aurora-Replica in Ihrem DB-Cluster zu erstellen. Beziehen Sie den Namen des DB-Clusters als Option `--db-cluster-identifier` mit ein. Optional können Sie mithilfe des Parameters `--availability-zone` eine Availability Zone für die Aurora-Replica festlegen, wie in den folgenden Beispielen dargestellt.

Mit dem folgenden Befehl beispielsweise wird eine neue MySQL 5.7-kompatible Aurora-Replik mit dem Namen erstell `sample-instance-us-west-2a`.

Für Linux, macOSoder Unix:

```
aws rds create-db-instance --db-instance-identifier sample-instance-us-west-2a \
    --db-cluster-identifier sample-cluster --engine aurora-mysql --db-instance-class
 db.r5.large \
    --availability-zone us-west-2a
```

Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance-us-west-2a ^
    --db-cluster-identifier sample-cluster --engine aurora-mysql --db-instance-class
 db.r5.large ^
    --availability-zone us-west-2a
```

Mit dem folgenden Befehl wird eine neue MySQL 5.7-kompatible Aurora-Replica mit dem Namen `sample-instance-us-west-2a` erstellt.

Für Linux, macOSoder Unix:

```
aws rds create-db-instance --db-instance-identifier sample-instance-us-west-2a \
    --db-cluster-identifier sample-cluster --engine aurora-mysql --db-instance-class
 db.r5.large \
    --availability-zone us-west-2a
```

Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance-us-west-2a ^
    --db-cluster-identifier sample-cluster --engine aurora --db-instance-class
 db.r5.large ^
    --availability-zone us-west-2a
```

Der folgende Befehl erstellt ein neues PostgreSQL-kompatibles Aurora-Replikat mit dem Namen `sample-instance-us-west-2a`.

Für Linux, macOSoder Unix:

```
aws rds create-db-instance --db-instance-identifier sample-instance-us-west-2a \
    --db-cluster-identifier sample-cluster --engine aurora-postgresql --db-instance-
class db.r5.large \
    --availability-zone us-west-2a
```

Windows:

```
aws rds create-db-instance --db-instance-identifier sample-instance-us-west-2a ^
    --db-cluster-identifier sample-cluster --engine aurora-postgresql --db-instance-
class db.r5.large ^
    --availability-zone us-west-2a
```

RDS-API

Rufen Sie die Aktion CreateDBInstance auf, um eine Aurora-Replica in Ihrem DB-Cluster zu erstellen. Beziehen Sie den Namen des DB-Clusters als Parameter `DBClusterIdentifier` mit ein. Optional können Sie mithilfe des Parameters `AvailabilityZone` eine Availability Zone für die Aurora-Replica angeben.

Verwalten von Performance und Skalierung für einen Aurora-DB-Cluster

Für die Verwaltung von Performance und Skalierung von Aurora DB-Clustern und DB-Instances stehen Ihnen folgende Möglichkeiten zur Verfügung:

Themen

Speicherskalierung

Der Aurora-Speicher wird automatisch mit den Daten in Ihrem Cluster-Volume skaliert. Wenn Ihre Daten zunehmen, wird Ihr Cluster-Volume-Speicher bis zu einem Maximum von 128 Tebibytes (TiB) oder 64 TiB erweitert. Die maximale Größe hängt von der Version der DB-Engine ab. Informationen dazu, welche Datentypen im Cluster-Volume enthalten sind, finden Sie unter Amazon Aurora-Speicher und -Zuverlässigkeit. Weitere Informationen zur maximalen Größe für eine bestimmte Version finden Sie unter Amazon Aurora-Größenbeschränkungen.

Die Größe Ihres Cluster-Volumes wird stündlich überprüft, um die Kosten für Ihren Speicherplatz zu bestimmen. Informationen zu den Preisen finden Sie in der Aurora-Preisliste.

Obwohl ein Aurora-Cluster-Volume in der Größe auf viele Tebibyte skaliert werden kann, wird nur der Speicherplatz berechnet, den Sie auf dem Volume verwenden. Der Mechanismus zur Bestimmung des fakturierten Speicherplatzes hängt von der Version Ihres Aurora-Clusters ab.

- Wenn Aurora-Daten aus dem Cluster-Volume entfernt werden, verringert sich der gesamte fakturierte Speicherplatz um einen entsprechenden Betrag. Dieses dynamische Größenanpassungsverhalten tritt auf, wenn zugrunde liegende Tabellenbereiche gelöscht oder neu organisiert werden, damit sie weniger Speicherplatz benötigen. So können Sie Speicherkosten senken, indem Sie Tabellen und Datenbanken löschen, die Sie nicht mehr benötigen. Die dynamische Größenanpassung gilt für bestimmte Aurora-Versionen. Im Folgenden werden die

Aurora-Versionen aufgeführt, bei denen die Größe des Cluster-Volumes beim Entfernen von Daten dynamisch geändert wird:

Aurora MySQL	• Version 3 (mit MySQL 8.0 kompatibel): alle unterstützten Versionen • Version 2 (kompatibel mit MySQL 5.7): 2.11 und höher
Aurora PostgreSQL	Alle unterstützten Versionen
Aurora Serverless v2	Alle unterstützten Versionen
Aurora Serverless v1	Alle unterstützten Versionen

- In Aurora-Versionen, die niedriger sind als die in der vorherigen Liste aufgeführten, kann das Cluster-Volume Speicherplatz wiederverwenden, der beim Entfernen von Daten frei wird, aber das Volume selbst nimmt nie an Größe ab.
- Diese Funktion wird schrittweise in den AWS Regionen bereitgestellt, in denen Aurora verfügbar ist. Abhängig von der Region, in der sich Ihr Cluster befindet, ist diese Funktion möglicherweise noch nicht verfügbar.

Die dynamische Größenanpassung gilt für Operationen, bei denen Tabellenbereiche innerhalb des Cluster-Volumes physisch entfernt oder in der Größe geändert werden. Daher gilt sie für SQL-Anweisungen wie `DROP TABLE`, `DROP DATABASE`, `TRUNCATE TABLE` und `ALTER TABLE ... DROP PARTITION`. Sie gilt nicht für das Löschen von Zeilen mit der `DELETE`-Anweisung. Wenn Sie eine große Anzahl von Zeilen aus einer Tabelle löschen, können Sie anschließend die Aurora MySQL `OPTIMIZE TABLE`-Anweisung ausführen oder die Aurora PostgreSQL `pg_repack`-Erweiterung verwenden, um die Tabelle zu reorganisieren und die Größe des Cluster-Volumes dynamisch zu ändern.

Für Aurora MySQL gelten die folgenden Überlegungen:

- Nachdem Sie Ihren DB-Cluster auf eine DB-Engine-Version aktualisiert haben, die dynamische Größenänderung unterstützt, und wenn die Funktion in dieser speziellen Version aktiviert ist AWS-Region, kann jeder Speicherplatz, der später durch bestimmte SQL-Anweisungen freigegeben wird, wie z. B.`DROP TABLE`, zurückgewonnen werden.

Wenn die Funktion in einem bestimmten Bereich explizit deaktiviert ist AWS-Region, ist der Speicherplatz möglicherweise nur wiederverwendbar — und nicht zurückforderbar —, selbst in Versionen, die dynamische Größenänderung unterstützen.

Die Funktion wurde zwischen November 2020 und März 2022 für bestimmte DB-Engine-Versionen (1.23.0—1.23.4, 2.09.0—2.09.3 und 2.10.0) aktiviert und ist in allen nachfolgenden Versionen standardmäßig aktiviert.

- Eine Tabelle wird intern in einem oder mehreren zusammenhängenden Fragmenten unterschiedlicher Größe gespeichert. Während der Ausführung von `TRUNCATE TABLE` Vorgängen ist der Speicherplatz, der dem ersten Fragment entspricht, wiederverwendbar und kann nicht zurückgewonnen werden. Andere Fragmente können zurückgewonnen werden. Während des `DROP TABLE` Betriebs kann Speicherplatz, der dem gesamten Tablespace entspricht, zurückgewonnen werden.
- Der `innodb_file_per_table` Parameter beeinflusst, wie der Tabellenspeicher organisiert ist. Wenn Tabellen Teil des System-Tablespace sind, wird durch das Löschen der Tabelle die Größe des System-Tablespace nicht verringert. Stellen Sie daher sicher, dass Sie `innodb_file_per_table` für DB-Cluster von Aurora MySQL auf 1 festlegen, um die dynamische Größenanpassung optimal zu nutzen.
- In Version 2.11 und höher wird der temporäre InnoDB-Tablespace gelöscht und beim Neustart neu erstellt. Dadurch wird der vom temporären Tabellenbereich belegte Speicherplatz für das System freigegeben und die Größe des Cluster-Volumes anschließend geändert. Um die dynamische Größenänderungsfunktion in vollem Umfang nutzen zu können, empfehlen wir Ihnen, Ihren DB-Cluster auf Version 2.11 oder höher zu aktualisieren.

> **Note**
>
> Mit der Funktion zur dynamischen Größenänderung wird Speicherplatz nicht sofort zurückgewonnen, wenn Tabellen in Tablespaces gelöscht werden, sondern schrittweise mit einer Geschwindigkeit von etwa 10 TB pro Tag. Speicherplatz im System-Tablespace wird nicht zurückgewonnen, da der System-Tablespace niemals entfernt wird. Nicht zurückgewonnener freier Speicherplatz in einem Tabellenraum wird wiederverwendet, wenn ein Vorgang Speicherplatz in diesem Tabellenraum benötigt. Die dynamische Größenanpassungsfunktion kann Speicherplatz nur dann zurückgewinnen, wenn sich der Cluster in einem verfügbaren Zustand befindet.

Sie können überprüfen, wie viel Speicherplatz ein Cluster verwendet, indem Sie die `VolumeBytesUsed` Metrik in überwachen. CloudWatch Weitere Informationen zu Speicherkosten finden Sie unter Informationen zur Abrechnung des Aurora-Datenspeichers.

- In der können Sie diese Zahl in einem Diagramm sehen AWS Management Console, indem Sie die `Monitoring` Registerkarte auf der Detailseite für den Cluster aufrufen.
- Mit dem können Sie einen Befehl ausführen AWS CLI, der dem folgenden Linux-Beispiel ähnelt. Ersetzen Sie Ihre eigenen Werte durch die Start- und Endzeit und den Namen des Clusters.

```
aws cloudwatch get-metric-statistics --metric-name "VolumeBytesUsed" \
  --start-time "$(date -d '6 hours ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" \
  --statistics Average Maximum Minimum \
  --dimensions Name=DBClusterIdentifier,Value=my_cluster_identifier
```

Die Ausgabe dieses Befehls sieht etwa so aus:

```
{
    "Label": "VolumeBytesUsed",
    "Datapoints": [
        {
            "Timestamp": "2020-08-04T21:25:00+00:00",
            "Average": 182871982080.0,
            "Minimum": 182871982080.0,
            "Maximum": 182871982080.0,
            "Unit": "Bytes"
        }
    ]
}
```

Die folgenden Beispiele zeigen, wie Sie mithilfe von AWS CLI Befehlen auf einem Linux-System die Speichernutzung für einen Aurora-Cluster im Laufe der Zeit verfolgen können. Die Parameter `--start-time` und `--end-time` definieren das Gesamtzeitintervall als einen Tag. Der Parameter `--period` fordert die Messungen in einstündigen Intervallen an. Es ist sinnlos, einen kleinen `--period`-Wert zu wählen, da die Metriken in Intervallen und nicht kontinuierlich erfasst werden. Außerdem werden Aurora-Speicheroperationen manchmal für einige Zeit im Hintergrund fortgesetzt, nachdem die entsprechende SQL-Anweisung beendet wurde.

Das erste Beispiel gibt die Ausgabe im Standard-JSON-Format zurück. Die Datenpunkte werden in beliebiger Reihenfolge zurückgegeben, nicht nach Zeitstempel sortiert. Sie können diese JSON-Daten in ein Diagrammwerkzeug importieren, um sie zu sortieren und zu visualisieren.

```
$ aws cloudwatch get-metric-statistics --metric-name "VolumeBytesUsed" \
  --start-time "$(date -d '1 day ago')" --end-time "$(date -d 'now')" --period 3600
  --namespace "AWS/RDS" --statistics Maximum --dimensions
 Name=DBClusterIdentifier,Value=my_cluster_id
{
    "Label": "VolumeBytesUsed",
    "Datapoints": [
        {
            "Timestamp": "2020-08-04T19:40:00+00:00",
            "Maximum": 182872522752.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2020-08-05T00:40:00+00:00",
            "Maximum": 198573719552.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2020-08-05T05:40:00+00:00",
            "Maximum": 206827454464.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2020-08-04T17:40:00+00:00",
            "Maximum": 182872522752.0,
            "Unit": "Bytes"
        },
... output omitted ...
```

In diesem Beispiel werden dieselben Daten zurückgegeben wie vorhin. Der Parameter `--output` stellt die Daten im kompakten Nur-Text-Format dar. Der Befehl `aws cloudwatch` übergibt seine Ausgabe an den Befehl `sort`. Der Parameter `-k` des Befehls `sort` sortiert die Ausgabe nach dem dritten Feld, dem Zeitstempel im UTC-Format (Universal Coordinated Time).

```
$ aws cloudwatch get-metric-statistics --metric-name "VolumeBytesUsed" \
  --start-time "$(date -d '1 day ago')" --end-time "$(date -d 'now')" --period 3600 \
  --namespace "AWS/RDS" --statistics Maximum --dimensions
 Name=DBClusterIdentifier,Value=my_cluster_id \
```

```
  --output text | sort -k 3
VolumeBytesUsed
DATAPOINTS  182872522752.0  2020-08-04T17:41:00+00:00 Bytes
DATAPOINTS  182872522752.0  2020-08-04T18:41:00+00:00 Bytes
DATAPOINTS  182872522752.0  2020-08-04T19:41:00+00:00 Bytes
DATAPOINTS  182872522752.0  2020-08-04T20:41:00+00:00 Bytes
DATAPOINTS  187667791872.0  2020-08-04T21:41:00+00:00 Bytes
DATAPOINTS  190981029888.0  2020-08-04T22:41:00+00:00 Bytes
DATAPOINTS  195587244032.0  2020-08-04T23:41:00+00:00 Bytes
DATAPOINTS  201048915968.0  2020-08-05T00:41:00+00:00 Bytes
DATAPOINTS  205368492032.0  2020-08-05T01:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T02:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T03:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T04:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T05:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T06:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T07:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T08:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T09:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T10:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T11:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T12:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T13:41:00+00:00 Bytes
DATAPOINTS  206827454464.0  2020-08-05T14:41:00+00:00 Bytes
DATAPOINTS  206833664000.0  2020-08-05T15:41:00+00:00 Bytes
DATAPOINTS  206833664000.0  2020-08-05T16:41:00+00:00 Bytes
```

Die sortierte Ausgabe zeigt an, wie viel Speicher zu Beginn und Ende des Überwachungszeitraums genutzt wurde. Sie können auch die Punkte in diesem Zeitraum finden, wenn Aurora mehr Speicher für den Cluster zugewiesen hat. Im folgenden Beispiel werden Linux-Befehle verwendet, um die `VolumeBytesUsed`-Start- und Endwerte als Gigabyte (GB) und als Gibibyte (GiB) neu zu formatieren. Gigabyte stehen für Einheiten, die in Potenzen von 10 gemessen werden und werden häufig in Diskussionen über Speicher für Rotationsfestplatten verwendet. Gibibytes stellen Einheiten dar, die in Zweierpotenzen gemessen werden. Aurora-Speichermessungen und -grenzwerte werden typischerweise in 2er-Potenzeinheiten wie Gibibyte und Tebibyte angegeben.

```
$ GiB=$((1024*1024*1024))
$ GB=$((1000*1000*1000))
$ echo "Start: $((182872522752/$GiB)) GiB, End: $((206833664000/$GiB)) GiB"
Start: 170 GiB, End: 192 GiB
$ echo "Start: $((182872522752/$GB)) GB, End: $((206833664000/$GB)) GB"
```

```
Start: 182 GB, End: 206 GB
```

Die `VolumeBytesUsed`-Metrik gibt an,für wie viel Speicher im Cluster Gebühren anfallen. Daher ist es am besten, diesen Wert nach Möglichkeit zu minimieren. Diese Metrik enthält jedoch keinen Speicher, den Aurora intern im Cluster verwendet und nicht berechnet. Wenn sich Ihr Cluster dem Speicherlimit nähert und möglicherweise nicht genügend Speicherplatz zur Verfügung steht, ist es hilfreich, die `AuroraVolumeBytesLeftTotal`-Metrik zu überwachen und zu maximieren. Im folgenden Beispiel wird eine ähnliche Berechnung ausgeführt wie oben, jedoch für `AuroraVolumeBytesLeftTotal` statt `VolumeBytesUsed`.

```
$ aws cloudwatch get-metric-statistics --metric-name "AuroraVolumeBytesLeftTotal" \
  --start-time "$(date -d '1 hour ago')" --end-time "$(date -d 'now')" --period 3600 \
  --namespace "AWS/RDS" --statistics Maximum --dimensions
 Name=DBClusterIdentifier,Value=my_old_cluster_id \
  --output text | sort -k 3
AuroraVolumeBytesLeftTotal
DATAPOINTS      140530528288768.0       2023-02-23T19:25:00+00:00       Count
$ TiB=$((1024*1024*1024*1024))
$ TB=$((1000*1000*1000*1000))
$ echo "$((69797067915264 / $TB)) TB remaining for this cluster"
69 TB remaining for this cluster
$ echo "$((69797067915264 / $TiB)) TiB remaining for this cluster"
63 TiB remaining for this cluster
```

Bei einem Cluster mit Aurora-MySQL-Version 2.09 oder höher oder Aurora PostgreSQL erhöht sich die von `VolumeBytesUsed` gemeldete Größe des freien Speichers, wenn Daten hinzugefügt werden, und verringert sich, wenn Daten entfernt werden. Im folgenden Beispiel wird gezeigt, wie dies geschieht. Dieser Bericht zeigt die maximale und minimale Speichergröße für einen Cluster in 15-Minuten-Intervallen an, wenn Tabellen mit temporären Daten erstellt und gelöscht werden. Der Bericht listet den Maximalwert vor dem Minimalwert auf. Um zu verstehen, wie sich die Speichernutzung innerhalb des 15-minütigen Intervalls verändert hat, interpretieren Sie daher die Zahlen von rechts nach links.

```
$ aws cloudwatch get-metric-statistics --metric-name "VolumeBytesUsed" \
  --start-time "$(date -d '4 hours ago')" --end-time "$(date -d 'now')" --period 1800 \
  --namespace "AWS/RDS" --statistics Maximum Minimum --dimensions
 Name=DBClusterIdentifier,Value=my_new_cluster_id
  --output text | sort -k 4
VolumeBytesUsed
DATAPOINTS 14545305600.0 14545305600.0 2020-08-05T20:49:00+00:00 Bytes
```

```
DATAPOINTS 14545305600.0 14545305600.0 2020-08-05T21:19:00+00:00 Bytes
DATAPOINTS 22022176768.0 14545305600.0 2020-08-05T21:49:00+00:00 Bytes
DATAPOINTS 22022176768.0 22022176768.0 2020-08-05T22:19:00+00:00 Bytes
DATAPOINTS 22022176768.0 22022176768.0 2020-08-05T22:49:00+00:00 Bytes
DATAPOINTS 22022176768.0 15614263296.0 2020-08-05T23:19:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-05T23:49:00+00:00 Bytes
DATAPOINTS 15614263296.0 15614263296.0 2020-08-06T00:19:00+00:00 Bytes
```

Das folgende Beispiel zeigt, wie bei einem Cluster mit Aurora MySQL Version 2.09 oder höher oder Aurora PostgreSQL die von `AuroraVolumeBytesLeftTotal` gemeldete Größe des freien Speichers die höhere 128 TiB-Größenbeschränkung widerspiegelt.

```
$ aws cloudwatch get-metric-statistics --region us-east-1 --metric-name
 "AuroraVolumeBytesLeftTotal" \
  --start-time "$(date -d '4 hours ago')" --end-time "$(date -d 'now')" --period 1800 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBClusterIdentifier,Value=pq-57 \
  --output text | sort -k 3
AuroraVolumeBytesLeftTotal
DATAPOINTS 140515818864640.0 2020-08-05T20:56:00+00:00 Count
DATAPOINTS 140515818864640.0 2020-08-05T21:26:00+00:00 Count
DATAPOINTS 140515818864640.0 2020-08-05T21:56:00+00:00 Count
DATAPOINTS 140514866757632.0 2020-08-05T22:26:00+00:00 Count
DATAPOINTS 140511020580864.0 2020-08-05T22:56:00+00:00 Count
DATAPOINTS 140503168843776.0 2020-08-05T23:26:00+00:00 Count
DATAPOINTS 140503168843776.0 2020-08-05T23:56:00+00:00 Count
DATAPOINTS 140515818864640.0 2020-08-06T00:26:00+00:00 Count
$ TiB=$((1024*1024*1024*1024))
$ TB=$((1000*1000*1000*1000))
$ echo "$((140515818864640 / $TB)) TB remaining for this cluster"
140 TB remaining for this cluster
$ echo "$((140515818864640 / $TiB)) TiB remaining for this cluster"
127 TiB remaining for this cluster
```

Skalierung von Instances

Sie können Ihr Aurora-DB-Cluster skalieren, indem Sie die DB-Instance-Klasse für jede DB-Instance im DB-Cluster ändern. Aurora unterstützt mehrere DB-Instance-Klassen, die für Aurora optimiert sind, abhängig von der Kompatibilität des Datenbankmoduls.

Datenbank-Engine	Skalierung von Instances
Amazon Aurora MySQL	Siehe Skalierung von Aurora MySQL-DB-Instances
Amazon Aurora PostgreSQL	Siehe Skalierung von Aurora PostgreSQL-DB-Instances

Skalierung von Lesevorgängen

Sie können eine Skalierung von Lesevorgängen für Ihren Aurora-DB-Cluster erreichen, indem Sie bis zu 15 Replicas in Ihrem DB-Cluster erstellen. Jede Aurora-Replica gibt dieselben Daten aus dem Cluster-Volume mit minimaler Replica-Verzögerung zurück – im Normalfall weniger als 100 Millisekunden, nachdem die primäre Instance eine Aktualisierung geschrieben hat. Wenn sich Ihr Datenverkehr mit Lesevorgänge erhöht, können Sie zusätzliche Aurora-Replicas erstellen und sie direkt verbinden, um die Auslastung von Schreibvorgängen für Ihr DB-Cluster zu verteilen. Aurora-Replicas müssen sich nicht in derselben DB-Instance-Klasse wie die primäre Instance befinden.

Informationen zum Hinzufügen von Aurora-Replicas zu einem DB-Cluster finden Sie unter Hinzufügen von Aurora-Replicas zu einem DB-Cluster.

Verwalten von Verbindungen

Die maximale Anzahl der zulässigen Verbindungen mit einer Aurora-DB-Instance wird durch den Parameter `max_connections` in der Instance-Ebenen-Parametergruppe für die DB-Instance festgelegt. Der Standardwert dieses Parameters hängt von der DB-Instance-Klasse ab, die für die Kompatibilität von DB-Instance und Datenbank-Engine verwendet wird.

Datenbank-Engine	Vorgabewert max_connections
Amazon Aurora MySQL	Siehe Maximale Verbindungen zu einer Aurora MySQL-DB-Instance
Amazon Aurora PostgreSQL	Siehe Maximale Verbindungen zu einer Aurora PostgreSQL-DB-Instance

> **Tip**
>
> Wenn Ihre Anwendungen häufig Verbindungen öffnen und schließen oder langlebige Verbindungen in großer Zahl offen lassen, empfehlen wir Ihnen, Amazon-RDS-Proxy zu verwenden. RDS-Proxy ist ein vollständig verwalteter, hochverfügbarer Datenbank-Proxy, der Datenbankverbindungen sicher und effizient per Verbindungspooling freigibt. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

Verwalten von Abfrageausführungsplänen

Mit der Abfrageplanverwaltung für Aurora PostgreSQL haben Sie die Kontrolle darüber, welche Pläne der Optimierer ausführt. Weitere Informationen finden Sie unter Verwalten von Abfrageausführungsplänen für Aurora PostgreSQL.

Klonen eines Volumes für einen Amazon-Aurora-DB-Cluster

Mithilfe der Aurora-Klonfunktion können Sie einen neuen Cluster erstellen, der anfänglich dieselben Datenseiten wie das Original enthält, aber ein separates und unabhängiges Volume darstellt. Der Prozess ist so konzipiert, dass er schnell und kostengünstig ist. Der neue Cluster mit dem zugehörigen Datenvolume wird als clone (Klon) bezeichnet. Das Erstellen eines Klons ist schneller und platzsparender als das physische Kopieren der Daten mit anderen Techniken, wie z. B. das Wiederherstellen eines Snapshots.

Themen

Übersicht über das Aurora-Klonen

Aurora verwendet ein copy-on-write Protokoll, um einen Klon zu erstellen. Dieser Mechanismus verwendet minimalen zusätzlichen Speicherplatz, um einen ersten Klon zu erstellen. Wenn der Klon zum ersten Mal erstellt wird, behält Aurora eine einzelne Kopie der Daten, die vom Aurora-DB-Quellcluster und dem neuen (geklonten) Aurora-DB-Cluster verwendet werden. Zusätzlicher Speicher wird nur zugewiesen, wenn Änderungen an Daten (auf dem Aurora-Speicher-Volume) durch den Aurora-DB-Quellcluster oder den Aurora-DB-Clusterklon vorgenommen werden. Weitere Informationen über das copy-on-write Protokoll finden Sie unterFunktionsweise des Klonens von Aurora.

Das Klonen von Aurora ist besonders nützlich, um Testumgebungen mit Ihren Produktionsdaten schnell einzurichten, ohne Datenbeschädigung zu riskieren. Sie können Klone für viele Arten von Anwendungen verwenden, z. B. für Folgende:

- Experimentieren Sie mit möglichen Änderungen (z. B. Schemaänderungen und Parametergruppenänderungen), um alle Auswirkungen zu bewerten.
- Führen Sie Workload-intensive Vorgänge aus, z. B. das Exportieren von Daten oder das Ausführen analytischer Abfragen auf dem Klon.

- Erstellen Sie eine Kopie Ihres Produktions-DB-Clusters zu Entwicklungs-, Test- oder anderen Zwecken.

Sie können mehr als einen Klon aus demselben Aurora-DB-Cluster erstellen. Sie können auch mehrere Klone aus einem anderen Klon erstellen.

Nachdem Sie einen Aurora-Klon erstellt haben, können Sie die Aurora-DB-Instances anders als den Aurora-DB-Quellcluster konfigurieren. Beispielsweise benötigen Sie möglicherweise keinen Klon für Entwicklungszwecke, um dieselben Hochverfügbarkeitsanforderungen zu erfüllen wie der Aurora-DB-Cluster für die Quellproduktion. In diesem Fall können Sie den Klon mit einer einzelnen Aurora-DB-Instance konfigurieren, anstatt mit mehreren DB-Instances, die vom Aurora-DB-Cluster verwendet werden.

Wenn Sie einen Clone mit einer anderen Bereitstellungskonfiguration als der Quelle erstellen, wird der Clone mit der neuesten Nebenversion der Aurora-DB-Engine der Quelle erstellt.

Wenn Sie Klone aus Ihren Aurora-DB-Clustern erstellen, werden die Klone in Ihrem Konto erstellt AWS — demselben Konto, dem der Aurora-DB-Cluster als Quelle gehört. Sie können Aurora-DB-Cluster Aurora Serverless v2 und -Clones jedoch auch mit anderen AWS Konten teilen und bereitstellen. Weitere Informationen finden Sie unter Kontoübergreifendes Klonen mit AWS RAM und Amazon Aurora.

Wenn Sie den Klon für Test-, Entwicklungs- oder andere Zwecke nicht mehr verwenden, können Sie ihn löschen.

Einschränkungen für das Aurora-Klonen

Das Klonen von Aurora hat derzeit die folgenden Einschränkungen:

- Sie können so viele Klone erstellen, wie Sie möchten, bis zur maximalen Anzahl von DB-Clustern, die in der AWS-Region zulässig sind.

  Sie können die Klone mithilfe des copy-on-write Protokolls oder des vollständigen Kopierprotokolls erstellen. Das Protokoll für die vollständige Kopie funktioniert wie eine Wiederherstellung. point-in-time
- Sie können keinen Clone in einer anderen AWS Region als dem Aurora-DB-Cluster der Quelle erstellen.
- Sie können keinen Klon von einem Aurora-DB-Cluster ohne die parallele Abfragefunktion für einen Cluster erstellen, der parallele Abfragen verwendet. Um Daten in einen Cluster zu bringen, der

parallele Abfragen verwendet, erstellen Sie einen Snapshot des ursprünglichen Clusters und stellen Sie ihn in dem Cluster wieder her, der die parallele Abfragefunktion verwendet.

- Sie können keinen Klon aus einem Aurora DB-Cluster erstellen, der keine DB-Instances hat. Sie können nur Aurora-DB-Cluster klonen, die über mindestens eine DB-Instance verfügen.
- Sie können einen Klon in einer anderen Virtual Private Cloud (VPC) als der des Aurora-DB-Clusters erstellen. In diesem Fall müssen die Subnetze der VPCs denselben Availability Zones zugeordnet sein.
- Sie können einen von Aurora bereitgestellten Klon aus einem bereitgestellten Aurora-DB-Cluster erstellen.
- Cluster mit Aurora Serverless v2-Instances folgen den gleichen Regeln wie bereitgestellte Cluster.
- Aurora Serverless v1:
  - Sie können einen bereitgestellten Clone aus einem Aurora Serverless v1 DB-Cluster erstellen.
  - Sie können einen Aurora Serverless v1 Clone aus einem Aurora Serverless v1 oder einem bereitgestellten DB-Cluster erstellen.
  - Sie können keinen Aurora Serverless v1 Clone aus einem unverschlüsselten, bereitgestellten Aurora-DB-Cluster erstellen.
  - Das kontoübergreifende Klonen unterstützt derzeit das Klonen von Aurora Serverless v1-DB-Clustern nicht. Weitere Informationen finden Sie unter Einschränkungen für kontoübergreifendes Klonen.
  - Ein geklonter Aurora Serverless v1-DB-Cluster hat das gleiche Verhalten und die gleichen Einschränkungen wie jeder Aurora Serverless v1-DB-Cluster. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Serverless v1.
  - Aurora Serverless v1-DB-Cluster sind immer verschlüsselt. Wenn Sie einen Aurora Serverless v1-DB-Cluster in einen bereitgestellten Aurora-DB-Cluster klonen, wird der bereitgestellte Aurora-DB-Cluster verschlüsselt. Sie können den Verschlüsselungsschlüssel auswählen, aber Sie können die Verschlüsselung nicht deaktivieren. Um von einem bereitgestellten Aurora-DB-Cluster auf einen zu klonenAurora Serverless v1, müssen Sie mit einem verschlüsselten, bereitgestellten Aurora-DB-Cluster beginnen.

Funktionsweise des Klonens von Aurora

Das Klonen von Aurora funktioniert auf der Speicherschicht eines Aurora-DB-Clusters. Es verwendet ein Copy-on-Write-Protokoll, das sowohl schnell als auch platzsparend in Bezug auf die

zugrunde liegenden langlebigen Medien ist, die das Aurora-Speichervolumen unterstützen. Weitere Informationen zu Aurora-Cluster-Volumes finden Sie unterÜbersicht über Amazon-Aurora-Speicher.

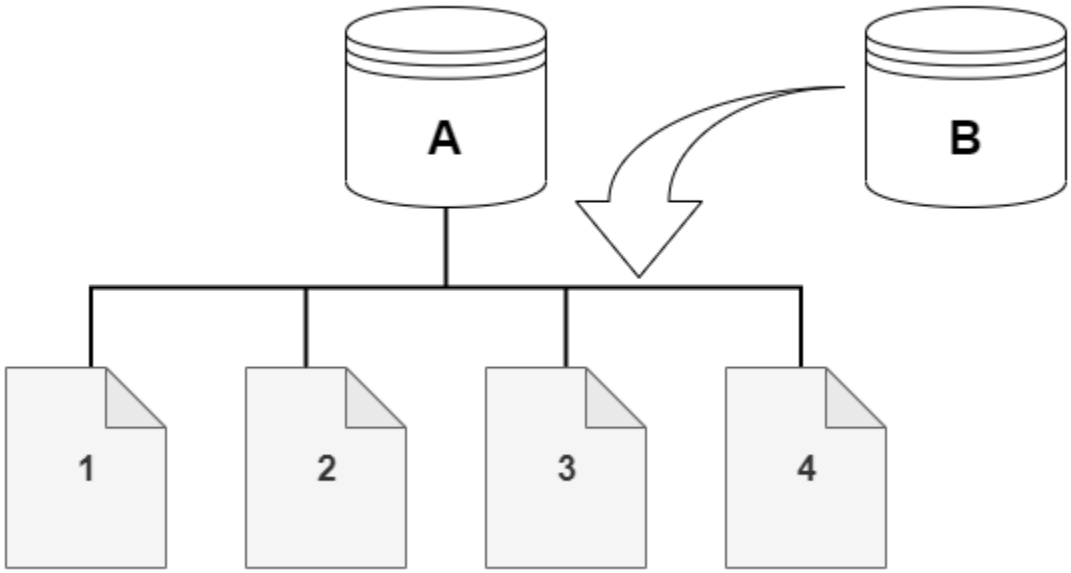
Themen

- Das Protokoll verstehen copy-on-write
- Löschen eines Quell-Cluster-Volumes

Das Protokoll verstehen copy-on-write

Ein Aurora-DB-Cluster speichert Daten in Seiten im zugrunde liegenden Aurora-Speicher-Volume.

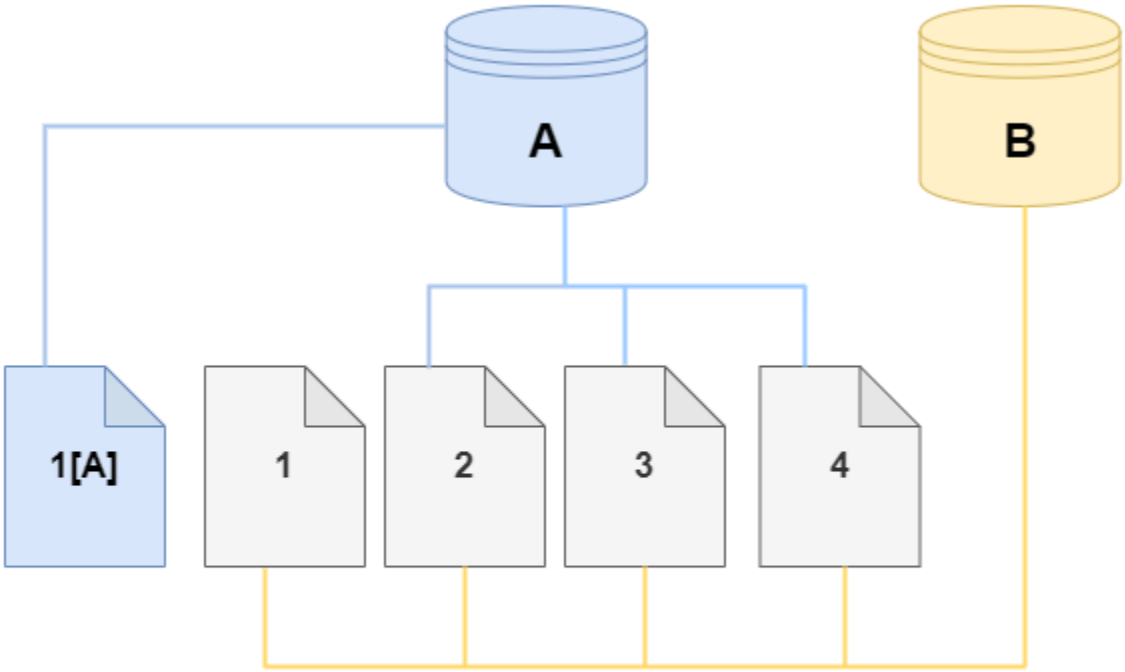
Im folgenden Diagramm finden Sie beispielsweise einen Aurora-DB-Cluster (A) mit vier Datenseiten 1, 2, 3 und 4. Stellen Sie sich vor, dass ein Klon, Klon B, aus dem Aurora-DB-Cluster erstellt wird. Wenn der Klon erstellt wird, werden keine Daten kopiert. Stattdessen verweist der Klon auf denselben Seitensatz wie der Aurora-DB-Quellcluster.



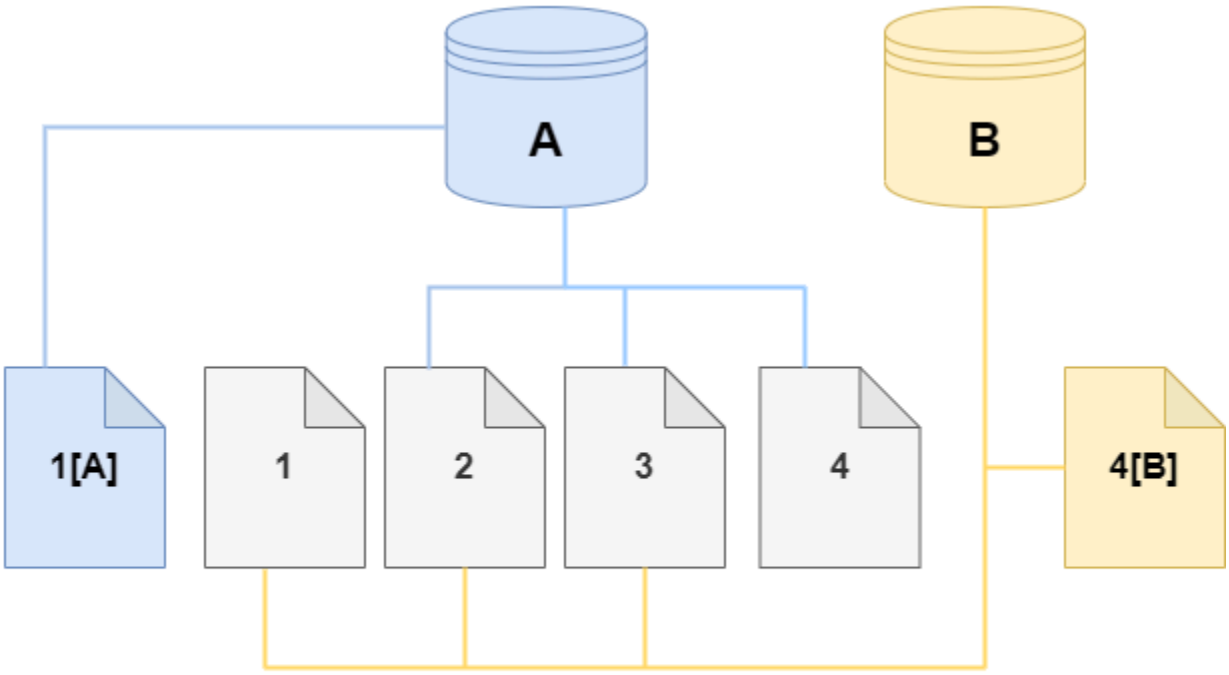
Wenn der Klon erstellt wird, ist normalerweise kein zusätzlicher Speicher erforderlich. Das copy-on-write Protokoll verwendet dasselbe Segment auf dem physischen Speichermedium wie das Quellsegment. Zusätzlicher Speicher ist nur erforderlich, wenn die Kapazität des Quellsegments für das gesamte Klonsegment nicht ausreicht. Wenn dies der Fall ist, wird das Quellsegment auf ein anderes physisches Gerät kopiert.

In den folgenden Diagrammen finden Sie ein Beispiel für das copy-on-write Protokoll in Aktion, das denselben Cluster A und seinen Klon B verwendet, wie oben gezeigt. Nehmen wir an, Sie nehmen

eine Änderung an Ihrem Aurora-DB-Cluster (A) vor, was zu einer Änderung der Daten auf Seite 1 führt. Anstatt auf die ursprüngliche Seite 1 zu schreiben, erstellt Aurora eine neue Seite 1 [A]. Das Aurora-DB-Cluster-Volume für Cluster (A) verweist nun auf Seite 1 [A], 2, 3 und 4, während der Klon (B) weiterhin auf die ursprünglichen Seiten verweist.



Auf dem Klon wird eine Änderung an Seite 4 auf dem Speichervolume vorgenommen. Anstatt auf die ursprüngliche Seite 4 zu schreiben, erstellt Aurora eine neue Seite, 4 [B]. Der Klon verweist nun auf die Seiten 1, 2, 3 und auf Seite 4[B], während der Cluster (A) weiterhin auf 1[A], 2, 3 und 4 verweist.



Da im Laufe der Zeit mehr Änderungen sowohl im Aurora-DB-Cluster-Quellvolume als auch im Klon auftreten, wird mehr Speicherplatz benötigt, um die Änderungen zu erfassen und zu speichern.

Löschen eines Quell-Cluster-Volumes

Anfänglich verwendet das Klon-Volume dieselben Datenseiten wie das ursprüngliche Volume, aus dem der Clone erstellt wurde. Solange das ursprüngliche Volume existiert, gilt das Clone-Volume nur als Eigentümer der Seiten, die der Clone erstellt oder geändert hat. Die `VolumeBytesUsed` Metrik für das Klon-Volume ist also zunächst klein und wächst nur, wenn die Daten zwischen dem ursprünglichen Cluster und dem Clone voneinander abweichen. Für Seiten, die zwischen dem Quell-Volume und dem Clone identisch sind, gelten die Speichergebühren nur für den ursprünglichen Cluster. Für weitere Informationen über die `VolumeBytesUsed`-Metrik siehe Metriken auf Clusterebene für Amazon Aurora.

Wenn Sie ein Quell-Cluster-Volume löschen, dem ein oder mehrere Klone zugeordnet sind, werden die Daten in den Cluster-Volumes der Klone nicht geändert. Aurora behält die Seiten bei, die zuvor dem Quell-Cluster-Volume gehörten. Aurora verteilt die Speicherabrechnung für die Seiten, die dem

gelöschten Cluster gehörten, neu. Nehmen wir zum Beispiel an, ein ursprünglicher Cluster hatte zwei Klone und dann wurde der ursprüngliche Cluster gelöscht. Die Hälfte der Datenseiten, die dem ursprünglichen Cluster gehörten, würde jetzt einem Klon gehören. Die andere Hälfte der Seiten würde dem anderen Klon gehören.

Wenn Sie den ursprünglichen Cluster löschen und weitere Klone erstellen oder löschen, verteilt Aurora weiterhin den Besitz der Datenseiten auf alle Klone, die dieselben Seiten gemeinsam nutzen. Daher stellen Sie möglicherweise fest, dass sich der Wert der `VolumeBytesUsed` Metrik für das Cluster-Volume eines Clones ändert. Der Metrikwert kann sinken, wenn mehr Klone erstellt werden und der Seitenbesitz auf mehr Cluster verteilt wird. Der Metrikwert kann auch steigen, wenn Klone gelöscht werden und der Seitenbesitz einer kleineren Anzahl von Clustern zugewiesen wird. Hinweise dazu, wie sich Schreibvorgänge auf Datenseiten auf Clone-Volumes auswirken, finden Sie unterDas Protokoll verstehen copy-on-write .

Wenn der ursprüngliche Cluster und die Klone demselben AWS Konto gehören, fallen alle Speichergebühren für diese Cluster auf dasselbe AWS Konto an. Wenn es sich bei einigen Clustern um kontenübergreifende Klone handelt, kann das Löschen des ursprünglichen Clusters zu zusätzlichen Speichergebühren für die AWS Konten führen, denen die kontenübergreifenden Klone gehören.

Nehmen wir beispielsweise an, dass ein Cluster-Volume 1000 verwendete Datenseiten hat, bevor Sie Klone erstellen. Wenn Sie diesen Cluster klonen, hat das Klon-Volume zunächst keine verwendeten Seiten. Wenn der Clone Änderungen an 100 Datenseiten vornimmt, werden nur diese 100 Seiten auf dem Clone-Volume gespeichert und als verwendet markiert. Die anderen 900 unveränderten Seiten des übergeordneten Volumes werden von beiden Clustern gemeinsam genutzt. In diesem Fall fallen für den übergeordneten Cluster Speichergebühren für 1000 Seiten und für das Clone-Volume für 100 Seiten an.

Wenn Sie das Quellvolume löschen, umfassen die Speichergebühren für den Clone die 100 Seiten, die er geändert hat, plus die 900 gemeinsam genutzten Seiten aus dem ursprünglichen Volume, also insgesamt 1000 Seiten.

Erstellen eines Amazon-Aurora-DB-Klons

Sie können einen Clone in demselben AWS Konto wie der Aurora-DB-Cluster als Quelle erstellen. Dazu können Sie das AWS Management Console oder das AWS CLI und die folgenden Verfahren verwenden.

Gehen Sie wie unter beschrieben vor, um einem anderen AWS Konto die Erstellung eines Klons oder die gemeinsame Nutzung eines Klons mit einem anderen AWS Konto zu ermöglichenKontoübergreifendes Klonen mit AWS RAM und Amazon Aurora.

Konsole

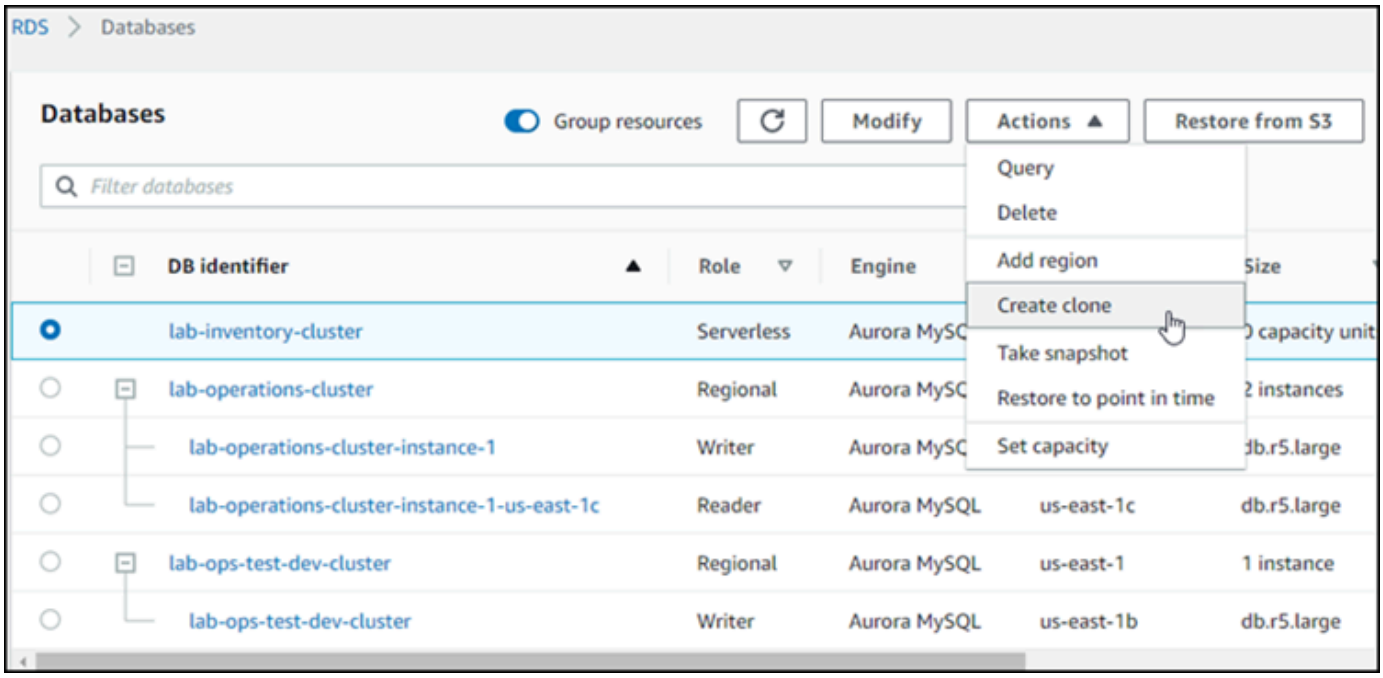
Das folgende Verfahren beschreibt das Klonen eines Aurora-DB-Clusters mittels der AWS Management Console.

Erstellen eines Klons anhand der AWS Management Console Ergebnisse in einem Aurora-DB-Cluster mit einer Aurora-DB-Instance.

Diese Anweisungen gelten für DB-Cluster, die demselben AWS Konto gehören, das den Clone erstellt. Wenn der DB-Cluster einem anderen AWS Konto gehört, finden Sie Kontoübergreifendes Klonen mit AWS RAM und Amazon Aurora stattdessen weitere Informationen unter.

Um einen Klon eines DB-Clusters zu erstellen, der Ihrem AWS Konto gehört, verwenden Sie den AWS Management Console

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie Ihren Aurora-DB-Cluster aus der Liste aus, und wählen Sie für Aktionen die Option Klon erstellen aus.



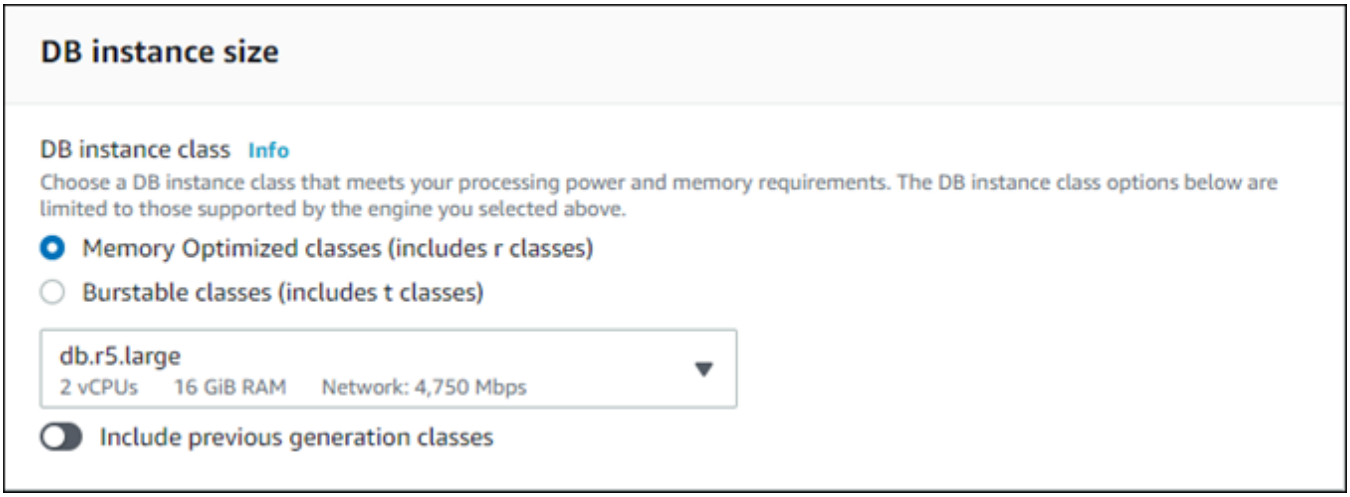
Die Seite „Klon erstellen“ wird geöffnet, auf der Sie Einstellungen, Konnektivität und andere Optionen für den Klon des Aurora-DB-Clusters konfigurieren können.

4. Geben Sie als DB-Instance-ID den Namen ein, den Sie Ihrem geklonten Aurora-DB-Cluster geben möchten.
5. Wählen Sie für Aurora Serverless v1 DB-Cluster als Kapazitätstyp „Bereitgestellt“ oder „Serverlos“.

   Sie können Serverless nur auswählen, wenn der Aurora-DB-Quellcluster ein Aurora Serverless v1-DB-Cluster oder ein bereitgestellter Aurora-DB-Cluster ist, der verschlüsselt ist.
6. Wählen Sie für Aurora Serverless v2 oder bereitgestellte DB-Cluster entweder Aurora I/O-Optimizedoder Aurora Standardfür die Cluster-Speicherkonfiguration aus.

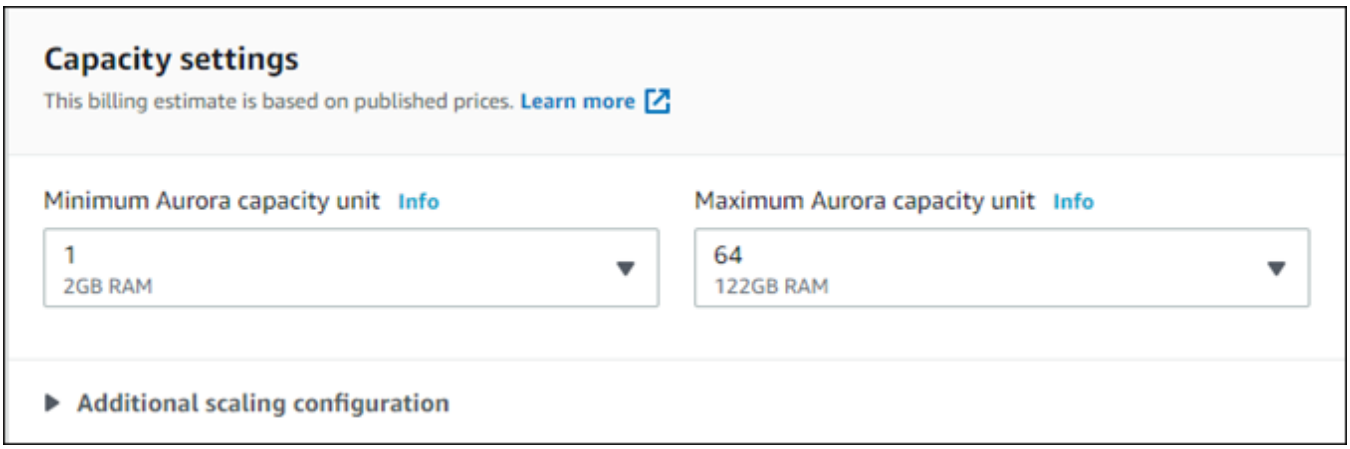
   Weitere Informationen finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora.
7. Wählen Sie die Größe der DB-Instance oder die DB-Cluster-Kapazität aus:

   - Wählen Sie für einen bereitgestellten Clone eine DB-Instance-Klasse aus.



     Sie können die bereitgestellte Einstellung akzeptieren oder eine andere DB-Instance-Klasse für Ihren Klon verwenden.

   - Wählen Sie für einen Aurora Serverless v1 Aurora Serverless v2 OR-Klon die Kapazitätseinstellungen aus.



Sie können die bereitgestellten Einstellungen akzeptieren oder sie für Ihren Clone ändern.

8. Wählen Sie je nach Bedarf weitere Einstellungen für Ihren Clone. Weitere Informationen zu Aurora DB-Cluster- und -Instance-Einstellungen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.
9. Wählen Sie „Klon erstellen“.

Wenn der Klon erstellt wird, wird er mit Ihren anderen Aurora-DB-Clustern im Abschnitt Datenbanken der Konsole aufgelistet und zeigt seinen aktuellen Status an. Ihr Klon ist einsatzbereit, wenn sein Status Verfügbar ist.

AWS CLI

Die Verwendung des AWS CLI zum Klonen Ihres Aurora-DB-Clusters umfasst einige Schritte.

Der `restore-db-cluster-to-point-in-time` AWS CLI Befehl, den Sie verwenden, führt zu einem leeren Aurora-DB-Cluster mit 0 Aurora-DB-Instances. Das heißt, der Befehl stellt nur den Aurora-DB-Cluster wieder her, nicht die DB-Instances für diesen Cluster. Sie tun dies separat, nachdem der Klon verfügbar ist. Die zwei Schritte im Prozess sind wie folgt:

1. Erstellen Sie den Klon mit dem CLI-Befehl restore-db-cluster-to-point-in-time. Die Parameter, die Sie mit diesem Befehl verwenden, steuern den Kapazitätstyp und andere Details des leeren Aurora-DB-Clusters (Klon), der erstellt wird.
2. Erstellen Sie die Aurora-DB-Instance für den Klon, indem Sie den CLI-Befehl create-db-instance verwenden, um die Aurora-DB-Instance im wiederhergestellten Aurora-DB-Cluster neu zu erstellen.

Themen

- Erstellen des Klons
- Überprüfen des Status und Abrufen von Klon-Details
- Erstellen einer Aurora-DB-Instance für Ihren Klon
- Zu verwendende Parameter für das Klonen

Erstellen des Klons

Die spezifischen Parameter, die Sie an den `restore-db-cluster-to-point-in-time`-CLI-Befehl übergeben, variieren. Was Sie übergeben, hängt vom Engine-Modus-Typ des Quell-DB-Clusters – Serverless oder bereitgestellt – und vom Typ des Klons ab, den Sie erstellen möchten.

So erstellen Sie einen Klon mit demselben Engine-Modus wie der Aurora-DB-Quellcluster

- Verwenden Sie den `restore-db-cluster-to-point-in-time`-CLI-Befehl und geben Sie Werte für die folgenden Parameter an:
  - `--db-cluster-identifier` – Wählen Sie einen aussagekräftigen Namen für Ihren Klon. Sie benennen den Klon, wenn Sie den CLI-Befehl restore-db-cluster-to-point-in-time verwenden. Anschließend übergeben Sie den Namen des Klons im CLI-Befehl create-db-instance.
  - `--restore-type` – Verwenden Sie `copy-on-write`, um einen Klon des Quell-DB-Clusters zu erstellen. Ohne diesen Parameter stellt `restore-db-cluster-to-point-in-time` den Aurora-DB-Cluster wieder her, anstatt einen Klon zu erstellen.
  - `--source-db-cluster-identifier` – Verwenden Sie den Namen des Aurora-DB-Quell-Clusters, den Sie klonen möchten.
  - `--use-latest-restorable-time`— Dieser Wert verweist auf die neuesten wiederherstellbaren Volume-Daten für den Quell-DB-Cluster. Verwenden Sie ihn, um Klone zu erstellen.

Im folgenden Beispiel wird ein Klon namens `my-clone` aus einem Cluster namens `my-source-cluster` erstellt.

Für LinuxmacOS, oderUnix:

```
aws rds restore-db-cluster-to-point-in-time \
    --source-db-cluster-identifier my-source-cluster \
    --db-cluster-identifier my-clone \
```

```
    --restore-type copy-on-write \
    --use-latest-restorable-time
```

Windows:

```
aws rds restore-db-cluster-to-point-in-time ^
    --source-db-cluster-identifier my-source-cluster ^
    --db-cluster-identifier my-clone ^
    --restore-type copy-on-write ^
    --use-latest-restorable-time
```

Der Befehl gibt das JSON-Objekt zurück, das Details des Klons enthält. Stellen Sie sicher, dass Ihr geklonter DB-Cluster verfügbar ist, bevor Sie versuchen, die DB-Instance für Ihren Klon zu erstellen. Weitere Informationen finden Sie unter Überprüfen des Status und Abrufen von Klon-Details.

Um einen Clone mit einem anderen Engine-Modus als dem Aurora-DB-Cluster der Quelle zu erstellen

- Verwenden Sie den `restore-db-cluster-to-point-in-time`-CLI-Befehl und geben Sie Werte für die folgenden Parameter an:
  - `--db-cluster-identifier` – Wählen Sie einen aussagekräftigen Namen für Ihren Klon. Sie benennen den Klon, wenn Sie den CLI-Befehl restore-db-cluster-to-point-in-time verwenden. Anschließend übergeben Sie den Namen des Klons im CLI-Befehl create-db-instance.
  - `--source-db-cluster-identifier` – Verwenden Sie den Namen des Aurora-DB-Quell-Clusters, den Sie klonen möchten.
  - `--restore-type` – Verwenden Sie `copy-on-write`, um einen Klon des Quell-DB-Clusters zu erstellen. Ohne diesen Parameter stellt `restore-db-cluster-to-point-in-time` den Aurora-DB-Cluster wieder her, anstatt einen Klon zu erstellen.
  - `--use-latest-restorable-time`— Dieser Wert verweist auf die neuesten wiederherstellbaren Volume-Daten für den Quell-DB-Cluster. Verwenden Sie ihn, um Klone zu erstellen.
  - `--engine-mode`— (Optional) Verwenden Sie diesen Parameter nur, um Klone zu erstellen, die einen anderen Typ als das Aurora-DB-Cluster der Quelle haben. Wählen Sie den mit `--engine-mode` zu übergebenden Wert wie folgt aus:
    - Verwenden Sie `provisioned`, um einen bereitgestellten Aurora-DB-Clusterklon aus einem Aurora Serverless-DB-Cluster zu erstellen.

    - Verwenden Sie `serverless`, um einen Aurora Serverless v1-DB-Cluster-Klon aus einem bereitgestellten Aurora-DB-Cluster zu erstellen. Wenn Sie den `serverless` Engine-Modus angeben, können Sie auch den `--scaling-configuration` auswählen.
- `--scaling-configuration`— (Optional) Verwenden Sie mit`--engine-mode serverless`, um die Mindest- und Höchstkapazität für einen Aurora Serverless v1 Clone zu konfigurieren. Wenn Sie diesen Parameter nicht verwenden, erstellt Aurora den Clone mit den Standardkapazitätswerten für die DB-Engine.
- `--serverless-v2-scaling-configuration`— (Optional) Verwenden Sie diesen Parameter, um die Mindest- und Höchstkapazität für einen Aurora Serverless v2 Clone zu konfigurieren. Wenn Sie diesen Parameter nicht verwenden, erstellt Aurora den Clone mit den Standardkapazitätswerten für die DB-Engine.

Das folgende Beispiel erstellt einen Aurora Serverless v1 Klon mit dem Namen`my-clone`, aus einem bereitgestellten Aurora-DB-Cluster namens`my-source-cluster`. Der bereitgestellte Aurora-DB-Cluster ist verschlüsselt.

Für LinuxmacOS, oderUnix:

```
aws rds restore-db-cluster-to-point-in-time \
    --source-db-cluster-identifier my-source-cluster \
    --db-cluster-identifier my-clone \
    --engine-mode serverless \
    --scaling-configuration MinCapacity=8,MaxCapacity=64 \
    --restore-type copy-on-write \
    --use-latest-restorable-time
```

Windows:

```
aws rds restore-db-cluster-to-point-in-time ^
    --source-db-cluster-identifier my-source-cluster ^
    --db-cluster-identifier my-clone ^
    --engine-mode serverless ^
    --scaling-configuration MinCapacity=8,MaxCapacity=64 ^
    --restore-type copy-on-write ^
    --use-latest-restorable-time
```

Diese Befehle geben das JSON-Objekt zurück, das Details des Klons enthält, den Sie zum Erstellen der DB-Instance benötigen. Dies ist erst möglich, wenn der Status des Klons (der leere Aurora-DB-Cluster) den Status Verfügbar hat.

> **Note**
>
> Der AWS -CLI-Befehl restore-db-cluster-to-point-in-time stellt nur das DB-Cluster wieder her, nicht die DB-Instances für dieses DB-Cluster. Sie müssen den Befehl create-db-instance aufrufen, um DB-Instances für den wiederhergestellten DB-Cluster zu erstellen, wobei Sie die ID des wiederhergestellten DB-Clusters in `--db-cluster-identifier` angeben. Sie können DB-Instances erst dann erstellen, wenn der Befehl `restore-db-cluster-to-point-in-time` abgeschlossen ist und der DB-Cluster verfügbar ist.

Angenommen, Sie haben einen Cluster mit dem Namen `tpch100g`, den Sie klonen möchten. Im folgenden Linux-Beispiel wird ein geklonter Cluster namens `tpch100g-clone` und eine primäre Instance mit dem Namen `tpch100g-clone-instance` für den neuen Clusters erstellt. Einige Parameter wie `--master-username` und `--master-user-password` müssen nicht angegeben werden. Aurora ermittelt diese automatisch aus dem ursprünglichen Cluster. Sie müssen die zu verwendende DB-Engine angeben. Daher testet das Beispiel den neuen Cluster, um den richtigen Wert für den Parameter `--engine` zu ermitteln.

```
$ aws rds restore-db-cluster-to-point-in-time \
  --source-db-cluster-identifier tpch100g \
  --db-cluster-identifier tpch100g-clone \
  --restore-type copy-on-write \
  --use-latest-restorable-time

$ aws rds describe-db-clusters \
  --db-cluster-identifier tpch100g-clone \
    --query '*[].[Engine]' \
    --output text
aurora-mysql

$ aws rds create-db-instance \
  --db-instance-identifier tpch100g-clone-instance \
  --db-cluster-identifier tpch100g-clone \
  --db-instance-class db.r5.4xlarge \
  --engine aurora-mysql
```

Überprüfen des Status und Abrufen von Klon-Details

Mit dem folgenden Befehl können Sie den Status Ihres neu erstellten leeren DB-Clusters überprüfen.

```
$ aws rds describe-db-clusters --db-cluster-identifier my-clone --query '*[].[Status]'
 --output text
```

Oder Sie können den Status und die anderen Werte, die Sie zum Erstellen der DB-Instance für Ihren Clone benötigen, mithilfe der folgenden AWS CLI Abfrage abrufen.

Für LinuxmacOS, oderUnix:

```
aws rds describe-db-clusters --db-cluster-identifier my-clone \
  --query '*[].
{Status:Status,Engine:Engine,EngineVersion:EngineVersion,EngineMode:EngineMode}'
```

Windows:

```
aws rds describe-db-clusters --db-cluster-identifier my-clone ^
  --query "*[].
{Status:Status,Engine:Engine,EngineVersion:EngineVersion,EngineMode:EngineMode}"
```

Diese Abfrage gibt eine Ausgabe ähnlich der folgenden zurück.

```
[
  {
        "Status": "available",
        "Engine": "aurora-mysql",
        "EngineVersion": "8.0.mysql_aurora.3.04.1",
        "EngineMode": "provisioned"
    }
]
```

Erstellen einer Aurora-DB-Instance für Ihren Klon

Verwenden Sie den CLI-Befehl create-db-instance, um die DB-Instance für Ihren Aurora Serverless v2 oder den bereitgestellten Clone zu erstellen. Sie erstellen keine DB-Instance für einen Clone. Aurora Serverless v1

Die DB-Instance erbt die `--master-user-password` Eigenschaften `--master-username` und vom Quell-DB-Cluster.

Im folgenden Beispiel wird eine DB-Instance für einen bereitgestellten Clone erstellt.

Für LinuxmacOS, oderUnix:

```
aws rds create-db-instance \
    --db-instance-identifier my-new-db \
    --db-cluster-identifier my-clone \
    --db-instance-class db.r5.4xlarge \
    --engine aurora-mysql
```

Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier my-new-db ^
    --db-cluster-identifier my-clone ^
    --db-instance-class db.r5.4xlarge ^
    --engine aurora-mysql
```

Zu verwendende Parameter für das Klonen

Die folgende Tabelle fasst die verschiedenen Parameter zusammen, die mit `restore-db-cluster-to-point-in-time` zum Klonen von Aurora-DB-Clustern verwendet werden.

Parameter	Beschreibung
`--source-db-cluster-identifier`	Verwenden Sie den Namen des Aurora-DB-Quell-Clusters, den Sie klonen möchten.
`--db-cluster-identifier`	Wählen Sie einen aussagekräftigen Namen für Ihren Klon, wenn Sie ihn mit dem `restore-db-cluster-to-point-in-time` Befehl erstellen. Dann übergeben Sie diesen Namen an den `create-db-instance` -Befehl.
`--restore-type`	Geben Sie `copy-on-write` als `--restore-type` an, um einen Klon des Quell-DB-Clusters zu erstellen, anstatt den Quell-Aurora-DB-Cluster wiederherzustellen.

Parameter	Beschreibung
`--use-latest-restorable-time`	Dieser Wert verweist auf die neuesten wiederherstellbaren Volume-Daten für den Quell-DB-Cluster. Verwenden Sie ihn, um Klone zu erstellen.
`--engine-mode`	Verwenden Sie diesen Parameter, um Klone zu erstellen, die einen anderen Typ als das Aurora-DB-Cluster der Quelle haben, und zwar mit einem der folgenden Werte: • Wird verwendet`provisioned` , um einen bereitgestellten DB-Cluster oder einen Aurora Serverless v2 Klon aus einem Aurora Serverless v1 DB-Cluster zu erstellen. • Wird verwendet`serverless` , um einen Aurora Serverless v1 Clone aus einem bereitgestellten oder einem Aurora Serverless v2 DB-Cluster zu erstellen. Wenn Sie den `serverless` Engine-Modus angeben, können Sie auch den `--scaling-configuration` auswählen.
`--scaling-configuration`	Verwenden Sie diesen Parameter, um die Mindest- und Höchstkapazität für einen Aurora Serverless v1 Clone zu konfigurieren. Wenn Sie diesen Parameter nicht angeben, erstellt Aurora den Clone mit den Standardkapazitätswerten für die DB-Engine.
`--serverless-v2-scaling-configuration`	Verwenden Sie diesen Parameter, um die Mindest- und Höchstkapazität für einen Aurora Serverless v2 Clone zu konfigurieren. Wenn Sie diesen Parameter nicht angeben, erstellt Aurora den Clone mit den Standardkapazitätswerten für die DB-Engine.

VPC-übergreifendes Klonen mit Amazon Aurora

Angenommen, Sie möchten dem ursprünglichen Cluster und dem Clone unterschiedliche Netzwerkzugriffskontrollen auferlegen. Sie können das Klonen beispielsweise verwenden, um eine Kopie eines Aurora-Produktionsclusters in einer anderen VPC für Entwicklung und Tests zu erstellen. Oder Sie können einen Klon als Teil einer Migration von öffentlichen Subnetzen zu privaten Subnetzen erstellen, um Ihre Datenbanksicherheit zu erhöhen.

In den folgenden Abschnitten wird gezeigt, wie die Netzwerkkonfiguration für den Clone so eingerichtet wird, dass der ursprüngliche Cluster und der Clone beide auf dieselben Aurora-Speicherknoten zugreifen können, auch von unterschiedlichen Subnetzen oder unterschiedlichen VPCs aus. Durch die vorherige Überprüfung der Netzwerkressourcen können Fehler beim Klonen vermieden werden, die möglicherweise schwer zu diagnostizieren sind.

Wenn Sie nicht wissen, wie Aurora mit VPCs, Subnetzen und DB-Subnetzgruppen interagiert, finden Sie zuerst weitere Informationen. Amazon VPCs und Amazon Aurora Sie können die Tutorials in diesem Abschnitt durcharbeiten, um diese Art von Ressourcen in der AWS Konsole zu erstellen und zu verstehen, wie sie zusammenpassen.

Da die Schritte das Umschalten zwischen den RDS- und EC2-Diensten beinhalten, verwenden die Beispiele AWS CLI-Befehle, um Ihnen zu helfen, zu verstehen, wie Sie solche Operationen automatisieren und die Ausgabe speichern können.

- Bevor Sie beginnen
- Sammeln von Informationen über die Netzwerkumgebung
- Netzwerkressourcen für den Clone erstellen
- Einen Aurora-Clone mit neuen Netzwerkeinstellungen erstellen

Bevor Sie beginnen

Bevor Sie mit der Einrichtung eines vPC-übergreifenden Klons beginnen, stellen Sie sicher, dass Sie über die folgenden Ressourcen verfügen:

- Ein Aurora-DB-Cluster, der als Quelle für das Klonen verwendet werden soll. Wenn Sie zum ersten Mal einen Aurora-DB-Cluster erstellen, lesen Sie die Tutorials unter Erste Schritte mit Amazon Aurora So richten Sie einen Cluster mit der MySQL- oder der PostgreSQL-Datenbank-Engine ein.
- Eine zweite VPC, wenn Sie beabsichtigen, einen VPC-übergreifenden Klon zu erstellen. Wenn Sie keine VPC haben, die Sie für den Clone verwenden können, finden Sie weitere Informationen unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4) oderTutorial: Erstellen einer VPC zur Verwendung mit einer DB–einem DB-Cluster (Dual-Stack-Modus).

Sammeln von Informationen über die Netzwerkumgebung

Beim VPC-übergreifenden Klonen kann sich die Netzwerkumgebung zwischen dem ursprünglichen Cluster und seinem Klon erheblich unterscheiden. Bevor Sie den Clone erstellen, sollten Sie Informationen über die VPC, die Subnetze, die DB-Subnetzgruppe und die AZs sammeln und

aufzeichnen, die im ursprünglichen Cluster verwendet wurden. Auf diese Weise können Sie die Wahrscheinlichkeit von Problemen minimieren. Wenn ein Netzwerkproblem auftritt, müssen Sie die Aktivitäten zur Problembehandlung nicht unterbrechen, um nach Diagnoseinformationen zu suchen. Die folgenden Abschnitte zeigen CLI-Beispiele zum Sammeln dieser Art von Informationen. Sie können die Details in einem beliebigen Format speichern, das Sie bei der Erstellung des Klons und bei der Problembehandlung verwenden können.

- Schritt 1: Überprüfen Sie die Availability Zones des ursprünglichen Clusters
- Schritt 2: Überprüfen Sie die DB-Subnetzgruppe des ursprünglichen Clusters
- Schritt 3: Überprüfen Sie die Subnetze des ursprünglichen Clusters
- Schritt 4: Überprüfen Sie die Availability Zones der DB-Instances im ursprünglichen Cluster
- Schritt 5: Überprüfen Sie die VPCs, die Sie für den Clone verwenden können

Schritt 1: Überprüfen Sie die Availability Zones des ursprünglichen Clusters

Bevor Sie den Clone erstellen, überprüfen Sie, welche AZs der ursprüngliche Cluster für seinen Speicher verwendet. Wie unter erklärtAmazon Aurora-Speicher und -Zuverlässigkeit, ist der Speicher für jeden Aurora-Cluster genau drei AZs zugeordnet. Da der die Vorteile der Trennung von Rechenleistung und Speicher Amazon-Aurora-DB-Cluster nutzt, gilt diese Regel unabhängig davon, wie viele Instances sich im Cluster befinden.

Führen Sie beispielsweise einen CLI-Befehl wie den folgenden aus und ersetzen Sie dabei Ihren eigenen Clusternamen durch. *my_cluster* Im folgenden Beispiel wird eine alphabetisch nach dem AZ-Namen sortierte Liste erstellt.

```
aws rds describe-db-clusters \
  --db-cluster-identifier my_cluster \
  --query 'sort_by(*[].AvailabilityZones[].{Zone:@},&Zone)' \
  --output text
```

Das folgende Beispiel zeigt eine Beispielausgabe des vorherigen `describe-db-clusters` Befehls. Es zeigt, dass der Speicher für den Aurora-Cluster immer drei AZs verwendet.

```
us-east-1c
us-east-1d
us-east-1e
```

Um einen Clone in einer Netzwerkumgebung zu erstellen, die nicht über alle Ressourcen verfügt, um eine Verbindung zu diesen AZs herzustellen, müssen Sie Subnetze erstellen, die mindestens zwei

dieser AZs zugeordnet sind, und dann eine DB-Subnetzgruppe erstellen, die diese zwei oder drei Subnetze enthält. Die folgenden Beispiele zeigen, wie das geht.

Schritt 2: Überprüfen Sie die DB-Subnetzgruppe des ursprünglichen Clusters

Wenn Sie dieselbe Anzahl von Subnetzen für den Clone wie im ursprünglichen Cluster verwenden möchten, können Sie die Anzahl der Subnetze aus der DB-Subnetzgruppe des ursprünglichen Clusters abrufen. Eine Aurora-DB-Subnetzgruppe enthält mindestens zwei Subnetze, die jeweils einer anderen AZ zugeordnet sind. Notieren Sie sich, welchen AZs die Subnetze zugeordnet sind.

Das folgende Beispiel zeigt, wie Sie die DB-Subnetzgruppe des ursprünglichen Clusters finden und dann rückwärts zu den entsprechenden AZs arbeiten. Ersetzen Sie im ersten Befehl den Namen Ihres Clusters durch. *my_cluster* Ersetzen Sie im zweiten Befehl den Namen der DB-Subnetzgruppe durch. *my_subnet*

```
aws rds describe-db-clusters --db-cluster-identifier my_cluster \
  --query '*[].DBSubnetGroup' --output text

aws rds describe-db-subnet-groups --db-subnet-group-name my_subnet_group \
  --query '*[].Subnets[].[SubnetAvailabilityZone.Name]' --output text
```

Die Beispielausgabe könnte für einen Cluster mit einer DB-Subnetzgruppe, die zwei Subnetze enthält, in etwa wie folgt aussehen. In diesem Fall `two-subnets` handelt es sich um einen Namen, der bei der Erstellung der DB-Subnetzgruppe angegeben wurde.

```
two-subnets

us-east-1d
us-east-1c
```

Bei einem Cluster, in dem die DB-Subnetzgruppe drei Subnetze enthält, könnte die Ausgabe wie folgt aussehen.

```
three-subnets

us-east-1f
us-east-1d
us-east-1c
```

Schritt 3: Überprüfen Sie die Subnetze des ursprünglichen Clusters

Wenn Sie weitere Informationen zu den Subnetzen im ursprünglichen Cluster benötigen, führen Sie AWS CLI-Befehle aus, die den folgenden ähneln. Sie können die Subnetzattribute wie IP-Adressbereiche, Besitzer usw. untersuchen. Auf diese Weise können Sie bestimmen, ob Sie verschiedene Subnetze in derselben VPC verwenden oder Subnetze mit ähnlichen Eigenschaften in einer anderen VPC erstellen möchten.

Finden Sie die Subnetz-IDs aller Subnetze, die in Ihrer VPC verfügbar sind.

```
aws ec2 describe-subnets --filters Name=vpc-id,Values=my_vpc \
  --query '*[].[SubnetId]' --output text
```

Finden Sie die genauen Subnetze, die in Ihrer DB-Subnetzgruppe verwendet werden.

```
aws rds describe-db-subnet-groups --db-subnet-group-name my_subnet_group \
  --query '*[].Subnets[].[SubnetIdentifier]' --output text
```

Geben Sie dann die Subnetze, die Sie untersuchen möchten, in einer Liste an, wie im folgenden Befehl. Ersetzen Sie die Namen Ihrer Subnetze usw. *my_subnet_1*

```
aws ec2 describe-subnets \
  --subnet-ids '["my_subnet_1","my_subnet2","my_subnet3"]'
```

Das folgende Beispiel zeigt die teilweise Ausgabe eines solchen `describe-subnets` Befehls. Die Ausgabe zeigt einige der wichtigen Attribute, die Sie für jedes Subnetz sehen können, z. B. die zugehörige AZ und die VPC, zu der es gehört.

```
{
    'Subnets': [
        {
            'AvailabilityZone': 'us-east-1d',
            'AvailableIpAddressCount': 54,
            'CidrBlock': '10.0.0.64/26',
            'State': 'available',
            'SubnetId': 'subnet-000a0bca00e0b0000',
            'VpcId': 'vpc-3f3c3fc3333b3ffb3',
            ...
        },
        {
            'AvailabilityZone': 'us-east-1c',
```

```
            'AvailableIpAddressCount': 55,
            'CidrBlock': '10.0.0.0/26',
            'State': 'available',
            'SubnetId': 'subnet-4b4dbfe4d4a4fd4c4',
            'VpcId': 'vpc-3f3c3fc3333b3ffb3',
            ...
```

Schritt 4: Überprüfen Sie die Availability Zones der DB-Instances im ursprünglichen Cluster

Sie können dieses Verfahren verwenden, um die AZs zu verstehen, die für die DB-Instances im ursprünglichen Cluster verwendet wurden. Auf diese Weise können Sie exakt dieselben AZs für die DB-Instances im Clone einrichten. Sie können auch mehr oder weniger DB-Instances im Clone verwenden, je nachdem, ob der Clone für Produktion, Entwicklung und Tests usw. verwendet wird.

Führen Sie für jede Instance im ursprünglichen Cluster einen Befehl wie den folgenden aus. Stellen Sie zunächst sicher, dass die Instanz die Erstellung abgeschlossen hat und sich im `Available` Status befindet. Ersetzen Sie die Instanz-ID durch*`my_instance`*.

```
aws rds describe-db-instances --db-instance-identifier my_instance \
  --query '*[].AvailabilityZone' --output text
```

Das folgende Beispiel zeigt die Ausgabe der Ausführung des vorherigen `describe-db-instances` Befehls. Der Aurora-Cluster hat vier Datenbank-Instances. Daher führen wir den Befehl viermal aus und ersetzen dabei jedes Mal eine andere DB-Instance-ID. Die Ausgabe zeigt, wie diese DB-Instances auf maximal drei AZs verteilt sind.

```
us-east-1a
us-east-1c
us-east-1d
us-east-1a
```

Nachdem der Clone erstellt wurde und Sie ihm DB-Instances hinzufügen, können Sie dieselben AZ-Namen in den `create-db-instance` Befehlen angeben. Sie können dies tun, um DB-Instances im neuen Cluster einzurichten, die für genau dieselben AZs wie im ursprünglichen Cluster konfiguriert sind.

Schritt 5: Überprüfen Sie die VPCs, die Sie für den Clone verwenden können

Wenn Sie beabsichtigen, den Clone in einer anderen VPC als der ursprünglichen zu erstellen, können Sie eine Liste der für Ihr Konto verfügbaren VPC-IDs abrufen. Sie können diesen Schritt auch ausführen, wenn Sie zusätzliche Subnetze in derselben VPC wie der ursprüngliche Cluster erstellen

müssen. Wenn Sie den Befehl zum Erstellen eines Subnetzes ausführen, geben Sie die VPC-ID als Parameter an.

Führen Sie den folgenden CLI-Befehl aus, um alle VPCs für Ihr Konto aufzulisten:

```
aws ec2 describe-vpcs --query '*[].[VpcId]' --output text
```

Das folgende Beispiel zeigt eine Beispielausgabe des vorherigen `describe-vpcs` Befehls. Die Ausgabe zeigt, dass das aktuelle AWS Konto vier VPCs enthält, die als Quelle oder Ziel für das VPC-übergreifende Klonen verwendet werden können.

```
vpc-fd111111
vpc-2222e2cd2a222f22e
vpc-33333333a33333d33
vpc-4ae4d4de4a4444dad
```

Sie können dieselbe VPC als Ziel für den Clone oder eine andere VPC verwenden. Wenn sich der ursprüngliche Cluster und der Clone in derselben VPC befinden, können Sie dieselbe DB-Subnetzgruppe für den Clone wiederverwenden. Sie können auch eine andere DB-Subnetzgruppe erstellen. Beispielsweise könnte die neue DB-Subnetzgruppe private Subnetze verwenden, während die DB-Subnetzgruppe des ursprünglichen Clusters öffentliche Subnetze verwenden könnte. Wenn Sie den Clone in einer anderen VPC erstellen, stellen Sie sicher, dass in der neuen VPC genügend Subnetze vorhanden sind und dass die Subnetze den richtigen AZs aus dem ursprünglichen Cluster zugeordnet sind.

Netzwerkressourcen für den Clone erstellen

Wenn Sie beim Sammeln der Netzwerkinformationen festgestellt haben, dass zusätzliche Netzwerkressourcen für den Clone benötigt werden, können Sie diese Ressourcen erstellen, bevor Sie versuchen, den Clone einzurichten. Beispielsweise müssen Sie möglicherweise mehr Subnetze, Subnetze, die bestimmten AZs zugeordnet sind, oder eine neue DB-Subnetzgruppe erstellen.

- Schritt 1: Erstellen Sie die Subnetze für den Clone
- Schritt 2: Erstellen Sie die DB-Subnetzgruppe für den Clone

Schritt 1: Erstellen Sie die Subnetze für den Clone

Wenn Sie neue Subnetze für den Clone erstellen müssen, führen Sie einen Befehl aus, der dem folgenden ähnelt. Möglicherweise müssen Sie dies tun, wenn Sie den Clone in einer anderen VPC

erstellen oder wenn Sie eine andere Netzwerkänderung vornehmen, z. B. private Subnetze anstelle von öffentlichen Subnetzen verwenden.

AWS generiert automatisch die ID des Subnetzes. Ersetzen Sie den Namen der VPC des Klons durch. *my_vpc* Wählen Sie den Adressbereich für die `--cidr-block` Option, um mindestens 16 IP-Adressen in dem Bereich zuzulassen. Sie können alle anderen Eigenschaften einbeziehen, die Sie angeben möchten. Führen Sie den Befehl aus`aws ec2 create-subnet help`, um alle Auswahlmöglichkeiten zu sehen.

```
aws ec2 create-subnet --vpc-id my_vpc \
  --availability-zone AZ_name --cidr-block IP_range
```

Das folgende Beispiel zeigt einige wichtige Attribute eines neu erstellten Subnetzes.

```
{
    'Subnet': {
        'AvailabilityZone': 'us-east-1b',
        'AvailableIpAddressCount': 59,
        'CidrBlock': '10.0.0.64/26',
        'State': 'available',
        'SubnetId': 'subnet-44b4a44f4e44db444',
        'VpcId': 'vpc-555fc5df555e555dc',
        ...
        }
}
```

Schritt 2: Erstellen Sie die DB-Subnetzgruppe für den Clone

Wenn Sie den Clone in einer anderen VPC oder einer anderen Gruppe von Subnetzen innerhalb derselben VPC erstellen, erstellen Sie eine neue DB-Subnetzgruppe und geben sie bei der Erstellung des Clones an.

Stellen Sie sicher, dass Sie alle folgenden Details kennen. Sie können all diese Informationen in der Ausgabe der vorherigen Beispiele finden.

1. VPC des ursprünglichen Clusters. Anweisungen finden Sie unter Schritt 3: Überprüfen Sie die Subnetze des ursprünglichen Clusters.
2. VPC des Klons, wenn Sie ihn in einer anderen VPC erstellen. Anweisungen finden Sie unter Schritt 5: Überprüfen Sie die VPCs, die Sie für den Clone verwenden können.
3. Drei AZs, die dem Aurora-Speicher für den ursprünglichen Cluster zugeordnet sind. Anweisungen finden Sie unter Schritt 1: Überprüfen Sie die Availability Zones des ursprünglichen Clusters.

4. Zwei oder drei AZs, die der DB-Subnetzgruppe für den ursprünglichen Cluster zugeordnet sind. Anweisungen finden Sie unter Schritt 2: Überprüfen Sie die DB-Subnetzgruppe des ursprünglichen Clusters.
5. Die Subnetz-IDs und zugehörigen AZs aller Subnetze in der VPC, die Sie für den Clone verwenden möchten. Verwenden Sie denselben `describe-subnets` Befehl wie in Schritt 3: Überprüfen Sie die Subnetze des ursprünglichen Clusters und ersetzen Sie dabei die VPC-ID der Ziel-VPC.

Prüfen Sie, wie viele AZs sowohl dem Speicher des ursprünglichen Clusters als auch den Subnetzen in der Ziel-VPC zugeordnet sind. Um den Clone erfolgreich zu erstellen, müssen zwei oder drei AZs gemeinsam sein. Wenn Sie weniger als zwei AZs gemeinsam haben, gehen Sie zurück zuSchritt 1: Erstellen Sie die Subnetze für den Clone. Erstellen Sie ein, zwei oder drei neue Subnetze, die den AZs zugeordnet sind, die dem Speicher des ursprünglichen Clusters zugeordnet sind.

Wählen Sie Subnetze in der Ziel-VPC aus, die denselben AZs zugeordnet sind wie der Aurora-Speicher im ursprünglichen Cluster. Wählen Sie idealerweise drei AZs aus. Auf diese Weise haben Sie die größte Flexibilität, um die DB-Instances des Clone auf mehrere AZs zu verteilen, um eine hohe Verfügbarkeit der Rechenressourcen zu gewährleisten.

Führen Sie einen Befehl ähnlich dem folgenden aus, um die neue DB-Subnetzgruppe zu erstellen. Ersetzen Sie die IDs Ihrer Subnetze in der Liste. Wenn Sie die Subnetz-IDs mithilfe von Umgebungsvariablen angeben, achten Sie darauf, die `--subnet-ids` Parameterliste so in Anführungszeichen zu setzen, dass die IDs in doppelten Anführungszeichen stehen.

```
aws rds create-db-subnet-group --db-subnet-group-name my_subnet_group \
  --subnet-ids '["my_subnet_1","my_subnet_2","my_subnet3"]' \
  --db-subnet-group-description 'DB subnet group with 3 subnets for clone'
```

Das folgende Beispiel zeigt eine teilweise Ausgabe des `create-db-subnet-group` Befehls.

```
{
    'DBSubnetGroup': {
        'DBSubnetGroupName': 'my_subnet_group',
        'DBSubnetGroupDescription': 'DB subnet group with 3 subnets for clone',
        'VpcId': 'vpc-555fc5df555e555dc',
        'SubnetGroupStatus': 'Complete',
        'Subnets': [
            {
                'SubnetIdentifier': 'my_subnet_1',
```

```
                'SubnetAvailabilityZone': {
                    'Name': 'us-east-1c'
                },
                'SubnetStatus': 'Active'
            },
            {
                'SubnetIdentifier': 'my_subnet_2',
                'SubnetAvailabilityZone': {
                    'Name': 'us-east-1d'
                },
                'SubnetStatus': 'Active'
            }
            ...
        ],
        'SupportedNetworkTypes': [
            'IPV4'
        ]
    }
}
```

Zu diesem Zeitpunkt haben Sie den Klon noch nicht erstellt. Sie haben alle relevanten VPC- und Subnetzressourcen erstellt, sodass Sie beim Erstellen des Klons die entsprechenden Parameter für die `create-db-instance` Befehle `restore-db-cluster-to-point-in-time` und angeben können.

Einen Aurora-Clone mit neuen Netzwerkeinstellungen erstellen

Sobald Sie sichergestellt haben, dass die richtige Konfiguration von VPCs, Subnetzen, AZs und Subnetzgruppen für den neuen Cluster vorhanden ist, können Sie den eigentlichen Klonvorgang durchführen. In den folgenden CLI-Beispielen werden die Optionen wie`--db-subnet-group-name`, und hervorgehoben`--availability-zone`, `--vpc-security-group-ids` die Sie in den Befehlen zum Einrichten des Clones und seiner DB-Instances angeben.

- Schritt 1: Geben Sie die DB-Subnetzgruppe für den Clone an
- Schritt 2: Geben Sie die Netzwerkeinstellungen für Instances im Clone an
- Schritt 3: Herstellen der Konnektivität zwischen einem Clientsystem und einem Clone

Schritt 1: Geben Sie die DB-Subnetzgruppe für den Clone an

Wenn Sie den Clone erstellen, können Sie die richtigen VPC-, Subnetz- und AZ-Einstellungen konfigurieren, indem Sie eine DB-Subnetzgruppe angeben. Verwenden Sie die Befehle in den

vorherigen Beispielen, um alle Beziehungen und Zuordnungen zu überprüfen, die zur DB-Subnetzgruppe gehören.

Die folgenden Befehle veranschaulichen beispielsweise das Klonen eines ursprünglichen Clusters in einen Klon. Im ersten Beispiel ist der Quellcluster mit zwei Subnetzen und der Klon mit drei Subnetzen verknüpft. Das zweite Beispiel zeigt den umgekehrten Fall, nämlich das Klonen von einem Cluster mit drei Subnetzen zu einem Cluster mit zwei Subnetzen.

```
aws rds restore-db-cluster-to-point-in-time \
  --source-db-cluster-identifier cluster-with-3-subnets \
  --db-cluster-identifier cluster-cloned-to-2-subnets \
  --restore-type copy-on-write --use-latest-restorable-time \
  --db-subnet-group-name two-subnets
```

Wenn Sie beabsichtigen, Aurora Serverless v2-Instances im Clone zu verwenden, fügen Sie bei der Erstellung des Clones eine `--serverless-v2-scaling-configuration` Option hinzu, wie in der Abbildung gezeigt. Auf diese Weise können Sie die `db.serverless` Klasse verwenden, wenn Sie DB-Instances im Clone erstellen. Sie können den Klon auch später ändern, um dieses Skalierungskonfigurationsattribut hinzuzufügen. Die Kapazitätszahlen in diesem Beispiel ermöglichen es jeder Serverless v2-Instance im Cluster, zwischen 2 und 32 Aurora Capacity Units (ACUs) zu skalieren. Informationen zur Aurora Serverless v2-Funktion und zur Auswahl des Kapazitätsbereichs finden Sie unterVerwenden von Aurora Serverless v2.

```
aws rds restore-db-cluster-to-point-in-time \
  --source-db-cluster-identifier cluster-with-2-subnets \
  --db-cluster-identifier cluster-cloned-to-3-subnets \
  --restore-type copy-on-write --use-latest-restorable-time \
  --db-subnet-group-name three-subnets \
  --serverless-v2-scaling-configuration 'MinCapacity=2,MaxCapacity=32'
```

Unabhängig von der Anzahl der von den DB-Instances verwendeten Subnetze ist der Aurora-Speicher für den Quell-Cluster und den Clone drei AZs zugeordnet. Das folgende Beispiel listet die AZs auf, die sowohl dem ursprünglichen Cluster als auch dem Clone zugeordnet sind, für beide `restore-db-cluster-to-point-in-time` Befehle in den vorherigen Beispielen.

```
aws rds describe-db-clusters --db-cluster-identifier cluster-with-3-subnets \
  --query 'sort_by(*[].AvailabilityZones[].{Zone:@},&Zone)' --output text

us-east-1c
```

```
us-east-1d
us-east-1f

aws rds describe-db-clusters --db-cluster-identifier cluster-cloned-to-2-subnets \
  --query 'sort_by(*[].AvailabilityZones[].{Zone:@},&Zone)' --output text

us-east-1c
us-east-1d
us-east-1f

aws rds describe-db-clusters --db-cluster-identifier cluster-with-2-subnets \
  --query 'sort_by(*[].AvailabilityZones[].{Zone:@},&Zone)' --output text

us-east-1a
us-east-1c
us-east-1d

aws rds describe-db-clusters --db-cluster-identifier cluster-cloned-to-3-subnets \
  --query 'sort_by(*[].AvailabilityZones[].{Zone:@},&Zone)' --output text

us-east-1a
us-east-1c
us-east-1d
```

Da sich mindestens zwei der AZs zwischen jedem Paar von Original- und Klonclustern überschneiden, können beide Cluster auf denselben zugrunde liegenden Aurora-Speicher zugreifen.

Schritt 2: Geben Sie die Netzwerkeinstellungen für Instances im Clone an

Wenn Sie DB-Instances im Clone erstellen, erben diese standardmäßig die DB-Subnetzgruppe vom Cluster selbst. Auf diese Weise weist Aurora jede Instance automatisch einem bestimmten Subnetz zu und erstellt sie in der AZ, die dem Subnetz zugeordnet ist. Diese Wahl ist besonders für Entwicklungs- und Testsysteme praktisch, da Sie beim Hinzufügen neuer Instances zum Clone nicht die Subnetz-IDs oder AZs im Auge behalten müssen.

Als Alternative können Sie die AZ angeben, wenn Sie eine Aurora-DB-Instance für den Clone erstellen. Die AZ, die Sie angeben, muss aus der Gruppe von AZs stammen, die dem Clone zugeordnet sind. Wenn die DB-Subnetzgruppe, die Sie für den Clone verwenden, nur zwei Subnetze enthält, können Sie nur aus den AZs auswählen, die diesen beiden Subnetzen zugeordnet sind. Diese Wahl bietet Flexibilität und Stabilität für Systeme mit hoher Verfügbarkeit, da Sie sicherstellen können, dass sich die Writer-Instance und die Standby-Reader-Instance in unterschiedlichen AZs befinden. Oder wenn Sie dem Cluster weitere Leser hinzufügen, können Sie sicherstellen, dass diese

auf drei AZs verteilt sind. Auf diese Weise haben Sie selbst im seltenen Fall eines AZ-Fehlers immer noch eine Writer-Instance und eine weitere Reader-Instance in zwei anderen AZs.

Das folgende Beispiel fügt einem geklonten Aurora PostgreSQL-Cluster, der eine benutzerdefinierte DB-Subnetzgruppe verwendet, eine bereitgestellte DB-Instance hinzu.

```
aws rds create-db-instance --db-cluster-identifier my_aurora_postgresql_clone \
  --db-instance-identifier my_postgres_instance \
  --db-subnet-group-name my_new_subnet \
  --engine aurora-postgresql \
  --db-instance-class db.t4g.medium
```

Das folgende Beispiel zeigt die teilweise Ausgabe eines solchen Befehls.

```
{
  'DBInstanceIdentifier': 'my_postgres_instance',
  'DBClusterIdentifier': 'my_aurora_postgresql_clone',
  'DBInstanceClass': 'db.t4g.medium',
  'DBInstanceStatus': 'creating'
  ...
}
```

Das folgende Beispiel fügt eine Aurora Serverless v2-DB-Instance zu einem Aurora MySQL-Klon hinzu, der eine benutzerdefinierte DB-Subnetzgruppe verwendet. Um Serverless v2-Instances verwenden zu können, stellen Sie sicher, dass Sie die `--serverless-v2-scaling-configuration` Option für den `restore-db-cluster-to-point-in-time` Befehl angeben, wie in den vorherigen Beispielen gezeigt.

```
aws rds create-db-instance --db-cluster-identifier my_aurora_mysql_clone \
  --db-instance-identifier my_mysql_instance \
  --db-subnet-group-name my_other_new_subnet \
  --engine aurora-mysql \
  --db-instance-class db.serverless
```

Das folgende Beispiel zeigt eine teilweise Ausgabe eines solchen Befehls.

```
{
  'DBInstanceIdentifier': 'my_mysql_instance',
  'DBClusterIdentifier': 'my_aurora_mysql_clone',
  'DBInstanceClass': 'db.serverless',
```

```
  'DBInstanceStatus': 'creating'
  ...
}
```

Schritt 3: Herstellen der Konnektivität zwischen einem Clientsystem und einem Clone

Wenn Sie bereits von einem Clientsystem aus eine Verbindung zu einem Aurora-Cluster herstellen, möchten Sie möglicherweise dieselbe Art von Konnektivität für einen neuen Clone zulassen. Sie können beispielsweise von einer Amazon Cloud9-Instance oder EC2-Instance aus eine Verbindung zum ursprünglichen Cluster herstellen. Um Verbindungen von denselben oder neuen Clientsystemen, die Sie in der Ziel-VPC erstellen, zuzulassen, richten Sie äquivalente DB-Subnetzgruppen und VPC-Sicherheitsgruppen wie in der VPC ein. Geben Sie dann die Subnetzgruppe und die Sicherheitsgruppen an, wenn Sie den Clone erstellen.

In den folgenden Beispielen wird ein Aurora Serverless v2-Clone eingerichtet. Diese Konfiguration basiert auf der Kombination von `--engine-mode provisioned` und `--serverless-v2-scaling-configuration` bei der Erstellung des DB-Clusters und dann `--db-instance-class db.serverless` beim Erstellen jeder DB-Instance im Cluster. Der `provisioned` Engine-Modus ist die Standardeinstellung, sodass Sie diese Option auch weglassen können, wenn Sie dies bevorzugen.

```
aws rds restore-db-cluster-to-point-in-time \
  --source-db-cluster-identifier serverless-sql-postgres\
  --db-cluster-identifier serverless-sql-postgres-clone \
  --db-subnet-group-name 'default-vpc-1234' \
  --vpc-security-group-ids 'sg-4567' \
  --serverless-v2-scaling-configuration 'MinCapacity=0.5,MaxCapacity=16' \
  --restore-type copy-on-write \
  --use-latest-restorable-time
```

Geben Sie dann beim Erstellen der DB-Instances im Clone dieselbe `--db-subnet-group-name` Option an. Optional können Sie die `--availability-zone` Option einbeziehen und eine der AZs angeben, die den Subnetzen in dieser Subnetzgruppe zugeordnet sind. Diese AZ muss auch eine der AZs sein, die dem ursprünglichen Cluster zugeordnet sind.

```
aws rds create-db-instance \
  --db-cluster-identifier serverless-sql-postgres-clone \
  --db-instance-identifier serverless-sql-postgres-clone-instance \
  --db-instance-class db.serverless \
  --db-subnet-group-name 'default-vpc-987zyx654' \
```

```
  --availability-zone 'us-east-1c' \
  --engine aurora-postgresql
```

Verschieben eines Clusters von öffentlichen Subnetzen in private

Sie können das Klonen verwenden, um einen Cluster zwischen öffentlichen und privaten Subnetzen zu migrieren. Sie können dies tun, wenn Sie Ihrer Anwendung zusätzliche Sicherheitsebenen hinzufügen, bevor Sie sie in der Produktion einsetzen. In diesem Beispiel sollten Sie die privaten Subnetze und das NAT-Gateway bereits eingerichtet haben, bevor Sie den Klonvorgang mit Aurora starten.

Für die Schritte, die Aurora betreffen, können Sie dieselben allgemeinen Schritte wie in den vorherigen Beispielen für Sammeln von Informationen über die Netzwerkumgebung und befolgenEinen Aurora-Clone mit neuen Netzwerkeinstellungen erstellen. Der Hauptunterschied besteht darin, dass Sie, selbst wenn Sie über öffentliche Subnetze verfügen, die allen AZs des ursprünglichen Clusters zugeordnet sind, jetzt überprüfen müssen, ob Sie über genügend private Subnetze für einen Aurora-Cluster verfügen und dass diese Subnetze denselben AZs zugeordnet sind, die für Aurora-Speicher im ursprünglichen Cluster verwendet werden. Ähnlich wie bei anderen Anwendungsfällen beim Klonen können Sie die DB-Subnetzgruppe für den Clone entweder mit drei oder zwei privaten Subnetzen erstellen, die den erforderlichen AZs zugeordnet sind. Wenn Sie jedoch zwei private Subnetze in der DB-Subnetzgruppe verwenden, benötigen Sie ein drittes privates Subnetz, das der dritten AZ zugeordnet ist, die für Aurora-Speicher im ursprünglichen Cluster verwendet wird.

Anhand dieser Checkliste können Sie überprüfen, ob alle Voraussetzungen für diese Art von Klonvorgang erfüllt sind.

- Notieren Sie die drei AZs, die dem ursprünglichen Cluster zugeordnet sind. Anweisungen finden Sie unter Schritt 1: Überprüfen Sie die Availability Zones des ursprünglichen Clusters.
- Notieren Sie die drei oder zwei AZs, die den öffentlichen Subnetzen in der DB-Subnetzgruppe für den ursprünglichen Cluster zugeordnet sind. Anweisungen finden Sie unter Schritt 3: Überprüfen Sie die Subnetze des ursprünglichen Clusters.
- Erstellen Sie private Subnetze, die allen drei AZs zugeordnet sind, die dem ursprünglichen Cluster zugeordnet sind. Führen Sie auch alle anderen Netzwerkeinstellungen durch, z. B. die Einrichtung eines NAT-Gateways, um mit den privaten Subnetzen kommunizieren zu können. Anweisungen finden Sie unter Erstellen eines Subnetzes im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

- Erstellen Sie eine neue DB-Subnetzgruppe, die drei oder zwei der privaten Subnetze enthält, die von Anfang an mit den AZs verknüpft sind. Anweisungen finden Sie unter Schritt 2: Erstellen Sie die DB-Subnetzgruppe für den Clone.

Wenn alle Voraussetzungen erfüllt sind, können Sie die Datenbankaktivität auf dem ursprünglichen Cluster unterbrechen, während Sie den Clone erstellen, und Ihre Anwendung so einstellen, dass er verwendet wird. Nachdem der Clone erstellt wurde und Sie sich vergewissert haben, dass Sie eine Verbindung zu ihm herstellen, Ihren Anwendungscode ausführen usw. können, können Sie die Verwendung des ursprünglichen Clusters einstellen.

nd-to-end Beispiel für die Erstellung eines vPC-übergreifenden Klons

Beim Erstellen eines Klons in einer anderen VPC als dem Original werden dieselben allgemeinen Schritte wie in den vorherigen Beispielen verwendet. Da die VPC-ID eine Eigenschaft der Subnetze ist, geben Sie die VPC-ID nicht wirklich als Parameter an, wenn Sie einen der RDS-CLI-Befehle ausführen. Der Hauptunterschied besteht darin, dass Sie mit größerer Wahrscheinlichkeit neue Subnetze, neue Subnetze, die bestimmten AZs zugeordnet sind, eine VPC-Sicherheitsgruppe und eine neue DB-Subnetzgruppe erstellen müssen. Dies gilt insbesondere, wenn dies der erste Aurora-Cluster ist, den Sie in dieser VPC erstellen.

Anhand dieser Checkliste können Sie überprüfen, ob alle Voraussetzungen für die Durchführung dieser Art von Klonvorgang erfüllt sind.

- Notieren Sie die drei AZs, die dem ursprünglichen Cluster zugeordnet sind. Anweisungen finden Sie unter Schritt 1: Überprüfen Sie die Availability Zones des ursprünglichen Clusters.
- Notieren Sie die drei oder zwei AZs, die den Subnetzen in der DB-Subnetzgruppe für den ursprünglichen Cluster zugeordnet sind. Anweisungen finden Sie unter Schritt 2: Überprüfen Sie die DB-Subnetzgruppe des ursprünglichen Clusters.
- Erstellen Sie Subnetze, die allen drei AZs zugeordnet sind, die dem ursprünglichen Cluster zugeordnet sind. Anweisungen finden Sie unter Schritt 1: Erstellen Sie die Subnetze für den Clone.
- Führen Sie eine andere Netzwerkkonfiguration durch, z. B. die Einrichtung einer VPC-Sicherheitsgruppe, für Clientsysteme, Anwendungsserver usw., um mit den DB-Instances im Clone kommunizieren zu können. Anweisungen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen.
- Erstellen Sie eine neue DB-Subnetzgruppe, die drei oder zwei der Subnetze enthält, die den AZs vom ersten Punkt an zugeordnet sind. Anweisungen finden Sie unter Schritt 2: Erstellen Sie die DB-Subnetzgruppe für den Clone.

Wenn alle Voraussetzungen erfüllt sind, können Sie die Datenbankaktivität auf dem ursprünglichen Cluster unterbrechen, während Sie den Clone erstellen, und Ihre Anwendung so einstellen, dass er verwendet wird. Nachdem der Clone erstellt wurde und Sie überprüft haben, ob Sie eine Verbindung zu ihm herstellen, Ihren Anwendungscode ausführen usw. können, können Sie überlegen, ob Sie sowohl das Original als auch die Klone weiterlaufen lassen oder die Verwendung des ursprünglichen Clusters einstellen möchten.

Die folgenden Linux-Beispiele zeigen die Reihenfolge der AWS CLI-Operationen zum Klonen eines Aurora-DB-Clusters von einer VPC auf eine andere. Einige Felder, die für die Beispiele nicht relevant sind, werden in der Befehlsausgabe nicht angezeigt.

Zunächst überprüfen wir die IDs der Quell- und Ziel-VPCs. Der beschreibende Name, den Sie einer VPC bei ihrer Erstellung zuweisen, wird in den VPC-Metadaten als Tag dargestellt.

```
$ aws ec2 describe-vpcs --query '*[].[VpcId,Tags]'
[
    [
        'vpc-0f0c0fc0000b0ffb0',
        [
            {
                'Key': 'Name',
                'Value': 'clone-vpc-source'
            }
        ]
    ],
    [
        'vpc-9e99d9f99a999bd99',
        [
            {
                'Key': 'Name',
                'Value': 'clone-vpc-dest'
            }
        ]
    ]
]
```

Der ursprüngliche Cluster ist bereits in der Quell-VPC vorhanden. Um den Clone mit demselben Satz von AZs für den Aurora-Speicher einzurichten, überprüfen wir die AZs, die vom ursprünglichen Cluster verwendet wurden.

```
$ aws rds describe-db-clusters --db-cluster-identifier original-cluster \
```

```
  --query 'sort_by(*[].AvailabilityZones[].{Zone:@},&Zone)' --output text

us-east-1c
us-east-1d
us-east-1f
```

Wir stellen sicher, dass es Subnetze gibt, die den vom ursprünglichen Cluster verwendeten AZs entsprechen: `us-east-1cus-east-1d`, und`us-east-1f`.

```
$ aws ec2 create-subnet --vpc-id vpc-9e99d9f99a999bd99 \
  --availability-zone us-east-1c --cidr-block 10.0.0.128/28
{
    'Subnet': {
        'AvailabilityZone': 'us-east-1c',
        'SubnetId': 'subnet-3333a33be3ef3e333',
        'VpcId': 'vpc-9e99d9f99a999bd99',
    }
}

$ aws ec2 create-subnet --vpc-id vpc-9e99d9f99a999bd99 \
--availability-zone us-east-1d --cidr-block 10.0.0.160/28
{
    'Subnet': {
        'AvailabilityZone': 'us-east-1d',
        'SubnetId': 'subnet-4eeb444cd44b4d444',
        'VpcId': 'vpc-9e99d9f99a999bd99',
    }
}

$ aws ec2 create-subnet --vpc-id vpc-9e99d9f99a999bd99 \
--availability-zone us-east-1f --cidr-block 10.0.0.224/28
{
    'Subnet': {
        'AvailabilityZone': 'us-east-1f',
        'SubnetId': 'subnet-66eea6666fb66d66c',
        'VpcId': 'vpc-9e99d9f99a999bd99',
    }
}
```

Dieses Beispiel bestätigt, dass es Subnetze gibt, die den erforderlichen AZs in der Ziel-VPC VPC sind.

```
aws ec2 describe-subnets --query 'sort_by(*[] | [?VpcId == `vpc-9e99d9f99a999bd99`] |
```

```
[].{SubnetId:SubnetId,VpcId:VpcId,AvailabilityZone:AvailabilityZone},
 &AvailabilityZone)' --output table

-------------------------------------------------------------------------
|                           DescribeSubnets                             |
+------------------+---------------------------+-------------------------+
| AvailabilityZone |         SubnetId          |          VpcId          |
+------------------+---------------------------+-------------------------+
|  us-east-1a      |  subnet-000ff0e00000c0aea  |  vpc-9e99d9f99a999bd99  |
|  us-east-1b      |  subnet-1111d111111ca11b1  |  vpc-9e99d9f99a999bd99  |
|  us-east-1c      | subnet-3333a33be3ef3e333   |  vpc-9e99d9f99a999bd99  |
|  us-east-1d      | subnet-4eeb444cd44b4d444   |  vpc-9e99d9f99a999bd99  |
|  us-east-1f      | subnet-66eea6666fb66d66c   |  vpc-9e99d9f99a999bd99  |
+------------------+---------------------------+-------------------------+
```

Bevor Sie einen Aurora-DB-Cluster in der VPC erstellen, benötigen Sie eine DB-Subnetzgruppe mit Subnetzen, die den für Aurora-Speicher verwendeten AZs zugeordnet sind. Wenn Sie einen regulären Cluster erstellen, können Sie einen beliebigen Satz von drei AZs verwenden. Wenn Sie einen vorhandenen Cluster klonen, muss die Subnetzgruppe mit mindestens zwei der drei AZs übereinstimmen, die sie für Aurora-Speicher verwendet.

```
$ aws rds create-db-subnet-group \
  --db-subnet-group-name subnet-group-in-other-vpc \
  --subnet-ids
 '["subnet-3333a33be3ef3e333","subnet-4eeb444cd44b4d444","subnet-66eea6666fb66d66c"]' \
  --db-subnet-group-description 'DB subnet group with 3 subnets:
 subnet-3333a33be3ef3e333,subnet-4eeb444cd44b4d444,subnet-66eea6666fb66d66c'

{
    'DBSubnetGroup': {
        'DBSubnetGroupName': 'subnet-group-in-other-vpc',
        'DBSubnetGroupDescription': 'DB subnet group with 3 subnets:
 subnet-3333a33be3ef3e333,subnet-4eeb444cd44b4d444,subnet-66eea6666fb66d66c',
        'VpcId': 'vpc-9e99d9f99a999bd99',
        'SubnetGroupStatus': 'Complete',
        'Subnets': [
            {
                'SubnetIdentifier': 'subnet-4eeb444cd44b4d444',
                'SubnetAvailabilityZone': { 'Name': 'us-east-1d' }
            },
            {
                'SubnetIdentifier': 'subnet-3333a33be3ef3e333',
                'SubnetAvailabilityZone': { 'Name': 'us-east-1c' }
```

```
            },
            {
                'SubnetIdentifier': 'subnet-66eea6666fb66d66c',
                'SubnetAvailabilityZone': { 'Name': 'us-east-1f' }
            }
        ]
    }
}
```

Jetzt sind die Subnetze und die DB-Subnetzgruppe vorhanden. Das folgende Beispiel zeigt, `restore-db-cluster-to-point-in-time` dass der Cluster geklont wird. Die `--db-subnet-group-name` Option ordnet den Clone dem richtigen Satz von Subnetzen zu, die dem richtigen Satz von AZs aus dem ursprünglichen Cluster zugeordnet sind.

```
$ aws rds restore-db-cluster-to-point-in-time \
  --source-db-cluster-identifier original-cluster \
  --db-cluster-identifier clone-in-other-vpc \
  --restore-type copy-on-write --use-latest-restorable-time \
  --db-subnet-group-name subnet-group-in-other-vpc

{
  'DBClusterIdentifier': 'clone-in-other-vpc',
  'DBSubnetGroup': 'subnet-group-in-other-vpc',
  'Engine': 'aurora-postgresql',
  'EngineVersion': '15.4',
  'Status': 'creating',
  'Endpoint': 'clone-in-other-vpc.cluster-c0abcdef.us-east-1.rds.amazonaws.com'
}
```

Das folgende Beispiel bestätigt, dass der Aurora-Speicher im Clone denselben Satz von AZs wie im ursprünglichen Cluster verwendet.

```
$ aws rds describe-db-clusters --db-cluster-identifier clone-in-other-vpc \
  --query 'sort_by(*[].AvailabilityZones[].{Zone:@},&Zone)' --output text

us-east-1c
us-east-1d
us-east-1f
```

Zu diesem Zeitpunkt können Sie DB-Instances für den Clone erstellen. Stellen Sie sicher, dass die jeder Instance zugeordnete VPC-Sicherheitsgruppe Verbindungen aus den IP-Adressbereichen zulässt, die Sie für die EC2-Instances, Anwendungsserver usw. in der Ziel-VPC verwenden.

Kontoübergreifendes Klonen mit AWS RAM und Amazon Aurora

Wenn Sie AWS Resource Access Manager (AWS RAM) mit Amazon Aurora verwenden, können Sie Aurora-DB-Cluster und -Clones, die zu Ihrem AWS Konto gehören, mit einem anderen AWS Konto oder einer anderen Organisation teilen. Ein solches kontoübergreifendes Klonen ist viel schneller als das Erstellen und Wiederherstellen eines Datenbank-Snapshots. Sie können einen Klon eines Ihrer Aurora-DB-Cluster erstellen und den Klon freigeben. Oder Sie können Ihren Aurora-DB-Cluster mit einem anderen AWS Konto teilen und den Kontoinhaber den Clone erstellen lassen. Welchen Ansatz Sie wählen, hängt von Ihrem Anwendungsfall ab.

Beispielsweise müssen Sie möglicherweise regelmäßig einen Klon Ihrer Finanzdatenbank für das interne Revisionsteam Ihres Unternehmens freigeben. In diesem Fall hat Ihr Prüfungsteam ein eigenes AWS -Konto für die von ihm verwendeten Anwendungen. Sie können dem AWS Konto des Prüfungsteams die Erlaubnis erteilen, auf Ihren Aurora-DB-Cluster zuzugreifen und ihn nach Bedarf zu klonen.

Auf der anderen Seite, wenn ein externer Anbieter Ihre Finanzdaten prüft, ziehen Sie es möglicherweise vor, den Klon selbst zu erstellen. Sie geben dann dem externen Anbieter nur Zugriff auf den Klon.

Sie können auch kontenübergreifendes Klonen verwenden, um viele der gleichen Anwendungsfälle für das Klonen innerhalb desselben AWS Kontos zu unterstützen, z. B. Entwicklung und Testen. Beispielsweise könnte Ihre Organisation unterschiedliche AWS Konten für Produktion, Entwicklung, Tests usw. verwenden. Weitere Informationen finden Sie unter Übersicht über das Aurora-Klonen.

Daher möchten Sie vielleicht einen Clone mit einem anderen Konto teilen oder einem anderen AWS Konto erlauben, Klone Ihrer Aurora-DB-Cluster zu erstellen. AWS Verwenden Sie in beiden Fällen zunächst, AWS RAM um ein Share-Objekt zu erstellen. Vollständige Informationen zur gemeinsamen Nutzung von AWS Ressourcen zwischen AWS Konten finden Sie im AWS RAM Benutzerhandbuch.

Zum Erstellen eines kontoübergreifenden Clones sind Aktionen von dem AWS Konto, dem der ursprüngliche Cluster gehört, und von dem AWS Konto, das den Clone erstellt, erforderlich. Zuerst ändert der ursprüngliche Clusterbesitzer den Cluster, um es einem oder mehreren anderen Konten zu ermöglichen, ihn zu klonen. Wenn sich eines der Konten in einer anderen AWS Organisation befindet, wird eine Einladung zum Teilen AWS generiert. Das andere Konto muss die Einladung

annehmen, bevor Sie fortfahren können. Dann kann jedes autorisierte Konto den Cluster klonen. Während dieses Prozesses wird der Cluster durch seinen eindeutigen Amazon-Ressourcennamen (ARN) identifiziert.

Wie beim Klonen innerhalb desselben AWS Kontos wird zusätzlicher Speicherplatz nur verwendet, wenn die Quelle oder der Klon Änderungen an den Daten vornehmen. Zu diesem Zeitpunkt werden dann Gebühren für die Speicherung erhoben. Wenn der Quellen-Cluster gelöscht wird, werden Speicherkosten gleichmäßig auf die verbleibenden geklonten Cluster verteilt.

Themen

Einschränkungen für kontoübergreifendes Klonen

Kontoübergreifendes Aurora-Klonen hat folgende Einschränkungen:

- Sie können einen Aurora Serverless v1 Cluster nicht für mehrere AWS Konten klonen.
- Sie können keine Einladungen zu gemeinsam genutzten Ressourcen mit dem anzeigen oder annehmen AWS Management Console. Verwenden Sie die AWS CLI, die Amazon RDS-API oder die AWS RAM Konsole, um Einladungen zu gemeinsam genutzten Ressourcen anzuzeigen und anzunehmen.
- Sie können nur einen neuen Klon aus einem Klon erstellen, der mit Ihrem AWS Konto geteilt wurde.
- Sie können keine Ressourcen (Klone oder Aurora-DB-Cluster) teilen, die mit Ihrem AWS Konto geteilt wurden.
- Sie können maximal 15 kontoübergreifende Klone aus einem einzelnen Aurora-DB-Cluster erstellen.
- Jeder der 15 kontoübergreifenden Klone muss einem anderen Konto gehören. AWS Das heißt, Sie können innerhalb eines Kontos nur einen kontenübergreifenden Klon eines Clusters erstellen. AWS
- Nachdem Sie einen Cluster geklont haben, werden der ursprüngliche Cluster und sein Klon als identisch angesehen, um Grenzwerte für kontoübergreifende Klone durchzusetzen. Sie können innerhalb desselben Kontos keine kontenübergreifenden Klone sowohl des ursprünglichen Clusters als auch des geklonten Clusters erstellen. AWS Die Gesamtzahl der kontoübergreifenden Klone für den ursprünglichen Cluster und einen seiner Klone darf 15 nicht überschreiten.

- Sie können einen Aurora-DB-Cluster nicht mit anderen AWS Konten teilen, es sei denn, der Cluster befindet sich in einem `ACTIVE` Status.
- Sie können einen Aurora-DB-Cluster, der mit anderen AWS Konten geteilt wurde, nicht umbenennen.
- Sie können keinen kontoübergreifenden Klon eines Clusters erstellen, der mit dem RDS-Standardschlüssel verschlüsselt ist.
- Sie können in einem AWS Konto keine unverschlüsselten Klone aus verschlüsselten Aurora-DB-Clustern erstellen, die von einem anderen AWS Konto gemeinsam genutzt wurden. Der Clustereigentümer muss die Erlaubnis zum Zugriff auf den Quellcluster AWS KMS key. Sie können jedoch auch einen anderen Schlüssel verwenden, wenn Sie den Klon erstellen.

Erlauben Sie anderen AWS Konten, Ihren Cluster zu klonen

Um anderen AWS Konten das Klonen eines Clusters zu ermöglichen, dessen Eigentümer Sie sind, legen AWS RAM Sie die Freigabeberechtigung fest. Dadurch wird auch eine Einladung an jedes der anderen Konten gesendet, die sich in einer anderen AWS Organisation befinden.

Informationen zur gemeinsamen Nutzung von Ressourcen, die Ihnen gehören, in der AWS RAM Konsole finden Sie im AWS RAM Benutzerhandbuch unter Gemeinsame Nutzung von Ressourcen, die Ihnen gehören.

Themen

- Erteilen Sie anderen AWS Konten die Erlaubnis, Ihren Cluster zu klonen
- Prüfen Sie, ob ein Cluster, den Sie besitzen, mit anderen AWS Konten geteilt wird

Erteilen Sie anderen AWS Konten die Erlaubnis, Ihren Cluster zu klonen

Wenn der Cluster, den Sie gemeinsam nutzen, verschlüsselt ist, teilen Sie auch die AWS KMS key für den Cluster. Sie können AWS Identity and Access Management (IAM-) Benutzern oder Rollen in einem AWS Konto erlauben, einen KMS-Schlüssel in einem anderen Konto zu verwenden.

Dazu fügen Sie zunächst das externe Konto (Root-Benutzer) zur Schlüsselrichtlinie des KMS-Schlüssels hinzu. AWS KMS Sie fügen der Schlüsselrichtlinie nicht die einzelnen Benutzer oder Rollen hinzu, sondern nur das externe Konto, das sie enthält. Sie können nur einen von Ihnen erstellten KMS-Schlüssel freigeben, nicht den Standardschlüssel des RDS-Dienstes. Informationen zur Zugriffskontrolle für KMS-Schlüssel finden Sie unter Authentifizierung und Zugriffskontrolle für AWS KMS.

Konsole

So gewähren Sie die Berechtigung zum Klonen Ihres Clusters

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den DB-Cluster aus, den Sie freigeben möchten, um seine Details-Seite anzuzeigen, und wählen Sie dann die Registerkarte Connectivity & security (Konnektivität und Sicherheit) aus.
4. Geben Sie im Abschnitt DB-Cluster mit anderen AWS Konten teilen die numerische Konto-ID für das AWS Konto ein, dem Sie das Klonen dieses Clusters erlauben möchten. Bei Konto-IDs in derselben Organisation können Sie die ersten Zeichen in das Feld eintippen und dann aus dem Menü auswählen.

   > **Important**
   >
   > In manchen Fällen möchten Sie vielleicht, dass ein Konto, das sich nicht in derselben AWS -Organisation befindet wie Ihr Konto, einen Cluster klont. In diesen Fällen meldet die Konsole aus Sicherheitsgründen nicht, wer diese Konto-ID besitzt oder ob das Konto existiert.
   > Seien Sie vorsichtig bei der Eingabe von Kontonummern, die sich nicht in derselben AWS Organisation wie Ihr AWS Konto befinden. Überprüfen Sie sofort, ob Sie die Freigabe für das beabsichtigte Konto erteilt haben.

5. Überprüfen Sie auf der Bestätigungsseite, dass die von Ihnen angegebene Konto-ID richtig ist. Geben Sie im Bestätigungsfeld `share` ein, um dies zu bestätigen.

   Auf der Detailseite wird unter Konten, mit denen dieser DB-Cluster gemeinsam genutzt wird, ein Eintrag mit der angegebenen AWS Konto-ID angezeigt. Die Spalte Status zeigt ursprünglich den Status Pending (Ausstehend) an.
6. Wenden Sie sich an den Besitzer des anderen AWS Kontos, oder melden Sie sich bei diesem Konto an, wenn Sie beide besitzen. Weisen Sie den Besitzer des anderen Kontos an, die Freigabeeinladung anzunehmen und den DB-Cluster zu klonen, wie nachfolgend beschrieben.

AWS CLI

So gewähren Sie die Berechtigung zum Klonen Ihres Clusters

1. Tragen Sie die Daten für die erforderlichen Parameter zusammen. Sie benötigen den ARN für Ihren Cluster und die numerische ID für das andere AWS Konto.
2. Führen Sie den AWS RAM CLI-Befehl aus `create-resource-share`.

   Für LinuxmacOS, oderUnix:

   ```
   aws ram create-resource-share --name descriptive_name \
     --region region \
     --resource-arns cluster_arn \
     --principals other_account_ids
   ```

   Windows:

   ```
   aws ram create-resource-share --name descriptive_name ^
     --region region ^
     --resource-arns cluster_arn ^
     --principals other_account_ids
   ```

   Geben Sie, um mehrere Konto-IDs für den `--principals`-Parameter einzuschließen, IDs mit Leerzeichen voneinander getrennt ein. Um anzugeben, ob die genehmigten Konto-IDs außerhalb Ihrer AWS -Organisation sein können, schließen Sie auch den `--allow-external-principals`- bzw. den `--no-allow-external-principals`-Parameter für `create-resource-share` ein.

AWS RAM API

So gewähren Sie die Berechtigung zum Klonen Ihres Clusters

1. Tragen Sie die Daten für die erforderlichen Parameter zusammen. Sie benötigen den ARN für Ihren Cluster und die numerische ID für das andere AWS Konto.
2. Rufen Sie die AWS RAM API-Operation CreateResourceShare auf und geben Sie die folgenden Werte an:

   - Geben Sie die Konto-ID für ein oder mehrere AWS Konten als `principals` Parameter an.
   - Geben Sie die ARN mindestens eines Aurora-DB-Clusters als `resourceArns`-Parameter an.

- Geben Sie an, ob sich die genehmigten Konto-IDs außerhalb Ihrer AWS -Organisation befinden dürfen, indem Sie einen booleschen Wert für den `allowExternalPrincipals`-Parameter einfügen.

Neuerstellen eines Clusters, der den RDS-Standardschlüssel verwendet

Wenn der verschlüsselte Cluster, den Sie freigeben möchten, den RDS-Standardschlüssel verwendet, stellen Sie sicher, dass der Cluster neu erstellt wird. Erstellen Sie dazu einen manuellen Snapshot Ihres DB-Clusters, verwenden Sie eine AWS KMS key, und stellen Sie den Cluster dann in einem neuen Cluster wieder her. Geben Sie dann den neuen Cluster frei. Führen Sie die folgenden Schritte aus, um diesen Vorgang durchzuführen.

So erstellen Sie einen verschlüsselten Cluster neu, der den RDS-Standardschlüssel verwendet

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots aus.
3. Wählen Sie Ihren Snapshot aus.
4. Wählen Sie unter Actions (Aktionen) die Option Copy Snapshot (Snapshot kopieren) und anschließend Enable encryption (Verschlüsselung aktivieren) aus.
5. Wählen Sie für AWS KMS key den neuen Verschlüsselungscode, den Sie verwenden möchten.
6. Stellen Sie den kopierten Snapshot wieder her. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot. Die neue DB-Instance verwendet Ihren neuen Verschlüsselungsschlüssel.
7. (Optional) Löschen Sie den alten DB-Cluster, wenn Sie ihn nicht mehr benötigen. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Löschen eines DB-Cluster-Snapshots. Bevor Sie dies tun, überprüfen Sie, ob Ihr neuer Cluster über alle notwendigen Daten verfügt und ob Ihre Anwendung erfolgreich darauf zugreifen kann.

Prüfen Sie, ob ein Cluster, den Sie besitzen, mit anderen AWS Konten geteilt wird

Sie können überprüfen, ob andere Benutzer die Berechtigung für die Freigabe eines Clusters haben. Dies kann hilfreich sein, um zu wissen, ob der Cluster sich dem Limit für die maximale Anzahl an kontoübergreifenden Klonen nähert.

Die Verfahren zur gemeinsamen Nutzung von Ressourcen mithilfe der AWS RAM Konsole finden Sie im AWS RAM Benutzerhandbuch unter Gemeinsame Nutzung von Ressourcen, die Ihnen gehören.

AWS CLI

Finden Sie heraus, ob ein Cluster, den Sie besitzen, mit anderen AWS Konten gemeinsam genutzt wird

- Rufen Sie den AWS RAM CLI-Befehl `list-principals`auf und verwenden Sie dabei Ihre Konto-ID als Ressourcenbesitzer und den ARN Ihres Clusters als Ressourcen-ARN. Sie können mit dem folgenden Befehl alle Freigaben anzeigen. Die Ergebnisse geben an, welche AWS Konten den Cluster klonen dürfen.

```
aws ram list-principals \
    --resource-arns your_cluster_arn \
    --principals your_aws_id
```

AWS RAM API

Um herauszufinden, ob ein Cluster, den Sie besitzen, mit anderen AWS Konten geteilt wird

- Rufen Sie den AWS RAM API-Vorgang auf ListPrincipals. Verwenden Sie Ihre Konto-ID als Ressourcenbesitzer und den ARN Ihres Clusters als Ressourcen-ARN.

Einen Cluster klonen, der einem anderen AWS Konto gehört

Um einen Cluster zu klonen, der einem anderen AWS Konto gehört, holen Sie sich AWS RAM die Erlaubnis ein, den Klon zu erstellen. Wenn Sie die erforderliche Berechtigung haben, verwenden Sie das Standardverfahren zum Klonen eines Aurora-Clusters.

Sie können auch überprüfen, ob es sich bei einem Cluster, den Sie besitzen, um einen Klon eines Clusters handelt, der einem anderen AWS Konto gehört.

Informationen zu den Verfahren für die Arbeit mit Ressourcen, die anderen Benutzern gehören, AWS RAM finden Sie im AWS RAM Benutzerhandbuch unter Zugreifen auf Ressourcen, die mit Ihnen geteilt wurden.

Themen

- Einladungen zum Klonen von Clustern anzeigen, die anderen AWS Konten gehören

- Annahme von Einladungen zur gemeinsamen Nutzung von Clustern, die anderen AWS Konten gehören
- Einen Aurora-Cluster klonen, der einem anderen AWS Konto gehört
- Überprüfen, ob ein DB-Cluster ein kontoübergreifender Klon ist

Einladungen zum Klonen von Clustern anzeigen, die anderen AWS Konten gehören

Um mit Einladungen zum Klonen von Clustern zu arbeiten, die AWS Konten in anderen AWS Organisationen gehören AWS CLI, verwenden Sie die, die AWS RAM Konsole oder die AWS RAM API. Aktuell können Sie dieses Verfahren nicht mithilfe der Amazon RDS-Konsole durchführen.

Die Verfahren zur Verwendung von Einladungen in der AWS RAM Konsole finden Sie im AWS RAM Benutzerhandbuch unter Zugreifen auf Ressourcen, die mit Ihnen geteilt wurden.

AWS CLI

Um Einladungen zum Klonen von Clustern anzuzeigen, die anderen AWS Konten gehören

1. Führen Sie den AWS RAM CLI-Befehl aus `get-resource-share-invitations`.

   ```
   aws ram get-resource-share-invitations --region region_name
   ```

   Die Ergebnisse des vorausgehenden Befehls zeigen alle Einladungen, Cluster zu klonen, an, einschließlich aller Einladungen, die Sie bereits angenommen oder abgelehnt haben.
2. (Optional) Filtern Sie die Liste, um nur die Einladungen anzuzeigen, die eine Aktion Ihrerseits erforderlich machen. Fügen Sie dafür den -Parameter hinz `--query 'resourceShareInvitations[?status==`PENDING`]'`.

AWS RAM API

Um Einladungen zum Klonen von Clustern zu sehen, die anderen AWS Konten gehören

1. Rufen Sie den AWS RAM API-Vorgang auf `GetResourceShareInvitations`. Diese Operation gibt all diese Einladungen zurück, einschließlich derer, die Sie bereits angenommen oder abgelehnt haben.
2. (Optional) Suchen Sie nur die Einladungen, die eine Aktion Ihrerseits erforderlich machen, indem Sie das Rückgabefeld `resourceShareAssociations` für den `status`-Wert `PENDING` aktivieren.

Annahme von Einladungen zur gemeinsamen Nutzung von Clustern, die anderen AWS Konten gehören

Sie können Einladungen zur gemeinsamen Nutzung von Clustern annehmen, die anderen AWS Konten gehören, die sich in anderen AWS Organisationen befinden. Verwenden Sie die APIs, die AWS RAM und die AWS CLI RDS-APIs oder die AWS RAM Konsole, um mit diesen Einladungen zu arbeiten. Aktuell können Sie dieses Verfahren nicht mithilfe der RDS-Konsole durchführen.

Die Verfahren zur Verwendung von Einladungen in der AWS RAM Konsole finden Sie im AWS RAM Benutzerhandbuch unter Zugreifen auf mit Ihnen geteilte Ressourcen.

AWS CLI

So nehmen Sie eine Einladung zur gemeinsamen Nutzung eines Clusters von einem anderen AWS Konto aus an

1. Suchen Sie den Einladungs-ARN, indem Sie den AWS RAM CLI-Befehl ausführen `get-resource-share-invitations`, wie oben gezeigt.
2. Nehmen Sie die Einladung an, indem Sie den AWS RAM CLI-Befehl aufrufen `accept-resource-share-invitation`, wie im Folgenden gezeigt.

   Für LinuxmacOS, oderUnix:

   ```
   aws ram accept-resource-share-invitation \
     --resource-share-invitation-arn invitation_arn \
     --region region
   ```

   Windows:

   ```
   aws ram accept-resource-share-invitation ^
     --resource-share-invitation-arn invitation_arn ^
     --region region
   ```

AWS RAM und RDS-API

So nehmen Sie Einladung zur Freigabe eines Clusters, der jemand anderem gehört, an

1. Suchen Sie den Einladungs-ARN, indem Sie den AWS RAM API-Vorgang aufrufen `GetResourceShareInvitations`, wie oben gezeigt.

2. Übergeben Sie diesen ARN als `resourceShareInvitationArn` Parameter an den RDS-API-Vorgang AcceptResourceShareInvitation.

Einen Aurora-Cluster klonen, der einem anderen AWS Konto gehört

Nachdem Sie die Einladung von dem AWS Konto angenommen haben, dem der DB-Cluster gehört, wie oben gezeigt, können Sie den Cluster klonen.

Konsole

Um einen Aurora-Cluster zu klonen, der einem anderen AWS Konto gehört

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.

   Ganz oben in der Datenbankliste sollten Sie mindestens ein Element mit dem Role (Rolle)-Wert `Shared from account #account_id` sehen. Aus Sicherheitsgründen können Sie nur eingeschränkte Informationen über die ursprünglichen Cluster sehen. Die Eigenschaften, die Sie sehen können, sind solche wie etwa die Datenbank-Engine und -Version, die in Ihrem geklonten Cluster identisch sein müssen.
3. Wählen Sie den Cluster aus, den Sie vorhaben zu klonen.
4. Wählen Sie für Actions (Aktionen) Create clone (Klon erstellen) aus.
5. Gehen Sie entsprechend dem Verfahren unter Konsole vor, um die Einrichtung des geklonten Clusters durchzuführen.
6. Aktivieren Sie je nach Bedarf die Verschlüsselung für den geklonten Cluster. Wenn der Cluster, den Sie klonen, verschlüsselt ist, müssen Sie die Verschlüsselung für den geklonten Cluster aktivieren. Das AWS -Konto, das den Cluster für Sie freigegeben hat, muss auch den KMS-Schlüssel freigeben, der zur Verschlüsselung des Clusters verwendet wurde. Sie können denselben KMS-Schlüssel zur Verschlüsselung des Klons verwenden oder Ihren eigenen KMS-Schlüssel. Sie können keinen kontoübergreifenden Klon für einen Cluster erstellen, der mit dem Standard-KMS-Schlüssel verschlüsselt ist.

   Das Konto, dem der Verschlüsselungsschlüssel gehört, muss dem Zielkonto die Berechtigung zur Verwendung des Schlüssels mithilfe einer Schlüsselrichtlinie erteilen. Dieser Vorgang ist ähnlich dem Verfahren, mit dem verschlüsselte Snapshots freigegeben werden, mithilfe einer Schlüsselrichtlinie, die dem Zielkonto die Berechtigung zur Verwendung des Schlüssels gewährt.

AWS CLI

Um einen Aurora-Cluster zu klonen, der einem anderen AWS Konto gehört

1. Nehmen Sie die Einladung von dem AWS Konto an, dem der DB-Cluster gehört, wie oben gezeigt.
2. Klonen Sie den Cluster, indem Sie den vollständigen ARN des Quell-Clusters im `source-db-cluster-identifier`-Parameter des RDS-CLI-Befehls `restore-db-cluster-to-point-in-time` angeben, wie nachfolgend gezeigt.

   Wenn der als `source-db-cluster-identifier` übergebene ARN nicht freigegeben wurde, wird derselbe Fehler zurückgegeben, wie wenn der angegebene Cluster nicht vorhanden ist.

   Für LinuxmacOS, oderUnix:

   ```
   aws rds restore-db-cluster-to-point-in-time \
     --source-db-cluster-identifier=arn:aws:rds:arn_details \
     --db-cluster-identifier=new_cluster_id \
     --restore-type=copy-on-write \
     --use-latest-restorable-time
   ```

   Windows:

   ```
   aws rds restore-db-cluster-to-point-in-time ^
     --source-db-cluster-identifier=arn:aws:rds:arn_details ^
     --db-cluster-identifier=new_cluster_id ^
     --restore-type=copy-on-write ^
     --use-latest-restorable-time
   ```

3. Wenn der Cluster, den Sie klonen, verschlüsselt ist, verschlüsseln Sie Ihren geklonten Cluster, indem Sie einen `kms-key-id`-Parameter einfügen. Dieser `kms-key-id`-Wert kann derselbe sein, der zur Verschlüsselung des ursprünglichen DB-Clusters verwendet wurde, oder Ihr eigener KMS-Schlüssel. Ihr Konto muss über die Berechtigung zum Verwenden dieses Verschlüsselungsschlüssels verfügen.

   Für LinuxmacOS, oderUnix:

   ```
   aws rds restore-db-cluster-to-point-in-time \
     --source-db-cluster-identifier=arn:aws:rds:arn_details \
     --db-cluster-identifier=new_cluster_id \
   ```

```
  --restore-type=copy-on-write \
  --use-latest-restorable-time \
  --kms-key-id=arn:aws:kms:arn_details
```

Windows:

```
aws rds restore-db-cluster-to-point-in-time ^
  --source-db-cluster-identifier=arn:aws:rds:arn_details ^
  --db-cluster-identifier=new_cluster_id ^
  --restore-type=copy-on-write ^
  --use-latest-restorable-time ^
  --kms-key-id=arn:aws:kms:arn_details
```

Das Konto, dem der Verschlüsselungsschlüssel gehört, muss dem Zielkonto die Berechtigung zur Verwendung des Schlüssels mithilfe einer Schlüsselrichtlinie erteilen. Dieser Vorgang ist ähnlich dem Verfahren, mit dem verschlüsselte Snapshots freigegeben werden, mithilfe einer Schlüsselrichtlinie, die dem Zielkonto die Berechtigung zur Verwendung des Schlüssels gewährt. Nachfolgend sehen Sie ein Beispiel für eine Schlüsselrichtlinie.

```
{
  "Id": "key-policy-1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::account_id:user/KeyUser",
        "arn:aws:iam::account_id:root"
      ]},
      "Action": [
        "kms:CreateGrant",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow attachment of persistent resources",
```

```
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::account_id:user/KeyUser",
        "arn:aws:iam::account_id:root"
      ]},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
    }
  ]
}
```

> **Note**
>
> Der AWS -CLI-Befehl restore-db-cluster-to-point-in-time stellt nur das DB-Cluster wieder her, nicht die DB-Instances für dieses DB-Cluster. Um DB-Instances für den wiederhergestellten DB-Cluster zu erstellen, rufen Sie den Befehl create-db-instance auf. Geben Sie die ID des wiederhergestellten DB-Clusters in `--db-cluster-identifier` an.
> Sie können DB-Instances erst dann erstellen, wenn der Befehl `restore-db-cluster-to-point-in-time` abgeschlossen ist und der DB-Cluster verfügbar ist.

RDS-API

Um einen Aurora-Cluster zu klonen, der einem anderen AWS Konto gehört

1. Nehmen Sie die Einladung von dem AWS Konto an, dem der DB-Cluster gehört, wie oben gezeigt.
2. Klonen Sie den Cluster, indem Sie den vollständigen ARN des Quell-Clusters im `SourceDBClusterIdentifier`-Parameter der RDS-API-Operation `RestoreDBClusterToPointInTime` angeben.

   Wenn der als `SourceDBClusterIdentifier` übergebene ARN nicht freigegeben wurde, dann wird derselbe Fehler zurückgegeben, wie wenn der angegebene Cluster nicht vorhanden ist.

3. Wenn der Cluster, den Sie klonen, verschlüsselt ist, fügen Sie einen `KmsKeyId`-Parameter ein, um Ihren geklonten Cluster zu verschlüsseln. Dieser `kms-key-id`-Wert kann derselbe sein, der zur Verschlüsselung des ursprünglichen DB-Clusters verwendet wurde, oder Ihr eigener KMS-Schlüssel. Ihr Konto muss über die Berechtigung zum Verwenden dieses Verschlüsselungsschlüssels verfügen.

   Wenn Sie ein Volume klonen, muss das Zielkonto die Berechtigung haben, den Verschlüsselungsschlüssel zu verwenden, der zum Verschlüsseln des Quellclusters verwendet wird. Aurora verschlüsselt den neuen geklonten Cluster mit dem in `KmsKeyId` angegebenen Verschlüsselungsschlüssel.

   Das Konto, dem der Verschlüsselungsschlüssel gehört, muss dem Zielkonto die Berechtigung zur Verwendung des Schlüssels mithilfe einer Schlüsselrichtlinie erteilen. Dieser Vorgang ist ähnlich dem Verfahren, mit dem verschlüsselte Snapshots freigegeben werden, mithilfe einer Schlüsselrichtlinie, die dem Zielkonto die Berechtigung zur Verwendung des Schlüssels gewährt. Nachfolgend sehen Sie ein Beispiel für eine Schlüsselrichtlinie.

```
{
  "Id": "key-policy-1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::account_id:user/KeyUser",
        "arn:aws:iam::account_id:root"
      ]},
      "Action": [
        "kms:CreateGrant",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow attachment of persistent resources",
      "Effect": "Allow",
```

```
      "Principal": {"AWS": [
        "arn:aws:iam::account_id:user/KeyUser",
        "arn:aws:iam::account_id:root"
      ]},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
    }
  ]
}
```

> **Note**
>
> Der RDS-API-Vorgang RestoreDB ClusterTo PointIn Time stellt nur den DB-Cluster wieder her, nicht die DB-Instances für diesen DB-Cluster. Um DB-Instances für den wiederhergestellten DB-Cluster zu erstellen, rufen Sie die RDS-API-Operation CreateDBInstance auf. Geben Sie die ID des wiederhergestellten DB-Clusters in `DBClusterIdentifier` an. Sie können DB-Instances erst erstellen, nachdem die Operation `RestoreDBClusterToPointInTime` abgeschlossen ist und der DB-Cluster verfügbar ist.

Überprüfen, ob ein DB-Cluster ein kontoübergreifender Klon ist

Das `DBClusters`-Objekt gibt an, ob der jeweilige Cluster ein kontoübergreifender Klon ist. Sie können die Cluster, für die Sie die Berechtigungen zum Klonen haben, anzeigen, indem Sie die `include-shared`-Option beim Ausführen des RDS-CLI-Befehls `describe-db-clusters` verwenden. Sie können jedoch die meisten Konfigurationsdetails für solche Cluster nicht anzeigen.

AWS CLI

Überprüfen, ob ein DB-Cluster ein kontoübergreifender Klon ist

- Rufen Sie den RDS-CLI-Befehl auf `describe-db-clusters`.

Das folgende Beispiel zeigt, wie tatsächliche oder potenzielle kontoübergreifende Klon-DB-Cluster in der `describe-db-clusters`-Ausgabe angezeigt werden. Bei vorhandenen Clustern, die Ihrem AWS Konto gehören, gibt das `CrossAccountClone` Feld an, ob es sich bei dem Cluster um einen Klon eines DB-Clusters handelt, der einem anderen Konto gehört. AWS

In einigen Fällen kann ein Eintrag in dem `DBClusterArn` Feld eine andere AWS Kontonummer als Ihre haben. In diesem Fall steht dieser Eintrag für einen Cluster, der einem anderen AWS Konto gehört und den Sie klonen können. Solche Einträge haben wenige andere Felder als `DBClusterArn`. Wenn Sie einen geklonten Cluster erstellen, geben Sie dieselben `StorageEncrypted`-, `Engine`- und `EngineVersion`-Werte wie im Original-Cluster an.

```
$aws rds describe-db-clusters --include-shared --region us-east-1
{
  "DBClusters": [
      {
          "EarliestRestorableTime": "2023-02-01T21:17:54.106Z",
          "Engine": "aurora-mysql",
          "EngineVersion": "8.0.mysql_aurora.3.02.0",
          "CrossAccountClone": false,
...
      },
      {
          "EarliestRestorableTime": "2023-02-09T16:01:07.398Z",
          "Engine": "aurora-mysql",
          "EngineVersion": "8.0.mysql_aurora.3.02.0",
          "CrossAccountClone": true,
...
      },
      {
          "StorageEncrypted": false,
          "DBClusterArn": "arn:aws:rds:us-east-1:12345678:cluster:cluster-
abcdefgh",
          "Engine": "aurora-mysql",
          "EngineVersion": "8.0.mysql_aurora.3.02.0
  ]
}
```

RDS-API

Überprüfen, ob ein DB-Cluster ein kontoübergreifender Klon ist

- Rufen Sie die RDS-API-Operation DescribeDBClusters auf.

  Bei vorhandenen Clustern, die Ihrem AWS Konto gehören, gibt das `CrossAccountClone` Feld an, ob es sich bei dem Cluster um einen Klon eines DB-Clusters handelt, der einem anderen AWS Konto gehört. Einträge mit einer anderen AWS Kontonummer im `DBClusterArn` Feld stehen für Cluster, die Sie klonen können und die anderen AWS Konten gehören. Diese Einträge haben wenige andere Felder als `DBClusterArn`. Wenn Sie einen geklonten Cluster erstellen, geben Sie dieselben `StorageEncrypted`-, `Engine`- und `EngineVersion`-Werte wie im Original-Cluster an.

  Das folgende Beispiel zeigt einen Rückgabewert, der sowohl tatsächliche als auch potenzielle geklonte Cluster zeigt.

```
{
  "DBClusters": [
      {
          "EarliestRestorableTime": "2023-02-01T21:17:54.106Z",
          "Engine": "aurora-mysql",
          "EngineVersion": "8.0.mysql_aurora.3.02.0",
          "CrossAccountClone": false,
...
      },
      {
          "EarliestRestorableTime": "2023-02-09T16:01:07.398Z",
          "Engine": "aurora-mysql",
          "EngineVersion": "8.0.mysql_aurora.3.02.0",
          "CrossAccountClone": true,
...
      },
      {
          "StorageEncrypted": false,
          "DBClusterArn": "arn:aws:rds:us-east-1:12345678:cluster:cluster-
abcdefgh",
          "Engine": "aurora-mysql",
          "EngineVersion": "8.0.mysql_aurora.3.02.0"
      }
  ]
```

```
}
```

Integrieren von Aurora in anderen AWS-Services

Integrieren Sie Amazon Aurora in andere AWS-Services, damit Sie Ihren Aurora-DB-Cluster erweitern können, um zusätzliche Funktionen in der AWS Cloud zu verwenden.

Themen

Integrieren von AWS-Services mit Amazon Aurora MySQL

Amazon Aurora MySQL ist auch in anderen AWS-Services integriert, damit Sie Ihren Aurora-MySQL-DB-Cluster erweitern können, um zusätzliche Funktionen in der AWS Cloud zu verwenden. Ihr Aurora-MySQL-DB-Cluster kann AWS-Services verwenden, um Folgendes durchzuführen:

- Rufen Sie synchron oder asynchron eine AWS Lambda-Funktion mit den nativen Funktionen `lambda_sync` oder `lambda_async` auf. Oder rufen Sie asynchron eine AWS Lambda-Funktion mit der Prozedur `mysql.lambda_async` auf.
- Laden Sie Daten aus Text- und XML-Dateien, die in einem Amazon S3-Bucket gespeichert sind, mithilfe des Befehls `LOAD DATA FROM S3` oder `LOAD XML FROM S3` in Ihren DB-Cluster.
- Speichern Sie Daten in die Textdateien, die in einem Amazon S3-Bucket aus Ihrem DB-Cluster gespeichert sind, mithilfe des Befehls `SELECT INTO OUTFILE S3`.
- Automatisches Hinzufügen oder Entfernen von Aurora-Replicas mit Auto Scaling von Anwendungen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Auto Scaling mit Aurora Replicas.

Weitere Informationen zum Integrieren von Aurora MySQL mit anderen AWS-Services finden Sie unter Integrieren von Amazon Aurora MySQL in anderen AWS-Services.

Integrieren von AWS-Services mit Amazon Aurora PostgreSQL

Amazon Aurora PostgreSQL ist auch in anderen AWS-Services integriert, damit Sie Ihren Aurora-PostgreSQL-DB-Cluster erweitern können, um zusätzliche Funktionen in der AWS-Cloud zu verwenden. Ihr Aurora-PostgreSQL-DB-Cluster kann AWS-Services verwenden, um Folgendes durchzuführen:

- Performance bei Ihren relationalen Datenbank-Workloads mit Performance Insights schnell ermitteln, anzeigen und beurteilen.
- Automatisches Hinzufügen oder Entfernen von Aurora-Replicas mit Aurora-Auto Scaling. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Auto Scaling mit Aurora Replicas.

Weitere Informationen zum Integrieren von Aurora PostgreSQL mit anderen AWS-Services finden Sie unter Integrieren von Amazon Aurora PostgreSQL in anderen AWS-Services.

Verwenden von Amazon Aurora Auto Scaling mit Aurora Replicas

Um Ihre Konnektivitäts- und Workload-Anforderungen zu erfüllen, passt Aurora Auto Scaling dynamisch die Anzahl der Aurora-Replicas (Reader-DB-Instances) an, die für einen Aurora-DB-Cluster bereitgestellt werden. Aurora Auto Scaling ist für Aurora MySQL und Aurora PostgreSQL verfügbar. Mithilfe von Aurora Auto Scaling kann Ihr Aurora-DB-Cluster plötzliche Konnektivitäts- oder Workloaderhöhungen bewältigen. Wenn die Konnektivität oder Workload abnimmt, entfernt Aurora Auto Scaling unnötige Aurora-Replicas, sodass Sie nicht für nicht genutzte bereitgestellte DB-Instances zahlen müssen.

Sie definieren und wenden eine Skalierungsrichtlinie auf einen Aurora DB-Cluster an. Die Skalierungsrichtlinie definiert die minimale und maximale Anzahl von Aurora-Replicas, die Aurora Auto Scaling verwalten kann. Basierend auf der Richtlinie passt Aurora Auto Scaling die Anzahl der Aurora Replicas als Reaktion auf die tatsächlichen Workloads, die anhand von CloudWatch Amazon-Metriken und Zielwerten bestimmt werden, nach oben oder unten an.

Sie können die verwenden AWS Management Console , um eine Skalierungsrichtlinie anzuwenden, die auf einer vordefinierten Metrik basiert. Alternativ können Sie entweder die AWS CLI oder die Aurora Auto Scaling Scaling-API verwenden, um eine Skalierungsrichtlinie anzuwenden, die auf einer vordefinierten oder benutzerdefinierten Metrik basiert.

Themen

- Aurora Auto Scaling und Performance Insights

Bevor Sie beginnen

Bevor Sie Aurora Auto Scaling mit einem Aurora-DB-Cluster verwenden können, müssen Sie zunächst einen Aurora-DB-Cluster mit einer primären (Writer-)DB-Instance erstellen. Weitere Informationen zum Erstellen eines Aurora-DB-Clusters finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Aurora Auto Scaling skaliert einen DB-Cluster nur, wenn sich der DB-Cluster im verfügbaren Status befindet.

Wenn Aurora Auto Scaling eine neue Aurora-Replica hinzufügt, gehört die neue Aurora-Replica derselben DB-Instance-Klasse an, die auch von der primären Instance verwendet wird. Weitere Informationen zu DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen. Die Hochstufungsebene für neue Aurora Replicas ist auf die niedrigste Priorität eingestellt, die standardmäßig 15 ist. Dies bedeutet, dass während eines Failovers eine Replica mit einer höheren Priorität, wie beispielsweise eine manuell erstellte, zuerst hochgestuft wird. Weitere Informationen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.

Aurora Auto Scaling entfernt nur die Aurora-Replicas, die es selbst erstellt hat.

Um von Aurora Auto Scaling zu profitieren, müssen Ihre Anwendungen Verbindungen zu neuen Aurora-Replicas unterstützen. Hierfür empfehlen wir die Verwendung des Aurora-Reader-Endpunkts. Sie können einen Treiber wie den AWS JDBC-Treiber verwenden. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

> **Note**
>
> Aurora Global Databases unterstützen derzeit kein Aurora Auto Scaling für sekundäre DB-Cluster.

Aurora-Auto Scaling-Richtlinien

Aurora Auto Scaling verwendet eine Skalierungsrichtlinie, um die Anzahl der Aurora-Replicas in einem Aurora-DB-Cluster anzupassen. Aurora-Auto Scaling besteht aus folgenden Komponenten:

- Eine serviceverknüpfte Rolle

- Eine Zielmetrik
- Minimale und maximale Kapazität
- Eine Ruhephase

Themen

Serviceverknüpfte Rolle

Aurora Auto Scaling verwendet die serviceverknüpfte Rolle `AWSServiceRoleForApplicationAutoScaling_RDSCluster`. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen für Application Auto Scaling im Benutzerhandbuch zu Application Auto Scaling.

Zielmetrik

Bei dieser Art von Richtlinien wird eine vordefinierte oder benutzerdefinierte Metrik und ein Zielwert für die Metrik in einer Konfiguration der Skalierungsrichtlinien für die Zielverfolgung festgelegt. Aurora Auto Scaling erstellt und verwaltet CloudWatch Alarme, die die Skalierungsrichtlinie auslösen, und berechnet die Skalierungsanpassung auf der Grundlage der Metrik und des Zielwerts. Die Skalierungsrichtlinie fügt Aurora-Repliken hinzu oder entfernt sie, wenn erforderlich, um die Metrik auf dem angegebenen Zielwert oder in der Nähe davon zu halten. Abgesehen davon, dass eine Skalierungsrichtlinie für die Ziel-Nachverfolgung die Metrik nahe an dem Zielwert hält, passt sie sich auch an die Schwankungen in der Metrik aufgrund einer sich ändernden Workload an. Eine solche Richtlinie minimiert auch schnelle Schwankungen in der Anzahl der verfügbaren Aurora-Repliken für Ihren DB-Cluster.

Nehmen wir zum Beispiel eine Skalierungsrichtlinie, die die vordefinierte durchschnittliche CPU-Auslastung verwendet. Eine solche Richtlinie kann die CPU-Auslastung bei einem bestimmten Prozentsatz der Auslastung halten, z. B. bei 40 Prozent.

> **Note**
>
> Für jeden Aurora DB-Cluster können Sie nur eine Auto-Scaling-Richtlinie für jede Zielmetrik erstellen.

Minimale und maximale Kapazität

Sie können die maximale Anzahl von Aurora-Replicas angeben, die von Application Auto Scaling verwaltet werden sollen. Dieser Wert muss auf 0 – 15 gesetzt werden und gleich oder größer als der für die Mindestanzahl von Aurora-Replicas angegebene Wert sein.

Sie können auch die minimale Anzahl von Aurora-Replicas angeben, die von Application Auto Scaling verwaltet werden sollen. Dieser Wert muss auf 0 – 15 gesetzt werden und gleich oder kleiner als der für die maximal Anzahl von Aurora-Replicas angegebene Wert sein.

> **Note**
>
> Die minimale und maximale Kapazität wird für einen Aurora DB-Cluster festgelegt. Die angegebenen Werte gelten für alle mit diesem Aurora DB-Cluster verknüpften Richtlinien.

Ruhephase

Sie können die Reaktionsfähigkeit einer Skalierungsrichtlinie für die Zielverfolgung anpassen, indem Sie Ruhephasen hinzufügen, nachdem eine Skalierung Ihres Aurora DB-Clusters erfolgt ist. Eine Ruhephase blockiert nachfolgende Scale-in- oder Scale-out-Anforderungen bis zum Ablauf der Frist. Diese Blockierungen verlangsamen das Löschen von Aurora-Replicas in Ihrem Aurora-DB-Cluster für Scale-In-Anforderungen und das Erstellen von Aurora-Replicas für Scale-Out-Anforderungen.

Sie können die folgenden Ruhephasen angeben:

- Eine Scale-In-Aktivität reduziert die Anzahl der Aurora-Replicas in Ihrem Aurora-DB-Cluster. Eine Scale-In-Ruhephase gibt die Zeitspanne in Sekunden an, nach der eine Scale-In-Aktivität abgeschlossen sein muss, bevor eine weitere Scale-In-Aktivität gestartet werden kann.
- Eine Scale-Out-Aktivität erhöht die Anzahl der Aurora-Replicas in Ihrem Aurora-DB-Cluster. Eine Scale-Out-Ruhephase gibt die Zeitspanne in Sekunden an, nach der eine Scale-Out-Aktivität abgeschlossen sein muss, bevor eine weitere Scale-Out-Aktivität gestartet werden kann.

> **Note**
>
> Eine Ruhephase zum Aufskalieren wird ignoriert, wenn eine nachfolgende Anforderung zum Aufskalieren für eine größere Anzahl von Aurora-Replikaten gilt als die erste Anforderung.

Wenn Sie keine Ruhephase für das Ab- bzw. Aufskalieren festlegen, wird jeweils der Standardwert von 300 Sekunden verwendet.

Aktivieren oder Deaktivieren von Scale-In-Aktivitäten

Sie können die Scale-In-Aktivitäten für eine Richtlinie aktivieren oder deaktivieren. Die Aktivierung von Scale-In-Aktivitäten ermöglicht es der Skalierungsrichtlinie, Aurora-Repliken zu löschen. Wenn die Scale-In-Aktivitäten aktiviert sind, gilt für die Scale-In-Aktivitäten die Scale-In-Ruhezeit in der Skalierungsrichtlinie. Das Deaktivieren von Scale-In-Aktivitäten verhindert das Löschen von Aurora-Repliken durch die Skalierungsrichtlinie.

> **Note**
>
> Scale-Out-Aktivitäten sind immer aktiviert, so dass die Skalierungsrichtlinie bei Bedarf Aurora-Replicas erstellen kann.

Hinzufügen einer Skalierungsrichtlinie zu einem Aurora-DB-Cluster

Sie können eine Skalierungsrichtlinie mithilfe der AWS Management Console, der oder der AWS CLI Application Auto Scaling API hinzufügen.

> **Note**
>
> Ein Beispiel für das Hinzufügen einer Skalierungsrichtlinie mithilfe von AWS CloudFormation finden Sie unter Deklarieren einer Skalierungsrichtlinie für einen Aurora-DB-Cluster im AWS CloudFormation Benutzerhandbuch.

Konsole

Sie können einem Aurora-DB-Cluster eine Skalierungsrichtlinie hinzufügen, indem Sie den verwenden AWS Management Console.

So fügen Sie eine automatische Skalierungsrichtlinie zu einem Aurora DB-Cluster hinzu:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Aurora DB-Cluster aus, zu dem Sie die Richtlinie hinzufügen möchten.
4. Wählen Sie die Registerkarte Logs & events (Protokolle und Ereignisse).
5. Wählen Sie im Abschnitt Auto scaling policies (Automatische Skalierungsrichtlinien) die Option Add (Hinzufügen) aus.

   Das Dialogfeld Add Auto Scaling policy (Auto Scaling-Richtlinie hinzufügen) wird aufgerufen.
6. Geben Sie unter Policy Name (Richtlinienname) den Namen der Richtlinie ein.
7. Wählen Sie für die Zielmetrik eine der nachstehenden Optionen aus:

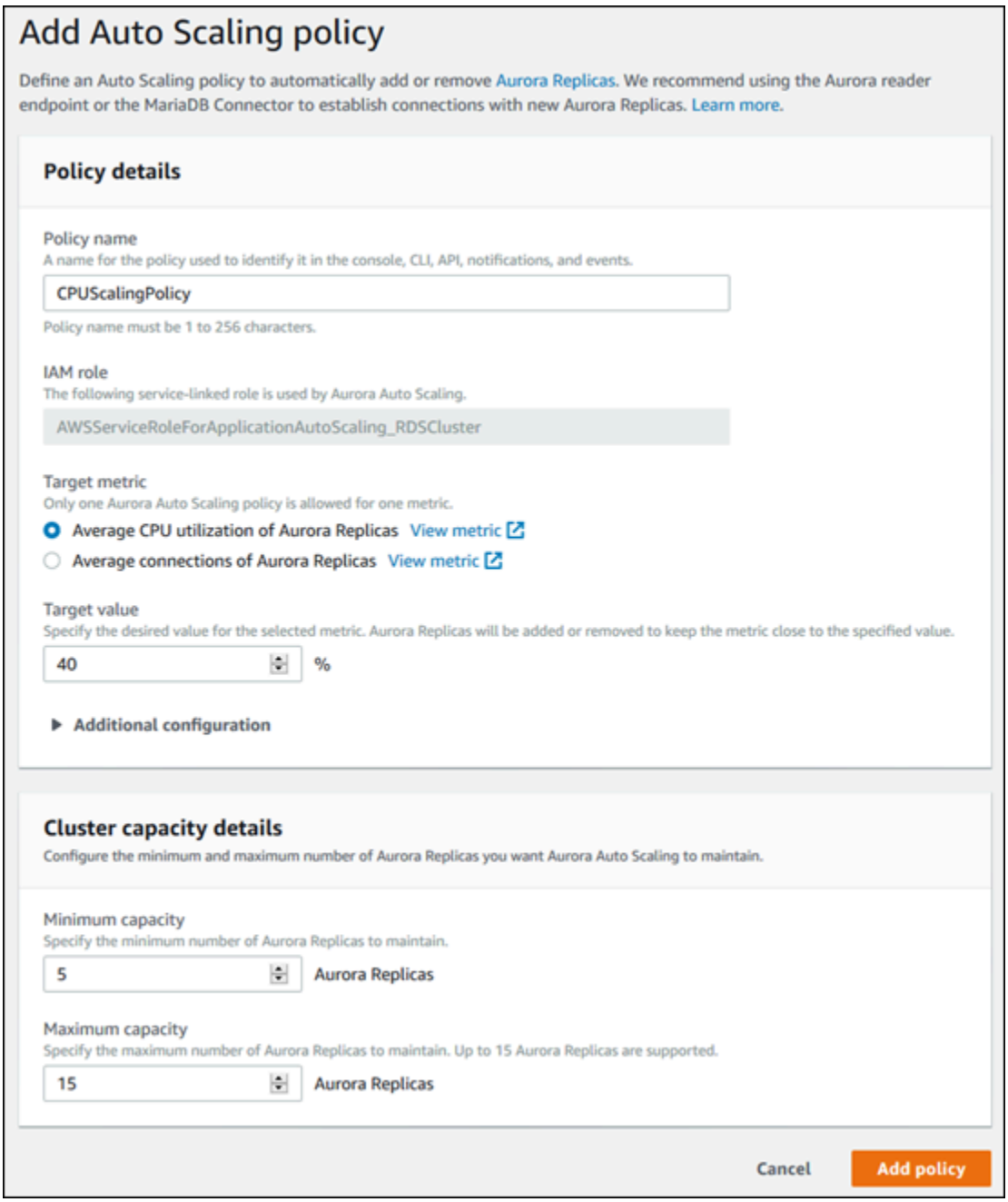
   - Average CPU utilization of Aurora Replicas (Durchschnittliche CPU-Nutzung von Aurora-Replicas), um eine Richtlinie zu erstellen, die auf der durchschnittlichen CPU-Auslastung basiert.
   - Average connections of Aurora Replicas (Durchschnittliche Verbindungen von Aurora-Repliken), um eine Richtlinie zu erstellen, die auf der durchschnittlichen Anzahl der Verbindungen zu den Aurora-Replicas basiert.
8. Geben Sie für den Zielwert eine der nachstehenden Optionen an:

   - Wenn Sie im vorherigen Schritt Average CPU utilization of Aurora Replicas (Durchschnittliche CPU-Nutzung von Aurora-Replicas) ausgewählt haben, geben Sie den Prozentsatz der CPU-Auslastung ein, den Sie auf Aurora-Replicas aufrechterhalten möchten.
   - Wenn Sie im vorherigen Schritt Average connections of Aurora Replicas (Durchschnittliche Verbindungen von Aurora-Replicas) ausgewählt haben, geben Sie die Anzahl der Verbindungen ein, die Sie aufrechterhalten möchten.

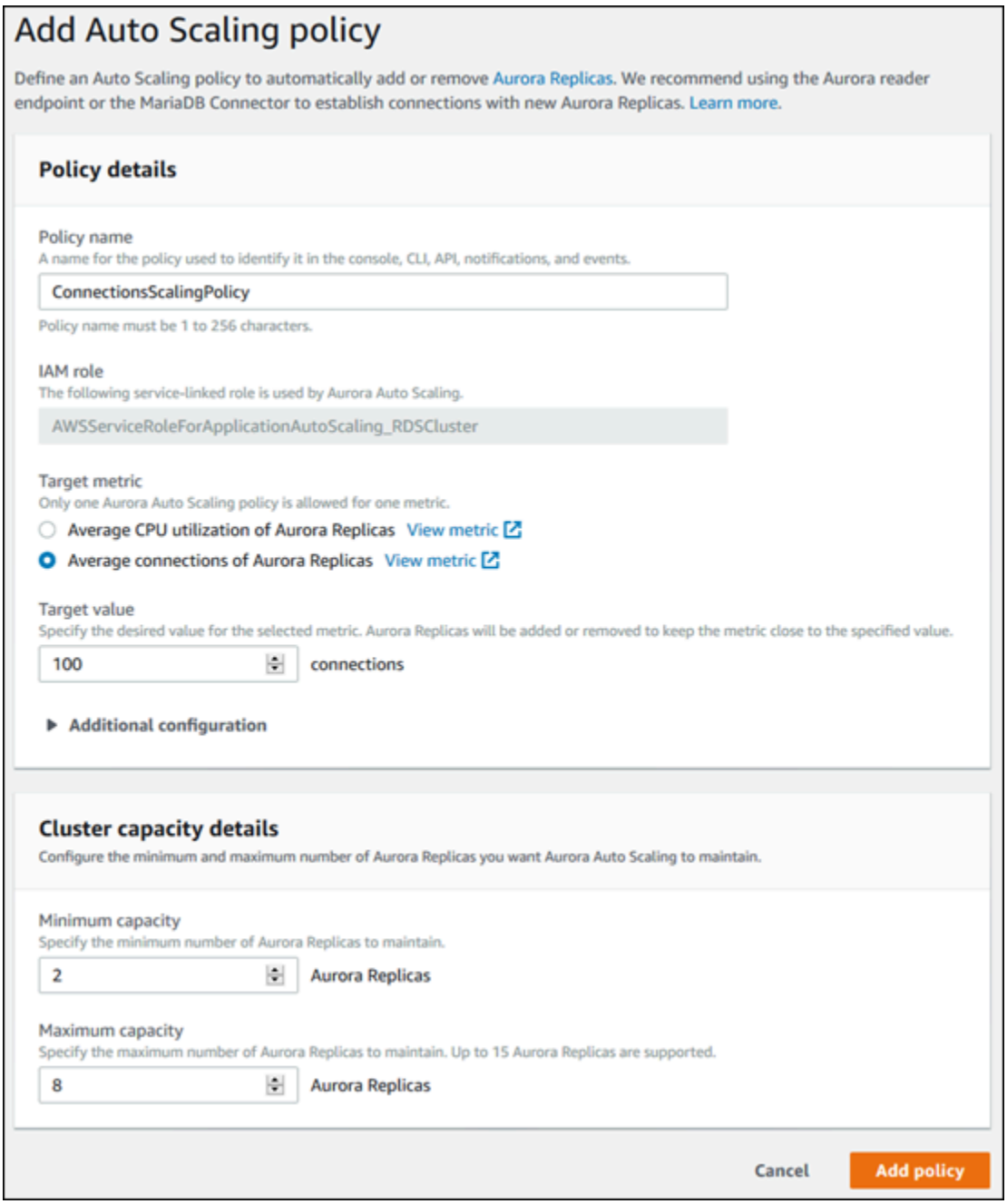
   Aurora-Replicas werden hinzugefügt oder entfernt, um die Metrik in der Nähe des angegebenen Wertes zu halten.

9. (Optional) Erweitern Sie Zusätzliche Konfigurationen, um eine Ruhephase zum Ab- oder Aufskalieren zu erstellen.
10. Geben Sie für Minimale Kapazität die minimale Anzahl von Aurora-Replicas ein, die die Aurora Auto Scaling-Richtlinie beibehalten soll.
11. Geben Sie für Maximale Kapazität die maximale Anzahl von Aurora-Replicas ein, die die Aurora Auto Scaling-Richtlinie beibehalten soll.
12. Wählen Sie Richtlinie hinzufügen aus.

Im folgenden Dialogfeld wird eine Auto Scaling-Richtlinie erstellt, die auf einer durchschnittlichen CPU-Auslastung von 40 Prozent basiert. Die Richtlinie legt ein Minimum von 5 Aurora-Replicas und ein Maximum von 15 Aurora-Replicas fest.



Das folgende Dialogfeld erstellt eine automatische Skalierungsrichtlinie, die auf einer durchschnittlichen Verbindungszahl von 100 basiert. Die Richtlinie legt ein Minimum von zwei Aurora-Replicas und ein Maximum von acht Aurora-Replicas fest.



AWS CLI oder Auto Scaling-API für Anwendungen

Sie können eine Skalierungsrichtlinie anwenden, die entweder auf einer vordefinierten oder einer benutzerdefinierten Metrik basiert. Dazu können Sie die AWS CLI oder die Application Auto Scaling API verwenden. Der erste Schritt ist die Registrierung Ihres Aurora-DB-Clusters mit Application Auto Scaling.

Registrieren eines Aurora-DB-Clusters

Bevor Sie Aurora Auto Scaling mit einem Aurora-DB-Cluster verwenden können, müssen Sie zunächst Ihren Aurora-DB-Cluster mit Application Auto Scaling registrieren. Damit legen Sie die Skalierungsdimension und die Grenzen fest, die auf diesen Cluster angewendet werden sollen. Application Auto Scaling skaliert den Aurora-DB-Cluster dynamisch entlang der skalierbaren `rds:cluster:ReadReplicaCount`-Dimension, die die Anzahl der Aurora-Replikate darstellt.

Um Ihren Aurora-DB-Cluster zu registrieren, können Sie entweder die AWS CLI oder die Application Auto Scaling Scaling-API verwenden.

AWS CLI

Verwenden Sie den `register-scalable-target` AWS CLI Befehl mit den folgenden Parametern, um Ihren Aurora-DB-Cluster zu registrieren:

- `--service-namespace` – Legen Sie diesen Wert auf fest `rds`.
- `--resource-id` – Die Ressourcenkennung für den Aurora-DB-Cluster. Für diesen Parameter lautet der Ressourcentyp `cluster` und die eindeutige Kennung ist der Name des Aurora-DB-Clusters, beispielsweise `cluster:myscalablecluster`.
- `--scalable-dimension` – Legen Sie diesen Wert auf fest `rds:cluster:ReadReplicaCount`.
- `--min-capacity` – Die minimale Anzahl an Reader-DB-Instances, die von Application Auto Scaling verwaltet werden sollen. Informationen zur Beziehung zwischen `--min-capacity`, `--max-capacity` und der Anzahl der DB-Instances in Ihrem Cluster finden Sie unter Minimale und maximale Kapazität.
- `--max-capacity` – Die maximale Anzahl an Reader-DB-Instances, die von Application Auto Scaling verwaltet werden sollen. Informationen zur Beziehung zwischen `--min-capacity`, `--max-capacity` und der Anzahl der DB-Instances in Ihrem Cluster finden Sie unter Minimale und maximale Kapazität.

Example

Im folgenden Beispiel registrieren Sie einen Aurora-DB-Cluster mit dem Namen `myscalablecluster`. Die Registrierung zeigt an, dass der DB-Cluster dynamisch skaliert werden soll, um zwischen einer und acht Aurora-Replicas zu haben.

Für LinuxmacOS, oderUnix:

```
aws application-autoscaling register-scalable-target \
    --service-namespace rds \
    --resource-id cluster:myscalablecluster \
    --scalable-dimension rds:cluster:ReadReplicaCount \
    --min-capacity 1 \
    --max-capacity 8 \
```

Windows:

```
aws application-autoscaling register-scalable-target ^
    --service-namespace rds ^
    --resource-id cluster:myscalablecluster ^
    --scalable-dimension rds:cluster:ReadReplicaCount ^
    --min-capacity 1 ^
    --max-capacity 8 ^
```

API für Application Auto Scaling

Um Ihren Aurora-DB-Cluster mit Auto Scaling von Anwendungen zu registrieren, verwenden Sie die Application Auto Scaling-API-Operation `RegisterScalableTarget` mit den folgenden Parametern:

- `ServiceNamespace` – Legen Sie diesen Wert auf fest `rds`.
- `ResourceID` – Die Ressourcenkennung für den Aurora-DB-Cluster. Für diesen Parameter lautet der Ressourcentyp `cluster` und die eindeutige Kennung ist der Name des Aurora-DB-Clusters, beispielsweise `cluster:myscalablecluster`.
- `ScalableDimension` – Legen Sie diesen Wert auf fest `rds:cluster:ReadReplicaCount`.
- `MinCapacity` – Die minimale Anzahl an Reader-DB-Instances, die von Application Auto Scaling verwaltet werden sollen. Informationen zur Beziehung zwischen `MinCapacity`, `MaxCapacity` und der Anzahl der DB-Instances in Ihrem Cluster finden Sie unter Minimale und maximale Kapazität.
- `MaxCapacity` – Die maximale Anzahl an Reader-DB-Instances, die von Application Auto Scaling verwaltet werden sollen. Informationen zur Beziehung zwischen `MinCapacity`, `MaxCapacity` und der Anzahl der DB-Instances in Ihrem Cluster finden Sie unter Minimale und maximale Kapazität.

Example

Im folgenden Beispiel registrieren Sie einen Aurora-DB-Cluster mit dem Namen `myscalablecluster` mit der Application Auto Scaling API. Diese Registrierung zeigt an, dass der DB-Cluster dynamisch skaliert werden soll, um zwischen eins bis acht Aurora-Repliken zu haben.

```
POST / HTTP/1.1
Host: autoscaling.us-east-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 219
X-Amz-Target: AnyScaleFrontendService.RegisterScalableTarget
X-Amz-Date: 20160506T182145Z
User-Agent: aws-cli/1.10.23 Python/2.7.11 Darwin/15.4.0 botocore/1.4.8
Content-Type: application/x-amz-json-1.1
Authorization: AUTHPARAMS

{
    "ServiceNamespace": "rds",
    "ResourceId": "cluster:myscalablecluster",
    "ScalableDimension": "rds:cluster:ReadReplicaCount",
    "MinCapacity": 1,
    "MaxCapacity": 8
}
```

Definieren einer Skalierungsrichtlinie für einen Aurora-DB-Cluster

Eine Konfiguration der Skalierungsrichtlinie für die Zielverfolgung wird durch einen JSON-Block repräsentiert, in dem die Metriken und Zielwerte definiert sind. Sie können die Konfiguration einer Skalierungsrichtlinie als JSON-Block in einer Textdatei speichern. Sie verwenden diese Textdatei, wenn Sie die AWS CLI oder die Application Auto Scaling Scaling-API aufrufen. Weitere Informationen zur Syntax der Richtlinienkonfiguration finden Sie unter `TargetTrackingScalingPolicyConfiguration` in der API-Referenz für Application Auto Scaling.

Die folgenden Optionen stehen zur Verfügung, um eine Konfiguration der Skalierungsrichtlinien für die Zielverfolgung zu definieren.

Themen

- Verwenden einer vordefinierten Metrik
- Verwenden einer benutzerdefinierten Metrik

- Verwenden von Ruhephasen
- Deaktivieren der Scale-In-Aktivität

Verwenden einer vordefinierten Metrik

Durch die Verwendung vordefinierter Metriken können Sie schnell eine Skalierungsrichtlinie für die Zielverfolgung für einen Aurora-DB-Cluster definieren, die sowohl mit der Zielverfolgung als auch mit der dynamischen Skalierung in Aurora Auto Scaling gut funktioniert.

Derzeit unterstützt Aurora die folgenden vordefinierten Metriken in Aurora Auto Scaling:

- ReaderAverageRDS-CPUUtilization — Der Durchschnittswert der `CPUUtilization` Metrik in CloudWatch allen Aurora Replicas im Aurora-DB-Cluster.
- RDS ReaderAverageDatabaseConnections — Der Durchschnittswert der `DatabaseConnections` Metrik in CloudWatch allen Aurora Replicas im Aurora-DB-Cluster.

Weitere Informationen über die Metriken `CPUUtilization` und `DatabaseConnections` finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora.

Um eine vordefinierte Metrik in Ihrer Skalierungsrichtlinie zu verwenden, erstellen Sie eine Zielverfolgungskonfiguration für Ihre Skalierungsrichtlinie. Diese Konfiguration muss eine `PredefinedMetricSpecification` für die vordefinierte Metrik und einen `TargetValue` für den Zielwert dieser Metrik enthalten.

Example

Das folgende Beispiel beschreibt eine typische Richtlinienkonfiguration für die Skalierung der Zielverfolgung für einen Aurora DB-Cluster. In dieser Konfiguration wird die vordefinierte Metrik `RDSReaderAverageCPUUtilization` verwendet, um den Aurora-DB-Cluster basierend auf einer durchschnittlichen CPU-Auslastung von 40 Prozent über alle Aurora-Replicas hinweg anzupassen.

```
{
    "TargetValue": 40.0,
    "PredefinedMetricSpecification":
    {
        "PredefinedMetricType": "RDSReaderAverageCPUUtilization"
    }
}
```

Verwenden einer benutzerdefinierten Metrik

Durch die Verwendung von benutzerdefinierten Metriken können Sie eine Skalierungsrichtlinie für die Zielverfolgung definieren, die Ihren individuellen Anforderungen entspricht. Sie können eine benutzerdefinierte Metrik basierend auf einer beliebigen Aurora-Metrik definieren, die sich proportional zur Skalierung ändert.

Nicht alle Aurora-Metriken funktionieren für die Zielverfolgung. Die Metrik muss eine gültige Auslastungsmetrik sein und beschreiben, wie ausgelastet eine Instance ist. Der Wert der Metrik muss sich proportional zur Anzahl der Aurora-Replicas im Aurora-DB-Cluster erhöhen oder verringern. Diese proportionale Erhöhung oder Verminderung ist notwendig, um die metrischen Daten zur proportionalen Skalierung oder in der Anzahl der Aurora-Repliken zu verwenden.

Example

Das folgende Beispiel beschreibt die Konfiguration einer Zielverfolgung für eine Skalierungsrichtlinie. In dieser Konfiguration passt eine benutzerdefinierte Metrik einen Aurora-DB-Cluster basierend auf einer durchschnittlichen CPU-Auslastung von 50 Prozent über alle Aurora-Replicas in einem Aurora-DB-Cluster namens a `my-db-cluster`.

```
{
    "TargetValue": 50,
    "CustomizedMetricSpecification":
    {
        "MetricName": "CPUUtilization",
        "Namespace": "AWS/RDS",
        "Dimensions": [
            {"Name": "DBClusterIdentifier","Value": "my-db-cluster"},
            {"Name": "Role","Value": "READER"}
        ],
        "Statistic": "Average",
        "Unit": "Percent"
    }
}
```

Verwenden von Ruhephasen

Sie können einen Wert in Sekunden für `ScaleOutCooldown` angeben, um eine Ruhephase für die Hochskalierung Ihres Aurora-DB-Clusters hinzuzufügen. Ähnlich können Sie einen Wert in Sekunden für `ScaleInCooldown` angeben, um eine Ruhephase für die Herunterskalierung Ihres Aurora-DB-Clusters hinzuzufügen. Weitere Informationen über `ScaleInCooldown` und `ScaleOutCooldown`

finden Sie unter `TargetTrackingScalingPolicyConfiguration` in der API-Referenz für Application Auto Scaling.

Example

Das folgende Beispiel beschreibt die Konfiguration einer Zielverfolgung für eine Skalierungsrichtlinie. In dieser Konfiguration wird die vordefinierte Metrik `RDSReaderAverageCPUUtilization` verwendet, um einen Aurora DB-Cluster anzupassen, basierend auf einer durchschnittlichen CPU-Auslastung von 40 Prozent über alle Aurora -Repliken hinweg in diesem Aurora DB-Cluster. Die Konfiguration sieht eine Scale-In-Ruhephase von 10 Minuten und eine Scale-Out-Ruhephase von 5 Minuten vor.

```
{
    "TargetValue": 40.0,
    "PredefinedMetricSpecification":
    {
        "PredefinedMetricType": "RDSReaderAverageCPUUtilization"
    },
    "ScaleInCooldown": 600,
    "ScaleOutCooldown": 300
}
```

Deaktivieren der Scale-In-Aktivität

Sie können durch die Konfiguration der Skalierungsrichtlinie für die Zielverfolgung verhindern, dass in Ihrem Aurora DB-Cluster ein Scale-In erfolgt, indem Sie die Scale-In-Aktivität deaktivieren. Das Deaktivieren der Scale-In-Aktivität verhindert das Löschen von Aurora-Repliken durch die Skalierungsrichtlinie, und erlaubt der Skalierungsrichtlinie dennoch, Repliken nach Bedarf zu erstellen.

Sie können einen booleschen Wert für `DisableScaleIn` angeben, um die Scale-In-Aktivität für Ihren Aurora-DB-Cluster zu aktivieren oder zu deaktivieren. Weitere Informationen über `DisableScaleIn` finden Sie unter `TargetTrackingScalingPolicyConfiguration` in der API-Referenz für Application Auto Scaling.

Example

Das folgende Beispiel beschreibt die Konfiguration einer Zielverfolgung für eine Skalierungsrichtlinie. In dieser Konfiguration passt die vordefinierte Metrik `RDSReaderAverageCPUUtilization` einen Aurora-DB-Cluster basierend auf einer durchschnittlichen CPU-Auslastung von 40 Prozent über alle

Aurora-Replicas in diesem Aurora-DB-Cluster hinweg an. Die Konfiguration deaktiviert die Scale-In-Aktivität für die Skalierungsrichtlinie.

```
{
    "TargetValue": 40.0,
    "PredefinedMetricSpecification":
    {
        "PredefinedMetricType": "RDSReaderAverageCPUUtilization"
    },
    "DisableScaleIn": true
}
```

Anwenden einer Skalierungsrichtlinie für einen Aurora-DB-Cluster

Nach der Registrierung Ihres Aurora-DB-Clusters mit Application Auto Scaling und der Definition einer Skalierungsrichtlinie wenden Sie die Skalierungsrichtlinie auf den registrierten Aurora-DB-Cluster an. Um eine Skalierungsrichtlinie auf einen Aurora-DB-Cluster anzuwenden, können Sie die AWS CLI oder die Application Auto Scaling Scaling-API verwenden.

AWS CLI

Um eine Skalierungsrichtlinie auf Ihren Aurora-DB-Cluster anzuwenden, verwenden Sie den `put-scaling-policy` AWS CLI Befehl mit den folgenden Parametern:

- `--policy-name` – Der Name der Skalierungsrichtlinie.
- `--policy-type` – Legen Sie diesen Wert auf fest `TargetTrackingScaling`.
- `--resource-id` – Die Ressourcenkennung für den Aurora-DB-Cluster. Für diesen Parameter lautet der Ressourcentyp `cluster` und die eindeutige Kennung ist der Name des Aurora-DB-Clusters, beispielsweise `cluster:myscalablecluster`.
- `--service-namespace` – Legen Sie diesen Wert auf fest `rds`.
- `--scalable-dimension` – Legen Sie diesen Wert auf fest `rds:cluster:ReadReplicaCount`.
- `--target-tracking-scaling-policy-configuration` – Die Konfiguration der Skalierungsrichtlinie für die Zielverfolgung, die für den Aurora-DB-Cluster verwendet werden soll.

Example

Im folgenden Beispiel wenden Sie eine Zielverfolgungs-Skalierungsrichtlinie namens `myscalablepolicy` auf einen Aurora-DB-Cluster namens `myscalablecluster` mit Application

Auto Scaling an. Dazu verwenden Sie eine Richtlinienkonfiguration, die in einer Datei mit dem Namen gespeichert is `config.json`.

Für LinuxmacOS, oderUnix:

```
aws application-autoscaling put-scaling-policy \
    --policy-name myscalablepolicy \
    --policy-type TargetTrackingScaling \
    --resource-id cluster:myscalablecluster \
    --service-namespace rds \
    --scalable-dimension rds:cluster:ReadReplicaCount \
    --target-tracking-scaling-policy-configuration file://config.json
```

Windows:

```
aws application-autoscaling put-scaling-policy ^
    --policy-name myscalablepolicy ^
    --policy-type TargetTrackingScaling ^
    --resource-id cluster:myscalablecluster ^
    --service-namespace rds ^
    --scalable-dimension rds:cluster:ReadReplicaCount ^
    --target-tracking-scaling-policy-configuration file://config.json
```

API für Application Auto Scaling

Um eine Skalierungsrichtlinie auf Ihren Aurora-DB-Cluster über die Application Auto Scaling API anzuwenden, verwenden Sie die Application Auto Scaling-API-Operation `PutScalingPolicy` mit den folgenden Parametern:

- `PolicyName` – Der Name der Skalierungsrichtlinie.
- `ServiceNamespace` – Legen Sie diesen Wert auf fest `rds`.
- `ResourceID` – Die Ressourcenkennung für den Aurora-DB-Cluster. Für diesen Parameter lautet der Ressourcentyp `cluster` und die eindeutige Kennung ist der Name des Aurora-DB-Clusters, beispielsweise `cluster:myscalablecluster`.
- `ScalableDimension` – Legen Sie diesen Wert auf fest `rds:cluster:ReadReplicaCount`.
- `PolicyType` – Legen Sie diesen Wert auf fest `TargetTrackingScaling`.
- `TargetTrackingScalingPolicyConfiguration` – Die Konfiguration der Skalierungsrichtlinie für die Zielverfolgung, die für den Aurora-DB-Cluster verwendet werden soll.

Example

Im folgenden Beispiel wenden Sie eine Zielverfolgungs-Skalierungsrichtlinie namens `myscalablepolicy` auf einen Aurora-DB-Cluster namens `myscalablecluster` mit Auto Scaling von Anwendungen an. Sie verwenden die Richtlinienkonfiguration `RDSReaderAverageCPUUtilization` basierend auf einer vordefinierten Metrik.

```
POST / HTTP/1.1
Host: autoscaling.us-east-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 219
X-Amz-Target: AnyScaleFrontendService.PutScalingPolicy
X-Amz-Date: 20160506T182145Z
User-Agent: aws-cli/1.10.23 Python/2.7.11 Darwin/15.4.0 botocore/1.4.8
Content-Type: application/x-amz-json-1.1
Authorization: AUTHPARAMS

{
    "PolicyName": "myscalablepolicy",
    "ServiceNamespace": "rds",
    "ResourceId": "cluster:myscalablecluster",
    "ScalableDimension": "rds:cluster:ReadReplicaCount",
    "PolicyType": "TargetTrackingScaling",
    "TargetTrackingScalingPolicyConfiguration": {
        "TargetValue": 40.0,
        "PredefinedMetricSpecification":
        {
            "PredefinedMetricType": "RDSReaderAverageCPUUtilization"
        }
    }
}
```

Bearbeiten einer Skalierungsrichtlinie

Sie können eine Skalierungsrichtlinie mit der AWS Management Console, der oder der AWS CLI Application Auto Scaling API bearbeiten.

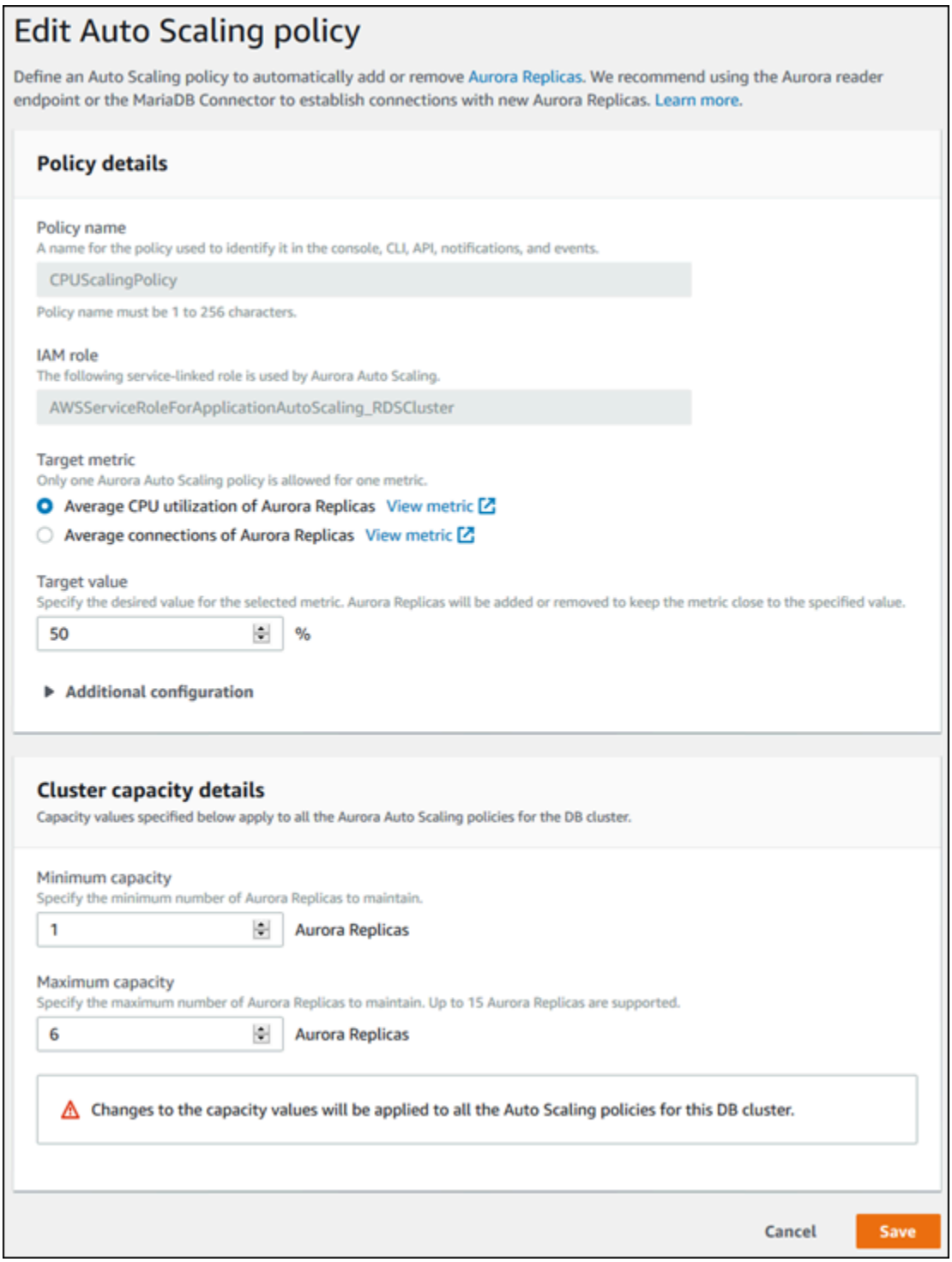
Konsole

Sie können eine Skalierungsrichtlinie bearbeiten, indem Sie die verwenden AWS Management Console.

So bearbeiten Sie eine automatische Skalierungsrichtlinie für einen Aurora DB-Cluster:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Aurora DB-Cluster aus, dessen automatische Skalierungsrichtlinie Sie bearbeiten möchten.
4. Wählen Sie die Registerkarte Logs & events (Protokolle und Ereignisse).
5. Wählen Sie im Abschnitt Auto scaling policies (Automatische Skalierungsrichtlinien) die betreffende automatische Skalierungsrichtlinie und dann Edit (Bearbeiten) aus.
6. Nehmen Sie die Änderungen an der Richtlinie vor.
7. Wählen Sie Save aus.

Im Folgenden sehen Sie ein Beispiel für das Dialogfeld Edit Auto Scaling policy (Auto Scaling-Richtlinie bearbeiten).



AWS CLI oder Auto Scaling-API für Anwendungen

Sie können die AWS CLI oder die Application Auto Scaling Scaling-API verwenden, um eine Skalierungsrichtlinie auf die gleiche Weise zu bearbeiten, wie Sie eine Skalierungsrichtlinie anwenden:

- Wenn Sie die verwenden AWS CLI, geben Sie den Namen der Richtlinie, die Sie bearbeiten möchten, im `--policy-name` Parameter an. Legen Sie neue Werte für die Parameter fest, die Sie ändern möchten.
- Wenn Sie die Application Auto Scaling API verwenden, geben Sie den Namen der zu bearbeitenden Richtlinie im Parameter `PolicyName` an. Legen Sie neue Werte für die Parameter fest, die Sie ändern möchten.

Weitere Informationen finden Sie unter Anwenden einer Skalierungsrichtlinie für einen Aurora-DB-Cluster.

Löschen einer Skalierungsrichtlinie

Sie können eine Skalierungsrichtlinie mithilfe der AWS Management Console, der oder der AWS CLI Application Auto Scaling API löschen.

Konsole

Sie können eine Skalierungsrichtlinie über die AWS Management Console löschen.

So löschen Sie eine automatische Skalierungsrichtlinie für einen Aurora DB-Cluster:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Aurora DB-Cluster aus, dessen automatische Skalierungsrichtlinie Sie löschen möchten.
4. Wählen Sie die Registerkarte Logs & events (Protokolle und Ereignisse).
5. Wählen Sie im Abschnitt Auto Scaling-Richtlinien die automatische Skalierungsrichtlinie und dann Löschen aus.

AWS CLI

Um eine Skalierungsrichtlinie aus Ihrem Aurora-DB-Cluster zu löschen, verwenden Sie den `delete-scaling-policy` AWS CLI Befehl mit den folgenden Parametern:

- `--policy-name` – Der Name der Skalierungsrichtlinie.

- `--resource-id` – Die Ressourcenkennung für den Aurora-DB-Cluster. Für diesen Parameter lautet der Ressourcentyp `cluster` und die eindeutige Kennung ist der Name des Aurora-DB-Clusters, beispielsweise `cluster:myscalablecluster`.
- `--service-namespace` – Legen Sie diesen Wert auf fest `rds`.
- `--scalable-dimension` – Legen Sie diesen Wert auf fest `rds:cluster:ReadReplicaCount`.

Example

Im folgenden Beispiel löschen Sie eine Zielverfolgungs-Skalierungsrichtlinie namens `myscalablepolicy` aus einem Aurora-DB-Cluster namens `myscalablecluster`.

Für LinuxmacOS, oderUnix:

```
aws application-autoscaling delete-scaling-policy \
    --policy-name myscalablepolicy \
    --resource-id cluster:myscalablecluster \
    --service-namespace rds \
    --scalable-dimension rds:cluster:ReadReplicaCount \
```

Windows:

```
aws application-autoscaling delete-scaling-policy ^
    --policy-name myscalablepolicy ^
    --resource-id cluster:myscalablecluster ^
    --service-namespace rds ^
    --scalable-dimension rds:cluster:ReadReplicaCount ^
```

API für Application Auto Scaling

Um eine Skalierungsrichtlinie aus Ihrem Aurora-DB-Cluster zu löschen, verwenden Sie die Application Auto Scaling-API-Operation `DeleteScalingPolicy` mit den folgenden Parametern:

- `PolicyName` – Der Name der Skalierungsrichtlinie.
- `ServiceNamespace` – Legen Sie diesen Wert auf fest `rds`.

- `ResourceID` – Die Ressourcenkennung für den Aurora-DB-Cluster. Für diesen Parameter lautet der Ressourcentyp `cluster` und die eindeutige Kennung ist der Name des Aurora-DB-Clusters, beispielsweise `cluster:myscalablecluster`.
- `ScalableDimension` – Legen Sie diesen Wert auf fest `rds:cluster:ReadReplicaCount`.

Example

Im folgenden Beispiel löschen Sie eine Zielverfolgungs-Skalierungsrichtlinie namens `myscalablepolicy` über die Application Auto Scaling API aus einem Aurora-DB-Cluster namens `myscalablecluster`.

```
POST / HTTP/1.1
Host: autoscaling.us-east-2.amazonaws.com
Accept-Encoding: identity
Content-Length: 219
X-Amz-Target: AnyScaleFrontendService.DeleteScalingPolicy
X-Amz-Date: 20160506T182145Z
User-Agent: aws-cli/1.10.23 Python/2.7.11 Darwin/15.4.0 botocore/1.4.8
Content-Type: application/x-amz-json-1.1
Authorization: AUTHPARAMS

{
    "PolicyName": "myscalablepolicy",
    "ServiceNamespace": "rds",
    "ResourceId": "cluster:myscalablecluster",
    "ScalableDimension": "rds:cluster:ReadReplicaCount"
}
```

DB-Instance-IDs und Tagging

Wenn ein Replikat von Aurora Auto Scaling hinzugefügt wird, wird seine DB-Instance-ID von `application-autoscaling-` vorangestellt, z.B. `application-autoscaling-61aabbcc-4e2f-4c65-b620-ab7421abc123`.

Das folgende Tag wird automatisch zur DB-Instance hinzugefügt. Sie können es auf der Registerkarte Tags der Detailseite der DB-Instance anzeigen.

Tag	Value
application-autoscaling:resourceId	cluster:mynewcluster-cluster

Weitere Informationen zu Amazon-RDS-Ressourcen-Tags finden Sie unter Markieren von Amazon RDS-Ressourcen.

Aurora Auto Scaling und Performance Insights

Sie können Performance Insights verwenden, um Replikate zu überwachen, die von Aurora Auto Scaling hinzugefügt wurden, genau wie bei jeder Reader-DB-Instance von Aurora.

Sie können Performance Insights nicht für einen Aurora-DB-Cluster aktivieren. Sie können Performance Insights für jede DB-Instance im DB-Cluster manuell aktivieren.

Wenn Sie Performance Insights für die Writer-DB-Instance in Ihrem Aurora-DB-Cluster aktivieren, wird Performance Insights für Reader-DB-Instances nicht automatisch aktiviert. Sie müssen Performance Insights manuell für die vorhandenen Reader-DB-Instances und die neuen Replikate aktivieren, die von Aurora Auto Scaling hinzugefügt wurden.

Weitere Informationen zum Verwenden von Performance Insights zur Überwachung von Aurora-DB-Clustern finden Sie unter Überwachung mit Performance Insights auf .

Warten eines Amazon Aurora-DB-Clusters

Amazon RDS führt in regelmäßigen Abständen Wartungsarbeiten an Amazon RDS-Ressourcen durch. Die Wartung beinhaltet in den meisten Fällen Aktualisierungen der folgenden Ressourcen in Ihrem DB-Cluster:

- Zugrundeliegende Hardware
- Zugrundeliegendes Betriebssystem
- Datenbank-Engine-Version

Häufig werden Betriebssystemupdates wegen Sicherheitsproblemen herausgegeben. Sie sollten sie so schnell wie möglich installieren.

Einige Wartungselemente erfordern, dass Amazon RDS Ihren DB-Cluster für kurze Zeit in den Offlinebetrieb versetzt. Zu den Wartungselementen, für die eine Ressource offline sein muss, gehört z. B. das Ausführen erforderlicher Patches für das Betriebssystem oder die Datenbank. Das erforderliche Patching wird automatisch und nur für Patches eingeplant, welche die Sicherheit und Instance-Zuverlässigkeit betreffen. Solche Patches treten selten auf, in der Regel einmal alle paar Monate. Es ist selten mehr als ein Bruchteil Ihres Wartungsfensters dafür erforderlich.

Aufgeschobene DB-Cluster- und DB-Instance-Änderungen, die nicht sofort zur Anwendung kommen sollen, werden während des Wartungszeitraums umgesetzt. Sie können beispielsweise wählen, DB-Instance-Klassen oder Cluster- oder DB-Parametergruppen während des Wartungsfensters zu ändern. Solche Änderungen, die Sie mit der Einstellung für ausstehenden Neustart angeben, werden nicht in der Liste der ausstehenden Wartungsarbeiten angezeigt. Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Um die Änderungen zu sehen, die für das nächste Wartungsfenster noch ausstehen, verwenden Sie den Befehl AWS CLI describe-db-clusters und überprüfen Sie das Feld. `PendingModifiedValues`

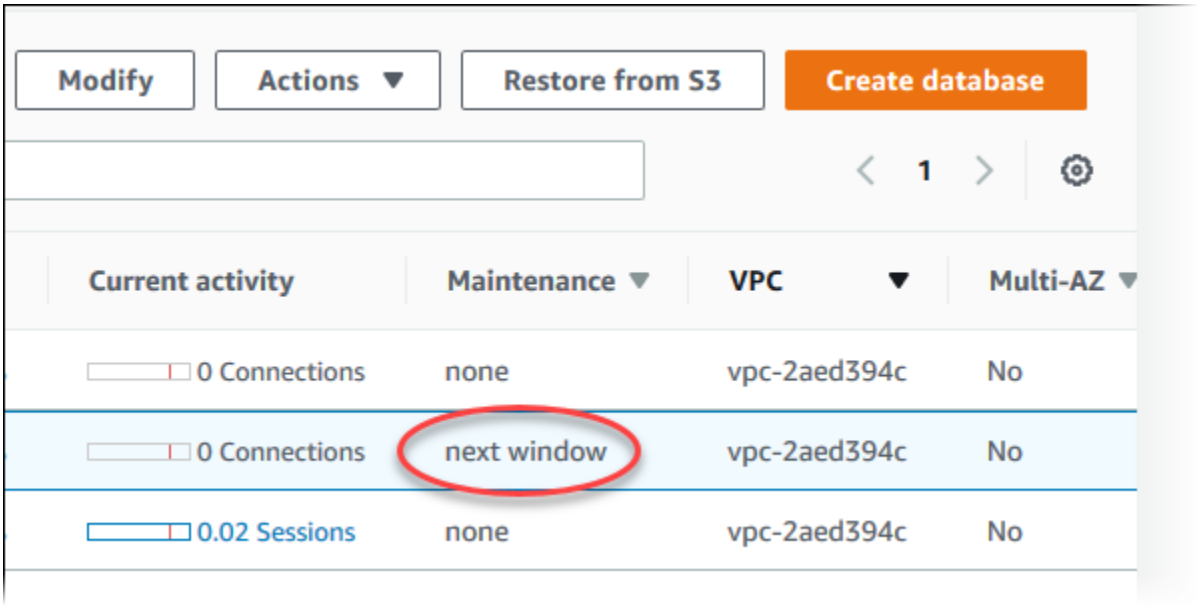
Themen

- Anzeigen ausstehender Wartung
- Anwenden von Updates für eine DB-einen DB-Cluster
- Das Amazon RDS-Wartungsfenster
- Anpassen des bevorzugten DB-Cluster-Wartungsfensters
- Automatische Nebenversions-Upgrades für Aurora-DB-Cluster
- Auswahl der Häufigkeit der Aurora MySQL-Wartungsupdates

- Arbeiten mit Betriebssystem-Updates

Anzeigen ausstehender Wartung

Prüfen Sie mithilfe der RDS-Konsole, der oder der RDS-API, ob ein Wartungsupdate für Ihren verfügbar ist. AWS CLI Wenn ein Update verfügbar ist, wird dies in der Amazon RDS-Konsole in der Spalte Maintenance (Wartung) für den DB-Cluster wie folgt angezeigt:



Wenn für eienn DB-Cluster keine Aktualisierung verfügbar ist, lautet ihr bzw. sein Spaltenwert none (keine).

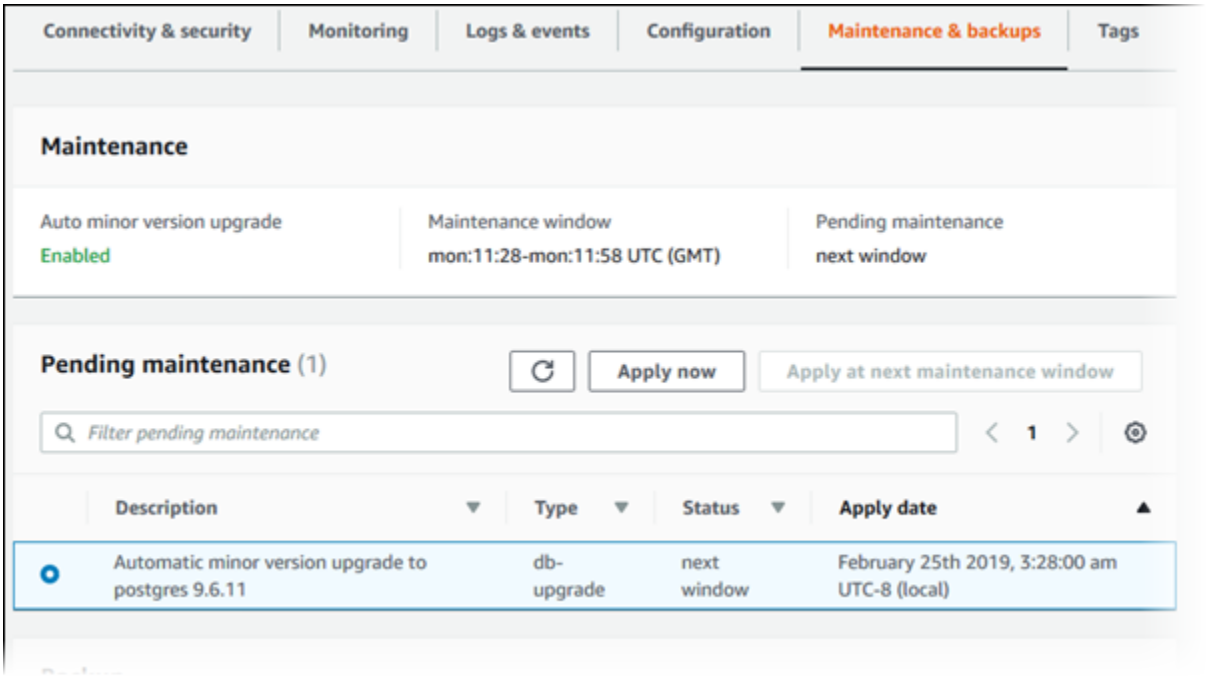
Wenn eine Wartungsaktualisierung für einen DB-Cluster verfügbar ist, sind die folgenden Spaltenwerte möglich:

- required (erforderlich) – Die Wartungsaktion wird auf die Ressource angewendet und kann nicht unbegrenzt aufgeschoben werden.
- available (verfügbar) – Die Wartungsaktion ist verfügbar, wird aber nicht automatisch auf die Ressource angewandt. Sie können sie manuell anwenden.
- next window (nächstes Fenster) – Die Wartungsmaßnahme wird im nächsten Wartungsfenster auf die Ressource angewandt.
- In progress (Läuft) – Die Wartungsmaßnahme wird derzeit auf die Ressource angewandt.

Wenn ein Update verfügbar ist, können Sie eine der folgenden Aktionen ausführen:

- Wenn der Wartungswert next window (nächstes Fenster) ist, schieben Sie die Wartungselemente durch Auswahl von defer upgrade (Upgrade aufschieben) in Actions (Aktionen) auf. Sie können eine Wartungsaktion nicht verschieben, wenn sie bereits gestartet wurde.
- Wenden Sie die Wartungselemente sofort an.
- Planen Sie die Wartungselemente so, dass sie während des nächsten Wartungsfensters gestartet werden.
- Keine Aktion.

Um eine Maßnahme zu ergreifen, wählen Sie den DB-Cluster aus, um ihre bzw. seine Details anzuzeigen. Wählen Sie dann Maintenance & backups (Wartung und Sicherungen). Die ausstehenden Wartungselemente werden angezeigt.



Der Wartungszeitraum legt fest, wann die ausstehenden Operationen gestartet werden, gibt aber keine Gesamtlaufzeit für diese Operationen vor. Wartungsarbeiten werden nicht zwingend vor Ende des Wartungszeitraums abgeschlossen. Sie können daher über die angegebene Endzeit hinaus fortgesetzt werden. Weitere Informationen finden Sie unter Das Amazon RDS-Wartungsfenster.

Allgemeine Informationen zum Aktualisieren von Amazon Aurora-Engines und Anleitungen zum Aktualisieren und Patchen dieser finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL und unter Amazon Aurora PostgreSQL-Aktualisierungen.

Sie können auch überprüfen, ob ein Wartungsupdate für Ihren verfügbar ist, indem Sie den `describe-pending-maintenance-actions` AWS CLI Befehl ausführen.

Anwenden von Updates für eine DB-einen DB-Cluster

Mit Amazon RDS können Sie auswählen, zu welchem Zeitpunkt Wartungsoperationen angewendet werden sollen. Sie können mithilfe der RDS-Konsole AWS Command Line Interface (AWS CLI) oder der RDS-API entscheiden, wann Amazon RDS Updates einführt.

Konsole

Verwalten eines Update für einen DB-Cluster

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den DB-Cluster aus, für die/den ein erforderliches Update angegeben ist.
4. Wählen Sie unter Aktionen eine der folgenden Optionen:

   - Jetzt Upgrade ausführen
   - Im nächsten Wartungszeitraum Upgrade ausführen

   > **Note**
   >
   > Wenn Sie Upgrade at next window (Im nächsten Wartungszeitraum Upgrade ausführen) auswählen und die Installation des Updates aufschieben möchten, können Sie die Option Defer upgrade (Upgrade verschieben) auswählen. Sie können eine Wartungsaktion nicht verschieben, wenn sie bereits gestartet wurde.
   > Um eine Wartungsaktion abzubrechen, ändern Sie die DB-Instance und deaktivieren Sie Auto minor version upgrade (Automatisches Upgrade einer Unterversion).

AWS CLI

Verwenden Sie den Befehl anzuwenden AWS CLI .

Example

LinuxmacOSUnixFür, oder:

```
aws rds apply-pending-maintenance-action \
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db \
```

```
    --apply-action system-update \
    --opt-in-type immediate
```

Windows:

```
aws rds apply-pending-maintenance-action ^
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db ^
    --apply-action system-update ^
    --opt-in-type immediate
```

> **Note**
>
> Um eine Wartungsaktion zu verschieben, geben Sie `undo-opt-in` für `--opt-in-type` an. Sie können `undo-opt-in` nicht für `--opt-in-type` angeben, wenn die Wartungsaktion bereits gestartet wurde.
> Um eine Wartungsaktion abzubrechen, führen Sie den AWS CLI -Befehl modify-db-instance aus und geben Sie `--no-auto-minor-version-upgrade` an.

Verwenden Sie den Befehl AWS CLI describe-pending-maintenance-actions, um eine Liste der Ressourcen zurückzugeben, für die mindestens ein Update aussteht.

Example

Für, oder: Linux macOS Unix

```
aws rds describe-pending-maintenance-actions \
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db
```

Windows:

```
aws rds describe-pending-maintenance-actions ^
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db
```

Sie können auch eine Liste von Ressourcen für einen zurückgeben, indem Sie den `--filters` Parameter des `describe-pending-maintenance-actions` AWS CLI Befehls angeben. Der Befehl hat das folgende Format für `--filters`: `Name=`*`filter-name`*`,Value=`*`resource-id`*`,...`.

Für den `Name`-Parameter eines Filters sind folgende Werte gültig:

- `db-instance-id` nimmt eine Liste von DB-Instance-Kennungen oder Amazon-Ressourcennamen (ARNs) an. In der zurückgegebenen Liste sind nur die aussehenden Wartungsaktionen für die DB-Instances aufgeführt, die diesen IDs bzw. ARNs entsprechen.
- `db-cluster-id` nimmt eine Liste von DB-Cluster-IDs oder Amazon-Ressourcennamen (ARNs) für Amazon Aurora an. In der zurückgegebenen Liste sind nur die aussehenden Wartungsaktionen für die DB-Cluster aufgeführt, die diesen IDs bzw. ARNs entsprechen.

In dem folgenden Beispiel wird eine Liste der aussehenden Wartungsaktionen für die DB-Cluster `sample-cluster1` und `sample-cluster2` zurückgegeben.

Example

Für LinuxmacOS, oderUnix:

```
aws rds describe-pending-maintenance-actions \
 --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

Windows:

```
aws rds describe-pending-maintenance-actions ^
 --filters Name=db-cluster-id,Values=sample-cluster1,sample-cluster2
```

RDS-API

Rufen Sie die Amazon-RDS-API-Operation `ApplyPendingMaintenanceAction` auf, um ein Update auf einem DB-Cluster zu installieren.

Rufen Sie die Amazon RDS-API-Operation `DescribePendingMaintenanceActions` auf, um eine Liste der Ressourcen zurückzugeben, für die mindestens ein Update aussteht.

Das Amazon RDS-Wartungsfenster

Das Wartungsfenster ist ein wöchentliches Zeitintervall, in dem alle Systemänderungen vorgenommen werden. Jeder hat ein wöchentliches Wartungsfenster. Das Wartungsfenster bietet die Möglichkeit, zu kontrollieren, wann Änderungen und Software-Patches vorgenommen werden.

RDS verbraucht während der Wartung einige Ressourcen auf Ihrem DB-Cluster. Sie können einen minimalen Einfluss auf die Leistung beobachten. Bei einer DB-Instance kann in seltenen Fällen ein Multi-AZ-Failover erforderlich sein, damit ein Wartungs-Update abgeschlossen werden kann.

Wenn ein Wartungsereignis für eine bestimmte Woche geplant ist, wird es während des 30-minütigen Wartungsfensters eingeleitet, das Sie festlegen. Die meisten Wartungsereignisse werden auch während des 30-minütigen Wartungsfensters abgeschlossen, obwohl größere Wartungsereignisse länger als 30 Minuten dauern können. Das Wartungsfenster wird angehalten, wenn der gestoppt wird.

Das 30-minütige Wartungsfenster wird zufällig aus einem 8-Stunden-Zeitraum pro Region ausgewählt. Wenn Sie beim Erstellen des DB-Clusters kein Wartungsfenster angeben, legt RDS ein 30-minütiges Wartungsfenster an einem zufällig ausgewählten Wochentag fest.

Nachfolgend finden Sie die Zeitblöcke für jede Region, aus der Standard-Wartungsfenster zugeordnet sind.

Name der Region	Region	Zeitblock
US East (Ohio)	us-east-2	03:00 - 11:00 UTC
USA Ost (Nord-Virginia)	us-east-1	03:00 - 11:00 UTC
USA West (Nordkalifornien)	us-west-1	06:00 - 14:00 UTC
USA West (Oregon)	us-west-2	06:00 - 14:00 UTC
Africa (Cape Town)	af-south-1	03:00 - 11:00 UTC
Asia Pacific (Hong Kong)	ap-east-1	06:00 - 14:00 UTC
Asien-Pazifik (Hyderabad)	ap-south-2	06:30 – 14:30 Uhr UTC
Asien-Pazifik (Jakarta)	ap-southeast-3	08:00–16:00 Uhr UTC
Asien-Pazifik (Melbourne)	ap-southeast-4	11:00–19:00 Uhr UTC
Asien-Pazifik (Mumbai)	ap-south-1	06:00 - 14:00 UTC

Name der Region	Region	Zeitblock
Asia Pacific (Osaka)	ap-northeast-3	22:00 - 23:59 UTC
Asia Pacific (Seoul)	ap-northeast-2	13:00 - 21:00 UTC
Asien-Pazifik (Singapur)	ap-southeast-1	14:00 - 22:00 UTC
Asien-Pazifik (Sydney)	ap-southeast-2	12:00 - 20:00 UTC
Asien-Pazifik (Tokio)	ap-northeast-1	13:00 - 21:00 UTC
Canada (Central)	ca-central-1	03:00 bis 11:00 Uhr UTC
Kanada West (Calgary)	ca-west-1	18:00 - 02:00 UTC
China (Beijing)	cn-north-1	06:00 - 14:00 UTC
China (Ningxia)	cn-northwest-1	06:00 - 14:00 UTC
Europe (Frankfurt)	eu-central-1	21:00 - 05:00 UTC
Europa (Irland)	eu-west-1	22:00 - 06:00 UTC
Europe (London)	eu-west-2	22:00 bis 06:00 Uhr UTC
Europa (Mailand)	eu-south-1	02:00 - 10:00 UTC
Europa (Paris)	eu-west-3	23:59 - 07:29 UTC
Europa (Spanien)	eu-south-2	02:00 - 10:00 UTC
Europe (Stockholm)	eu-north-1	23:00 - 07:00 UTC
Europa (Zürich)	eu-central-2	02:00 - 10:00 UTC
Israel (Tel Aviv)	il-central-1	03:00 bis 11:00 Uhr UTC

Name der Region	Region	Zeitblock
Naher Osten (Bahrain)	me-south-1	06:00 - 14:00 UTC
Naher Osten (VAE)	me-central-1	05:00–13:00 UHR UTC
Südamerika (São Paulo)	sa-east-1	00:00 - 08:00 UTC
AWS GovCloud (US-Ost)	us-gov-east-1	17:00 - 01:00 UTC
AWS GovCloud (US-West)	us-gov-west-1	06:00 - 14:00 UTC

Anpassen des bevorzugten DB-Cluster-Wartungsfensters

Der Wartungszeitraum für ein Aurora-DB-Cluster sollte in den Zeitraum mit der geringsten Nutzung fallen und daher unter Umständen von Zeit zu Zeit geändert werden. Ihr DB-Cluster ist während dieser Zeit nur dann nicht verfügbar, wenn die Updates, die angewendet werden, einen Ausfall erfordern. Der Ausfall dauert die minimale Zeit, die erforderlich ist, um die notwendigen Aktualisierungen vorzunehmen.

Konsole

So passen Sie den bevorzugten DB-Cluster-Wartungszeitraum an

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie das DB-Cluster aus, für das Sie den Wartungszeitraum ändern möchten.
4. Wählen Sie Ändern aus.
5. Aktualisieren Sie im Bereich Wartung den Wartungszeitraum.
6. Klicken Sie auf Weiter.

   Überprüfen Sie auf der Bestätigungsseite Ihre Änderungen.

7. Um die Änderungen sofort auf das Wartungsfenster anzuwenden, wählen Sie im Abschnitt Schedule of modifications (Änderungsplan) die Option Immediately (Sofort) .
8. Wählen Sie Cluster ändern aus, um Ihre Änderungen zu speichern.

   Klicken Sie anderenfalls auf Zurück, um Ihre Änderungen zu bearbeiten, oder klicken Sie auf Abbrechen, um Ihre Änderungen zu verwerfen.

AWS CLI

Verwenden Sie den AWS CLI `modify-db-cluster`Befehl mit den folgenden Parametern, um das bevorzugte Wartungsfenster für DB-Cluster anzupassen:

- `--db-cluster-identifier`
- `--preferred-maintenance-window`

Example

Im folgenden Codebeispiel wird der Wartungszeitraum auf dienstags von 4:00 Uhr bis 4:30 Uhr (UTC) festgelegt.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
--db-cluster-identifier my-cluster \
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

Windows:

```
aws rds modify-db-cluster ^
--db-cluster-identifier my-cluster ^
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

RDS-API

Verwenden Sie die Amazon RDS-API-Operaion `ModifyDBCluster` mit den folgenden Parametern, um das bevorzugte Wartungsfenster für Ihren DB-Cluster anzupassen:

- `DBClusterIdentifier`
- `PreferredMaintenanceWindow`

Automatische Nebenversions-Upgrades für Aurora-DB-Cluster

Die Einstellung Automatisches Unterversion-Upgrade gibt an, ob Aurora Upgrades automatisch auf den DB-Cluster anwendet. Diese Upgrades umfassen neue Unterversionen mit zusätzlichen Funktionen und Patches mit Fehlerbehebungen.

Diese Einstellung ist standardmäßig aktiviert. Wählen Sie für jeden neuen DB-Cluster den entsprechenden Wert für diese Einstellung aus. Dieser Wert basiert auf der Wichtigkeit, der erwarteten Lebensdauer und dem Umfang der Verifizierungstests, die Sie nach jedem Upgrade durchführen.

Anweisungen zum Ein- und Ausschalten der Einstellung Automatisches Unterversion-Upgrade finden Sie im Folgenden:

- Aktivieren automatischer Nebenversions-Upgrades für einen Aurora-DB-Cluster
- Aktivieren automatischer Unterversion-Upgrades für einzelne DB-Instances in einem Aurora-DB-Cluster

> **Important**
>
> Wir empfehlen dringend, dass Sie diese Einstellung für neue und bestehende DB-Cluster auf den DB-Cluster anwenden und nicht einzeln auf die DB-Instances im Cluster. Wenn diese Einstellung für eine DB-Instance in Ihrem Cluster deaktiviert ist, wird der DB-Cluster nicht automatisch aktualisiert.

Die folgende Tabelle zeigt, wie die Einstellung Automatisches Unterversion-Upgrade funktioniert, wenn sie auf Cluster- und Instance-Ebene angewendet wird.

Aktion	Cluster-Einstellung	Instance-Einstellungen	Wurde der Cluster automatisch aktualisiert?
Sie legen diese Einstellung im DB-Cluster auf „true“ fest.	True	„True“ für alle neuen und bestehenden Instances	Ja

Aktion	Cluster-Einstellung	Instance-Einstellungen	Wurde der Cluster automatisch aktualisiert?
Sie legen diese Einstellung im DB-Cluster auf „false“ fest.	False	„False“ für alle neuen und bestehenden Instances	Nein
Die Einstellung wurde zuvor im DB-Cluster auf „true“ festgelegt. Sie legen sie auf mindestens einer DB-Instance auf „false“ fest.	Ändert sich in „false“	„False“ für eine oder mehrere Instances	Nein
Die Einstellung wurde zuvor im DB-Cluster auf „false“ festgelegt. Sie legen die Einstellung für mindestens eine, aber nicht für alle DB-Instances auf „true“ fest.	False	„True“ für eine oder mehrere Instances, aber nicht für alle Instances	Nein
Die Einstellung wurde zuvor im DB-Cluster auf „false“ festgelegt. Sie legen die Einstellung für alle DB-Instances auf „true“ fest.	Ändert sich in „true“	„True“ für alle Instances	Ja

Automatische Upgrades von Nebenversionen werden im Voraus über ein Amazon-RDS-DB-Clusterereignis mit der Kategorie `maintenance` und der ID `RDS-EVENT-0156` kommuniziert.

Weitere Informationen finden Sie unter Amazon RDS-Ereigniskategorien und Ereignisnachrichten für Aurora.

Automatische Aktualisierungen erfolgen während des Wartungsfensters. Wenn die einzelnen DB-Instances im DB-Cluster andere Wartungsfenster haben als das Cluster-Wartungsfenster, hat das Cluster-Wartungsfenster Vorrang.

Weitere Informationen über Engine-Updates für Aurora PostgreSQL finden Sie unter Amazon Aurora PostgreSQL-Aktualisierungen.

Weitere Informationen zur Einstellung für automatische Nebenversions-Upgrades für Aurora MySQL finden Sie unter Aktivieren von automatischen Upgrades zwischen Aurora MySQL-Nebenversionen. Weitere Informationen über Engine-Updates für Aurora MySQL finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.

Aktivieren automatischer Nebenversions-Upgrades für einen Aurora-DB-Cluster

Gehen Sie vor, wie im allgemeinen Verfahren unter Ändern des DB-Clusters über die Konsole, die CLI und die API beschrieben.

Konsole

Wählen Sie im Abschnitt Wartung der Seite DB-Cluster ändern das Kontrollkästchen Automatisches Nebenversions-Upgrade aktivieren aus.

AWS CLI

Rufen Sie den Befehl AWS CLI modify-db-cluster auf. Geben Sie den Namen Ihres DB-Clusters für die `--db-cluster-identifier`-Option und `true` für die `--auto-minor-version-upgrade`-Option an. Optional können Sie die `--apply-immediately`-Option angeben, um diese Einstellung sofort für Ihren DB-Cluster zu aktivieren.

RDS-API

Rufen Sie die ModifyDBCluster-API-Operation auf und geben Sie den Namen Ihres DB-Clusters für den `DBClusterIdentifier`-Parameter und `true` für den `AutoMinorVersionUpgrade`-Parameter an. Legen Sie optional den Parameter `ApplyImmediately` auf `true` fest, um diese Einstellung für Ihren DB-Cluster sofort zu aktivieren.

Aktivieren automatischer Unterversion-Upgrades für einzelne DB-Instances in einem Aurora-DB-Cluster

Gehen Sie vor, wie im allgemeinen Verfahren unter Ändern einer DB-Instance in einem DB-Cluster beschrieben.

Konsole

Wählen Sie im Abschnitt Wartung der Seite DB-Instance ändern das Kontrollkästchen Automatisches Nebenversions-Upgrade aktivieren aus.

AWS CLI

Rufen Sie den Befehl modify-db-instance auf. AWS CLI Geben Sie den Namen Ihrer DB-Instance für die `--db-instance-identifier`-Option und `true` für die `--auto-minor-version-upgrade`-Option an. Optional können Sie die `--apply-immediately`-Option angeben, um diese Einstellung sofort für Ihre DB-Instance zu aktivieren. Führen Sie einen separaten `modify-db-instance`-Befehl für jede DB-Instance in dem Cluster aus.

RDS-API

Rufen Sie die ModifyDBInstance-API-Operation auf und geben Sie den Namen Ihres DB-Clusters für den `DBInstanceIdentifier`-Parameter und `true` für den `AutoMinorVersionUpgrade`-Parameter an. Legen Sie optional den Parameter `ApplyImmediately` auf `true` fest, um diese Einstellung für Ihre DB-Instance sofort zu aktivieren. Rufen Sie für jede DB-Instance in dem Cluster eine separate `ModifyDBInstance`-Operation auf.

Sie können einen CLI-Befehl wie den folgenden verwenden, um den Status der Einstellung `AutoMinorVersionUpgrade` für alle DB-Instances in Ihren Aurora-MySQL-Clustern zu überprüfen.

```
aws rds describe-db-instances \
  --query '*[].
{DBClusterIdentifier:DBClusterIdentifier,DBInstanceIdentifier:DBInstanceIdentifier,AutoMinorVer
```

Die Ausgabe dieses Befehls sieht etwa so aus:

```
[
  {
      "DBInstanceIdentifier": "db-writer-instance",
      "DBClusterIdentifier": "my-db-cluster-57",
```

```
        "AutoMinorVersionUpgrade": true
    },
    {
        "DBInstanceIdentifier": "db-reader-instance1",
        "DBClusterIdentifier": "my-db-cluster-57",
        "AutoMinorVersionUpgrade": false
    },
    {
        "DBInstanceIdentifier": "db-writer-instance2",
        "DBClusterIdentifier": "my-db-cluster-80",
        "AutoMinorVersionUpgrade": true
    },
... output omitted ...
```

In diesem Beispiel ist die Einstellung Automatisches Nebenversions-Upgrade aktivieren für den DB-Cluster `my-db-cluster-57` deaktiviert, da sie für eine der DB-Instances im Cluster deaktiviert ist.

Auswahl der Häufigkeit der Aurora MySQL-Wartungsupdates

Sie können steuern, ob Aurora MySQL-Upgrades für jeden DB-Cluster häufig oder selten stattfinden. Die beste Wahl hängt von Ihrer Verwendung von Aurora MySQL und den Prioritäten für Ihre Anwendungen ab, die unter Aurora ausgeführt werden. Informationen über die Aurora-MySQL-LTS-Versionen (Langzeitstabilität), die weniger häufige Upgrades erfordern, finden Sie unterAurora MySQL Long-Term Support- (LTS, Langzeit-Support) Versionenaus.

Sie können einen Aurora MySQL-Cluster selten aktualisieren, wenn einige oder alle der folgenden Bedingungen zutreffen:

- Ihr Testzyklus für Ihre Anwendung dauert bei einer Aktualisierung der Aurora MySQL-Datenbank-Engine sehr lange.
- Sie haben viele DB-Cluster oder viele Anwendungen, die alle auf der gleichen Aurora MySQL-Version ausgeführt werden. Sie ziehen es vor, alle Ihre DB-Cluster und die zugehörigen Anwendungen gleichzeitig upzugraden.
- Sie verwenden sowohl Aurora MySQL als auch RDS für MySQL. Sie möchten, dass die Aurora-MySQL-Cluster und die DB-Instances von RDS für MySQL mit demselben MySQL-Level kompatibel bleiben.
- Ihre Aurora MySQL-Anwendung befindet sich in der Produktion oder ist anderweitig geschäftskritisch. Sie können sich keine Ausfallzeiten für Upgrades außerhalb seltener Fälle für kritische Patches leisten.

- Ihre Aurora MySQL-Anwendung ist nicht durch Leistungsprobleme oder Funktionslücken eingeschränkt, die in nachfolgenden Aurora MySQL-Versionen behoben werden.

Wenn die vorstehenden Faktoren auf Ihre Situation zutreffen, können Sie die Anzahl der erzwungenen Upgrades für einen Aurora MySQL DB-Cluster begrenzen. Dies geschieht, indem Sie beim Erstellen oder Aktualisieren dieses DB-Clusters eine bestimmte Aurora MySQL-Version wählen, die als "Long-Term Support" (LTS)-Version bekannt ist. Dadurch wird die Anzahl der Upgrade-Zyklen, Testzyklen und upgradebedingten Ausfälle für diesen DB-Cluster minimiert.

Sie können einen Aurora MySQL-Cluster häufig aktualisieren, wenn einige oder alle der folgenden Bedingungen zutreffen:

- Der Testzyklus für Ihre Anwendung ist unkompliziert und kurz.
- Ihre Anwendung befindet sich noch in der Entwicklungsphase.
- Ihre Datenbankumgebung verwendet eine Vielzahl von Aurora MySQL-Versionen oder Aurora MySQL- und RDS für MySQL-Versionen. Jeder Aurora MySQL-Cluster hat seinen eigenen Upgrade-Zyklus.
- Sie warten auf spezifische Leistungs- oder Funktionsverbesserungen, bevor Sie Ihre Nutzung von Aurora MySQL erhöhen.

Wenn die vorhergehenden Faktoren auf Ihre Situation zutreffen, können Sie Aurora aktivieren, um wichtige Upgrades häufiger anzuwenden. Dazu führen Sie ein Upgrade eines DB-Clusters von Aurora MySQL auf eine aktuellere Version von Aurora MySQL als die LTS-Version durch. Auf diese Weise stehen Ihnen die neuesten Leistungssteigerungen, Bugfixes und Funktionen schneller zur Verfügung.

Arbeiten mit Betriebssystem-Updates

DB-Instances in DB-Cluster von Aurora MySQL und Aurora PostgreSQL erfordern gelegentlich Betriebssystemaktualisierungen. Amazon RDS aktualisiert das Betriebssystem auf eine neuere Version, um die Datenbankleistung und der allgemeine Sicherheitsstatus der Kunden zu verbessern. In der Regel dauern die Updates etwa 10 Minuten. Betriebssystem-Updates ändern nicht die DB-Engine-Version oder die DB-Instance-Klasse einer DB-Instance.

Wir empfehlen, zuerst die Reader-DB-Instances in einem DB-Cluster und dann die Writer-DB-Instance zu aktualisieren. Es wird davon abgeraten, Reader- und Writer-Instances gleichzeitig zu aktualisieren, da es im Falle eines Failovers zu Ausfallzeiten kommen kann.

Wir empfehlen, die AWS Treiber zu verwenden, um ein schnelleres Datenbank-Failover zu erreichen. Weitere Informationen finden Sie unter Mit den AWS Treibern eine Verbindung zu Aurora-DB-Clustern herstellen.

Es gibt zwei Arten von Betriebssystem-Updates, die sich durch die Beschreibung unterscheiden, die in der ausstehenden Wartungsaktion für die DB-Instance sichtbar ist:

- Upgrade der Betriebssystemdistribution – Wird für die Migration auf die neueste unterstützte Hauptversion von Amazon Linux verwendet. Ihre Beschreibung in der ausstehenden Wartungsaktion lautet `New Operating System upgrade is available`.
- Betriebssystem-Patch – Wird verwendet, um verschiedene Sicherheitskorrekturen anzuwenden und manchmal um die Datenbankleistung zu verbessern. Ihre Beschreibung in der ausstehenden Wartungsaktion lautet `New Operating System patch is available`.

Betriebssystem-Updates können entweder optional oder obligatorisch sein:

- Ein optionales Update kann jederzeit angewendet werden. Obwohl diese Updates optional sind, empfehlen wir Ihnen, sie regelmäßig anzuwenden, um Ihre RDS-Flotte auf dem neuesten Stand zu halten. RDS wendet diese Updates nicht automatisch an.

  Wenn Sie benachrichtigt werden möchten, sobald ein neuer optionaler System-Patch verfügbar ist, können Sie RDS-EVENT-0230 in der Kategorie „Sicherheitspatch-Ereignis“ abonnieren. Informationen zum Abonnieren von RDS-Ereignissen finden Sie unter Abonnieren von Amazon RDS-Ereignisbenachrichtigungen.

  > **Note**
  >
  > `RDS-EVENT-0230` gilt nicht für Upgrades der Betriebssystemdistribution.

- Ein obligatorisches Update ist erforderlich. Wir senden vor dem obligatorischen Update eine Benachrichtigung. Die Benachrichtigung kann ein Fälligkeitsdatum enthalten. Planen Sie Ihr Update vor diesem Fälligkeitsdatum. Nach dem angegebenen Fälligkeitsdatum aktualisiert Amazon RDS das Betriebssystem für Ihre DB-Instance während eines Ihrer zugewiesenen Wartungsfenster automatisch auf die neueste Version.

  Upgrades der Betriebssystemdistribution sind obligatorisch.

> **Note**
>
> Es ist möglicherweise erforderlich, im Hinblick auf alle optionalen und obligatorischen Updates auf dem Laufenden zu bleiben, um verschiedene Compliance-Auflagen zu erfüllen. Wir empfehlen Ihnen, alle von RDS zur Verfügung gestellten Updates während Ihrer Wartungsfenster routinemäßig anzuwenden.

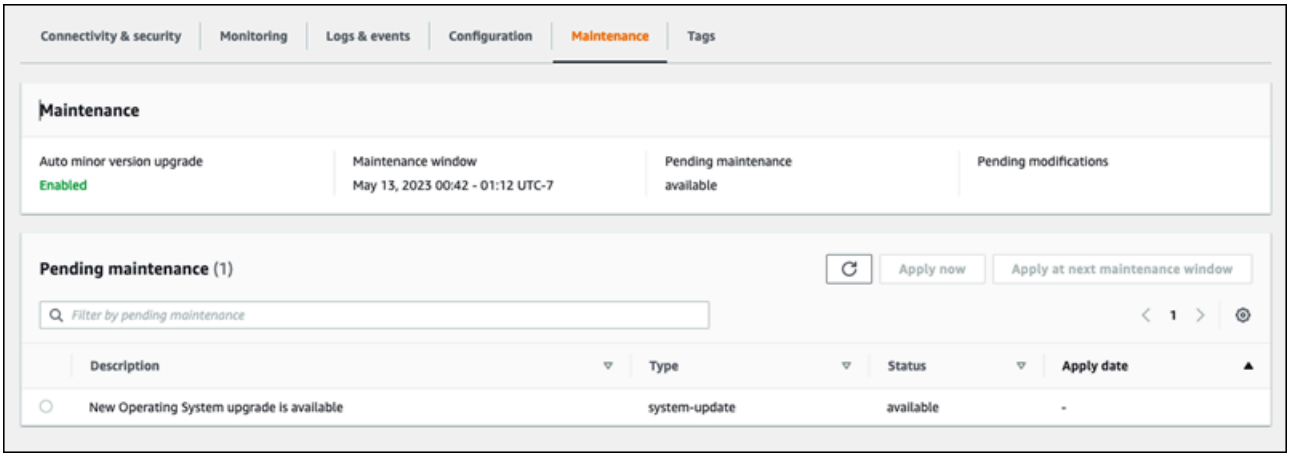
Sie können das AWS Management Console oder das verwenden AWS CLI , um Informationen über die Art der Betriebssystemaktualisierung abzurufen.

Konsole

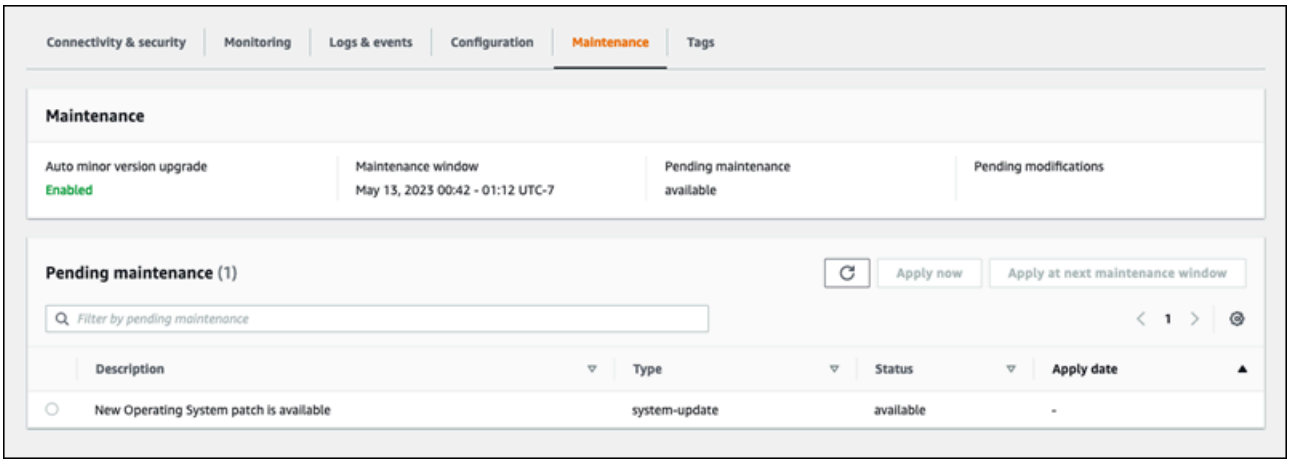
Um Aktualisierungsinformationen mit dem zu erhalten AWS Management Console

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und anschließend die MySQL-DB-Instance aus.
3. Wählen Sie Maintenance (Wartung und Backups) aus.
4. Suchen Sie im Abschnitt Ausstehende Wartungen das Betriebssystem-Update und überprüfen Sie den Wert Beschreibung.

In der AWS Management Console ist die Beschreibung eines Betriebssystem-Distributions-Upgrades auf Neues Betriebssystem-Upgrade ist verfügbar gesetzt, wie in der folgenden Abbildung dargestellt. Dieses Upgrade ist obligatorisch.



Für einen Betriebssystem-Patch ist die Beschreibung auf Neuer Betriebssystem-Patch ist verfügbar festgelegt, wie in der folgenden Abbildung dargestellt.



AWS CLI

Um Aktualisierungsinformationen von zu erhalten AWS CLI, verwenden Sie den Befehl describe-pending-maintenance-actions.

```
aws rds describe-pending-maintenance-actions
```

Die folgende Ausgabe zeigt ein Upgrade einer Betriebssystemdistribution.

```
{
  "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:db:mydb1",
  "PendingMaintenanceActionDetails": [
    {
      "Action": "system-update",
      "Description": "New Operating System upgrade is available"
    }
  ]
}
```

Die folgende Ausgabe zeigt einen Betriebssystem-Patch.

```
{
  "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:db:mydb2",
  "PendingMaintenanceActionDetails": [
    {
      "Action": "system-update",
      "Description": "New Operating System patch is available"
```

```
    }
  ]
}
```

Verfügbarkeit von Betriebssystem-Updates

Betriebssystem-Updates sind spezifisch für die DB-Engine-Version und die DB-Instance-Klasse. Daher erhalten oder erfordern DB-Instances Updates zu verschiedenen Zeiten. Wenn für Ihre DB-Instance basierend auf der Engine-Version und der Instance-Klasse ein Betriebssystemupdate erforderlich ist, wird das erforderliche Update in der Konsole angezeigt. Es kann auch angezeigt werden, indem Sie den Befehl AWS CLI describe-pending-maintenance-actions ausführen oder den RDS-API-Vorgang aufrufen. DescribePendingMaintenanceActions Wenn für Ihre Instance ein Update verfügbar ist, können Sie Ihr Betriebssystem aktualisieren, indem Sie den Anweisungen unter Anwenden von Updates für eine DB-einen DB-Cluster folgen.

Neustart eines Amazon Aurora DB-Clusters oder einer Amazon Aurora DB-Instance

Möglicherweise müssen Sie Ihren DB-Cluster oder einige Instances innerhalb des Clusters neu starten, normalerweise aus Wartungsgründen. Angenommen, Sie ändern die Parameter innerhalb einer Parametergruppe oder ordnen Ihrem Cluster eine andere Parametergruppe zu. In diesen Fällen müssen Sie den Cluster neu starten, damit die Änderungen wirksam werden. In ähnlicher Weise können Sie eine oder mehrere Reader-DB-Instances innerhalb des Clusters neu starten. Sie können die Neustartvorgänge für einzelne Instances anordnen, um Ausfallzeiten für den gesamten Cluster zu minimieren.

Die für den Neustart der einzelnen DB-Instances in Ihrem Cluster erforderliche Zeit hängt von der Datenbankaktivität zum Zeitpunkt des Neustarts ab. Dies hängt auch vom Wiederherstellungsprozess Ihrer spezifischen DB-Engine ab. Wenn dies praktisch ist, reduzieren Sie die Datenbankaktivität auf dieser bestimmten Instance, bevor Sie den Neustartvorgang starten. Dadurch kann die zum Neustart der Datenbank erforderliche Zeit verkürzt werden.

Sie können jede DB-Instance in Ihrem Cluster nur neu starten, wenn sie sich im verfügbaren Status befindet. Eine DB-Instance kann aus mehreren Gründen nicht verfügbar sein. Dazu gehören der Status der gestoppten Cluster, eine Änderung, die auf die Instance angewendet wird und eine Wartungsfensteraktion, sowie ein Versionsupgrade.

Beim Neustart einer DB-Instance wird der Datenbank-Engine-Prozess neu gestartet. Das Neustarten einer DB-Instance bewirkt einen vorübergehenden Nutzungsausfall, wobei der Status für diese Instance währenddessen auf Wird neu gestartet … gesetzt wird.

> **Note**
>
> Wenn eine DB-Instance nicht die neuesten Änderungen an ihrer zugehörigen DB-Parametergruppe verwendet, wird die DB-Parametergruppe mit dem Status „Ausstehender Neustart“ AWS Management Console angezeigt. Die Parametergruppe pending-reboot führt während des nächsten Wartungsfensters nicht zu einem automatischen Neustart. Damit die neuesten Parameteränderungen für diese DB-Instance übernommen werden, starten Sie die DB-Instance manuell neu. Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Themen

Neustarten einer DB-Instance in einem Aurora Cluster

Dieses Verfahren ist der wichtigste Vorgang, den Sie beim Durchführen von Neustarts mit Aurora ausführen. Viele der Wartungsverfahren beinhalten das Neustarten einer oder mehrerer Aurora DB-Instances in einer bestimmten Reihenfolge.

Konsole

Neustarten einer DB-Instance

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die DB-Instance aus, die Sie neu starten möchten.
3. Wählen Sie unter Aktionen die Option Neustart aus.

   Die Seite DB-Instance neu starten wird angezeigt.
4. Wählen Sie Neustart aus, um Ihrer DB-Instance neu zu starten.

   Oder klicken Sie auf Abbrechen.

AWS CLI

Um eine DB-Instance mithilfe von neu zu starten AWS CLI, rufen Sie den `reboot-db-instance`Befehl auf.

Example

Für LinuxmacOS, oderUnix:

```
aws rds reboot-db-instance \
    --db-instance-identifier mydbinstance
```

Windows:

```
aws rds reboot-db-instance ^
    --db-instance-identifier mydbinstance
```

RDS-API

Um eine DB-Instance mithilfe der Amazon RDS-API neu zu starten, rufen Sie den Vorgang `RebootDBInstance` auf.

Neustart eines Aurora-Clusters mit Leseverfügbarkeit

Mit der Leseverfügbarkeitsfunktion können Sie die Writer-Instance Ihres Aurora-Clusters neu starten, ohne die Reader-Instances im primären oder sekundären DB-Cluster neu starten zu müssen. Dies kann dazu beitragen, die hohe Verfügbarkeit des Clusters für Lesevorgänge aufrechtzuerhalten, während Sie die Writer-Instance neu starten. Sie können die Reader-Instances später nach einem für Sie geeigneten Zeitplan neu starten. In einem Produktionscluster können Sie beispielsweise die Reader-Instances nacheinander neu starten und erst beginnen, nachdem der Neustart der primären Instance abgeschlossen ist. Folgen Sie für jede DB-Instance, die Sie neu starten, dem Verfahren unter Neustarten einer DB-Instance in einem Aurora Cluster.

Die Leseverfügbarkeitsfunktion für primäre DB-Cluster ist in Aurora MySQL Version 2.10 und höher verfügbar. Die Leseverfügbarkeit für sekundäre DB-Cluster ist in Aurora MySQL Version 3.06 und höher verfügbar.

Diese Funktion steht standardmäßig für die folgenden Aurora-PostgreSQL-Versionen zur Verfügung:

- 15.2 und höhere 15-Versionen
- 14.7 und höhere 14-Versionen
- 13.10 und höhere 13-Versionen
- 12.14 und höhere 12-Versionen

Weitere Informationen zur Leseverfügbarkeitsfunktion in Aurora PostgreSQL finden Sie unter Verbesserung der Leseverfügbarkeit von Aurora Replicas.

Vor dieser Funktion führte der Neustart der primären Instance zu einem Neustart für jede Reader-Instance gleichzeitig. Wenn auf Ihrem Aurora-Cluster eine ältere Version ausgeführt wird, verwenden Sie stattdessen das Neustartverfahren in Neustart eines Aurora-Clusters ohne Leseverfügbarkeit.

> **Note**
>
> Die Änderung des Neustartverhaltens in Aurora-DB-Clustern mit Leseverfügbarkeit unterscheidet sich für globale Aurora-Datenbanken in Aurora MySQL-Versionen vor 3.06. Wenn Sie die Writer-Instance für den primären Cluster in einer globalen Aurora-Datenbank neu starten, bleiben die Reader-Instances im primären Cluster verfügbar. Die DB-Instances in sekundären Clustern werden jedoch gleichzeitig neu gestartet.
> Eine eingeschränkte Version der verbesserten Leseverfügbarkeitsfunktion wird von den globalen Aurora-Datenbanken für die Aurora PostgreSQL-Versionen 12.16, 13.12, 14.9, 15.4 und höher unterstützt.

Sie starten den Cluster häufig neu, nachdem Sie Änderungen an Clusterparametergruppen vorgenommen haben. Sie nehmen Parameteränderungen vor, indem Sie die Verfahren in befolge Arbeiten mit Parametergruppen. Angenommen, Sie starten die Writer-DB-Instance in einem Aurora-Cluster neu, um Änderungen an Cluster-Parametern anzuwenden. Einige oder alle Reader-DB-Instances verwenden möglicherweise weiterhin die alten Parametereinstellungen. Die verschiedenen Parametereinstellungen haben jedoch keinen Einfluss auf die Datenintegrität des Clusters. Alle Clusterparameter, die sich auf die Organisation von Datendateien auswirken, werden nur von der Writer-DB-Instance verwendet.

Beispielsweise können Sie in einem Aurora-MySQL-Cluster Cluster-Parameter wie `binlog_format` und `innodb_purge_threads` auf der Writer-Instance vor den Reader-Instances aktualisieren. Nur die Writer-Instance schreibt binäre Protokolle und löscht Datensätze für das Rückgängigmachen. Bei Parametern, die die Interpretation von SQL-Anweisungen oder Abfrageausgaben ändern, müssen Sie möglicherweise darauf achten, die Reader-Instances sofort neu zu starten. Sie tun dies, um unerwartetes Anwendungsverhalten bei Abfragen zu vermeiden. Angenommen, Sie ändern den `lower_case_table_names` Parameter und starten die Writer-Instance neu. In diesem Fall können die Reader-Instances möglicherweise erst auf eine neu erstellte Tabelle zugreifen, wenn sie alle neu gestartet wurden.

Eine Liste aller Aurora MySQL Clusterparameter finden Sie unter Parameter auf Cluster-Ebene.

Eine Liste aller Cluster-Parameter von Aurora PostgreSQL finden Sie unter Aurora-PostgreSQL-Parameter auf Cluster-Ebene.

> **Tip**
>
> Aurora MySQL startet möglicherweise noch einige der Reader-Instances zusammen mit der Writer-Instance neu, wenn Ihr Cluster einen Workload mit hohem Durchsatz verarbeitet. Die Verringerung der Anzahl der Neustarts gilt auch während des Failovervorgangs. Aurora MySQL startet nur die Writer-DB-Instance und das Failover-Ziel während eines Failovers neu. Andere Reader-DB-Instances im Cluster bleiben verfügbar, um Abfragen über Verbindungen zum Reader-Endpunkt fortzusetzen. So können Sie die Verfügbarkeit während eines Failovers verbessern, indem Sie mehr als eine Reader-DB-Instance in einem Cluster haben.

Neustart eines Aurora-Clusters ohne Leseverfügbarkeit

Ohne die Funktion zur Leseverfügbarkeit starten Sie einen ganzen Aurora-DB-Cluster neu, indem Sie die Writer-DB-Instance dieses Clusters neu starten. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Neustarten einer DB-Instance in einem Aurora Cluster.

Ein Neustart der Writer-DB-Instance initiiert auch einen Neustart für jede Reader-DB-Instance im Cluster. Auf diese Weise werden alle clusterweiten Parameteränderungen gleichzeitig auf alle DB-Instances angewendet. Der Neustart aller DB-Instances führt jedoch zu einem kurzen Ausfall für den Cluster. Die Reader DB-Instances bleiben nicht verfügbar, bis die Writer DB-Instance den Neustart beendet hat und verfügbar wird.

Dieses Neustartverhalten gilt für alle DB-Cluster, die in Aurora MySQL Version 2.09 und niedriger erstellt wurden.

Für Aurora PostgreSQL gilt dieses Verhalten für die folgenden Versionen:

- 14.6 und niedrigere 14-Versionen
- 13.9 und niedrigere 13-Versionen
- 12.13 und niedrigere 12-Versionen
- Alle PostgreSQL-11-Versionen

In der RDS-Konsole hat die Writer-DB-Instance den Wert Writer in der Spalte Rolle auf der Seite Datenbanken. In der RDS CLI enthält die Ausgabe des `describe-db-clusters`-Befehls einen Abschnitt `DBClusterMembers`. Das `DBClusterMembers`-Element, das die Writer-DB-Instance repräsentiert, hat einen Wert von `true` für das `IsClusterWriter` Feld.

> **Important**
>
> Mit der Funktion zur Leseverfügbarkeit ist das Neustartverhalten in Aurora MySQL anders als in Aurora PostgreSQL: Die Reader-DB-Instances bleiben normalerweise verfügbar, während Sie die Writer-Instance neu starten. Dann können Sie die Reader-Instances zu einem geeigneten Zeitpunkt neu starten. Sie können die Reader-Instances nach einem gestaffelten Zeitplan neu starten, wenn einige Reader-Instances immer verfügbar sein sollen. Weitere Informationen finden Sie unter Neustart eines Aurora-Clusters mit Leseverfügbarkeit.

Überprüfung der Betriebszeit für Aurora Cluster und Instances

Sie können die Dauer seit dem letzten Neustart für jede DB-Instance in Ihrem Aurora Cluster überprüfen und überwachen. Die CloudWatch `EngineUptime` Amazon-Metrik gibt die Anzahl der Sekunden seit dem letzten Start einer DB-Instance an. Sie können diese Metrik zu einem bestimmten Zeitpunkt untersuchen, um die Verfügbarkeit der DB-Instance zu ermitteln. Sie können diese Metrik auch im Laufe der Zeit überwachen, um zu erkennen, wann die Instance neu gestartet wird.

Sie können die `EngineUptime` Metrik auch auf Clusterebene untersuchen. Die `Minimum`- und `Maximum`- Dimensionen geben die kleinsten und größten Verfügbarkeitswerte für alle DB-Instances im Cluster an. Um zu überprüfen, wann eine Reader-Instance in einem Cluster zuletzt neu gestartet oder aus einem anderen Grund neu gestartet wurde, überwachen Sie die Metrik auf Clusterebene mithilfe der `Minimum`-Dimension. Um zu überprüfen, welche Instance im Cluster am längsten ohne Neustart gelaufen ist, überwachen Sie die Metrik auf Clusterebene mithilfe der `Maximum`-Dimension. Sie möchten beispielsweise bestätigen, dass alle DB-Instances im Cluster nach einer Konfigurationsänderung neu gestartet wurden.

> **Tip**
>
> Für eine langfristige Überwachung empfehlen wir, die `EngineUptime`-Metrik für einzelne Instances statt auf Clusterebene zu überwachen. Die `EngineUptime`-Metrik auf Clusterebene wird auf Null gesetzt, wenn dem Cluster eine neue DB-Instance hinzugefügt wird. Solche Clusteränderungen können im Rahmen von Wartungs- und Skalierungsvorgängen auftreten, wie sie von Auto Scaling durchgeführt werden.

Die folgenden CLI-Beispiele zeigen, wie die `EngineUptime`-Metrik für die Writer- und Reader-Instances in einem Cluster untersucht wird. Die Beispiele verwenden einen Cluster namens

`tpch100g`. Dieser Cluster hat eine Writer-DB-Instance `instance-1234`. Er hat auch zwei Reader-DB-Instances, `instance-7448` und `instance-6305`.

Zuerst startet der `reboot-db-instance`-Befehl eine der Reader-Instances neu. Der `wait`-Befehl wartet, bis die Instance mit dem Neustart abgeschlossen ist.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-6305
{
    "DBInstance": {
        "DBInstanceIdentifier": "instance-6305",
        "DBInstanceStatus": "rebooting",
...
$ aws rds wait db-instance-available --db-instance-id instance-6305
```

Der CloudWatch `get-metric-statistics` Befehl untersucht die `EngineUptime` Metrik in den letzten fünf Minuten in Intervallen von einer Minute. Die Betriebszeit für die `instance-6305` Instance wird auf Null zurückgesetzt und beginnt wieder nach oben zu zählen. In diesem AWS CLI Beispiel für Linux wird die `$()` Variablenersetzung verwendet, um die entsprechenden Zeitstempel in die CLI-Befehle einzufügen. Es verwendet auch den `sort` Linux-Befehl, um die Ausgabe bis zum Zeitpunkt der Erfassung der Metrik zu ordnen. Dieser Zeitstempelwert ist das dritte Feld in jeder Ausgabezeile.

```
$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" \
  --period 60 --namespace "AWS/RDS" --statistics Maximum \
  --dimensions Name=DBInstanceIdentifier,Value=instance-6305 --output text \
  | sort -k 3
EngineUptime
DATAPOINTS 231.0 2021-03-16T18:19:00+00:00 Seconds
DATAPOINTS 291.0 2021-03-16T18:20:00+00:00 Seconds
DATAPOINTS 351.0 2021-03-16T18:21:00+00:00 Seconds
DATAPOINTS 411.0 2021-03-16T18:22:00+00:00 Seconds
DATAPOINTS 471.0 2021-03-16T18:23:00+00:00 Seconds
```

Die minimale Betriebszeit für den Cluster wird auf Null zurückgesetzt, da eine der Instances im Cluster neu gestartet wurde. Die maximale Betriebszeit für den Cluster wird nicht zurückgesetzt, da mindestens eine der DB-Instances im Cluster verfügbar blieb.

```
$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" \
```

```
  --period 60 --namespace "AWS/RDS" --statistics Minimum \
  --dimensions Name=DBClusterIdentifier,Value=tpch100g --output text \
  | sort -k 3
EngineUptime
DATAPOINTS 63099.0 2021-03-16T18:12:00+00:00 Seconds
DATAPOINTS 63159.0 2021-03-16T18:13:00+00:00 Seconds
DATAPOINTS 63219.0 2021-03-16T18:14:00+00:00 Seconds
DATAPOINTS 63279.0 2021-03-16T18:15:00+00:00 Seconds
DATAPOINTS 51.0 2021-03-16T18:16:00+00:00 Seconds

$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" \
  --period 60 --namespace "AWS/RDS" --statistics Maximum \
  --dimensions Name=DBClusterIdentifier,Value=tpch100g --output text \
  | sort -k 3
EngineUptime
DATAPOINTS 63389.0 2021-03-16T18:16:00+00:00 Seconds
DATAPOINTS 63449.0 2021-03-16T18:17:00+00:00 Seconds
DATAPOINTS 63509.0 2021-03-16T18:18:00+00:00 Seconds
DATAPOINTS 63569.0 2021-03-16T18:19:00+00:00 Seconds
DATAPOINTS 63629.0 2021-03-16T18:20:00+00:00 Seconds
```

Dann startet ein anderer `reboot-db-instance` Befehl die Writer-Instance des Clusters neu. Ein anderer `wait` Befehl wird pausiert, bis die Writer-Instance mit dem Neustart abgeschlossen ist.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-1234
{
  "DBInstanceIdentifier": "instance-1234",
  "DBInstanceStatus": "rebooting",
...
$ aws rds wait db-instance-available --db-instance-id instance-1234
```

Jetzt zeigt die `EngineUptime` Metrik für die Writer-Instance, dass die Instance `instance-1234` kürzlich neu gestartet wurde. Die Reader-Instance `instance-6305` wurde zusammen mit der Writer-Instance ebenfalls automatisch neu gestartet. Auf diesem Cluster wird Aurora MySQL 2.09 ausgeführt, wodurch die Reader-Instances nicht weiter ausgeführt werden, wenn die Writer-Instance neu gestartet wird.

```
$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" \
  --period 60 --namespace "AWS/RDS" --statistics Maximum \
  --dimensions Name=DBInstanceIdentifier,Value=instance-1234 --output text \
```

```
  | sort -k 3
EngineUptime
DATAPOINTS 63749.0 2021-03-16T18:22:00+00:00 Seconds
DATAPOINTS 63809.0 2021-03-16T18:23:00+00:00 Seconds
DATAPOINTS 63869.0 2021-03-16T18:24:00+00:00 Seconds
DATAPOINTS 41.0 2021-03-16T18:25:00+00:00 Seconds
DATAPOINTS 101.0 2021-03-16T18:26:00+00:00 Seconds

$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" \
  --period 60 --namespace "AWS/RDS" --statistics Maximum \
  --dimensions Name=DBInstanceIdentifier,Value=instance-6305 --output text \
  | sort -k 3
EngineUptime
DATAPOINTS 411.0 2021-03-16T18:22:00+00:00 Seconds
DATAPOINTS 471.0 2021-03-16T18:23:00+00:00 Seconds
DATAPOINTS 531.0 2021-03-16T18:24:00+00:00 Seconds
DATAPOINTS 49.0 2021-03-16T18:26:00+00:00 Seconds
```

Beispiele für Aurora Neustartvorgänge

Die folgenden Aurora MySQL Beispiele zeigen verschiedene Kombinationen von Neustartvorgängen für Reader- und Writer-DB-Instances in einem Aurora DB-Cluster. Nach jedem Neustart demonstrieren SQL-Abfragen die Verfügbarkeit der Instances im Cluster.

Themen

- Finden der Writer- und Reader-Instances für einen Aurora-Cluster
- Neustart einer einzelnen Reader-Instance
- Neustart der Writer-Instance
- Den Writer und die Reader unabhängig neu starten
- Anwenden einer Clusterparameteränderung auf einen Cluster der Aurora MySQL Version 2.10

Finden der Writer- und Reader-Instances für einen Aurora-Cluster

In einem Aurora MySQL Cluster mit mehreren DB-Instances ist es wichtig zu wissen, welche der Writer und welche die Reader sind. Die Writer- und Reader-Instances können auch Rollen wechseln, wenn ein Failover-Vorgang stattfindet. Daher ist es am besten, eine Überprüfung wie die folgende durchzuführen, bevor Sie eine Operation ausführen, die eine Writer- oder Reader-Instance erfordert. In diesem Fall identifizieren die `False`-Werte für `IsClusterWriter` die Reader-

Instances, `instance-6305` und `instance-7448`. Der `True` Wert identifiziert die Writer-Instance `instance-1234`.

```
$ aws rds describe-db-clusters --db-cluster-id tpch100g \
  --query "*[].['Cluster:',DBClusterIdentifier,DBClusterMembers[*].
['Instance:',DBInstanceIdentifier,IsClusterWriter]]" \
  --output text
Cluster:     tpch100g
Instance:    instance-6305    False
Instance:    instance-7448    False
Instance:    instance-1234    True
```

Bevor wir mit den Beispielen für den Neustart beginnen, hat die Writer-Instance eine Betriebszeit von ungefähr einer Woche. Die SQL-Abfrage in diesem Beispiel zeigt eine MySQL-spezifische Möglichkeit, die Betriebszeit zu überprüfen. Sie können diese Technik in einer Datenbankanwendung verwenden. Eine weitere Technik, bei der das AWS CLI und für beide Aurora-Engines verwendet wird, finden Sie unterÜberprüfung der Betriebszeit für Aurora Cluster und Instances.

```
$ mysql -h instance-7448.a12345.us-east-1.rds.amazonaws.com -P 3306 -u my-user -p
...
mysql> select date_sub(now(), interval variable_value second) "Last Startup",
    -> time_format(sec_to_time(variable_value),'%Hh %im') as "Uptime"
    -> from performance_schema.global_status
    -> where variable_name='Uptime';
+----------------------------+---------+
| Last Startup               | Uptime  |
+----------------------------+---------+
| 2021-03-08 17:49:06.000000 | 174h 42m|
+----------------------------+---------+
```

Neustart einer einzelnen Reader-Instance

In diesem Beispiel wird eine der Reader-DB-Instances neu gestartet. Vielleicht wurde diese Instance von einer riesigen Abfrage oder vielen gleichzeitigen Verbindungen überlastet. Oder vielleicht fiel sie wegen eines Netzwerkproblems hinter die Writer-Instance zurück. Nach dem Start des Neustartvorgangs verwendet das Beispiel einen `wait` Befehl, um anzuhalten, bis die Instance verfügbar ist. Zu diesem Zeitpunkt hat die Instance eine Betriebszeit von einigen Minuten.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-6305
{
```

```
    "DBInstance": {
        "DBInstanceIdentifier": "instance-6305",
        "DBInstanceStatus": "rebooting",
...
    }
}
$ aws rds wait db-instance-available --db-instance-id instance-6305
$ mysql -h instance-6305.a12345.us-east-1.rds.amazonaws.com -P 3306 -u my-user -p
...
mysql> select date_sub(now(), interval variable_value second) "Last Startup",
    -> time_format(sec_to_time(variable_value),'%Hh %im') as "Uptime"
    -> from performance_schema.global_status
    -> where variable_name='Uptime';
+----------------------------+---------+
| Last Startup               | Uptime  |
+----------------------------+---------+
| 2021-03-16 00:35:02.000000 | 00h 03m |
+----------------------------+---------+
```

Der Neustart der Reader-Instance hatte keinen Einfluss auf die Verfügbarkeit der Writer-Instance. Sie hat immer noch eine Betriebszeit von etwa einer Woche.

```
$ mysql -h instance-7448.a12345.us-east-1.rds.amazonaws.com -P 3306 -u my-user -p
...
mysql> select date_sub(now(), interval variable_value second) "Last Startup",
    -> time_format(sec_to_time(variable_value),'%Hh %im') as "Uptime"
    -> from performance_schema.global_status where variable_name='Uptime';
+----------------------------+----------+
| Last Startup               | Uptime   |
+----------------------------+----------+
| 2021-03-08 17:49:06.000000 | 174h 49m |
+----------------------------+----------+
```

Neustart der Writer-Instance

In diesem Beispiel wird die Writer-Instance neu gestartet. Auf diesem Cluster wird Aurora MySQL Version 2.09 ausgeführt. Da die Aurora MySQL Version niedriger als 2.10 ist, werden beim Neustart der Writer-Instance auch alle Reader-Instances im Cluster neu gestartet.

Ein `wait` Befehl wird angehalten, bis der Neustart abgeschlossen ist. Jetzt wird die Betriebszeit für diese Instance auf Null zurückgesetzt. Es ist möglich, dass ein Neustartvorgang für Writer- und Reader-DB-Instances erheblich unterschiedliche Zeiten in Anspruch nehmen kann. Die Writer- und

Reader-DB-Instances führen je nach ihren Rollen verschiedene Arten von Bereinigungsvorgängen aus.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-1234
{
    "DBInstance": {
        "DBInstanceIdentifier": "instance-1234",
        "DBInstanceStatus": "rebooting",
...
    }
}
$ aws rds wait db-instance-available --db-instance-id instance-1234
$ mysql -h instance-1234.a12345.us-east-1.rds.amazonaws.com -P 3306 -u my-user -p
...
mysql> select date_sub(now(), interval variable_value second) "Last Startup",
    -> time_format(sec_to_time(variable_value),'%Hh %im') as "Uptime"
    -> from performance_schema.global_status where variable_name='Uptime';
+----------------------------+---------+
| Last Startup               | Uptime  |
+----------------------------+---------+
| 2021-03-16 00:40:27.000000 | 00h 00m |
+----------------------------+---------+
```

Nach dem Neustart für die Writer-DB-Instance haben beide Reader-DB-Instances auch ihre Betriebszeit zurückgesetzt. Durch den Neustart der Writer-Instance wurden die Reader-Instances ebenfalls neu gestartet. Dieses Verhalten gilt für Aurora PostgreSQL Cluster und Aurora MySQL Cluster vor Version 2.10.

```
$ mysql -h instance-7448.a12345.us-east-1.rds.amazonaws.com -P 3306 -u my-user -p
...
mysql> select date_sub(now(), interval variable_value second) "Last Startup",
    -> time_format(sec_to_time(variable_value),'%Hh %im') as "Uptime"
    -> from performance_schema.global_status where variable_name='Uptime';
+----------------------------+---------+
| Last Startup               | Uptime  |
+----------------------------+---------+
| 2021-03-16 00:40:35.000000 | 00h 00m |
+----------------------------+---------+

$ mysql -h instance-6305.a12345.us-east-1.rds.amazonaws.com -P 3306 -u my-user -p
...
mysql> select date_sub(now(), interval variable_value second) "Last Startup",
```

```
    -> time_format(sec_to_time(variable_value),'%Hh %im') as "Uptime"
    -> from performance_schema.global_status where variable_name='Uptime';
+----------------------------+---------+
| Last Startup               | Uptime  |
+----------------------------+---------+
| 2021-03-16 00:40:33.000000 | 00h 01m |
+----------------------------+---------+
```

Den Writer und die Reader unabhängig neu starten

Diese nächsten Beispiele zeigen einen Cluster, der Aurora MySQL Version 2.10 ausführt. In dieser Aurora MySQL Version und höher können Sie die Writer-Instance neu starten, ohne Neustarts für alle Reader-Instances zu verursachen. Auf diese Weise kommt es bei Ihren abfrachintensiven Anwendungen zu keinem Ausfall, wenn Sie die Writer-Instance neu starten. Sie können die Reader-Instances später neu starten. Sie können diese Neustarts zu einem Zeitpunkt mit geringem Abfrageverkehr durchführen. Sie können die Reader-Instances auch nacheinander neu starten. Auf diese Weise steht immer mindestens eine Reader-Instance für den Abfrageverkehr Ihrer Anwendung zur Verfügung.

Im folgenden Beispiel wird ein Cluster namens `cluster-2393` verwendet, auf dem Aurora MySQL Version `5.7.mysql_aurora.2.10.0` ausgeführt wird. Dieser Cluster hat eine Writer-Instance namens `instance-9404` und drei Reader-Instances namens `instance-6772`, `instance-2470` und `instance-5138`.

```
$ aws rds describe-db-clusters --db-cluster-id cluster-2393 \
  --query "*[].['Cluster:',DBClusterIdentifier,DBClusterMembers[*].
['Instance:',DBInstanceIdentifier,IsClusterWriter]]" \
  --output text
Cluster:        cluster-2393
Instance:       instance-5138        False
Instance:       instance-2470        False
Instance:       instance-6772        False
Instance:       instance-9404        True
```

Die Überprüfung des `uptime` Werts jeder Datenbankinstance mit dem Befehl `mysql` zeigt, dass jede ungefähr die gleiche Betriebszeit hat. Hier ist zum Beispiel die Betriebszeit für `instance-5138`.

```
mysql> SHOW GLOBAL STATUS LIKE 'uptime';
+---------------+-------+
| Variable_name | Value |
```

```
+---------------+-------+
| Uptime        | 3866  |
+---------------+-------+
```

Durch die Verwendung können wir die entsprechenden Verfügbarkeitsinformationen abrufen CloudWatch, ohne uns tatsächlich bei den Instances anmelden zu müssen. Auf diese Weise kann ein Administrator die Datenbank überwachen, aber keine Tabellendaten anzeigen oder ändern. In diesem Fall geben wir einen Zeitraum von fünf Minuten an und überprüfen den Betriebszeitwert jede Minute. Die zunehmenden Betriebszeitwerte zeigen, dass die Instances in diesem Zeitraum nicht neu gestartet wurden.

```
$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBInstanceIdentifier,Value=instance-9404 \
  --output text | sort -k 3
EngineUptime
DATAPOINTS 4648.0 2021-03-17T23:42:00+00:00 Seconds
DATAPOINTS 4708.0 2021-03-17T23:43:00+00:00 Seconds
DATAPOINTS 4768.0 2021-03-17T23:44:00+00:00 Seconds
DATAPOINTS 4828.0 2021-03-17T23:45:00+00:00 Seconds
DATAPOINTS 4888.0 2021-03-17T23:46:00+00:00 Seconds

$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBInstanceIdentifier,Value=instance-6772 \
  --output text | sort -k 3
EngineUptime
DATAPOINTS 4315.0 2021-03-17T23:42:00+00:00 Seconds
DATAPOINTS 4375.0 2021-03-17T23:43:00+00:00 Seconds
DATAPOINTS 4435.0 2021-03-17T23:44:00+00:00 Seconds
DATAPOINTS 4495.0 2021-03-17T23:45:00+00:00 Seconds
DATAPOINTS 4555.0 2021-03-17T23:46:00+00:00 Seconds
```

Jetzt starten wir eine der Reader-Instances neu, `instance-5138`. Wir warten darauf, dass die Instance nach dem Neustart wieder verfügbar ist. Die Überwachung der Betriebszeit über einen Zeitraum von fünf Minuten zeigt, dass die Betriebszeit während dieser Zeit auf Null zurückgesetzt wurde. Der letzte Betriebszeitwert wurde fünf Sekunden nach Abschluss des Neustarts gemessen.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-5138
```

```
{
  "DBInstanceIdentifier": "instance-5138",
  "DBInstanceStatus": "rebooting"
}
$ aws rds wait db-instance-available --db-instance-id instance-5138

$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBInstanceIdentifier,Value=instance-5138 \
  --output text | sort -k 3
EngineUptime
DATAPOINTS 4500.0 2021-03-17T23:46:00+00:00 Seconds
DATAPOINTS 4560.0 2021-03-17T23:47:00+00:00 Seconds
DATAPOINTS 4620.0 2021-03-17T23:48:00+00:00 Seconds
DATAPOINTS 4680.0 2021-03-17T23:49:00+00:00 Seconds
DATAPOINTS  5.0 2021-03-17T23:50:00+00:00 Seconds
```

Als Nächstes führen wir einen Neustart für die Writer-Instance durch, `instance-9404`. Wir vergleichen die Betriebszeit-Werte für die Writer-Instance und eine der Reader-Instances. Auf diese Weise können wir sehen, dass der Neustart des Writers für die Reader keinen Neustart verursacht hat. In Versionen vor Aurora MySQL 2.10 würden die Verfügbarkeitswerte für alle Reader gleichzeitig mit dem Writer zurückgesetzt.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-9404
{
  "DBInstanceIdentifier": "instance-9404",
  "DBInstanceStatus": "rebooting"
}
$ aws rds wait db-instance-available --db-instance-id instance-9404

$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBInstanceIdentifier,Value=instance-9404 \
  --output text | sort -k 3
EngineUptime
DATAPOINTS 371.0 2021-03-17T23:57:00+00:00 Seconds
DATAPOINTS 431.0 2021-03-17T23:58:00+00:00 Seconds
DATAPOINTS 491.0 2021-03-17T23:59:00+00:00 Seconds
DATAPOINTS 551.0 2021-03-18T00:00:00+00:00 Seconds
DATAPOINTS  37.0  2021-03-18T00:01:00+00:00 Seconds
```

```
$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBInstanceIdentifier,Value=instance-6772 \
  --output text | sort -k 3
EngineUptime
DATAPOINTS 5215.0 2021-03-17T23:57:00+00:00 Seconds
DATAPOINTS 5275.0 2021-03-17T23:58:00+00:00 Seconds
DATAPOINTS 5335.0 2021-03-17T23:59:00+00:00 Seconds
DATAPOINTS 5395.0 2021-03-18T00:00:00+00:00 Seconds
DATAPOINTS 5455.0 2021-03-18T00:01:00+00:00 Seconds
```

Um sicherzustellen, dass alle Reader-Instances dieselben Änderungen an den Konfigurationsparametern haben wie die Writer-Instance, starten Sie alle Reader-Instances nach dem Writer neu. Dieses Beispiel startet alle Reader neu und wartet dann, bis alle verfügbar sind, bevor Sie fortfahren.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-6772
{
  "DBInstanceIdentifier": "instance-6772",
  "DBInstanceStatus": "rebooting"
}

$ aws rds reboot-db-instance --db-instance-identifier instance-2470
{
  "DBInstanceIdentifier": "instance-2470",
  "DBInstanceStatus": "rebooting"
}

$ aws rds reboot-db-instance --db-instance-identifier instance-5138
{
  "DBInstanceIdentifier": "instance-5138",
  "DBInstanceStatus": "rebooting"
}

$ aws rds wait db-instance-available --db-instance-id instance-6772
$ aws rds wait db-instance-available --db-instance-id instance-2470
$ aws rds wait db-instance-available --db-instance-id instance-5138
```

Jetzt können wir sehen, dass die Writer-DB-Instance die höchste Betriebszeit hat. Der Betriebszeitwert dieser Instance stieg während des gesamten Überwachungszeitraums stetig an. Die Reader DB-Instances wurden alle nach dem Reader neu gestartet. Wir können den Punkt

innerhalb des Überwachungszeitraums sehen, an dem jeder Reader neu gestartet wurde und seine Betriebszeit auf Null zurückgesetzt wurde.

```
$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBInstanceIdentifier,Value=instance-9404 \
  --output text | sort -k 3
EngineUptime
DATAPOINTS 457.0 2021-03-18T00:08:00+00:00 Seconds
DATAPOINTS 517.0 2021-03-18T00:09:00+00:00 Seconds
DATAPOINTS 577.0 2021-03-18T00:10:00+00:00 Seconds
DATAPOINTS 637.0 2021-03-18T00:11:00+00:00 Seconds
DATAPOINTS  697.0 2021-03-18T00:12:00+00:00 Seconds

$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBInstanceIdentifier,Value=instance-2470 \
  --output text | sort -k 3
EngineUptime
DATAPOINTS 5819.0 2021-03-18T00:08:00+00:00 Seconds
DATAPOINTS  35.0  2021-03-18T00:09:00+00:00 Seconds
DATAPOINTS 95.0 2021-03-18T00:10:00+00:00 Seconds
DATAPOINTS 155.0 2021-03-18T00:11:00+00:00 Seconds
DATAPOINTS 215.0 2021-03-18T00:12:00+00:00 Seconds

$ aws cloudwatch get-metric-statistics --metric-name "EngineUptime" \
  --start-time "$(date -d '5 minutes ago')" --end-time "$(date -d 'now')" --period 60 \
  --namespace "AWS/RDS" --statistics Minimum --dimensions
 Name=DBInstanceIdentifier,Value=instance-5138 \
  --output text | sort -k 3
EngineUptime
DATAPOINTS 1085.0 2021-03-18T00:08:00+00:00 Seconds
DATAPOINTS 1145.0 2021-03-18T00:09:00+00:00 Seconds
DATAPOINTS 1205.0 2021-03-18T00:10:00+00:00 Seconds
DATAPOINTS  49.0  2021-03-18T00:11:00+00:00 Seconds
DATAPOINTS 109.0 2021-03-18T00:12:00+00:00 Seconds
```

Anwenden einer Clusterparameteränderung auf einen Cluster der Aurora MySQL Version 2.10

Das folgende Beispiel veranschaulicht, wie Sie eine Parameteränderung auf alle DB-Instances in Ihrem Aurora MySQL 2.10-Cluster anwenden. Mit dieser Aurora MySQL Version starten Sie die Writer-Instance und alle Reader-Instances unabhängig neu.

Das Beispiel verwendet den MySQL-Konfigurationsparameter `lower_case_table_names` zur Veranschaulichung. Wenn sich diese Parametereinstellung zwischen den Writer- und Reader-DB-Instances unterscheidet, kann eine Abfrage möglicherweise nicht auf eine Tabelle zugreifen, die mit einem Namen in Großbuchstaben oder gemischten Buchstaben deklariert wurde. Oder wenn sich zwei Tabellennamen nur in Groß- und Kleinbuchstaben unterscheiden, kann eine Abfrage auf die falsche Tabelle zugreifen.

Dieses Beispiel zeigt, wie Sie die Writer- und Reader-Instances im Cluster ermitteln können, indem Sie das `IsClusterWriter` Attribut jeder Instance untersuchen. Der Cluster heißt `cluster-2393`. Der Cluster hat eine Writer-Instance namens `instance-9404`. Die Reader-Instances im Cluster heißen `instance-5138` und `instance-2470`.

```
$ aws rds describe-db-clusters --db-cluster-id cluster-2393 \
  --query '*[].[DBClusterIdentifier,DBClusterMembers[*].
[DBInstanceIdentifier,IsClusterWriter]]' \
  --output text
cluster-2393
instance-5138        False
instance-2470        False
instance-9404        True
```

Um die Auswirkungen der Änderung des `lower_case_table_names` Parameters zu demonstrieren, richten wir zwei DB-Cluster-Parametergruppen ein. Für die `lower-case-table-names-0` Parametergruppe ist dieser Parameter auf 0 festgelegt. Die `lower-case-table-names-1` Parametergruppe hat diese Parametergruppe auf 1 festgelegt.

```
$ aws rds create-db-cluster-parameter-group --description 'lower-case-table-names-0' \
  --db-parameter-group-family aurora-mysql5.7 \
  --db-cluster-parameter-group-name lower-case-table-names-0
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "lower-case-table-names-0",
        "DBParameterGroupFamily": "aurora-mysql5.7",
```

```
        "Description": "lower-case-table-names-0"
    }
}

$ aws rds create-db-cluster-parameter-group --description 'lower-case-table-names-1' \
  --db-parameter-group-family aurora-mysql5.7 \
  --db-cluster-parameter-group-name lower-case-table-names-1
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "lower-case-table-names-1",
        "DBParameterGroupFamily": "aurora-mysql5.7",
        "Description": "lower-case-table-names-1"
    }
}

$ aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name lower-case-table-names-0 \
  --parameters
 ParameterName=lower_case_table_names,ParameterValue=0,ApplyMethod=pending-reboot
{
    "DBClusterParameterGroupName": "lower-case-table-names-0"
}

$ aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name lower-case-table-names-1 \
    --parameters
 ParameterName=lower_case_table_names,ParameterValue=1,ApplyMethod=pending-reboot
{
    "DBClusterParameterGroupName": "lower-case-table-names-1"
}
```

Der Standardwert von `lower_case_table_names` ist 0. Bei dieser Parametereinstellung unterscheidet sich die Tabelle `foo` von der Tabelle `F00`. In diesem Beispiel wird überprüft, dass der Parameter immer noch seine Standardeinstellung hat. Dann erstellt das Beispiel drei Tabellen, die sich nur in Groß- und Kleinbuchstaben in ihren Namen unterscheiden.

```
mysql> create database lctn;
Query OK, 1 row affected (0.07 sec)

mysql> use lctn;
Database changed
mysql> select @@lower_case_table_names;
+--------------------------+
```

```
| @@lower_case_table_names |
+--------------------------+
|                        0 |
+--------------------------+

mysql> create table foo (s varchar(128));
mysql> insert into foo values ('Lowercase table name foo');

mysql> create table Foo (s varchar(128));
mysql> insert into Foo values ('Mixed-case table name Foo');

mysql> create table FOO (s varchar(128));
mysql> insert into FOO values ('Uppercase table name FOO');

mysql> select * from foo;
+--------------------------+
| s                        |
+--------------------------+
| Lowercase table name foo |
+--------------------------+

mysql> select * from Foo;
+---------------------------+
| s                         |
+---------------------------+
| Mixed-case table name Foo |
+---------------------------+

mysql> select * from FOO;
+--------------------------+
| s                        |
+--------------------------+
| Uppercase table name FOO |
+--------------------------+
```

Als Nächstes verknüpfen wir die DB-Parametergruppe mit dem Cluster, um den `lower_case_table_names` Parameter auf 1 festzulegen. Diese Änderung wird erst wirksam, nachdem jede DB-Instance neu gestartet wurde.

```
$ aws rds modify-db-cluster --db-cluster-identifier cluster-2393 \
  --db-cluster-parameter-group-name lower-case-table-names-1
{
  "DBClusterIdentifier": "cluster-2393",
```

```
  "DBClusterParameterGroup": "lower-case-table-names-1",
  "Engine": "aurora-mysql",
  "EngineVersion": "5.7.mysql_aurora.2.10.0"
}
```

Der erste Neustart, den wir machen, ist für die Writer-DB-Instance. Dann warten wir, bis die Instance wieder verfügbar wird. An diesem Punkt stellen wir eine Verbindung zum Writer-Endpunkt her und stellen sicher, dass die Writer-Instance den geänderten Parameterwert hat. Der `SHOW TABLES` Befehl bestätigt, dass die Datenbank die drei verschiedenen Tabellen enthält. Abfragen, die sich auf Tabellen mit den Namen `foo`, `Foo` oder `F00` beziehen, greifen jedoch alle auf die Tabelle zu, deren Name nur aus Kleinbuchstaben besteht, `foo` .

```
# Rebooting the writer instance
$ aws rds reboot-db-instance --db-instance-identifier instance-9404
$ aws rds wait db-instance-available --db-instance-id instance-9404
```

Abfragen, die den Cluster-Endpunkt verwenden, zeigen nun die Auswirkungen der Parameteränderung. Unabhängig davon, ob der Tabellenname in der Abfrage aus Groß-, Kleinbuchstaben- oder gemischten Buchstaben besteht, greift die SQL-Anweisung auf die Tabelle zu, deren Name ganz aus Kleinbuchstaben besteht.

```
mysql> select @@lower_case_table_names;
+--------------------------+
| @@lower_case_table_names |
+--------------------------+
|                        1 |
+--------------------------+

mysql> use lctn;
mysql> show tables;
+----------------+
| Tables_in_lctn |
+----------------+
| FOO            |
| Foo            |
| foo            |
+----------------+

mysql> select * from foo;
+--------------------------+
| s                        |
```

```
+--------------------------+
| Lowercase table name foo |
+--------------------------+

mysql> select * from Foo;
+--------------------------+
| s                        |
+--------------------------+
| Lowercase table name foo |
+--------------------------+

mysql> select * from FOO;
+--------------------------+
| s                        |
+--------------------------+
| Lowercase table name foo |
+--------------------------+
```

Das nächste Beispiel zeigt die gleichen Abfragen wie das vorherige. In diesem Fall verwenden die Abfragen den Reader-Endpunkt und werden auf einer der Reader DB-Instances ausgeführt. Diese Instances wurden noch nicht neu gestartet. Somit haben sie immer noch die ursprüngliche Einstellung für den `lower_case_table_names` Parameter. Das bedeutet, dass Abfragen auf jede der `foo`-, `Foo`- und `F00`-Tabellen zugreifen können.

```
mysql> select @@lower_case_table_names;
+--------------------------+
| @@lower_case_table_names |
+--------------------------+
|                        0 |
+--------------------------+

mysql> use lctn;

mysql> select * from foo;
+--------------------------+
| s                        |
+--------------------------+
| Lowercase table name foo |
+--------------------------+

mysql> select * from Foo;
+--------------------------+
| s                         |
```

```
+---------------------------+
| Mixed-case table name Foo |
+---------------------------+

mysql> select * from FOO;
+---------------------------+
| s                         |
+---------------------------+
| Uppercase table name FOO |
+---------------------------+
```

Als Nächstes starten wir eine der Reader-Instances neu und warten darauf, dass sie wieder verfügbar ist.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-2470
{
  "DBInstanceIdentifier": "instance-2470",
  "DBInstanceStatus": "rebooting"
}
$ aws rds wait db-instance-available --db-instance-id instance-2470
```

Während eine Abfrage mit dem Instance-Endpunkt für `instance-2470` verbunden ist, zeigt eine Abfrage, dass der neue Parameter in Kraft ist.

```
mysql> select @@lower_case_table_names;
+---------------------------+
| @@lower_case_table_names |
+---------------------------+
|                         1 |
+---------------------------+
```

Zu diesem Zeitpunkt werden die beiden Reader-Instances im Cluster mit unterschiedlichen `lower_case_table_names` Einstellungen ausgeführt. Daher verwendet jede Verbindung zum Reader-Endpunkt des Clusters einen Wert für diese Einstellung, der unvorhersehbar ist. Es ist wichtig, die andere Reader-Instance sofort neu zu starten, damit beide konsistente Einstellungen haben.

```
$ aws rds reboot-db-instance --db-instance-identifier instance-5138
{
  "DBInstanceIdentifier": "instance-5138",
  "DBInstanceStatus": "rebooting"
```

```
}
$ aws rds wait db-instance-available --db-instance-id instance-5138
```

Das folgende Beispiel bestätigt, dass alle Reader-Instances dieselbe Einstellung für den `lower_case_table_names` Parameter haben. Die Befehle überprüfen den `lower_case_table_names` Einstellungswert für jede Reader-Instance. Dann zeigt derselbe Befehl, der den Reader-Endpunkt verwendet, dass jede Verbindung zum Reader-Endpunkt eine der Reader-Instances verwendet, welche jedoch nicht vorhersehbar ist.

```
# Check lower_case_table_names setting on each reader instance.

$ mysql -h instance-5138.a12345.us-east-1.rds.amazonaws.com \
  -u my-user -p -e 'select @@aurora_server_id, @@lower_case_table_names'
+--------------------------+--------------------------+
| @@aurora_server_id       | @@lower_case_table_names |
+--------------------------+--------------------------+
| instance-5138            |                        1 |
+--------------------------+--------------------------+

$ mysql -h instance-2470.a12345.us-east-1.rds.amazonaws.com \
  -u my-user -p -e 'select @@aurora_server_id, @@lower_case_table_names'
+--------------------------+--------------------------+
| @@aurora_server_id       | @@lower_case_table_names |
+--------------------------+--------------------------+
| instance-2470            |                        1 |
+--------------------------+--------------------------+

# Check lower_case_table_names setting on the reader endpoint of the cluster.

$ mysql -h cluster-2393.cluster-ro-a12345.us-east-1.rds.amazonaws.com \
  -u my-user -p -e 'select @@aurora_server_id, @@lower_case_table_names'
+--------------------------+--------------------------+
| @@aurora_server_id       | @@lower_case_table_names |
+--------------------------+--------------------------+
| instance-5138            |                        1 |
+--------------------------+--------------------------+

# Run query on writer instance

$ mysql -h cluster-2393.cluster-a12345.us-east-1.rds.amazonaws.com \
  -u my-user -p -e 'select @@aurora_server_id, @@lower_case_table_names'
+--------------------------+--------------------------+
| @@aurora_server_id       | @@lower_case_table_names |
```

```
+--------------------------+--------------------------+
| instance-9404            |                        1 |
+--------------------------+--------------------------+
```

Wenn die Parameteränderung überall angewendet wird, können wir die Auswirkungen der Einstellung von sehe `lower_case_table_names=1`. Unabhängig davon, ob die Tabelle als `foo` , `Foo` oder `F00` bezeichnet wird, wandelt die Abfrage den Namen in `foo` um und greift jeweils auf dieselbe Tabelle zu.

```
mysql> use lctn;

mysql> select * from foo;
+--------------------------+
| s                        |
+--------------------------+
| Lowercase table name foo |
+--------------------------+

mysql> select * from Foo;
+--------------------------+
| s                        |
+--------------------------+
| Lowercase table name foo |
+--------------------------+

mysql> select * from FOO;
+--------------------------+
| s                        |
+--------------------------+
| Lowercase table name foo |
+--------------------------+
```

Löschen von Aurora-DB-Clustern und -DB-Instances

Sie können einen Aurora-DB-Cluster löschen, wenn Sie ihn nicht mehr benötigen. Durch Löschen des Clusters wird das Cluster-Volume entfernt, das all Ihre Daten enthält. Bevor Sie den Cluster löschen, können Sie einen Snapshot Ihrer Daten speichern. Sie können den Snapshot später wiederherstellen, um einen neuen Cluster erstellen, der dieselben Daten enthält.

Sie können auch DB-Instances aus einem Cluster löschen, während der Cluster selbst und die darin enthaltenen Daten erhalten bleiben. Durch Löschen von DB-Instances können Sie die Kosten senken, wenn der Cluster nicht ausgelastet ist und Sie nicht die Rechenkapazität mehrerer DB-Instances benötigen.

Themen

Löschen eines Aurora-Dönnen einen Cluster nicht löschen,B-Clusters

Aurora bietet keine Methode zum Löschen eines DB-Clusters in einem Schritt. Dadurch soll bewusst verhindert werden, dass Sie versehentlich Daten verlieren oder Ihre Anwendung offline schalten. Aurora-Anwendungen sind in der Regel geschäftskritisch und erfordern hohe Verfügbarkeit. Deshalb lässt sich mit Aurora die Kapazität des Clusters einfach durch Hinzufügen und Entfernen von DB-Instances aufwärts und abwärts skalieren. Um den Cluster selbst zu entfernen, müssen Sie eine separate Auswahl treffen.

Verwenden Sie das folgende allgemeine Verfahren, um alle DB-Instances aus einem Cluster zu entfernen und dann den Cluster selbst zu löschen.

1. Löschen Sie alle Reader-Instances im Cluster. Verwenden Sie das Verfahren in Löschen einer DB-Instance aus einem Aurora-DB-Cluster.

   Wenn der Cluster Reader-Instances enthält, reduziert das Löschen einer der Instances nur die Rechenkapazität des Clusters. Indem die Reader-Instances zuerst gelöscht werden, wird

sichergestellt, dass der Cluster während des gesamten Verfahrens verfügbar bleibt und keine unnötigen Failover-Vorgänge durchführt.

2. Löschen Sie die Writer-Instance aus dem Cluster. Verwenden Sie erneut das Verfahren in Löschen einer DB-Instance aus einem Aurora-DB-Cluster.

   Wenn Sie die DB-Instances löschen, bleiben der Cluster und das zugehörige Cluster-Volume auch nach dem Löschen aller DB-Instances bestehen.

3. Löschen Sie den DB-Cluster.

   - AWS Management Console – Wählen Sie den Cluster aus und wählen Sie dann Löschen im Menü Aktionen aus. Sie können die folgenden Optionen auswählen, um die Daten aus dem Cluster beizubehalten, falls Sie sie später benötigen:
     - Erstellen Sie einen finalen Snapshot des Cluster-Volumes. Standardmäßig wird ein finaler Snapshot erstellt.
     - Sie müssen automatisierte Sicherungen aufbewahren. Die Standardeinstellung ist, automatisierte Backups nicht beizubehalten.

     > **Note**
     >
     > Automatisierte Backups für Aurora Serverless v1 -DB-Cluster werden nicht beibehalten.

     Aurora erfordert außerdem, dass Sie bestätigen, dass Sie den Cluster löschen möchten.
   - CLI und API – Rufen Sie den CLI-Befehl `delete-db-cluster` oder die API-Operation `DeleteDBCluster` auf. Sie können die folgenden Optionen auswählen, um die Daten aus dem Cluster beizubehalten, falls Sie sie später benötigen:
     - Erstellen Sie einen finalen Snapshot des Cluster-Volumes.
     - Sie müssen automatisierte Sicherungen aufbewahren.

     > **Note**
     >
     > Automatisierte Backups für Aurora Serverless v1 -DB-Cluster werden nicht beibehalten.

Themen

- Erstellen eines leeren Aurora-Clusters
- Löschen eines Aurora-Clusters mit einer einzigen DB-Instance
- Löschen eines Aurora-Clusters mit mehreren DB-Instances

Erstellen eines leeren Aurora-Clusters

Sie können einen leeren DB-Cluster über die AWS Management Console, die AWS CLI oder die Amazon-RDS-API löschen.

> **Tip**
>
> Sie können einen Cluster ohne DB-Instances behalten, um Ihre Daten zu behalten, ohne dass CPU-Gebühren für den Cluster anfallen. Sie können den Cluster schnell wieder verwenden, indem Sie eine oder mehrere neue DB-Instances für den Cluster erstellen. Sie können auch Aurora-spezifische administrative Vorgänge auf dem Cluster durchführen, während ihm keine DB-Instances zugeordnet sind. Sie können bloß nicht auf die Daten zugreifen oder Vorgänge durchführen, die eine Verbindung mit einer DB-Instance erfordern.

Konsole

So löschen Sie einen DB-Cluster

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken und dann den DB-Cluster aus, den Sie löschen möchten.
3. Klicken Sie bei Actions auf Delete.
4. Wählen Sie Abschließenden Snapshot erstellen? aus, um einen endgültigen DB-Snapshot für den DB-Cluster zu erstellen. Dies ist die Standardeinstellung.
5. Wenn Sie einen endgültigen Snapshot erstellen möchten, geben Sie den Final snapshot name (Name des endgültigen Snapshots) ein.
6. Wählen Sie Retain automated backups (Automatisierte Sicherungen aufbewahren), um automatisierte Sicherungen aufzubewahren. Dies ist nicht die Standardeinstellung.
7. Geben Sie **`delete me`** in das Feld ein.
8. Wählen Sie Löschen aus.

CLI

Um einen leeren Aurora-DB-Cluster mithilfe der zu löschenAWS CLI, rufen Sie den Befehl aufdelete-db-cluster.

Angenommen, der leere Cluster `deleteme-zero-instances` wurde nur für Entwicklungs- und Testzwecke verwendet und enthält keine wichtigen Daten. In diesem Fall müssen Sie beim Löschen des Clusters keinen Snapshot des Cluster-Volumes aufbewahren. Das folgende Beispiel zeigt, dass ein Cluster keine DB-Instances enthält, und veranschaulicht dann, wie der leere Cluster gelöscht wird, ohne einen finalen Snapshot zu erstellen oder automatisierte Backups beizubehalten.

```
$ aws rds describe-db-clusters --db-cluster-identifier deleteme-zero-instances --output
 text \
  --query '*[].["Cluster:",DBClusterIdentifier,DBClusterMembers[*].
["Instance:",DBInstanceIdentifier,IsClusterWriter]]
Cluster:        deleteme-zero-instances

$ aws rds delete-db-cluster --db-cluster-identifier deleteme-zero-instances \
  --skip-final-snapshot \
  --delete-automated-backups
{
  "DBClusterIdentifier": "deleteme-zero-instances",
  "Status": "available",
  "Engine": "aurora-mysql"
}
```

RDS-API

Um einen leeren Aurora-DB-Cluster über die Amazon RDS-API zu löschen, rufen Sie die Operation DeleteDBCluster auf.

Löschen eines Aurora-Clusters mit einer einzigen DB-Instance

Sie können die letzte DB-Instance auch dann löschen, wenn der DB-Cluster einen aktivierten Löschschutz hat. In diesen Fall bleibt der DB-Cluster selbst bestehen und die Daten werden beibehalten. Sie können wieder auf die Daten zugreifen, indem Sie dem Cluster eine neue DB-Instance hinzufügen.

Das folgende Beispiel zeigt, wie der Befehl `delete-db-cluster` fehlschlägt, wenn der Cluster noch zugeordnete DB-Instances hat. Dieser Cluster hat eine einzige Writer-DB-Instance. Wenn wir die DB-Instances im Cluster untersuchen, überprüfen wir das Attribut `IsClusterWriter` der einzelnen Instances. Der Cluster könnte eine oder keine Writer-DB-Instance haben. Der Wert `true`

steht für eine Writer-DB-Instance. Der Wert `false` steht für eine Reader-DB-Instance. Der Cluster könnte keine, eine oder viele Reader-DB-Instances haben. In diesem Fall löschen wir die Writer-DB-Instance mit dem Befehl `delete-db-instance`. Sobald die DB-Instance in den Status `deleting` wechselt, können wir auch den Cluster löschen. Nehmen wir für dieses Beispiel außerdem an, dass der Cluster keine Daten enthält, die erhalten bleiben müssen. Daher erstellen wir keinen Snapshot des Cluster-Volumes oder behalten automatisierte Backups bei.

```
$ aws rds delete-db-cluster --db-cluster-identifier deleteme-writer-only --skip-final-
snapshot
An error occurred (InvalidDBClusterStateFault) when calling the DeleteDBCluster
 operation:
  Cluster cannot be deleted, it still contains DB instances in non-deleting state.

$ aws rds describe-db-clusters --db-cluster-identifier deleteme-writer-only \
  --query '*[].[DBClusterIdentifier,Status,DBClusterMembers[*].
[DBInstanceIdentifier,IsClusterWriter]]'
[
    [
        "deleteme-writer-only",
        "available",
        [
            [
                "instance-2130",
                true
            ]
        ]
    ]
]

$ aws rds delete-db-instance --db-instance-identifier instance-2130
{
  "DBInstanceIdentifier": "instance-2130",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql"
}

$ aws rds delete-db-cluster --db-cluster-identifier deleteme-writer-only \
  --skip-final-snapshot \
  --delete-automated-backups
{
  "DBClusterIdentifier": "deleteme-writer-only",
  "Status": "available",
  "Engine": "aurora-mysql"
```

```
}
```

Löschen eines Aurora-Clusters mit mehreren DB-Instances

Wenn der Cluster mehrere DB-Instances enthält, gibt es normalerweise eine einzige Writer-Instance und eine oder mehrere Reader-Instances. Die Reader-Instances unterstützen die hohe Verfügbarkeit, indem sie im Standby-Modus sind und übernehmen, wenn die Writer-Instance auf ein Problem stößt. Sie können Reader-Instances auch verwenden, um den Cluster aufwärts zu skalieren, um einen leseintensiven Workload zu bewältigen, ohne zusätzlichen Overhead für die Writer-Instance zu verursachen.

Um einen Cluster mit mehreren Reader-DB-Instances zu löschen, löschen Sie zuerst die Reader-Instances und dann die Writer-Instance. Wenn Sie die Writer-Instance löschen, bleiben der Cluster und seine Daten bestehen. Sie löschen den Cluster separat.

- Informationen zum Löschen einer Aurora-DB-Instance finden Sie unter Löschen einer DB-Instance aus einem Aurora-DB-Cluster.
- Informationen zum Löschen der Writer-DB-Instance in einem Aurora-Cluster finden Sie unter Löschen eines Aurora-Clusters mit einer einzigen DB-Instance.
- Informationen zum Löschen eines leeren Aurora-Clusters finden Sie unter Erstellen eines leeren Aurora-Clusters.

Dieses CLI-Beispiel zeigt, wie ein Cluster gelöscht wird, der sowohl eine Writer-DB-Instance als auch eine einzige Reader-DB-Instance enthält. Die `describe-db-clusters`-Ausgabe zeigt, dass `instance-7384` die Writer-Instance und `instance-1039` die Reader-Instance ist. Im Beispiel wird zuerst die Reader-Instance gelöscht, da das Löschen der Writer-Instance, während noch eine Reader-Instance vorhanden ist, zu einem Failover-Vorgang führen würde. Es ist nicht sinnvoll, die Reader-Instance zu einer Writer-Instance zu befördern, wenn Sie diese Instance ebenfalls löschen möchten. Nehmen wir wiederum an, dass diese `db.t2.small`-Instances nur für Entwicklung und Tests verwendet werden, sodass der Löschvorgang den finalen Snapshot überspringt und keine automatisierten Backups beibehält.

```
$ aws rds delete-db-cluster --db-cluster-identifier deleteme-writer-and-reader --skip-
final-snapshot

An error occurred (InvalidDBClusterStateFault) when calling the DeleteDBCluster
 operation:
  Cluster cannot be deleted, it still contains DB instances in non-deleting state.
```

```
$ aws rds describe-db-clusters --db-cluster-identifier deleteme-writer-and-reader --
output text \
  --query '*[].["Cluster:",DBClusterIdentifier,DBClusterMembers[*].
["Instance:",DBInstanceIdentifier,IsClusterWriter]]
Cluster:        deleteme-writer-and-reader
Instance:       instance-1039  False
Instance:       instance-7384   True

$ aws rds delete-db-instance --db-instance-identifier instance-1039
{
  "DBInstanceIdentifier": "instance-1039",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql"
}

$ aws rds delete-db-instance --db-instance-identifier instance-7384
{
  "DBInstanceIdentifier": "instance-7384",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql"
}

$ aws rds delete-db-cluster --db-cluster-identifier deleteme-writer-and-reader \
  --skip-final-snapshot \
  --delete-automated-backups
{
  "DBClusterIdentifier": "deleteme-writer-and-reader",
  "Status": "available",
  "Engine": "aurora-mysql"
}
```

Das folgende Beispiel zeigt, wie ein DB-Cluster mit einer Writer-DB-Instance und mehreren Reader-DB-Instances gelöscht wird. Dabei wird die präzise Ausgabe des `describe-db-clusters`-Befehls verwendet, um einen Bericht über die Writer- und Reader-Instances abzurufen. Auch hier löschen wir alle Reader-DB-Instances, bevor wir die Writer-DB-Instance löschen. Es spielt keine Rolle, in welcher Reihenfolge wir die Reader-DB-Instances löschen.

Angenommen, dieser Cluster mit mehreren DB-Instances enthält Daten, die aufbewahrt werden sollen. Daher enthält der `delete-db-cluster`-Befehl in diesem Beispiel die Parameter `--no-skip-final-snapshot` und `--final-db-snapshot-identifier`, um Details zu dem

zu erstellenden Snapshot anzugeben. Enthalten ist außerdem der Parameter `--no-delete-automated-backups` zur Beibehaltung automatisierter Backups.

```
$ aws rds describe-db-clusters --db-cluster-identifier deleteme-multiple-readers --
output text \
  --query '*[].["Cluster:",DBClusterIdentifier,DBClusterMembers[*].
["Instance:",DBInstanceIdentifier,IsClusterWriter]]
Cluster:        deleteme-multiple-readers
Instance:       instance-1010   False
Instance:       instance-5410   False
Instance:       instance-9948   False
Instance:       instance-8451   True

$ aws rds delete-db-instance --db-instance-identifier instance-1010
{
  "DBInstanceIdentifier": "instance-1010",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql"
}

$ aws rds delete-db-instance --db-instance-identifier instance-5410
{
  "DBInstanceIdentifier": "instance-5410",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql"
}

$ aws rds delete-db-instance --db-instance-identifier instance-9948
{
  "DBInstanceIdentifier": "instance-9948",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql"
}

$ aws rds delete-db-instance --db-instance-identifier instance-8451
{
  "DBInstanceIdentifier": "instance-8451",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql"
}

$ aws rds delete-db-cluster --db-cluster-identifier deleteme-multiple-readers \
  --no-delete-automated-backups \
```

```
  --no-skip-final-snapshot \
  --final-db-snapshot-identifier deleteme-multiple-readers-final-snapshot
{
  "DBClusterIdentifier": "deleteme-multiple-readers",
  "Status": "available",
  "Engine": "aurora-mysql"
}
```

Das folgende Beispiel zeigt, wie Sie prüfen können, ob der angeforderte Snapshot von Aurora erstellt wurde. Sie können Details zu diesem Snapshot anfordern, indem Sie seine Kennung angebe `deleteme-multiple-readers-final-snapshot`. Sie können auch einen Bericht zu allen Snapshots für den gelöschten Cluster abrufen, indem Sie die Cluster-Kennung angebe `deleteme-multiple-readers`. Beide Befehle liefern Informationen über denselben Snapshot.

```
$ aws rds describe-db-cluster-snapshots \
  --db-cluster-snapshot-identifier deleteme-multiple-readers-final-snapshot
{
    "DBClusterSnapshots": [
        {
            "AvailabilityZones": [],
            "DBClusterSnapshotIdentifier": "deleteme-multiple-readers-final-snapshot",
            "DBClusterIdentifier": "deleteme-multiple-readers",
            "SnapshotCreateTime": "11T01:40:07.354000+00:00",
            "Engine": "aurora-mysql",
...

$ aws rds describe-db-cluster-snapshots --db-cluster-identifier deleteme-multiple-
readers
{
    "DBClusterSnapshots": [
        {
            "AvailabilityZones": [],
            "DBClusterSnapshotIdentifier": "deleteme-multiple-readers-final-snapshot",
            "DBClusterIdentifier": "deleteme-multiple-readers",
            "SnapshotCreateTime": "11T01:40:07.354000+00:00",
            "Engine": "aurora-mysql",
...
```

Löschschutz für Aurora-DB-Cluster

Sie können keine Cluster löschen, für die der Löschschutz aktiviert ist. Sie können DB-Instances innerhalb des Clusters löschen, aber nicht den Cluster selbst. Auf diese Weise ist das Cluster-

Volume, das all Ihre Daten enthält, vor einem versehentlichen Löschen geschützt. Aurora erzwingt den Löschschutz für einen DB-Cluster, unabhängig davon, ob Sie versuchen, den Cluster mithilfe der Konsole, der AWS CLI oder der RDS-API zu löschen.

Wenn Sie mithilfe der einen Produktions-DB-Cluster erstellen, ist der Löschschutz standardmäßig aktivier AWS Management Console. Der Löschschutz ist jedoch standardmäßig deaktiviert, wenn Sie einen Cluster über die AWS CLI oder API erstellen. Das Aktivieren oder Deaktivieren des Löschschutzes führt nicht zu einem Ausfall. Um den Cluster löschen zu können, müssen Sie den Cluster bearbeiten und den Löschschutz deaktivieren. Weitere Informationen zum Aktivieren und Deaktivieren des Löschschutzes finden Sie unter Ändern des DB-Clusters über die Konsole, die CLI und die API.

> **Tip**
>
> Auch wenn alle DB-Instances gelöscht sind, können Sie auf die Daten zugreifen, indem Sie eine neue DB-Instance im Cluster erstellen.

Löschen eines angehaltenen Aurora-Clusters

Sie können einen Cluster nicht löschen, wenn er sich im Status `stopped` befindet. Starten Sie in diesem Fall den Cluster, bevor Sie ihn löschen. Weitere Informationen finden Sie unter Starten eines Aurora-DB-Clusters.

Löschen von Aurora MySQL-Clustern, die Read Replicas sind

Sie können eine DB-Instance in einem DB-Cluster für Aurora MySQL nicht löschen, wenn beide der folgenden Bedingungen erfüllt sind:

- Der DB-Cluster ist ein Lesereplikat eines anderen Aurora-DB-Clusters.
- Die DB-Instance ist die einzige Instance im DB-Cluster.

Um in diesem Fall eine DB-Instance zu löschen, stufen Sie zunächst den DB-Cluster hoch, sodass er kein Lesereplikat mehr ist. Nach dem Hochstufen können Sie die endgültige DB-Instance im DB-Cluster löschen. Weitere Informationen finden Sie unter Replizieren von Amazon-Aurora-MySQL-DB-Clustern über AWS-Regionen hinweg.

Der letzte Snapshot beim Löschen eines Clusters

In diesem Abschnitt zeigen die Beispiele, wie Sie auswählen können, ob Sie beim Löschen eines Aurora-Clusters einen endgültigen Snapshot erstellen möchten. Wenn Sie einen endgültigen Snapshot erstellen möchten, der angegebene Name jedoch mit einem vorhandenen Snapshot übereinstimmt, wird der Vorgang mit einem Fehler beendet. Überprüfen Sie in diesem Fall die Snapshot-Details, um zu bestätigen, ob sie Ihr aktuelles Detail darstellt oder ob es sich um einen älteren Snapshot handelt. Wenn der vorhandene Snapshot nicht über die neuesten Daten verfügt, die Sie beibehalten möchten, benennen Sie den Snapshot um und versuchen Sie es erneut, oder geben Sie einen anderen Namen für den Parameter endgültiger Snapshot aus.

Löschen einer DB-Instance aus einem Aurora-DB-Cluster

Sie können eine DB-Instance aus einem Aurora-DB-Cluster im Rahmen des Löschens des gesamten Clusters löschen. Wenn Ihr Cluster eine bestimmte Anzahl von DB-Instances enthält, so müssen zum Löschen des Clusters all diese DB-Instances gelöscht werden. Sie können auch eine oder mehrere Reader-Instances aus einem Cluster löschen, während der Cluster weiter ausgeführt wird. Dadurch können Sie die Rechenkapazität und die damit verbundenen Kosten reduzieren, wenn Ihr Cluster nicht ausgelastet ist.

Sie müssen den Namen der Instance angeben, um eine DB-Instance zu löschen.

Sie können eine DB-Instance mithilfe der AWS Management Console, der AWS CLI oder der RDS-API löschen.

> **Note**
>
> Wenn einAurora-Replikat gelöscht wird, wird der Instance-Endpunkt sofort entfernt und dasAurora-Replikat wird vom Reader-Endpunkt entfernt. Wenn Anweisungen vorhanden sind, die auf dem Aurora Replica ausgeführt werden, das gerade gelöscht wird, besteht eine Übergangsfrist von drei Minuten. Vorhandene Anweisungen können während der Nachfrist beendet werden. Nach Ablauf der Nachfrist wird das Aurora-Replikat geschlossen und gelöscht.

Bei Aurora-DB-Clustern wird durch das Löschen einer DB-Instance nicht unbedingt der gesamte Cluster gelöscht. Sie können eine DB-Instance in einem Aurora-Cluster löschen, um die Rechenkapazität und die damit verbundenen Kosten zu reduzieren, wenn der Cluster nicht

ausgelastet ist. Informationen zu den besonderen Bedingungen bei Aurora-Clustern mit einer einzigen oder keiner DB-Instance finden Sie unter Löschen eines Aurora-Clusters mit einer einzigen DB-Instance und Erstellen eines leeren Aurora-Clusters.

> **Note**
>
> Sie können einen DB-Cluster nicht löschen, wenn für ihn Löschschutz aktiviert ist. Weitere Informationen finden Sie unter Löschschutz für Aurora-DB-Cluster.
> Sie können den Löschschutz deaktivieren, indem Sie den DB-Cluster bearbeiten. Weitere Informationen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Konsole

So löschen Sie eine DB-Instance in einem DB-Cluster

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die DB-Instance aus, die Sie löschen möchten.
3. Klicken Sie bei Actions auf Delete.
4. Geben Sie **`delete me`** in das Feld ein.
5. Wählen Sie Löschen aus.

AWS CLI

Um eine DB-Instance mithilfe der zu löschenAWS CLI, rufen Sie den delete-db-instance Befehl auf und geben Sie den `--db-instance-identifier` Wert an.

Example

Für Linux, macOSoder Unix:

```
aws rds delete-db-instance \
    --db-instance-identifier mydbinstance
```

Windows:

```
aws rds delete-db-instance ^
    --db-instance-identifier mydbinstance
```

RDS-API

Zum Löschen einer DB-Instance mit der Amazon-RDS-API rufen Sie die Operation DeleteDBInstance auf und legen den Parameter `DBInstanceIdentifier` fest.

> **Note**
>
> Wenn der Status einer DB-Instance `deleting` lautet, wird der Wert des CA-Zertifikats nicht in der RDS-Konsole oder in der Ausgabe für AWS CLI-Befehle oder RDS-API-Operationen angezeigt. Weitere Informationen zu CA-Zertifikaten finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

Markieren von Amazon RDS-Ressourcen

Ein Amazon RDS-Tag ist ein Name-Wert-Paar, das Sie definieren und einer Amazon RDS-Ressource wie einer DB-Instance oder einem DB-Snapshot zuordnen. Der Name wird als der Schlüssel bezeichnet. Optional können Sie einen Wert für den Schlüssel angeben.

Sie können die AWS Management Console AWS CLI, oder die Amazon RDS-API verwenden, um Tags zu Amazon RDS-Ressourcen hinzuzufügen, aufzulisten und zu löschen. Wenn Sie die CLI oder API verwenden, müssen Sie den Amazon-Ressourcennamen (ARN) für die RDS-Ressource angeben, mit der Sie arbeiten möchten. Weitere Informationen zum Konstruieren eines ARN finden Sie unter Erstellen eines ARN für Amazon RDS.

Themen

Warum Amazon RDS-Ressourcen-Tags verwenden?

Sie können Tags verwenden, um Folgendes zu tun:

- Kategorisieren Sie Ihre RDS-Ressourcen nach Anwendung, Projekt, Abteilung, Umgebung usw. Sie könnten beispielsweise einen Tag-Schlüssel verwenden, um eine Kategorie zu definieren, wobei der Tag-Wert ein Element in dieser Kategorie ist. Sie könnten das Tag erstellen`environment=prod`. Oder Sie können einen Tag-Schlüssel `project` und einen Tag-Wert von definieren`Salix`, was darauf hinweist, dass dem Salix-Projekt eine Amazon RDS-Ressource zugewiesen ist.
- Automatisieren Sie Aufgaben im Ressourcenmanagement. Sie könnten beispielsweise ein Wartungsfenster für markierte Instanzen erstellen`environment=prod`, das sich von dem Fenster für markierte Instanzen unterscheide`environment=test`. Sie könnten auch automatische DB-Snapshots für markierte `environment=prod` Instances konfigurieren.
- Steuern Sie den Zugriff auf RDS-Ressourcen innerhalb einer IAM-Richtlinie. Hierzu können Sie den globalen Bedingungsschlüssel `aws:ResourceTag/`*`tag-key`* verwenden. Eine Richtlinie

könnte es beispielsweise nur Benutzern in der `DBAdmin` Gruppe ermöglichen, DB-Instances zu ändern, die mit `environment=prod` gekennzeichnet sind. Informationen zur Verwaltung des Zugriffs auf markierte Ressourcen mit IAM-Richtlinien finden Sie unter Identity and Access Management für Amazon Aurora Steuern des Zugriffs auf AWS Ressourcen im AWS Identity and Access Management-Benutzerhandbuch.

- Überwachen Sie Ressourcen anhand eines Tags. Sie können beispielsweise ein CloudWatch Amazon-Dashboard für DB-Instances erstellen, die mit gekennzeichnet sind`environment=prod`.
- Verfolgen Sie die Kosten, indem Sie die Ausgaben für Ressourcen mit ähnlichen Tags gruppieren. Wenn Sie beispielsweise RDS-Ressourcen, die mit dem Salix-Projekt verknüpft sind`project=Salix`, mit taggen, können Sie Kostenberichte für dieses Projekt erstellen und Ausgaben diesem Projekt zuordnen. Weitere Informationen finden Sie unter So funktioniert die AWS Abrechnung mit Tags in Amazon RDS.

So funktionieren Amazon RDS-Ressourcen-Tags

AWS wendet Ihren Tags keine semantische Bedeutung an. Tags werden streng als Zeichenfolgen interpretiert.

Themen

- Tag-Sets in Amazon RDS
- Tag-Struktur in Amazon RDS
- Amazon RDS-Ressourcen, die für das Tagging in Frage kommen
- So funktioniert die AWS Abrechnung mit Tags in Amazon RDS

Tag-Sets in Amazon RDS

Jede Amazon RDS-Ressource hat einen Container, der als Tag-Set bezeichnet wird. Der Container enthält alle Tags, die der Ressource zugewiesen sind. Eine Ressource hat genau einen Tagsatz.

Ein Tag-Set enthält 0—50 Tags. Wenn Sie einer RDS-Ressource ein Tag mit demselben Schlüssel hinzufügen wie ein bereits vorhandenes Tag der Ressource, überschreibt der neue Wert den alten.

Tag-Struktur in Amazon RDS

Die Struktur eines RDS-Tags sieht wie folgt aus:

Tag-Schlüssel

Der Schlüssel ist der erforderliche Name des Tags. Der Zeichenkettenwert muss 1—128 Unicode-Zeichen lang sein und darf nicht mit einem `aws:` oder als Präfix versehen werden. `rds:` Die Zeichenfolge kann nur den Satz von Unicode-Buchstaben, Ziffern, Leerzeichen,,_,., : / =+, - und enthalten. @ Der Java-Regex ist. `"^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*)$"` Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Somit sind die Schlüssel `project` und B `Project` unterschiedlich.

Ein Schlüssel ist für einen Tagsatz eindeutig. Sie können beispielsweise kein Schlüsselpaar in einem Tag-Set haben, bei dem der Schlüssel zwar derselbe, aber unterschiedliche Werte hat, wie `project=Trinity` z. B. und. `project=Xanadu`

Tag-Wert

Der Wert ist ein optionaler Zeichenkettenwert des Tags. Der Zeichenkettenwert muss 1—256 Unicode-Zeichen lang sein. Die Zeichenfolge kann nur den Satz von Unicode-Buchstaben, Ziffern, Leerzeichen,_,.,:, / = +-, und enthalten. @ Der Java-Regex ist. `"^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*)$"` Bei Tag-Werten muss die Groß- und Kleinschreibung beachtet werden. Somit sind die Werte `prod` und 2 `Prod` unterschiedlich.

Werte müssen in einem Tag-Set nicht eindeutig sein und können Null sein. Es ist z. B. ein Schlüssel-Wert-Paar in einem Tag-Satz `project=Trinity` und `cost-center=Trinity` möglich.

Amazon RDS-Ressourcen, die für das Tagging in Frage kommen

Sie können die folgenden Amazon RDS-Ressourcen kennzeichnen:

- DB-Instances
- DB-Cluster
- DB-Cluster-Endpunkte
- Read Replicas
- DB-Snapshots
- DB-Cluster-Snapshots
- Reservierte DB-Instances
- Ereignisabonnements
- DB-Optionsgruppen

- DB-Parametergruppen
- DB-Cluster-Parametergruppen
- DB-Subnetzgruppen
- RDS Proxys
- RDS Proxy-Endpunkte

> **Note**
>
> Derzeit können Sie RDS Proxys und RDS-Proxy-Endpunkte nicht per AWS Management Console markieren.

- Blau/Grün-Bereitstellungen
- Null-ETL-Integrationen (Vorschau)

So funktioniert die AWS Abrechnung mit Tags in Amazon RDS

Verwenden Sie Tags, um Ihre AWS Rechnung so zu organisieren, dass sie Ihrer eigenen Kostenstruktur entspricht. Melden Sie sich dazu an, um Ihre AWS-Konto Rechnung mit den Tag-Schlüsselwerten zu erhalten. Um dann die Kosten kombinierter Ressourcen anzuzeigen, organisieren Sie Ihre Fakturierungsinformationen nach Ressourcen mit gleichen Tag-Schlüsselwerten. Beispielsweise können Sie mehrere Ressourcen mit einem bestimmten Anwendungsnamen markieren und dann Ihre Fakturierungsinformationen so organisieren, dass Sie die Gesamtkosten dieser Anwendung über mehrere Services hinweg sehen können. Weitere Informationen finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS Billing -Benutzerhandbuch.

So funktionieren Kostenzuweisungs-Tags mit DB-Cluster-Snapshots

Sie können einem DB-Cluster-Snapshot ein Tag hinzufügen. Diese Gruppierung erscheint jedoch nicht in Ihrer Rechnung. Damit Kostenzuweisungs-Tags auf DB-Cluster-Snapshots angewendet werden können, müssen die folgenden Bedingungen erfüllt sein:

- Die Tags müssen an die übergeordnete DB-Instance angehängt werden.
- Die übergeordnete DB-Instance muss genauso vorhanden sein AWS-Konto wie der DB-Cluster-Snapshot.
- Die übergeordnete DB-Instance muss genauso vorhanden sein AWS-Region wie der DB-Cluster-Snapshot.

DB-Cluster-Snapshots gelten als verwaist, wenn sie nicht in derselben Region wie die übergeordnete DB-Instance existieren. Die Kosten für verwaiste Snapshots werden in einer einzigen Zeile ohne Tags zusammengefasst. Kontoübergreifende DB-Cluster-Snapshots gelten nicht als verwaist, wenn die folgenden Bedingungen erfüllt sind:

- Sie befinden sich in derselben Region wie die übergeordnete DB-Instance.
- Die übergeordnete DB-Instance gehört dem Quellkonto.

> **Note**
>
> Wenn die übergeordnete DB-Instance einem anderen Konto gehört, gelten die Kostenzuweisungs-Tags nicht für kontenübergreifende Snapshots im Zielkonto.

Bewährte Methoden für das Taggen von Amazon RDS-Ressourcen

Wir empfehlen Ihnen, sich bei der Verwendung von Tags an die folgenden bewährten Methoden zu halten:

- Dokumentieren Sie Konventionen für die Verwendung von Tags, die von allen Teams in Ihrer Organisation befolgt werden. Stellen Sie insbesondere sicher, dass die Namen sowohl beschreibend als auch konsistent sind. Standardisieren Sie beispielsweise das Format, `environment:prod` anstatt einige Ressourcen mit zu kennzeichnen. `env:production`

  > **Important**
  >
  > Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags.

- Automatisieren Sie das Tagging, um Konsistenz zu gewährleisten. Sie können beispielsweise die folgenden Techniken verwenden:
  - Fügen Sie Tags in eine AWS CloudFormation Vorlage ein. Wenn Sie Ressourcen mit der Vorlage erstellen, werden die Ressourcen automatisch markiert.
  - Definieren und wenden Sie Tags mithilfe von AWS Lambda Funktionen an.
  - Erstellen Sie ein SSM-Dokument, das Schritte zum Hinzufügen von Tags zu Ihren RDS-Ressourcen enthält.

- Verwenden Sie Tags nur bei Bedarf. Sie können bis zu 50 Tags für eine einzelne RDS-Ressource hinzufügen. Eine bewährte Methode besteht jedoch darin, eine unnötige Zunahme und Komplexität von Tags zu vermeiden.
- Überprüfen Sie die Tags regelmäßig auf Relevanz und Richtigkeit. Entfernen oder ändern Sie veraltete Tags nach Bedarf.
- Erwägen Sie das Erstellen von Tags mit dem AWS Tag-Editor in der AWS Management Console. Sie können den Tag-Editor verwenden, um mehreren unterstützten AWS Ressourcen, einschließlich RDS-Ressourcen, gleichzeitig Tags hinzuzufügen. Weitere Informationen finden Sie unter Tag Editor im Benutzerhandbuch von AWS Resource Groups.

Verwaltung von Tags in Amazon RDS

Sie haben die folgenden Möglichkeiten:

- Erstellen Sie Tags, wenn Sie eine Ressource erstellen, z. B. wenn Sie den AWS CLI Befehl ausführen`create-db-instance`.
- Fügen Sie mithilfe des Befehls Tags zu einer vorhandenen Ressource hinzu`add-tags-to-resource`.
- Listet mithilfe des Befehls Tags auf, die mit einer bestimmten Ressource verknüpft sind`list-tags-for-resource`.
- Aktualisieren Sie die Tags mithilfe des Befehls`add-tags-to-resource`.
- Entfernen Sie mithilfe des Befehls Tags aus einer Ressource`remove-tags-from-resource`.

Die folgenden Verfahren zeigen, wie Sie typische Tagging-Operationen für Ressourcen durchführen können, die sich auf DB-Instances und Aurora-DB-Cluster beziehen. Beachten Sie, dass Tags für Autorisierungszwecke zwischengespeichert werden. Aus diesem Grund können beim Hinzufügen oder Aktualisieren von Tags zu Amazon RDS-Ressourcen mehrere Minuten vergehen, bis die Änderungen verfügbar sind.

Konsole

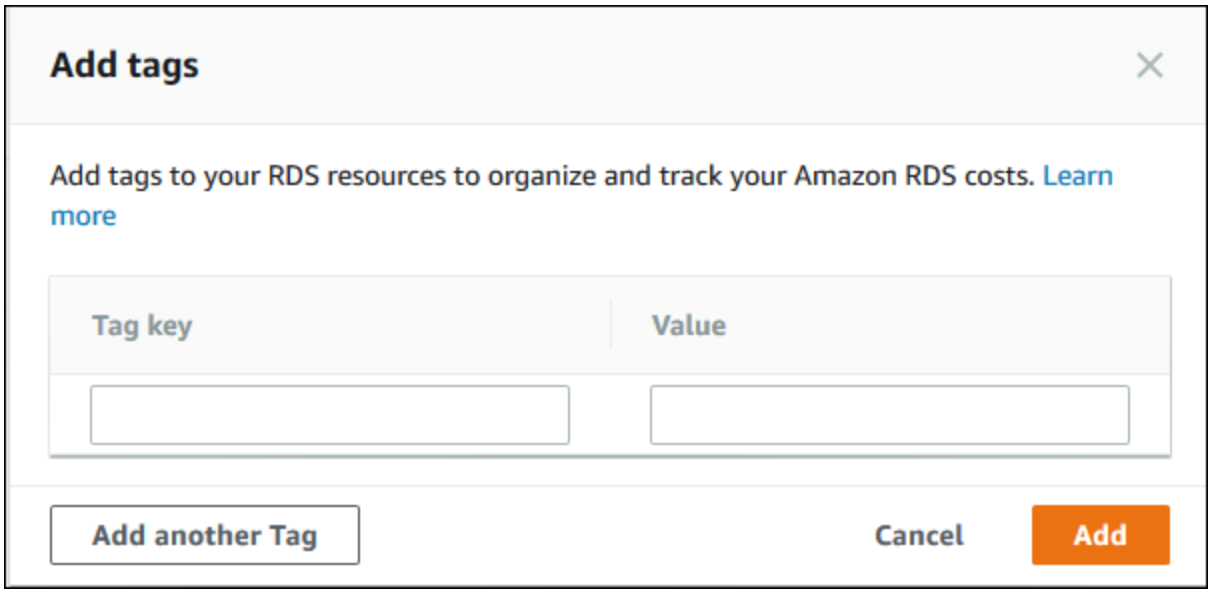
Amazon RDS-Ressourcen werden auf die gleiche Weise wie andere Ressourcen getaggt. Die folgenden Schritte zeigen, wie Sie eine Amazon RDS-DB-Instance taggen.

So fügen Sie ein Tag zu einer DB-Instance hinzu

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.

   > **Note**
   >
   > Geben Sie unter Filter databases (Datenbanken filtern) eine Textzeichenfolge ein, um die Liste der DB-Instances im Bereich Databases (Datenbanken) zu filtern. Es werden nur DB-Instances angezeigt, welche die Zeichenfolge enthalten.

3. Wählen Sie den Namen der DB-Instance aus, die Sie mit einem Tag versehen möchten, um deren Details anzuzeigen.
4. Scrollen Sie im Detailbereich nach unten zum Bereich Tags.
5. Wählen Sie Add aus. Das Fenster Add tags (Tags hinzufügen) wird angezeigt.



6. Geben Sie einen Wert für Tag key (Tag-Schlüssel) und Wert ein.
7. Wenn Sie ein weiteres Tag hinzufügen möchten, wählen Sie Add another Tag (Weiteres Tag hinzufügen) aus und geben Sie unter Tag key (Tag-Schlüssel) und Wert einen Wert ein.

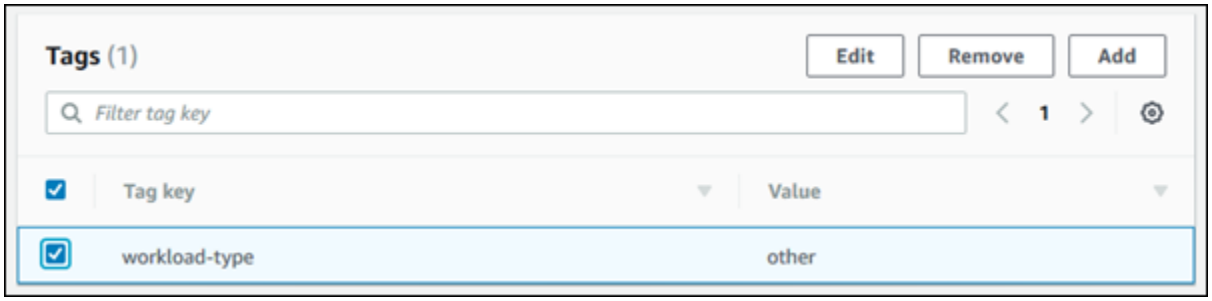
   Wiederholen Sie diesen Schritt, bis Sie alle Tags hinzugefügt haben.
8. Wählen Sie Add aus.

So löschen Sie ein Tag aus einer DB-Instance

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.

   > **Note**
   >
   > Geben Sie im Feld Databases (Datenbanken) eine Textzeichenfolge ein, um die Liste der DB-Instances im Bereich Databases (Datenbanken) zu filtern. Es werden nur DB-Instances angezeigt, welche die Zeichenfolge enthalten.

3. Wählen Sie den Namen der entsprechenden DB-Instance aus, um deren Details anzuzeigen.
4. Scrollen Sie im Detailbereich nach unten zum Bereich Tags.
5. Wählen Sie das Tag aus, das Sie löschen möchten.



6. Wählen Sie Löschen und dann im Fenster Löschen von Tags erneut Löschen aus.

AWS CLI

Mithilfe der können Sie Tags für eine DB-Instance hinzufügen, auflisten oder entferne AWS CLI.

- Verwenden Sie den AWS CLI Befehl, um einer Amazon RDS-Ressource ein oder mehrere Tags hinzuzufügen `add-tags-to-resource`.
- Verwenden Sie den AWS CLI Befehl, um die Tags auf einer Amazon RDS-Ressource aufzulisten `list-tags-for-resource`.
- Verwenden Sie den AWS CLI Befehl, um ein oder mehrere Tags aus einer Amazon RDS-Ressource zu entfernen `remove-tags-from-resource`.

Weitere Informationen zum Erstellen des erforderlichen ARN finden Sie unter Erstellen eines ARN für Amazon RDS.

RDS-API

Mithilfe der Amazon RDS-API können Sie Tags für eine DB-Instance hinzufügen, auflisten oder entfernen.

- Verwenden Sie die API-Operation `AddTagsToResource`, um ein Tag zu einer Amazon RDS-Ressource hinzuzufügen.
- Verwenden Sie die API-Operation , um die Tags für eine Amazon RDS-Ressource aufzulisten `ListTagsForResource`.
- Verwenden Sie die API-Operation `RemoveTagsFromResource`, um Tags aus einer Amazon RDS-Ressource zu entfernen.

Weitere Informationen zum Erstellen des erforderlichen ARN finden Sie unter Erstellen eines ARN für Amazon RDS.

Wenn Sie in der Amazon RDS-API mit XML arbeiten, nutzen Sie das folgende Schema:

```
<Tagging>
    <TagSet>
        <Tag>
            <Key>Project</Key>
            <Value>Trinity</Value>
        </Tag>
        <Tag>
            <Key>User</Key>
            <Value>Jones</Value>
        </Tag>
    </TagSet>
</Tagging>
```

Die folgende Tabelle enthält eine Liste der zulässigen XML-Tags und deren Eigenschaften. Bei den Werten für `Key` und wird zwischen Groß- und Kleinschreibung `Value` unterschieden. Zum Beispiel `PROJECT=Trinity` sind `project=Trinity` und unterschiedliche Tags.

Markieren von Elementen	Beschreibung
TagSet	Ein Tag-Satz ist ein Container für alle Tags, die einer Amazon Amazon RDS-Ressource zugewiesen sind. Es ist nur ein Tag-Satz pro Ressource zulässig. Sie arbeiten mit einem TagSet nur über die Amazon RDS-API.
Tag	Ein Tag ist ein benutzerdefiniertes Schlüssel-Wert-Paar. Ein Tag-Satz kann 1 bis 50 Tags enthalten.
Schlüssel	Ein Schlüssel ist der erforderliche Name des Tags. Einschränkungen finden Sie unterTag-Struktur in Amazon RDS. Der Zeichenfolgenwert kann aus 1 bis 128 Unicode-Zeichen bestehen. Ihm darf kein "`aws:`" oder "`rds:`" als Präfix vorangestellt werden. Die Zeichenfolge darf nur Unicode-Zeichen, Ziffern, Leerzeichen sowie "_", ".", "/", "=", "+", "-" enthalten (Java-Regex: "^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*)"). Schlüssel müssen in einem Tag-Satz eindeutig sein. Sie können z. B. in einem Tag-Satz kein Schlüsselpaar mit gleichem Schlüssel, aber unterschiedlichen Werten verwenden, wie "Projekt/Trinity" und "Projekt/Xanadu".
Value	Ein Wert ist der optionale Wert des Tags. Informationen zu Einschränkungen finden Sie unterTag-Struktur in Amazon RDS. Der Zeichenfolgenwert kann aus 1 bis 256 Unicode-Zeichen bestehen. Ihm darf kein "`aws:`" oder "`rds:`" als Präfix vorangestellt werden. Die Zeichenfolge darf nur Unicode-Zeichen, Ziffern, Leerzeichen sowie "_", ".", "/", "=", "+", "-" enthalten (Java-Regex: "^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*)"). Die Werte innerhalb eines Tag-Satzes müssen nicht eindeutig und können null sein. Sie können beispielsweise über ein Schlüssel-Wert-Paar in einem Tag-Satz "Projekt/Trinity" und "Kostenstelle/Trinity" verfügen.

Kopieren von Tags in DB-Cluster-Snapshots

Wenn Sie einen DB-Cluster erstellen oder wiederherstellen, können Sie angeben, dass die Tags aus dem Cluster in Snapshots des DB-Clusters kopiert werden. Das Kopieren von Tags stellt sicher, dass die Metadaten für die DB-Snapshots mit denen des Quell-DB-Clusters übereinstimmen. Es wird außerdem sichergestellt, dass alle Zugriffsrichtlinien für die DB-Snapshots auch mit denen des Quell-DB-Clusters übereinstimmen. Tags werden nicht standardmäßig kopiert.

Sie können für die folgenden Aktionen festlegen, dass Tags in DB-Snapshots kopiert werden:

- Erstellen eines DB-Clusters
- Einen DB-Cluster wiederherstellen
- Erstellen eines Lesereplikats
- Kopieren eines DB-Cluster-Snapshots

> **Note**
>
> In einigen Fällen können Sie einen Wert für den `--tags` Parameter des Befehls AWS CLI create-db-snapshot angeben. Oder Sie geben mindestens ein Tag für die API-Operation CreateDBSnapshot an. In diesen Fällen kopiert RDS keine Tags von der Quell-DB-Instance in den neuen DB-Snapshot. Diese Funktionalität gilt sogar, wenn in der Quell-DB-Instance die Option `--copy-tags-to-snapshot` (`CopyTagsToSnapshot`) aktiviert ist.
> Wenn Sie diesen Ansatz verwenden, können Sie eine Kopie einer DB-Instance aus einem DB-Snapshot erstellen. Dieser Ansatz vermeidet das Hinzufügen von Tags, die nicht für die neue DB-Instance gelten. Sie erstellen Ihren DB-Snapshot mithilfe des AWS CLI `create-db-snapshot` Befehls (oder der `CreateDBSnapshot` RDS-API-Operation). Nachdem Sie Ihren DB-Snapshot erstellt haben, können Sie Tags hinzufügen. Dieser Vorgang wird später in diesem Thema beschrieben.

Tutorial: Verwenden Sie Tags, um festzulegen, welcher Aurora-DB-Cluster stoppt.

Angenommen, Sie erstellen eine Reihe von Aurora-DB-Clustern in einer Entwicklungs- oder Testumgebung. Sie müssen alle diese Cluster mehrere Tage lang beibehalten. Einige der Cluster führen über Nacht Tests durch. Andere Cluster können über Nacht angehalten und am nächsten

Tag wieder gestartet werden. Das folgende Beispiel zeigt, wie Sie denjenigen Clustern ein Tag zuweisen, die sich dafür eignen, über Nacht angehalten zu werden. Dann zeigt das Beispiel, wie ein Skript erkennen kann, welche Cluster dieses Tag haben und wie diese Cluster anschließend angehalten werden. In diesem Beispiel spielt der Wertanteil des Schlüssel-Wert-Paares keine Rolle. Das Vorhandensein des `stoppable`-Tags bedeutet, dass das Cluster diese benutzerdefinierte Eigenschaft besitzt.

Festlegen, welche Aurora-DB-Cluster angehalten werden sollen

1. Bestimmen Sie den ARN eines Clusters, den Sie als anhaltbar kennzeichnen wollen.

   Die Befehle und APIs zum Markieren funktionieren mit Hilfe von ARNs. Auf diese Weise können sie nahtlos über AWS Regionen, AWS Konten und verschiedene Ressourcentypen hinweg funktionieren, die möglicherweise identische Kurznamen haben. Sie können in CLI-Befehlen, die mit Clustern arbeiten, den ARN anstelle der Cluster-ID angeben. Ersetzen Sie den Namen Ihres eigenen Clusters durch *`dev-test-cluster`*. Ersetzen Sie in nachfolgenden Befehlen mit ARN-Parametern den ARN Ihres eigenen Clusters. Der ARN enthält Ihre eigene AWS Konto-ID und den Namen der AWS Region, in der sich Ihr Cluster befindet.

   ```
   $ aws rds describe-db-clusters --db-cluster-identifier dev-test-cluster \
     --query "*[].{DBClusterArn:DBClusterArn}" --output text
   arn:aws:rds:us-east-1:123456789:cluster:dev-test-cluster
   ```

2. Fügen Sie das Tag `stoppable` zu diesem Cluster hinzu.

   Der Name für dieses Tag wird von Ihnen ausgewählt. Dieser Ansatz bedeutet, dass Sie vermeiden können, eine Namenskonvention zu entwickeln, die alle relevanten Informationen in Namen codiert. In einer solchen Konvention können Sie Informationen im DB-Instance-Namen oder Namen anderer Ressourcen codieren. Da das Tag in diesem Beispiel als Attribut behandelt wird, das entweder vorhanden ist oder nicht, wird der `Value=`-Teil des `--tags`-Parameters weggelassen.

   ```
   $ aws rds add-tags-to-resource \
     --resource-name arn:aws:rds:us-east-1:123456789:cluster:dev-test-cluster \
     --tags Key=stoppable
   ```

3. Bestätigen Sie, dass das Tag im Cluster vorhanden ist.

   Diese Befehle rufen die Tag-Informationen für das Cluster im JSON-Format und in einfachem tabulatorgetrenntem Text ab.

```
$ aws rds list-tags-for-resource \
  --resource-name arn:aws:rds:us-east-1:123456789:cluster:dev-test-cluster
{
    "TagList": [
        {
            "Key": "stoppable",
            "Value": ""

        }
    ]
}
$ aws rds list-tags-for-resource \
  --resource-name arn:aws:rds:us-east-1:123456789:cluster:dev-test-cluster --output
 text
TAGLIST stoppable
```

4. Um alle Cluster anzuhalten, die als `stoppable` bezeichnet werden, bereiten Sie eine Liste aller Ihrer Cluster vor. Gehen Sie die Liste durch und prüfen Sie, ob jedes Cluster mit dem entsprechenden Attribut gekennzeichnet ist.

   Dieses Linux-Beispiel verwendet Shell-Skripts, um die Liste der Cluster-ARNs in einer temporären Datei zu speichern und dann CLI-Befehle für jedes Cluster auszuführen.

```
$ aws rds describe-db-clusters --query "*[].[DBClusterArn]" --output text >/tmp/
cluster_arns.lst
$ for arn in $(cat /tmp/cluster_arns.lst)
do
  match="$(aws rds list-tags-for-resource --resource-name $arn --output text | grep
 'TAGLIST\tstoppable')"
  if [[ ! -z "$match" ]]
  then
      echo "Cluster $arn is tagged as stoppable. Stopping it now."
# Note that you can specify the full ARN value as the parameter instead of the
 short ID 'dev-test-cluster'.
      aws rds stop-db-cluster --db-cluster-identifier $arn
  fi
done

Cluster arn:aws:rds:us-east-1:123456789:cluster:dev-test-cluster is tagged as
 stoppable. Stopping it now.
{
    "DBCluster": {
```

```
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-east-1e",
            "us-east-1c",
            "us-east-1d"
        ],
        "BackupRetentionPeriod": 1,
        "DBClusterIdentifier": "dev-test-cluster",
        ...
```

Sie können ein solches Skript am Ende eines jeden Tages ausführen, um sicherzustellen, dass nicht benötigte Cluster angehalten werden. Sie können einen Job auch mit einem Dienstprogramm wie `cron` planen, um jede Nacht eine solche Überprüfung durchzuführen. Sie könnten so beispielsweise vorgehen, wenn einige Cluster versehentlich weiter ausgeführt wurden. Hier könnten Sie eine Feinabstimmung des Befehls vornehmen, mit dem die Liste der zu prüfenden Cluster vorbereitet wird.

Der folgende Befehl erzeugt eine Liste Ihrer Cluster mit dem Status `available`. Das Skript kann Cluster ignorieren, die bereits angehalten wurden, da sie unterschiedliche Statuswerte wie `stopped` oder `stopping` haben.

```
$ aws rds describe-db-clusters \
  --query '*[].{DBClusterArn:DBClusterArn,Status:Status}|[?Status == `available`]|[].
{DBClusterArn:DBClusterArn}' \
  --output text
arn:aws:rds:us-east-1:123456789:cluster:cluster-2447
arn:aws:rds:us-east-1:123456789:cluster:cluster-3395
arn:aws:rds:us-east-1:123456789:cluster:dev-test-cluster
arn:aws:rds:us-east-1:123456789:cluster:pg2-cluster
```

> **Tip**
>
> Sie können die Tags zuweisen und Cluster mit Hilfe dieser Tags finden, um die Kosten auf andere Weise zu senken. Nehmen wir zum Beispiel das Szenario mit Aurora-DB-Clustern, die für Entwicklungs- und Testzwecke verwendet werden. Hier können Sie festlegen, dass einige Cluster am Ende eines jeden Tages gelöscht werden oder dass nur ihre Reader-DB-Instances gelöscht werden. Oder Sie können einige so festlegen, dass ihre DB-Instances in Zeiten erwarteter geringer Auslastung in kleine DB-Instance-Klassen geändert werden.

Arbeiten mit Amazon-Ressourcennamen (ARN) in Amazon RDS

In Amazon Web Services erstellte Ressourcen werden anhand eines Amazon-Ressourcennamens (ARN) eindeutig identifiziert. Für bestimmte Amazon RDS-Operationen müssen Sie eine Amazon RDS-Ressource eindeutig identifizieren, indem Sie ihren ARN angeben. Wenn Sie beispielsweise ein Lesereplikat einer RDS-DB-Instance erstellen, müssen Sie den ARN für die Quell-DB-Instance bereitstellen.

Erstellen eines ARN für Amazon RDS

In Amazon Web Services erstellte Ressourcen werden anhand eines Amazon-Ressourcennamens (ARN) eindeutig identifiziert. Sie können mithilfe der folgenden Syntax einen ARN für eine Amazon RDS-Ressource erstellen.

`arn:aws:rds:<region>:<account number>:<resourcetype>:<name>`

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	rds.us-east-2.amazonaws.com	HTTPS
		rds-fips.us-east-2.api.aws	HTTPS
		rds.us-east-2.api.aws	HTTPS
		rds-fips.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	rds.us-east-1.amazonaws.com	HTTPS
		rds-fips.us-east-1.api.aws	HTTPS
		rds-fips.us-east-1.amazonaws.com	HTTPS
		rds.us-east-1.api.aws	HTTPS
USA West (Nordkalifornien)	us-west-1	rds.us-west-1.amazonaws.com	HTTPS
		rds.us-west-1.api.aws	HTTPS
		rds-fips.us-west-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
		rds-fips.us-west-1.api.aws	HTTPS
USA West (Oregon)	us-west-2	rds.us-west-2.amazonaws.com	HTTPS
		rds-fips.us-west-2.amazonaws.com	HTTPS
		rds.us-west-2.api.aws	HTTPS
		rds-fips.us-west-2.api.aws	HTTPS
Afrika (Kapstadt)	af-south-1	rds.af-south-1.amazonaws.com	HTTPS
		rds.af-south-1.api.aws	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	rds.ap-east-1.amazonaws.com	HTTPS
		rds.ap-east-1.api.aws	HTTPS
Asien-Pazifik (Hyderabad)	ap-south-2	rds.ap-south-2.amazonaws.com	HTTPS
		rds.ap-south-2.api.aws	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	rds.ap-southeast-3.amazonaws.com	HTTPS
		rds.ap-southeast-3.api.aws	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	rds.ap-southeast-4.amazonaws.com	HTTPS
		rds.ap-southeast-4.api.aws	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	rds.ap-south-1.amazonaws.com	HTTPS
		rds.ap-south-1.api.aws	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Osaka)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com	HTTPS
		rds.ap-northeast-3.api.aws	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com	HTTPS
		rds.ap-northeast-2.api.aws	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com	HTTPS
		rds.ap-southeast-1.api.aws	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com	HTTPS
		rds.ap-southeast-2.api.aws	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com	HTTPS
		rds.ap-northeast-1.api.aws	HTTPS
Kanada (Zentral)	ca-central-1	rds.ca-central-1.amazonaws.com	HTTPS
		rds.ca-central-1.api.aws	HTTPS
		rds-fips.ca-central-1.api.aws	HTTPS
		rds-fips.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	rds.ca-west-1.amazonaws.com	HTTPS
		rds-fips.ca-west-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Frankfurt)	eu-central-1	rds.eu-central-1.amazonaws.com rds.eu-central-1.api.aws	HTTPS HTTPS
Europa (Irland)	eu-west-1	rds.eu-west-1.amazonaws.com rds.eu-west-1.api.aws	HTTPS HTTPS
Europa (London)	eu-west-2	rds.eu-west-2.amazonaws.com rds.eu-west-2.api.aws	HTTPS HTTPS
Europa (Mailand)	eu-south-1	rds.eu-south-1.amazonaws.com rds.eu-south-1.api.aws	HTTPS HTTPS
Europa (Paris)	eu-west-3	rds.eu-west-3.amazonaws.com rds.eu-west-3.api.aws	HTTPS HTTPS
Europa (Spanien)	eu-south-2	rds.eu-south-2.amazonaws.com rds.eu-south-2.api.aws	HTTPS HTTPS
Europa (Stockholm)	eu-north-1	rds.eu-north-1.amazonaws.com rds.eu-north-1.api.aws	HTTPS HTTPS
Europa (Zürich)	eu-central-2	rds.eu-central-2.amazonaws.com rds.eu-central-2.api.aws	HTTPS HTTPS
Israel (Tel Aviv)	il-central-1	rds.il-central-1.amazonaws.com rds.il-central-1.api.aws	HTTPS HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Naher Osten (Bahrain)	me-south-1	rds.me-south-1.amazonaws.com rds.me-south-1.api.aws	HTTPS HTTPS
Naher Osten (VAE)	me-central-1	rds.me-central-1.amazonaws.com rds.me-central-1.api.aws	HTTPS HTTPS
Südamerika (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com rds.sa-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com rds.us-gov-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (US-West)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com rds.us-gov-west-1.api.aws	HTTPS HTTPS

Die folgende Tabelle zeigt das Format, das Sie beim Erstellen eines ARN für einen bestimmten Amazon RDS-Ressourcentyp verwenden sollten.

Ressourcentyp	ARN-Format
DB-Instance	arn:aws:rds:*<region>*:*<account>* :db:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :db:my-mysql-instance-1`
DB-Cluster	arn:aws:rds:*<region>*:*<account>* :cluster:*<name>*

Ressourcentyp	ARN-Format
	Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :cluster: my-aurora-cluster-1`
Ereignisabonnement	arn:aws:rds:*<region>*:*<account>* :es:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :es:my-subscription`
DB-Parametergruppe	arn:aws:rds:*<region>*:*<account>* :pg:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :pg:my-param-enable-logs`
DB-Cluster-Parametergruppe	arn:aws:rds:*<region>*:*<account>* :cluster-pg:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :cluster-pg: my-cluster-param-timezone`
Reservierte DB-Instance	arn:aws:rds:*<region>*:*<account>* :ri:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :ri:my-reserved-postgresql`

Ressourcentyp	ARN-Format
DB-Sicherheitsgruppe	arn:aws:rds:*<region>*:*<account>* :secgrp:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :secgrp:my-public`
Automatisierter DB-Snapshot	arn:aws:rds:*<region>*:*<account>* :snapshot:rds:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :snapshot:rds: my-mysql-db-2019-07-22-07-23`
Automatisierter DB-Cluster-Snapshot	arn:aws:rds:*<region>*:*<account>* :cluster-snapshot:rds:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :cluster-snapshot:rds: my-aurora-cluster-2019-07-22-16-16`
Manueller DB-Snapshot	arn:aws:rds:*<region>*:*<account>* :snapshot:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :snapshot: my-mysql-db-snap`
Manueller DB-Cluster-Snapshot	arn:aws:rds:*<region>*:*<account>* :cluster-snapshot:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :cluster-snapshot: my-aurora-cluster-snap`

Ressourcentyp	ARN-Format
DB-Subnetzgruppe	arn:aws:rds:*<region>*:*<account>* :subgrp:*<name>* Zum Beispiel: `arn:aws:rds: us-east-2 :123456789012 :subgrp:my-subnet-10`

Abrufen eines vorhandenen ARN

Sie können den ARN einer RDS-Ressource mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder der RDS-API abrufen.

Konsole

Um einen ARN von der zu erhalten AWS Management Console, navigieren Sie zu der Ressource, für die Sie einen ARN benötigen, und sehen Sie sich die Details für diese Ressource an.

Sie können den ARN für einen DB-Cluster beispielsweise auf der Seite Konfiguration der DB-Cluster-Details abrufen.

AWS CLI

Um einen ARN AWS CLI für eine bestimmte RDS-Ressource abzurufen, verwenden Sie den `describe` Befehl für diese Ressource. Die folgende Tabelle zeigt jeden AWS CLI Befehl und die ARN-Eigenschaft, die mit dem Befehl verwendet wird, um einen ARN abzurufen.

AWS CLI Befehl	ARN-Eigenschaft
describe-event-subscriptions	EventSubscriptionArn
describe-certificates	CertificateArn
describe-db-parameter-groups	DB ParameterGroup Arn
describe-db-cluster-parameter-groups	DB ClusterParameter GroupArn

AWS CLI Befehl	ARN-Eigenschaft
describe-db-instances	DB InstanceArn
describe-db-security-groups	DB SecurityGroup Arn
describe-db-snapshots	DB SnapshotArn
describe-events	SourceArn
describe-reserved-db-instances	Reservierte Datenbank InstanceArn
describe-db-subnet-groups	DB Arn SubnetGroup
describe-db-clusters	DB ClusterArn
describe-db-cluster-snapshots	DB ClusterSnapshot Arn

Mit dem folgenden AWS CLI Befehl wird beispielsweise der ARN für eine DB-Instance abgerufen.

Example

Für LinuxmacOS, oderUnix:

```
aws rds describe-db-instances \
--db-instance-identifier DBInstanceIdentifier \
--region us-west-2 \
--query "*[].{DBInstanceIdentifier:DBInstanceIdentifier,DBInstanceArn:DBInstanceArn}"
```

Windows:

```
aws rds describe-db-instances ^
--db-instance-identifier DBInstanceIdentifier ^
--region us-west-2 ^
--query "*[].{DBInstanceIdentifier:DBInstanceIdentifier,DBInstanceArn:DBInstanceArn}"
```

Die Ausgabe dieses Befehls sieht wie folgt aus:

```
[
    {
```

```
        "DBInstanceArn": "arn:aws:rds:us-west-2:account_id:db:instance_id",
        "DBInstanceIdentifier": "instance_id"
    }
]
```

RDS-API

Um einen ARN für eine bestimmte RDS-Ressource abzurufen, können Sie die folgenden RDS-API-Operationen aufrufen und die folgenden ARN-Eigenschaften verwenden.

RDS-API-Operation	ARN-Eigenschaft
DescribeEventAbonnements	EventSubscriptionArn
DescribeCertificates	CertificateArn
B beschrieben ParameterGroups	DB Arn ParameterGroup
Beschriebene DB-Gruppen ClusterParameter	DB ClusterParameter GroupArn
DescribeDBInstances	DB InstanceArn
Beschrieben B SecurityGroups	DB Arn SecurityGroup
DescribeDBSnapshots	DB SnapshotArn
DescribeEvents	SourceArn
DescribeReservedDB-Instances	Reservierte Datenbank InstanceArn
Beschriebenes B SubnetGroups	DB Arn SubnetGroup
DescribeDBClusters	DB ClusterArn
Beschrieben B ClusterSnapshots	DB Arn ClusterSnapshot

Amazon-Aurora-Updates

Amazon Aurora veröffentlicht regelmäßig Updates. Aktualisierungen werden auf das Amazon-Aurora-DB-Cluster während des Wartungszeitraums angewendet. Zu welchem Zeitpunkt Updates angewandt werden, ist von den Einstellungen für die Region und den Wartungszeitraum für das DB-Cluster und auch vom Typ des Updates abhängig. Aktualisierungen erfordern einen Neustart der Datenbank, daher kommt es zu einem Ausfall von 20 bis 30 Sekunden. Danach können Sie wieder mit der Nutzung Ihres DB-Clusters oder der Cluster fortfahren. Sie können die Einstellungen für den Wartungszeitraum in der anzeigen und ändern AWS Management Console.

> **Note**
>
> Die Zeit, die zum Neustart Ihrer DB-Instance benötigt wird, hängt vom Absturz-Wiederherstellungsprozess, der Datenbankaktivität zum Zeitpunkt des Neustarts und dem Verhalten Ihrer spezifischen DB-Engine ab. Wir empfehlen, während eines Neustarts die Datenbankaktivitäten möglichst zu minimieren, um die Dauer des Neustarts zu verkürzen. Die Reduzierung der Datenbankaktivität reduziert die Rollback-Aktivität für übertragene Transaktionen.

Informationen zu Betriebssystem-Updates für Amazon Aurora finden Sie unter Arbeiten mit Betriebssystem-Updates.

Einige Updates sind für eine Datenbank-Engine spezifisch, die von Aurora unterstützt wird. Weitere Informationen über Datenbank-Engine-Updates finden Sie in der folgenden Tabelle.

Datenbank-Engine	Aktualisierungen
Amazon Aurora MySQL	Siehe Datenbank-Engine-Updates für Amazon Aurora MySQL
Amazon Aurora PostgreSQL	Siehe Amazon Aurora PostgreSQL-Aktualisierungen

Identifizieren Ihrer Amazon-Aurora-Version

Amazon Aurora umfasst bestimmte Funktionen, die allgemein für Aurora und für alle Aurora-DB-Cluster verfügbar sind. Amazon Aurora umfasst andere Funktionen, die spezifisch für eine bestimmte

Datenbank-Engine sind, die Aurora unterstützt. Diese Funktionen stehen nur denjenigen Aurora-DB-Clustern zur Verfügung, die diese Datenbank-Engine verwenden, wie z. B. Aurora PostgreSQL.

Eine Aurora-DB-Instance hat zwei Versionsnummern, die Aurora-Versionsnummer und die Versionsnummer der Aurora-Datenbankengine. Aurora-Versionsnummern verwenden das folgende Format.

```
<major version>.<minor version>.<patch version>
```

Um die Aurora-Versionsnummer aus einer Aurora-DB-Instance abzurufen, die eine bestimmte Datenbank-Engine verwendet, verwenden Sie eine der folgenden Abfragen.

Datenbank-Engine	Abfragen
Amazon Aurora MySQL	`SELECT AURORA_VERSION();` `SHOW @@aurora_version;`
Amazon Aurora PostgreSQL	`SELECT AURORA_VERSION();`

Verwenden von Amazon RDS Extended Support

Mit Amazon RDS Extended Support können Sie Ihre Datenbank auf einer Haupt-Engine-Version gegen Aufpreis über das Ende des Aurora-Standard-Supports hinaus ausführen. Am Tag, an dem der Standardsupport für Aurora endet, Amazon Aurora Ihre Datenbanken automatisch bei RDS Extended Support. Die automatische Registrierung bei RDS Extended Support ändert nichts an der Datenbank-Engine und beeinträchtigt nicht die Verfügbarkeit oder Leistung Ihrer DB-Instance.

Dieses kostenpflichtige Angebot gibt Ihnen mehr Zeit für ein Upgrade auf eine unterstützte Hauptversion der Engine.

Das Enddatum des Standard-Supports für Aurora für Aurora MySQL Version 2 ist beispielsweise der 31. Oktober 2024. Sie sind jedoch nicht bereit, vor diesem Datum manuell auf Aurora MySQL Version 3 zu aktualisieren. In diesem Fall registriert Amazon Aurora Ihren Cluster am 31. Oktober 2024 automatisch bei RDS Extended Support, und Sie können Aurora MySQL Version 2 weiterhin ausführen. Ab dem 1. Dezember 2024 berechnet Ihnen Amazon Aurora automatisch Gebühren für RDS Extended Support.

RDS Extended Support ist bis zu 3 Jahre nach dem Ende des Standard-Supports von Aurora für eine Hauptversion der Engine verfügbar (3 Jahre und 4 Monate für Aurora MySQL Version 2). Wenn Sie nach dieser Zeit Ihre Haupt-Engine-Version nicht auf eine unterstützte Version aktualisiert haben, aktualisiert Amazon Aurora automatisch Ihre Haupt-Engine-Version. Wir empfehlen, so schnell wie möglich auf eine unterstützte Haupt-Engine-Version zu aktualisieren.

Themen

Überblick über Amazon RDS Extended Support

Nach dem Ende des Standard-Supports für Aurora Amazon Aurora Ihre Datenbanken automatisch beim RDS Extended Support. Aurora aktualisiert Ihre DB-Instance automatisch auf die letzte

Nebenversion, die vor dem Ende des Standard-Supports für Aurora veröffentlicht wurde, sofern Sie diese Version noch nicht ausführen. Amazon Aurora aktualisiert Ihre Nebenversion erst nach Ablauf des Standard-Supportdatums für Aurora für Ihre Haupt-Engine-Version.

Sie können neue Datenbanken mit wichtigen Engine-Versionen erstellen, die das Ende des Standard-Supports für Aurora erreicht haben. Aurora registriert diese neuen Datenbanken automatisch beim RDS Extended Support und berechnet Ihnen für dieses Angebot Gebühren.

Wenn Sie vor dem Ende des Standard-Supports für Aurora ein Upgrade auf eine Engine durchführen, für die der Aurora-Standardsupport noch verfügbar ist, wird Amazon Aurora Ihre Engine nicht für RDS Extended Support registrieren.

Wenn Sie versuchen, einen Snapshot einer Datenbank wiederherzustellen, die mit einer Engine kompatibel ist, deren Standardsupport für Aurora abgelaufen ist, aber nicht für RDS Extended Support registriert ist, versucht Amazon Aurora, den Snapshot so zu aktualisieren, dass er mit der neuesten Engine-Version kompatibel ist, die noch unter Aurora-Standardunterstützung steht. Wenn die Wiederherstellung fehlschlägt, registriert Amazon Aurora Ihre Engine automatisch bei RDS Extended Support mit einer Version, die mit dem Snapshot kompatibel ist.

Sie können die Registrierung für RDS Extended Support jederzeit beenden. Um die Registrierung zu beenden, aktualisieren Sie jede registrierte Engine auf eine neuere Engine-Version, die immer noch unter der Standardunterstützung von Aurora steht. Das Ende der Registrierung für RDS Extended Support wird an dem Tag wirksam, an dem Sie ein Upgrade auf eine neuere Engine-Version abschließen, für die der Aurora-Standardsupport noch verfügbar ist.

Themen

Gebühren für Amazon RDS Extended Support

Ab dem Tag nach dem Ende des Standard-Supports von Aurora fallen Gebühren für alle Engines an, die für RDS Extended Support registriert sind. Informationen zum Ende des Standard-Supports für Aurora finden Sie unterAmazon-Aurora-Hauptversionen.

Die zusätzliche Gebühr für RDS Extended Support endet automatisch, wenn Sie eine der folgenden Maßnahmen ergreifen:

- Führen Sie ein Upgrade auf eine Engine-Version durch, für die der Standardsupport gilt.
- Löschen Sie die Datenbank, auf der nach dem Ende des Standard-Supports von Aurora eine Hauptversion ausgeführt wird.

Die Gebühren werden wieder aufgenommen, wenn Ihre Ziel-Engine-Version in future in den RDS Extended Support aufgenommen wird.

Beispielsweise wird für Aurora PostgreSQL 11 am 1. März 2024 der erweiterte Support eingeführt, die Gebühren beginnen jedoch erst am 1. April 2024. Sie führen am 30. April 2024 ein Upgrade Ihrer Aurora PostgreSQL 11-Datenbank auf 12 durch. Ihnen werden nur 30 Tage Extended Support auf in Rechnung gestellt. Sie führen 12 weiterhin auf dieser DB-Instance aus, nachdem der RDS-Standardsupport am 28. Februar 2025 abgelaufen ist. Für Ihre Datenbank fallen ab dem 1. März 2025 wieder RDS Extended Support-Gebühren an.

Weitere Informationen finden Sie unter Preise für Amazon Aurora.

Vermeidung von Gebühren für Amazon RDS Extended Support

Sie können vermeiden, dass RDS Extended Support in Rechnung gestellt wird, indem Sie verhindern, dass Aurora nach dem Ende des Standard-Supports von Aurora , einen Aurora-DB-Cluster oder einen globalen Cluster erstellt oder wiederherstellt. Verwenden Sie dazu die AWS CLI oder die RDS-API.

Geben Sie im AWS CLIopen-source-rds-extended-support-disabled die `--engine-lifecycle-support` Option an. Geben Sie in der RDS-API `open-source-rds-extended-support-disabled` den `LifeCycleSupport` Parameter an. Weitere Informationen finden Sie unter Erstellen , eines Aurora-DB-Clusters oder eines globalen Clusters oder Wiederherstellung , eines Aurora-DB-Clusters oder eines globalen Clusters.

Versionen mit Amazon RDS Extended Support

RDS Extended Support ist für Aurora MySQL Versionen 2 und 3 sowie für Aurora PostgreSQL Version 11 und höher verfügbar. Weitere Informationen finden Sie unter Amazon-Aurora-Hauptversionen.

RDS Extended Support ist nur für bestimmte Nebenversionen verfügbar. Weitere Informationen finden Sie unter Amazon-Aurora-Nebenversionen.

RDS Extended Support ist nur am verfügbarAurora Serverless v2. Er ist nicht verfügbar amAurora Serverless v1.

Amazon Aurora und Kundenverantwortlichkeiten mit Amazon RDS Extended Support

Im folgenden Inhalt werden die Verantwortlichkeiten von Amazon Aurora und Ihre Aufgaben mit RDS Extended Support beschrieben.

Themen

— Verantwortlichkeiten von Amazon Aurora

Nach dem Ende des Standard-Supports für Aurora Amazon Aurora Patches, Bugfixes und Upgrades für Engines bereit, die für RDS Extended Support registriert sind. Dies gilt für bis zu 3 Jahre oder bis Sie die Engines nicht mehr verwenden, je nachdem, was zuerst eintritt.

Die Patches beziehen sich auf kritische und hohe CVEs, wie sie in den CVSS-Schweregraden der National Vulnerability Database (NVD) definiert sind. Weitere Informationen finden Sie unter Kennzahlen zu Schwachstellen.

Ihre Aufgaben

Sie sind verantwortlich für die Installation der Patches, Bugfixes und Upgrades, die für oder globale Cluster bereitgestellt werden, die für RDS Extended Support registriert sind. Amazon Aurora behält sich das Recht vor, solche Patches, Bugfixes und Upgrades jederzeit zu ändern, zu ersetzen oder zurückzuziehen. Wenn ein Patch erforderlich ist, um Sicherheits- oder kritische Stabilitätsprobleme zu beheben, behält sich Amazon Aurora das Recht vor, Ihre , Aurora-DB-Cluster oder globalen Cluster mit dem Patch zu aktualisieren oder zu verlangen, dass Sie den Patch installieren.

Sie sind auch dafür verantwortlich, Ihre Engine vor dem Ende des RDS-Extended Support auf eine neuere Engine-Version aufzurüsten. Das Datum, an dem der erweiterte Support für RDS endet, liegt in der Regel 3 Jahre nach dem Community-Ende des . . Das Datum, an dem der erweiterte Support für RDS für Ihre Datenbank-Haupt-Engine-Version endet, finden Sie unterAmazon-Aurora-Hauptversionen.

Wenn Sie Ihre Engine nicht aufrüsten, wird Amazon RDS versuchen, Ihre Engine auf die neueste Engine-Version aufzurüsten, die vom Aurora-Standardsupport unterstützt wird. Wenn das Upgrade

fehlschlägt, behält sich Aurora das Recht vor, die , den Aurora-DB-Cluster oder den globalen Cluster, auf dem die Engine läuft, nach dem Ende des Standard-Supports von Aurora zu löschen. Vorher bewahrt Aurora jedoch Ihre Daten aus dieser Engine auf.

Erstellen , eines Aurora-DB-Clusters oder eines globalen Clusters mit Amazon RDS Extended Support

Wenn Sie , einen Aurora-DB-Cluster oder einen globalen Cluster erstellen, wählen Sie in der Konsole die Option RDS Extended Support aktivieren aus oder verwenden Sie die Option Extended Support im Parameter AWS CLI oder in der RDS-API.

> **Note**
>
> Wenn Sie die Einstellung RDS Extended Support nicht angeben, verwendet Aurora standardmäßig RDS Extended Support. Durch dieses Standardverhalten wird die Verfügbarkeit Ihrer Datenbank über das Ende des Standard-Supports von Aurora hinaus aufrechterhalten.

Themen

Überlegungen zum RDS Extended Support

Bevor Sie , einen Aurora-DB-Cluster oder einen globalen Cluster erstellen, sollten Sie die folgenden Punkte berücksichtigen:

- Nach Ablauf des Datums für das Ende des Standard-Supports für Aurora können Sie die Erstellung oder eines neuen globalen Clusters verhindern und so die Gebühren für den erweiterten RDS-Support vermeiden. Verwenden Sie dazu die AWS CLI oder die RDS-API. Geben Sie im AWS CLI`open-source-rds-extended-support-disabled` die `--engine-lifecycle-support` Option an. Geben Sie in der RDS-API `open-source-rds-extended-support-disabled` den `LifeCycleSupport` Parameter an. Wenn Sie angeben `open-source-rds-extended-support-disabled` und das Ende des Standard-Supports für Aurora abgelaufen ist, schlägt die Erstellung , eines Aurora-DB-Clusters oder eines globalen Clusters immer fehl.

- RDS Extended Support wird auf Clusterebene festgelegt. Mitglieder eines Clusters haben immer dieselbe Einstellung für RDS Extended Support in der RDS-Konsole, `--engine-lifecycle-support` in der AWS CLI und `EngineLifecycleSupport` in der RDS-API.

Weitere Informationen finden Sie unter Amazon-Aurora-Versionen.

Erstellen Sie , einen Aurora-DB-Cluster oder einen globalen Cluster mit RDS Extended Support

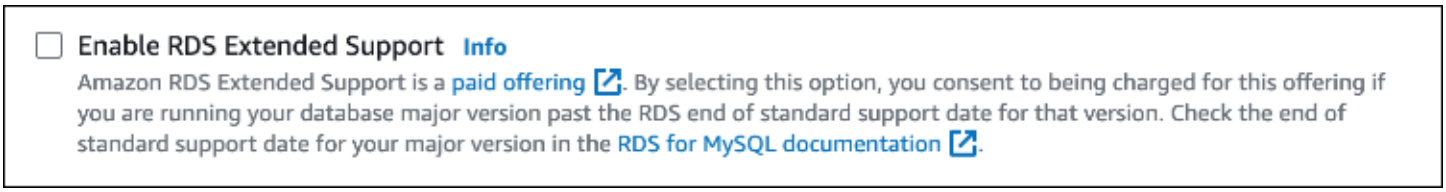
Sie können , einen Aurora-DB-Cluster oder einen globalen Cluster mit einer RDS Extended Support-Version mithilfe der AWS Management Console AWS CLI, der oder der RDS-API erstellen.

> **Note**
>
> Die AWS CLI `--engine-lifecycle-support` Option und der `EngineLifeCycle` RDS-API-Parameter sind derzeit nur für Aurora PostgreSQL verfügbar. Sie werden kurz vor Ablauf des Standard-Supportdatums für Aurora für Aurora MySQL verfügbar sein.

Konsole

Wenn Sie einen Aurora-DB-Cluster oder einen globalen Cluster, erstellen, wählen Sie im Abschnitt Engine-Optionen die Option RDS Extended Support aktivieren aus.

Die folgende Abbildung zeigt die Einstellung Enable RDS Extended Support:



AWS CLI

Wenn Sie den Befehl create-db-cluster oder create-global-cluster create-db-instance https://docs.aws.amazon.com/cli/latest/reference/rds/create-global-cluster.html) ausführen, wählen Sie RDS Extended Support aus, indem Sie für die Option angeben. AWS CLI `open-source-rds-extended-support` `--engine-lifecycle-support` Standardmäßig ist diese `open-source-rds-extended-support` Option auf eingestellt.

Um die Erstellung , eines neuen Aurora-DB-Clusters oder eines globalen Clusters nach dem Ende des Standard-Supports für Aurora zu verhindern, geben Sie `open-source-rds-extended-support-disabled` für die `--engine-lifecycle-support` Option an. Auf diese Weise vermeiden Sie alle damit verbundenen Gebühren für den RDS Extended Support.

RDS-API

Wenn Sie den Amazon RDS-API-Vorgang CreateDBCluster oder CreateGlobalCluster verwenden, wählen Sie RDS Extended Support aus, indem Sie den Parameter auf setzen. `EngineLifecycleSupport` `open-source-rds-extended-support` Dieser Parameter ist standardmäßig auf `open-source-rds-extended-support` festgelegt.

Um die Erstellung , eines neuen Aurora-DB-Clusters oder eines globalen Clusters nach dem Ende des Standard-Supports für Aurora zu verhindern, geben Sie `open-source-rds-extended-support-disabled` für den `EngineLifecycleSupport` Parameter an. Auf diese Weise vermeiden Sie alle damit verbundenen Gebühren für den RDS Extended Support.

Weitere Informationen finden Sie unter den folgenden Themen:

- Um einen Aurora-DB-Cluster zu erstellen, folgen Sie den Anweisungen für Ihre DB-Engine unterErstellen eines Amazon Aurora-DB Clusters.
- Um einen globalen Cluster zu erstellen, folgen Sie den Anweisungen für Ihre DB-Engine unterErstellen einer Amazon Aurora Global Database.

Anzeige der Registrierung Ihrer oder globaler Cluster in Amazon RDS Extended Support

Sie können die Registrierung Ihrer oder globalen Cluster in RDS Extended Support mithilfe der AWS Management Console, der oder der AWS CLI RDS-API anzeigen.

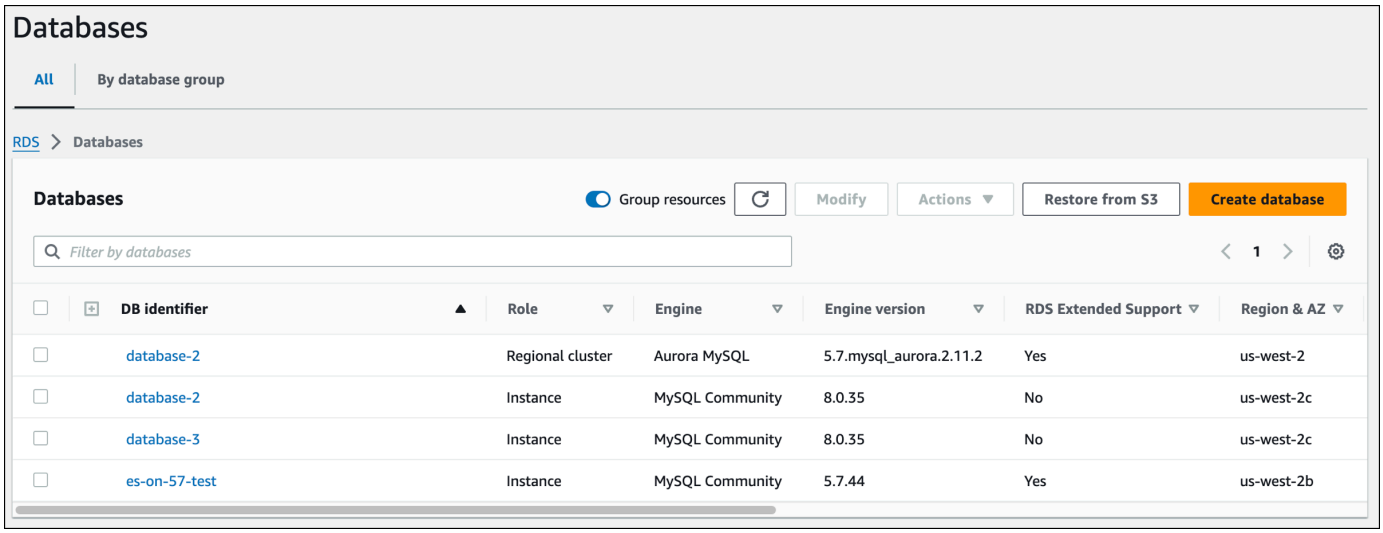
Konsole

So zeigen Sie die Registrierung Ihrer oder globalen Cluster in RDS Extended Support an

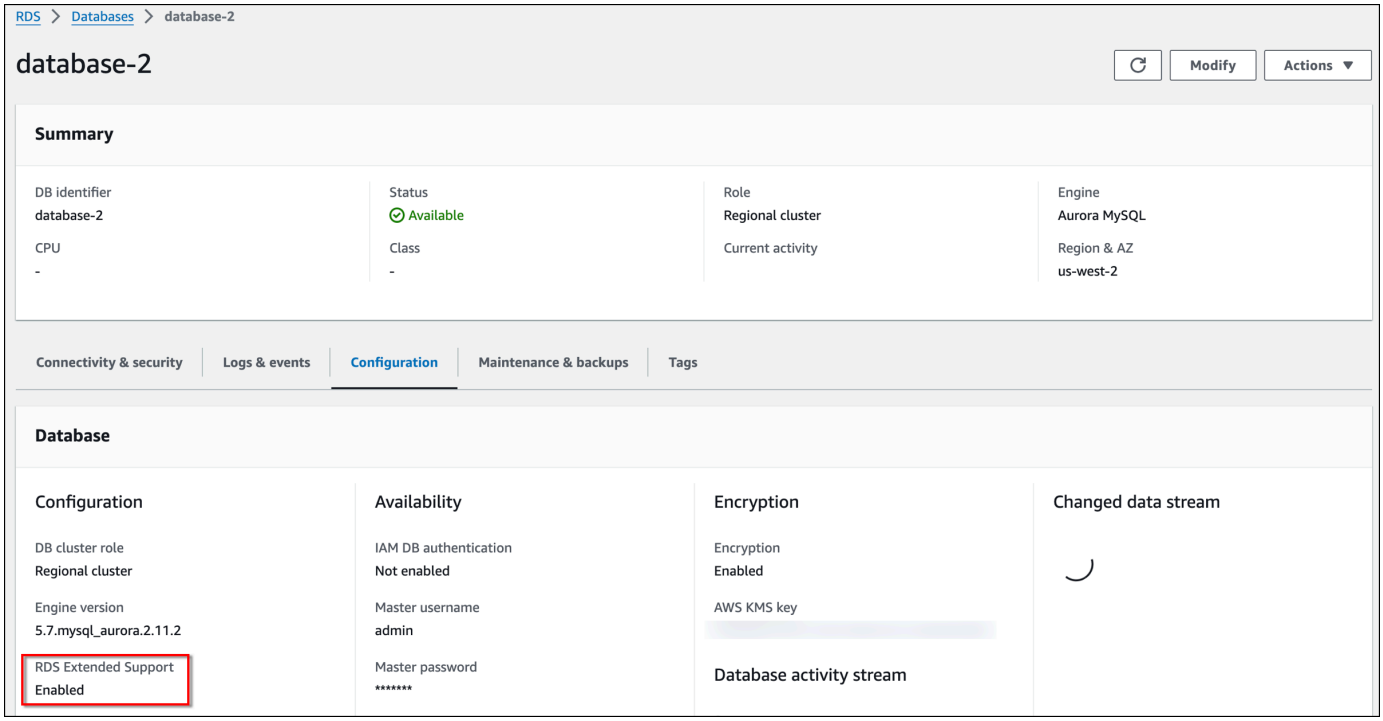
1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Datenbanken aus. Der Wert unter RDS Extended Support gibt an, ob , ein Aurora-DB-Cluster oder ein globaler Cluster für RDS Extended Support registriert ist. Wenn kein Wert angezeigt wird, ist RDS Extended Support für Ihre Datenbank nicht verfügbar.

> **Tip**
>
> Wenn die Spalte RDS Extended Support nicht angezeigt wird, wählen Sie das Symbol Einstellungen und aktivieren Sie dann RDS Extended Support.



3. Sie können die Registrierung auch auf der Registerkarte Konfiguration für jede Datenbank einsehen. Wählen Sie unter DB-ID eine Datenbank aus. Suchen Sie auf der Registerkarte Konfiguration unter Erweiterter Support nach, ob die Datenbank registriert ist oder nicht.



AWS CLI

Wenn RDS Extended Support für eine Datenbank verfügbar ist, enthält die Antwort den ParameterEngineLifecycleSupport. Der Wert `open-source-rds-extended-support` gibt an, dass , ein Aurora-DB-Cluster oder ein globaler Cluster bei RDS Extended Support registriert ist. Der Wert `open-source-rds-extended-support-disabled` gibt an, dass die Registrierung der oder des globalen Clusters in RDS Extended Support deaktiviert wurde.

Beispiel

Der folgende Befehl gibt Informationen für alle Ihre Aurora-DB-Cluster zurück:

```
aws rds describe-db-clusters
```

Die folgende Antwort zeigt, dass eine Aurora PostgreSQL-Engine, die auf dem Aurora-DB-Cluster läuft, bei RDS Extended Support registriert `database-1` ist:

```
{
    "DBClusterIdentifier": "database-1",
    ...
    "Engine": "aurora-postgresql",
```

```
    ...
    "EngineLifecycleSupport": "open-source-rds-extended-support"
}
```

RDS-API

Um die Registrierung Ihrer Datenbanken bei RDS Extended Support mithilfe der Amazon RDS-API einzusehen, verwenden Sie den Vorgang . DescribeGlobal

Wenn RDS Extended Support für eine Datenbank verfügbar ist, enthält die Antwort den ParameterEngineLifecycleSupport. Der Wert `open-source-rds-extended-support` gibt an, dass , ein Aurora-DB-Cluster oder ein globaler Cluster bei RDS Extended Support registriert ist. Der Wert `open-source-rds-extended-support-disabled` gibt an, dass die Registrierung der oder des globalen Clusters in RDS Extended Support deaktiviert wurde.

Wiederherstellung , eines Aurora-DB-Clusters oder eines globalen Clusters mit Amazon RDS Extended Support

Wenn Sie , einen Aurora-DB-Cluster oder einen globalen Cluster wiederherstellen, wählen Sie in der Konsole die Option RDS Extended Support aktivieren oder verwenden Sie die Option Extended Support im Parameter AWS CLI oder in der RDS-API.

> **Note**
>
> Wenn Sie die Einstellung RDS Extended Support nicht angeben, verwendet Aurora standardmäßig RDS Extended Support. Durch dieses Standardverhalten wird die Verfügbarkeit Ihrer Datenbank über das Ende des Standard-Supports von Aurora hinaus aufrechterhalten.

Themen

- Überlegungen zum RDS Extended Support
- Wiederherstellung , eines Aurora-DB-Clusters, eines DB-Clusters oder eines globalen Clusters mit RDS Extended Support

Überlegungen zum RDS Extended Support

Bevor Sie , einen Aurora-DB-Cluster oder einen globalen Cluster wiederherstellen, sollten Sie die folgenden Punkte berücksichtigen:

- Wenn Sie nach Ablauf des Aurora-DB-Cluster oder einen globalen Cluster von Amazon S3 wiederherstellen möchten, können Sie dies nur mit der AWS CLI oder der RDS-API tun. Verwenden Sie die `--engine-lifecycle-support` Option im AWS CLI Befehl restore-db-cluster-from-s3 oder den Parameter im RDS-API-Vorgang RestoreDB S3. `EngineLifecycleSupport` ClusterFrom
- Wenn Sie verhindern möchten, dass Aurora Ihre Datenbanken auf RDS Extended Support-Versionen zurücksetzt, geben Sie dies `open-source-rds-extended-support-disabled` in der AWS CLI oder der RDS-API an. Auf diese Weise vermeiden Sie alle damit verbundenen Gebühren für den RDS Extended Support.

  Wenn Sie diese Einstellung angeben, aktualisiert Amazon Aurora Ihre wiederhergestellte Datenbank automatisch auf eine neuere, unterstützte Hauptversion. Wenn das Upgrade die Prüfungen vor dem Upgrade nicht erfolgreich durchführt, führt Amazon Aurora ein sicheres Rollback zur Version der RDS Extended Support Engine durch. Diese Datenbank bleibt im RDS Extended Support-Modus, und Amazon Aurora berechnet Ihnen RDS Extended Support in Rechnung, bis Sie Ihre Datenbank manuell aktualisieren.
- RDS Extended Support wird auf Clusterebene festgelegt. Mitglieder eines Clusters haben immer dieselbe Einstellung für RDS Extended Support in der RDS-Konsole, `--engine-lifecycle-support` in der AWS CLI und `EngineLifecycleSupport` in der RDS-API.

Weitere Informationen finden Sie unter Amazon-Aurora-Versionen.

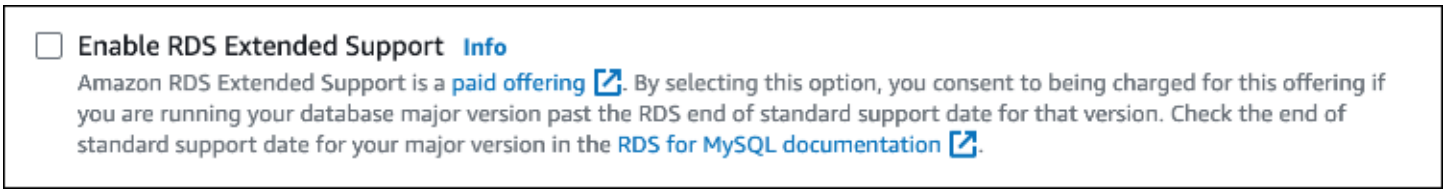
Wiederherstellung , eines Aurora-DB-Clusters, eines DB-Clusters oder eines globalen Clusters mit RDS Extended Support

Sie können , einen Aurora-DB-Cluster oder einen globalen Cluster mit einer RDS Extended Support-Version mithilfe der AWS Management Console AWS CLI, der oder der RDS-API wiederherstellen.

Konsole

Wenn Sie einen Aurora-DB-Cluster oder einen globalen Cluster, eine wiederherstellen, wählen Sie im Abschnitt Engine-Optionen die Option RDS Extended Support aktivieren aus.

Die folgende Abbildung zeigt die Einstellung Enable RDS Extended Support:



AWS CLI

Wenn Sie den Befehl restore-db-cluster-from-snapshot https://docs.aws.amazon.com/cli/latest/reference/rds/restore-db-cluster-from-snapshot.html ausführen, wählen Sie RDS Extended Support aus, indem Sie für die Option angeben. AWS CLI `open-source-rds-extended-support` `--engine-lifecycle-support`

Wenn Sie Gebühren im Zusammenhang mit RDS Extended Support vermeiden möchten, stellen Sie die `--engine-lifecycle-support` Option auf einop`en-source-rds-extended-support-disabled`. Standardmäßig ist diese Option auf eingestelltop`en-source-rds-extended-support`.

Sie können diesen Wert auch mit den folgenden AWS CLI Befehlen angeben:

- restore-db-cluster-from-s3
- restore-db-cluster-to-point-in-time

RDS-API

Wenn Sie den Amazon RDS-API-Vorgang RestoreDB ClusterFrom Snapshot RestoreDB aus, indem Sie den Parameter auf setzen. `EngineLifecycleSupport` `open-source-rds-extended-support`

Wenn Sie Gebühren im Zusammenhang mit RDS Extended Support vermeiden möchten, setzen Sie den `EngineLifecycleSupport` Parameter auf`open-source-rds-extended-support-disabled`. Dieser Parameter ist standardmäßig auf `open-source-rds-extended-support` festgelegt.

Sie können diesen Wert auch mithilfe der folgenden RDS-API-Operationen angeben:

- DB S3 wiederhergestellt ClusterFrom
- DB-Zeit ClusterTo PointIn wiederhergestellt

Weitere Informationen zur Wiederherstellung eines Aurora-DB-Clusters finden Sie in den Anweisungen für Ihre DB-Engine unterSichern und Wiederherstellen eines Amazon-Aurora-DB-Clusters.

Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen

Bei einer Blau/Grün-Bereitstellung wird eine Produktionsdatenbankumgebung in eine separate, synchronisierte Staging-Umgebung kopiert. Mithilfe von Blau/Grün-Bereitstellungen von Amazon RDS können Sie Änderungen an der Datenbank in der Staging-Umgebung vornehmen, ohne die Produktionsumgebung zu beeinträchtigen. Sie können beispielsweise die Haupt- oder Nebenversion der DB-Engine aktualisieren, Datenbankparameter ändern oder Schemaänderungen in der Staging-Umgebung vornehmen. Wenn Sie bereit sind, können Sie die Staging-Umgebung zur neuen Produktionsdatenbankumgebung hochstufen, wobei die Ausfallzeit in der Regel weniger als eine Minute beträgt.

Amazon Aurora erstellt die Staging-Umgebung durch Klonen des zugrunde liegenden Aurora-Speichervolumens in der Produktionsumgebung. Das Cluster-Volume in der Staging-Umgebung speichert nur inkrementelle Änderungen, die an dieser Umgebung vorgenommen wurden.

> **Note**
>
> Derzeit werden Blau/Grün-Bereitstellungen Aurora MySQL und Aurora PostgreSQL. Informationen zur Verfügbarkeit der Amazon-RDS-Engine finden Sie unter Verwenden von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen im Amazon-RDS-Benutzerhandbuch.

Themen

Übersicht über Blau/Grün-Bereitstellungen von Amazon RDS für Aurora

Mithilfe von Blau/Grün-Bereitstellungen von Amazon RDS können Sie Datenbankänderungen vornehmen und testen, bevor Sie sie in einer Produktionsumgebung implementieren. Mit einer Blau/Grün-Bereitstellung wird eine Staging-Umgebung erstellt, die die Produktionsumgebung kopiert. In einer Blau/Grün-Umgebung ist die blaue Umgebung die aktuelle Produktionsumgebung. Die grüne Umgebung ist die Staging-Umgebung. Die Staging-Umgebung bleibt mithilfe der logischen Replikation mit der aktuellen Produktionsumgebung synchronisiert.

Sie können Änderungen dem Aurora-DB-Cluster in der grünen Umgebung vornehmen, ohne die Produktions-Workloads zu beeinträchtigen. Sie können beispielsweise die Haupt- oder Nebenversion der DB-Engine aktualisieren, oder Datenbankparameter in der Staging-Umgebung ändern. Sie können Änderungen in der grünen Umgebung gründlich testen. Wenn Sie bereit sind, können Sie die Umgebungen umstellen, um die grüne Umgebung zur neuen Produktionsumgebung hochzustufen. Die Umstellung dauert in der Regel weniger als eine Minute, ohne dass Daten verloren gehen und Anwendungsänderungen erforderlich sind.

Da die grüne Umgebung eine Kopie der Topologie der Produktionsumgebung ist, werden der DB-Cluster und alle seine DB-Instances in der Bereitstellung kopiert. Die grüne Umgebung umfasst auch die vom DB-Cluster verwendeten Funktionen wie DB-Cluster-Snapshots, Performance Insights, verbesserte Überwachung und Aurora Serverless v2.

> **Note**
>
> Blue/Green-Bereitstellungen werden für Aurora MySQL und Aurora PostgreSQL unterstützt. Informationen zur Verfügbarkeit von Amazon RDS finden Sie unter Verwenden von Amazon RDS Blue/Green Deployments für Datenbank-Updates im Amazon RDS-Benutzerhandbuch.

Themen

- Bewährte Methoden für Blau/Grün-Bereitstellungen
- Einschränkungen für Blau/Grün-Bereitstellungen

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen finden Sie unter the section called “Blau/Grün-Bereitstellungen”.

Vorteile der Verwendung von Blau/Grün-Bereitstellung von Amazon RDS

Durch die Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS können Sie über Sicherheitspatches auf dem Laufenden bleiben, die Datenbankleistung verbessern und neuere Datenbankfunktionen mit kurzen, vorhersehbaren Ausfallzeiten einführen. Blau/Grün-Bereitstellungen reduzieren die Risiken und Ausfallzeiten für Datenbankaktualisierungen, wie Upgrades von Engine-Haupt- und -Nebenversionen.

Blau/Grün-Bereitstellungen bieten die folgenden Vorteile:

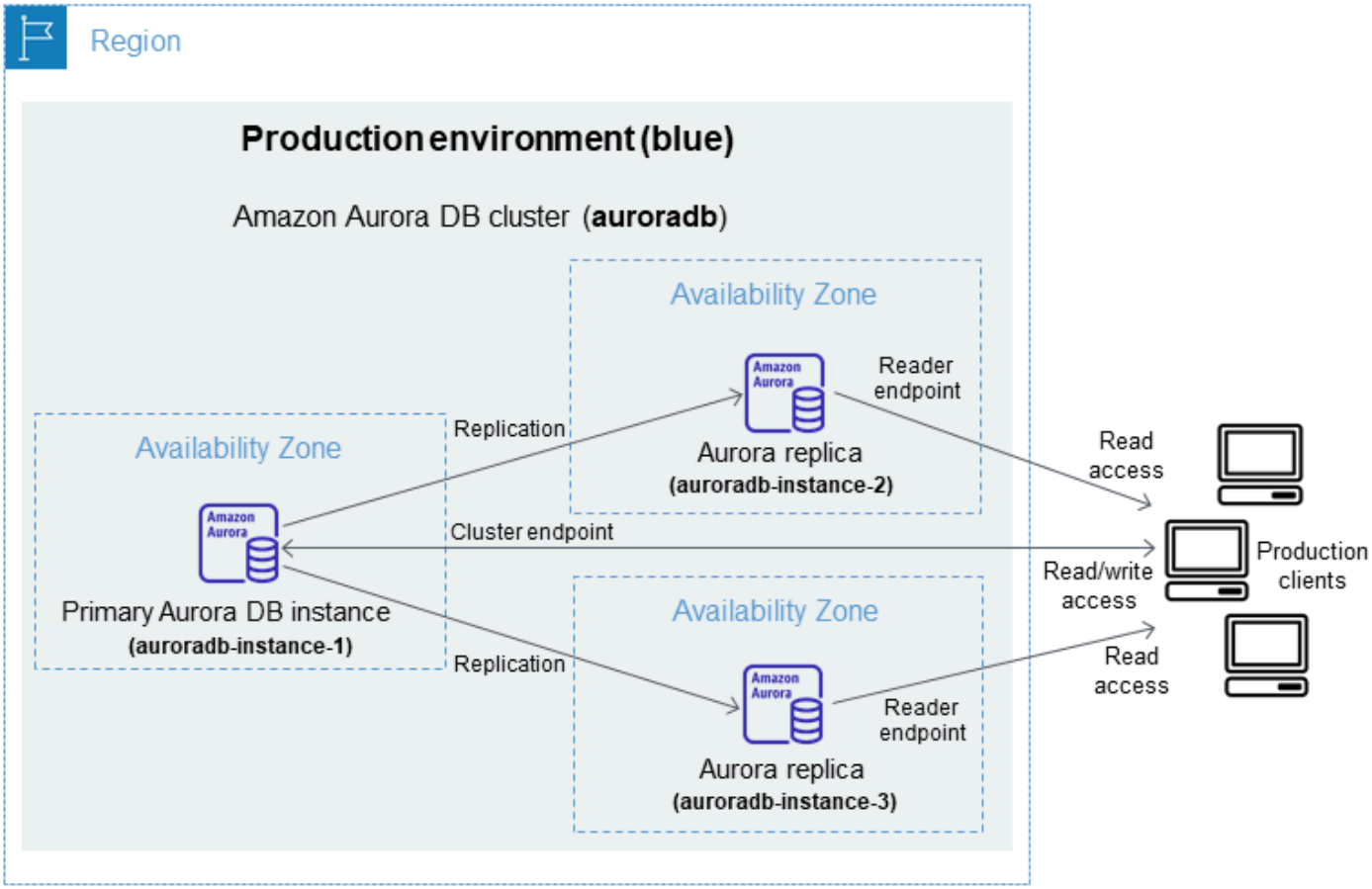
- Sie können ganz einfach eine produktionsreife Staging-Umgebung erstellen.
- Sie können Datenbankänderungen von der Produktionsumgebung in die Staging-Umgebung automatisch replizieren.
- Sie können Datenbankänderungen in einer sicheren Staging-Umgebung testen, ohne die Produktionsumgebung zu beeinträchtigen.
- Sie bleiben mit Datenbank-Patches und Systemaktualisierungen auf dem Laufenden.
- Sie können neue Datenbankfunktionen implementieren und testen.
- Sie können Ihre Staging-Umgebung auf die neue Produktionsumgebung umstellen, ohne Änderungen an Ihrer Anwendung vorzunehmen.
- Die Umstellung erfolgt durch den Einsatz des integrierten Integritätsschutzes völlig sicher.
- Es treten keine Datenverluste während der Umstellung auf.
- Die Umstellung erfolgt schnell, in der Regel in weniger als einer Minute, abhängig von Ihrer Workload.

Workflow einer Blau/Grün-Bereitstellung

Führen Sie die folgenden Hauptschritte aus, wenn Sie eine Blau/Grün-Bereitstellung für Aktualisierungen von Aurora-DB-Clustern verwenden möchten.

1. Identifizieren Sie einen Produktions-DB-Cluster, der aktualisiert werden muss.

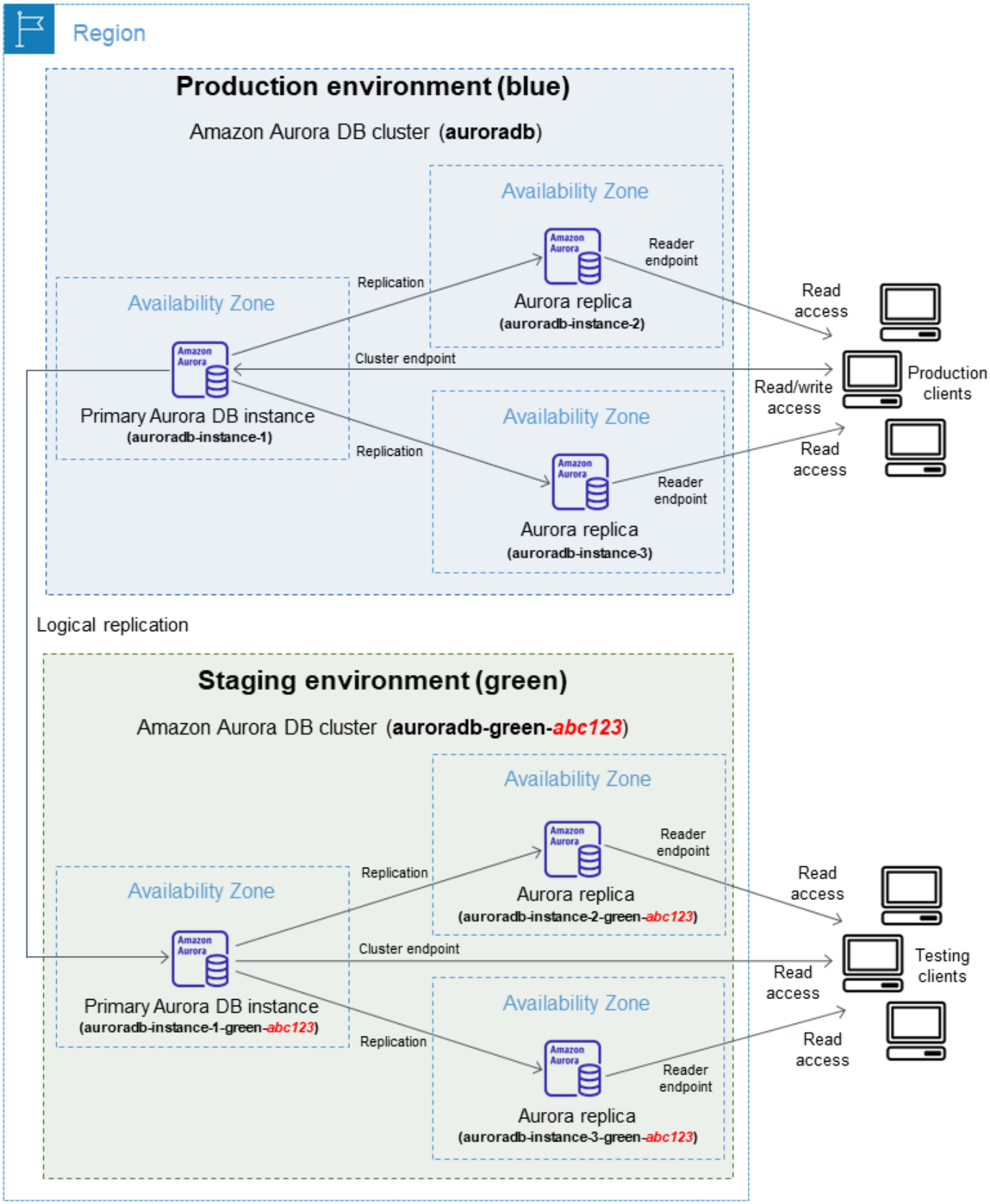
   Die folgende Abbildung zeigt ein Beispiel für einen Produktions-DB-Cluster.



2. Erstellen Sie die Blau/Grün-Bereitstellung. Anweisungen finden Sie unter Erstellen einer Blau/Grün-Bereitstellung.

   Die folgende Abbildung zeigt ein Beispiel für eine Blau/Grün-Bereitstellung der Produktionsumgebung aus Schritt 1. Bei der Erstellung der Blau/Grün-Bereitstellung kopiert RDS die vollständige Topologie und Konfiguration des Aurora-DB-Clusters, um die grüne Umgebung zu erstellen. Den Namen des kopierten DB-Clusters und der DB-Instances wird `-green-random-characters` angehängt. Die Staging-Umgebung in der Abbildung enthält den DB-Cluster (auroradb-green-*abc123*). Außerdem enthält sie die drei DB-Instances im DB-Cluster

(auroradb-instance1-green-*abc123*, auroradb-instance2-green-*abc123* und auroradb-instance3-green-*abc123*).


Region
Production environment (blue)
Amazon Aurora DB cluster (auroradb)
Availability Zone
Aurora replica
(auroradb-instance-2)
Reader endpoint
Replication
Availability Zone
Primary Aurora DB instance
(auroradb-instance-1)
Cluster endpoint
Read access
Production clients
Read/write access
Availability Zone
Aurora replica
(auroradb-instance-3)
Replication
Reader endpoint
Read access
Logical replication
Staging environment (green)
Amazon Aurora DB cluster (auroradb-green-abc123)
Availability Zone
Aurora replica
(auroradb-instance-2-green-abc123)
Reader endpoint
Replication
Availability Zone
Primary Aurora DB instance
(auroradb-instance-1-green-abc123)
Cluster endpoint
Read access
Testing clients
Read access
Availability Zone
Aurora replica
(auroradb-instance-3-green-abc123)
Replication
Reader endpoint
Read access

Wenn Sie die Blau/Grün-Deployment erstellen, können Sie Ihre DB-Engine-Version aktualisieren und eine andere DB-Cluster-Parametergruppe für den DB-Cluster in der grünen Umgebung angeben. Außerdem können Sie eine andere DB-Parametergruppe für die DB-Instances im DB-Cluster angeben.

RDS konfiguriert auch die Replikation von der primären DB-Instance in der blauen Umgebung zur primären DB-Instance in der grünen Umgebung.

> **Important**
>
> Für Aurora MySQL Version 3 erlaubt der DB-Cluster in der grünen Umgebung standardmäßig Schreibvorgänge, nachdem Sie die blaue/grüne Bereitstellung erstellt haben. Wir empfehlen, den DB-Cluster schreibgeschützt zu machen, indem Sie den `read_only` Parameter auf setzen `1` und den Cluster neu starten.

3. Nehmen Sie Änderungen an der Staging-Umgebung vor.

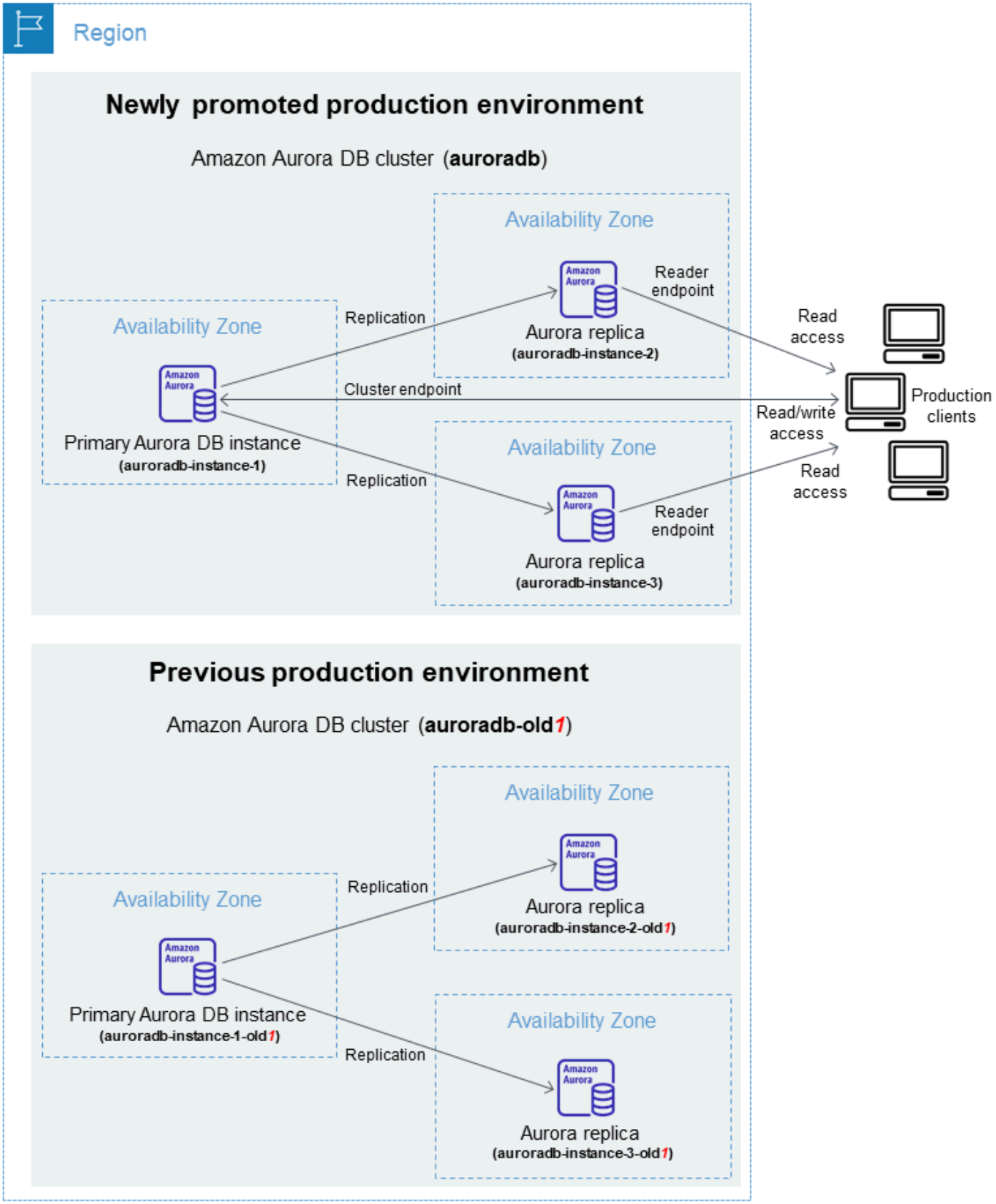
   Sie können beispielsweise Schemaänderungen an Ihrer Datenbank vornehmen oder die DB-Instance-Klasse ändern, die von einer oder mehreren DB-Instances in der grünen Umgebung verwendet wird.

   Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.
4. Testen Sie Ihre Staging-Umgebung.

   Während des Testens empfehlen wir, dass Sie Ihre Datenbanken in der grünen Umgebung schreibgeschützt lassen. Aktivieren Sie Schreibvorgänge in der grünen Umgebung mit Vorsicht, da sie zu Replikationskonflikten führen können. Sie können auch zu ungewollten Daten in den Produktionsdatenbanken nach der Umstellung führen. Um Schreibvorgänge für Aurora MySQL zu aktivieren, setzen Sie den `read_only` Parameter auf `0` und starten Sie dann die DB-Instance neu. Setzen Sie für Aurora PostgreSQL den `default_transaction_read_only` Parameter `off` auf Sitzungsebene auf.
5. Wenn Sie bereit sind, können Sie die Umstellung vornehmen und die Staging-Umgebung zur neuen Produktionsumgebung hochstufen. Anweisungen finden Sie unter Umstellen einer Blau/Grün-Bereitstellung.

   Die Umstellung führt zu Ausfallzeiten. Die Ausfallzeit beträgt normalerweise weniger als eine Minute, kann aber je nach Workload länger sein.

Die folgende Abbildung zeigt die DB-Cluster nach der Umstellung.


Region
Newly promoted production environment
Amazon Aurora DB cluster (auroradb)
Availability Zone
Amazon Aurora
Reader endpoint
Availability Zone
Replication
Aurora replica
(auroradb-instance-2)
Read access
Cluster endpoint
Production clients
Read/write access
Primary Aurora DB instance
(auroradb-instance-1)
Availability Zone
Replication
Read access
Reader endpoint
Aurora replica
(auroradb-instance-3)
Previous production environment
Amazon Aurora DB cluster (auroradb-old1)
Availability Zone
Availability Zone
Replication
Aurora replica
(auroradb-instance-2-old1)
Primary Aurora DB instance
(auroradb-instance-1-old1)
Availability Zone
Replication
Aurora replica
(auroradb-instance-3-old1)

Nach der Umstellung wird der Aurora-DB-Cluster in der grünen Umgebung zum neuen Produktions-DB-Cluster. Die Namen und Endpunkte in der aktuellen Produktionsumgebung werden der neu hochgestuften Produktionsumgebung zugewiesen, sodass keine Änderungen an Ihrer Anwendung erforderlich sind. Infolgedessen fließt Ihr Produktionsdatenverkehr jetzt in die neue Produktionsumgebung. Der DB-Cluster und die DB-Instances in der blauen Umgebung werden umbenannt, indem `-old`*n* an den aktuellen Namen angehängt wird, wobei *n* eine Zahl ist. Angenommen, der Name der DB-Instance in der blauen Umgebung lautet `auroradb-instance-1`. Nach der Umstellung könnte der Name der DB-Instance `auroradb-instance-1-old1` lauten.

In dem Beispiel in der Abbildung werden bei der Umstellung die folgenden Änderungen vorgenommen:

- Der DB-Cluster in der grünen Umgebung `auroradb-green-abc123` wird zum Produktions-DB-Cluster und erhält den Namen `auroradb`.
- Die DB-Instance in der grünen Umgebung `auroradb-instance1-green-abc123` wird zur Produktions-DB-Instance und erhält den Namen `auroradb-instance1`.
- Die DB-Instance in der grünen Umgebung `auroradb-instance2-green-abc123` wird zur Produktions-DB-Instance und erhält den Namen `auroradb-instance2`.
- Die DB-Instance in der grünen Umgebung `auroradb-instance3-green-abc123` wird zur Produktions-DB-Instance und erhält den Namen `auroradb-instance3`.
- Der DB-Cluster in der blauen Umgebung `auroradb` wird in `auroradb-old1` umbenannt.
- Die DB-Instance in der blauen Umgebung `auroradb-instance1` wird in `auroradb-instance1-old1` umbenannt.
- Die DB-Instance in der blauen Umgebung `auroradb-instance2` wird in `auroradb-instance2-old1` umbenannt.
- Die DB-Instance in der blauen Umgebung `auroradb-instance3` wird in `auroradb-instance3-old1` umbenannt.

6. Eine Blau/Grün-Bereitstellung, die Sie nicht mehr benötigen, können Sie löschen. Anweisungen finden Sie unter Löschen einer Blau/Grün-Bereitstellung.

   Nach der Umstellung wird die vorherige Produktionsumgebung nicht gelöscht, sodass Sie sie bei Bedarf für Regressionstests verwenden können.

Autorisierung des Zugangs zu Operationen in der Blau/Grün-Bereitstellung

Benutzer müssen über die erforderlichen Berechtigungen verfügen, um Operationen im Zusammenhang mit Blau/Grün-Bereitstellungen ausführen zu können. Sie können IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Sie können diese Richtlinien dann den IAM-Berechtigungssätzen oder -Rollen zuordnen, die diese Berechtigungen benötigen. Weitere Informationen finden Sie unter Identity and Access Management für Amazon Aurora.

Der Benutzer, der eine Blau/Grün-Bereitstellung erstellt, muss über Berechtigungen zum Ausführen folgender RDS-Operationen verfügen:

- `rds:AddTagsToResource`
- `rds:CreateDBCluster`
- `rds:CreateDBInstance`
- `rds:CreateDBClusterEndpoint`

Der Benutzer, der eine Blau/Grün-Bereitstellung umstellt, muss über Berechtigungen zum Ausführen folgender RDS-Operationen verfügen:

- `rds:ModifyDBCluster`
- `rds:PromoteReadReplicaDBCluster`

Der Benutzer, der eine Blau/Grün-Bereitstellung löscht, muss über Berechtigungen zum Ausführen folgender RDS-Operationen verfügen:

- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`
- `rds:DeleteDBClusterEndpoint`

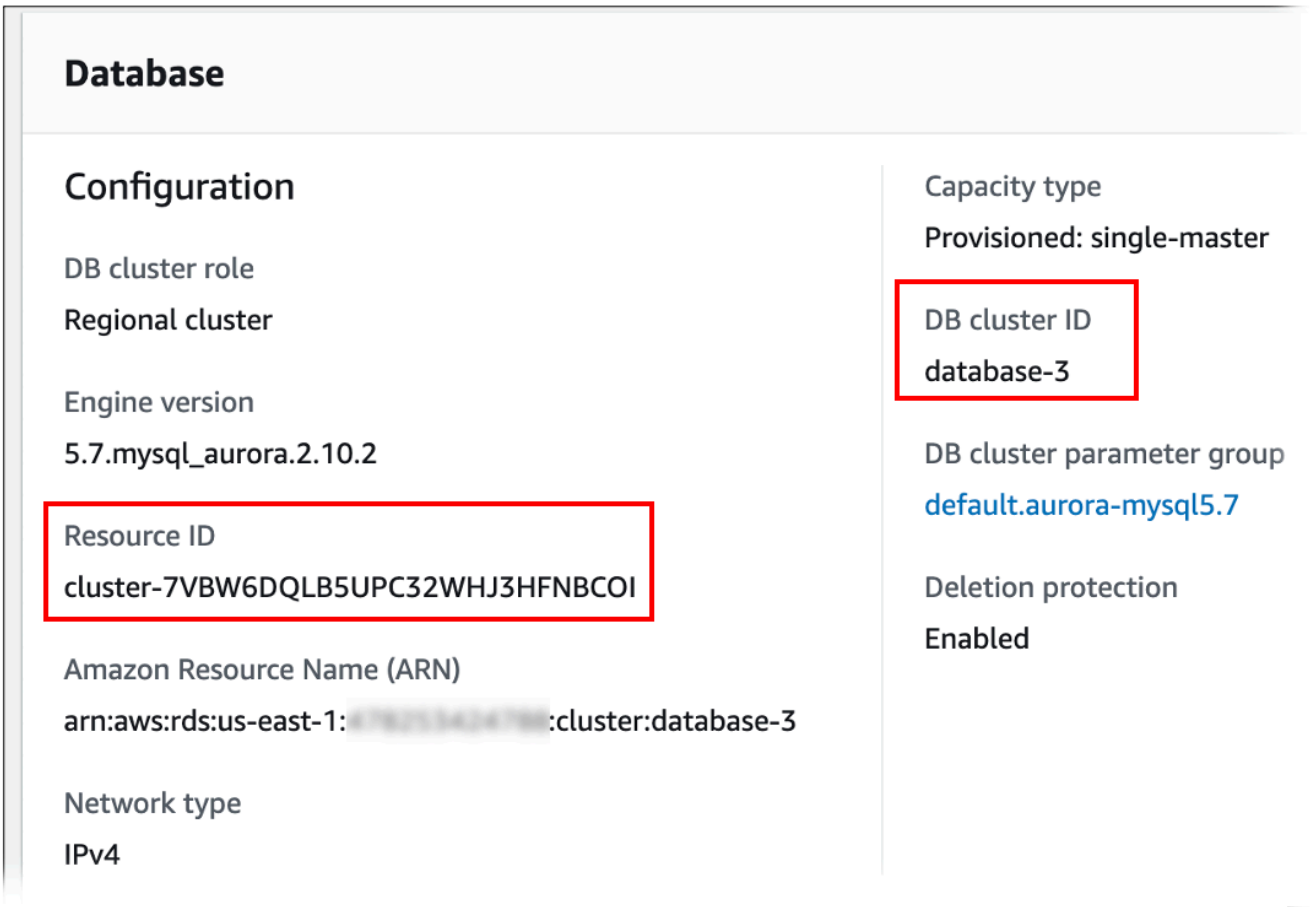
Aurora stellt in Ihrem Namen Ressourcen in der Staging-Umgebung bereit und ändert sie. Zu diesen Ressourcen gehören DB-Instances, die eine intern definierte Namenskonvention verwenden. Daher dürfen angehängte IAM-Richtlinien keine unvollständigen Muster für Ressourcennamen enthalten, wie `my-db-prefix-*` z. Nur Platzhalter (*) werden unterstützt. Im Allgemeinen empfehlen wir, Ressourcen-Tags und andere unterstützte Attribute anstelle von Platzhaltern zu verwenden, um

den Zugriff auf diese Ressourcen zu steuern. Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon RDS.

Überlegungen zur Blau/Grün-Bereitstellungen

Amazon RDS verfolgt Ressourcen in Blau/Grün-Bereitstellungen mit der `DbiResourceId` und `DbClusterResourceId` jeder Ressource. Diese Ressourcen-ID ist eine AWS-Region eindeutige, unveränderliche Kennung für die Ressource.

Die Ressourcen-ID ist getrennt von der DB-Cluster-ID:



Der Name (Cluster-ID) einer Ressource ändert sich, wenn Sie auf eine Blau/Grün-Bereitstellung umstellen, jede Ressource behält jedoch dieselbe Ressourcen-ID. Eine DB-Cluster-ID in der blauen Umgebung lautete beispielsweise `mycluster`. Nach der Umstellung könnte dieser DB-Cluster in `mycluster-old1` umbenannt sein. Die Ressourcen-ID des DB-Clusters ändert sich während der Umstellung jedoch nicht. Wenn also die grünen Ressourcen auf die neuen Produktionsressourcen hochgestuft werden, stimmen ihre Ressourcen-IDs nicht mit den blauen Ressourcen-IDs überein, die zuvor in der Produktion vorhanden waren.

Nach der Umstellung auf eine Blau/Grün-Bereitstellung sollten Sie erwägen, die Ressourcen-IDs auf die IDs der neu hochgestuften Produktionsressourcen für integrierte Funktionen und Dienste zu aktualisieren, die Sie mit den Produktionsressourcen verwendet haben. Berücksichtigen Sie insbesondere die folgenden Aktualisierungen:

- Wenn Sie die Filterung mithilfe der RDS-API und der Ressourcen-IDs durchführen, passen Sie die beim Filtern verwendeten Ressourcen-IDs nach der Umstellung an.
- Wenn Sie Ressourcen CloudTrail für die Überwachung verwenden, passen Sie die Benutzer von so an, CloudTrail dass sie die neuen Ressourcen-IDs nach dem Switchover verfolgen. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora-API-Aufrufen in AWS CloudTrail.
- Wenn Sie Datenbank-Aktivitätsstreams für Ressourcen in der blauen Umgebung verwenden, passen Sie Ihre Anwendung an, um die Datenbankereignisse für den neuen Stream nach der Umstellung zu überwachen. Weitere Informationen finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Datenbankaktivitätsstreams.
- Wenn Sie die Performance-Insights-API verwenden, passen Sie die Ressourcen-IDs in API-Aufrufen nach der Umstellung an. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .

  Sie können eine Datenbank mit demselben Namen nach der Umstellung überwachen, diese enthält jedoch nicht die Daten, die vor der Umstellung vorhanden waren.
- Wenn Sie in IAM-Richtlinien Ressourcen-IDs verwenden, stellen Sie sicher, dass Sie bei Bedarf die Ressourcen-IDs der neu hochgestuften Ressourcen hinzufügen. Weitere Informationen finden Sie unter Identity and Access Management für Amazon Aurora.
- Wenn Ihrer IAM-Rollen zugeordnet sind, stellen Sie sicher, dass Sie diese nach dem Switchover erneut zuordnen. Angehängte Rollen werden nicht automatisch in die grüne Umgebung kopiert.
- Wenn Sie sich mithilfe der IAM-Datenbankauthentifizierung bei Ihrem DB-Cluster authentifizieren, stellen Sie sicher, dass in der für den Datenbankzugriff verwendeten IAM-Richtlinie sowohl die blauen als auch die grünen Datenbanken unter dem Element `Resource` der Richtlinie aufgeführt sind. Dies ist erforderlich, um nach der Umstellung eine Verbindung mit der grünen Datenbank herzustellen. Weitere Informationen finden Sie unter the section called “Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff”.
- Wenn Sie einen manuellen DB-Cluster-Snapshot für einen DB-Cluster wiederherstellen möchten, der Teil einer Blau/Grün-Bereitstellung war, stellen Sie sicher, dass Sie den richtigen DB-Cluster-Snapshot wiederherstellen, indem Sie den Zeitpunkt überprüfen, zu dem der Snapshot erstellt wurde. Weitere Informationen finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.

- Amazon Aurora erstellt die Grün-Umgebung, indem das zugrunde liegende Aurora-Speichervolume in der Blau-Umgebung geklont wird. Das grüne Cluster-Volume speichert nur inkrementelle Änderungen, die in der Grün-Umgebung vorgenommen wurden. Wenn Sie den DB-Cluster in der Blau-Umgebung löschen, wächst die Größe des zugrunde liegenden Aurora-Speichervolumens in der Grün-Umgebung auf die volle Größe an. Weitere Informationen finden Sie unter the section called “Klonen eines Volumes für einen Aurora-DB-Cluster”.
- Wenn Sie dem DB-Cluster in der grünen Umgebung einer Blau/Grün-Bereitstellung eine DB-Instance hinzufügen, ersetzt die neue DB-Instance bei der Umstellung keine DB-Instance in der blauen Umgebung. Die neue DB-Instance wird jedoch im DB-Cluster beibehalten und wird in der neuen Produktionsumgebung zu einer DB-Instance.
- Wenn Sie eine DB-Instance im DB-Cluster der grünen Umgebung einer Blau/Grün-Bereitstellung löschen, können Sie keine neue DB-Instance erstellen, um sie in der Blau/Grün-Bereitstellung zu ersetzen.

  Wenn Sie eine neue DB-Instance mit demselben Namen und ARN wie die gelöschte DB-Instance erstellen, hat sie eine andere `DbiResourceId`. Sie ist folglich nicht Teil der grünen Umgebung.

  Das folgende Verhalten ergibt sich, wenn Sie eine DB-Instance im DB-Cluster der grünen Umgebung löschen:

  - Wenn die DB-Instance in der blauen Umgebung mit dem gleichen Namen vorhanden ist, wird sie nicht auf die DB-Instance in der grünen Umgebung umgestellt. Diese DB-Instance wird nicht umbenannt, indem dem DB-Instance-Namen `-old`*n* angefügt wird.
  - Jede Anwendung, die auf die DB-Instance in der blauen Umgebung verweist, verwendet nach der Umstellung weiterhin dieselbe DB-Instance.

Bewährte Methoden für Blau/Grün-Bereitstellungen

Nachfolgend sind bewährte Methoden für Blau/Grün-Bereitstellungen aufgeführt:

Allgemeine bewährte Methoden

- Testen Sie den Aurora-DB-Cluster in der grünen Umgebung gründlich, bevor Sie umstellen.
- Halten Sie Ihre Datenbanken in der grünen Umgebung schreibgeschützt. Wir empfehlen, Schreibvorgänge in der grünen Umgebung mit Vorsicht zu aktivieren, da sie zu Replikationskonflikten führen können. Sie können auch zu ungewollten Daten in den Produktionsdatenbanken nach der Umstellung führen.

- Wenn Sie eine Blau/Grün-Bereitstellung zur Implementierung von Schemaänderungen verwenden, nehmen Sie nur replikationskompatible Änderungen vor.

  Sie können beispielsweise neue Spalten am Ende einer Tabelle hinzufügen, ohne die Replikation von der blauen zur grünen Bereitstellung zu unterbrechen. Schemaänderungen, wie das Umbenennen von Spalten oder Tabellen, führen jedoch dazu, dass die Replikation zur Grün-Bereitstellung unterbrochen wird.

  Weitere Informationen zu replikationskompatiblen Änderungen finden Sie in der MySQL-Dokumentation unter Replikation mit unterschiedlichen Tabellendefinitionen auf Quelle und Replikat sowie unter Einschränkungen in der Dokumentation zur logischen Replikation in PostgreSQL.
- Verwenden Sie den Cluster-Endpunkt, den Reader-Endpunkt oder den benutzerdefinierten Endpunkt für alle Verbindungen in beiden Umgebungen. Verwenden Sie keine Instance-Endpunkte oder benutzerdefinierten Endpunkte mit statischen oder Ausschlusslisten.
- Wenn Sie auf eine Blau/Grün-Bereitstellung umstellen, befolgen Sie die bewährten Methoden für die Umstellung. Weitere Informationen finden Sie unter the section called “Bewährte Methoden für die Umstellung”.

Bewährte Methoden für Aurora PostgreSQL

- Überwachen Sie den Write-Through-Cache für die logische Replikation in Aurora PostgreSQL und nehmen Sie gegebenenfalls Anpassungen am Cache-Puffer vor. Weitere Informationen finden Sie unter the section called “Überwachung des Write-Through-Cache für die logische Replikation”.
- Wenn Ihre Datenbank über ausreichend freien Speicher verfügt, erhöhen Sie den Wert des `logical_decoding_work_mem` DB-Parameters in der blauen Umgebung. Dadurch muss auf der Festplatte weniger dekodiert werden und stattdessen wird Arbeitsspeicher beansprucht. Sie können den freien Speicher mit der Metrik überwachen. `FreeableMemory` CloudWatch Weitere Informationen finden Sie unter the section called “CloudWatch Metriken für Aurora”.
- Aktualisieren Sie alle Ihre PostgreSQL-Erweiterungen auf die neueste Version, bevor Sie eine Blau/Grün-Bereitstellung erstellen. Weitere Informationen finden Sie unter the section called “Aktualisieren von PostgreSQL-Erweiterungen”.
- Wenn Sie die `aws_s3`-Erweiterung verwenden, stellen Sie sicher, dass Sie dem DB-Cluster der grünen über eine IAM-Rolle Zugriff auf Amazon S3 gewähren, nachdem die grüne Umgebung erstellt wurde. Dadurch können die Import- und Exportbefehle auch nach der Umstellung weiter

funktionieren. Anweisungen finden Sie unter the section called “Einrichten des Zugriffs auf einen Amazon S3-Bucket”.

- Wenn Sie eine höhere Engine-Version für die grüne Umgebung angeben, führen Sie den `ANALYZE` Vorgang für alle Datenbanken aus, um die `pg_statistic` Tabelle zu aktualisieren. Optimizer-Statistiken werden während eines größeren Versionsupgrades nicht übertragen. Sie müssen daher alle Statistiken neu generieren, um Leistungsprobleme zu vermeiden. Weitere bewährte Methoden bei größeren Versionsupgrades finden Sie unter.
- Vermeiden Sie es, Trigger so zu konfigurieren, als `ENABLE REPLICA` `ENABLE ALWAYS` ob der Trigger auf der Quelle verwendet wird, um Daten zu manipulieren. Andernfalls leitet das Replikationssystem die Änderungen weiter und führt den Trigger aus, was zu Duplizierungen führt.
- Transaktionen mit langer Laufzeit können zu erheblichen Verzögerungen bei der Replikation führen. Um die Verzögerung bei Replikaten zu verringern, sollten Sie Folgendes in Betracht ziehen:
  - Reduzieren Sie lang andauernde Transaktionen, die verzögert werden können, bis die grüne Umgebung die blaue Umgebung eingeholt hat.
  - Initiieren Sie an stark frequentierten Tischen einen manuellen Vakuum-Freeze-Vorgang, bevor Sie die blaue/grüne Bereitstellung erstellen.
  - Deaktivieren Sie für PostgreSQL Version 12 und höher den `index_cleanup` Parameter für große oder ausgelastete Tabellen, um die normale Wartungsrate bei blauen Datenbanken zu erhöhen.
- Eine langsame Replikation kann dazu führen, dass Sender und Empfänger häufig neu gestartet werden, was die Synchronisation verzögert. Um sicherzustellen, dass sie aktiv bleiben, deaktivieren Sie Timeouts, indem Sie den `wal_sender_timeout` Parameter auf `0` in der blauen Umgebung und den `wal_receiver_timeout` Parameter auf `0` in der grünen Umgebung setzen.

Einschränkungen für Blau/Grün-Bereitstellungen

Die folgenden Einschränkungen gelten für Blau/Grün-Bereitstellungen:

Themen

- Allgemeine Einschränkungen für Blau/Grün-Bereitstellungen
- Einschränkungen der PostgreSQL-Erweiterung für Blue/Green-Bereitstellungen
- Einschränkungen für Änderungen bei Blau/Grün-Bereitstellungen
- Einschränkungen der logischen Replikation von PostgreSQL für Blau/Grün-Bereitstellungen

Allgemeine Einschränkungen für Blau/Grün-Bereitstellungen

Die folgenden Einschränkungen gelten für Blau/Grün-Bereitstellungen:

- Die Aurora-MySQL-Versionen 2.08 und 2.09 werden als Quell- oder Zielversionen für Upgrades nicht unterstützt.
- Sie können einen Cluster, der Teil einer blauen/grünen Bereitstellung ist, nicht beenden und starten.
- Blaue/grüne Bereitstellungen unterstützen nicht die Verwaltung von Masterbenutzerkennwörtern mit. AWS Secrets Manager
- Wenn Sie eine blaue/grüne Bereitstellung aus einem Aurora MySQL-Quell-DB-Cluster erstellen, für den Backtrack aktiviert ist, wird der grüne DB-Cluster ohne Backtracking-Unterstützung erstellt. Das liegt daran, dass Backtracking nicht mit der Replikation von Binärprotokollen (Binlog) funktioniert, die für Blue/Green-Bereitstellungen erforderlich ist. Weitere Informationen finden Sie unter the section called “Rückverfolgen eines DB-Clusters”.

  Wenn Sie versuchen, einen Backtrack auf dem blauen DB-Cluster zu erzwingen, wird die blaue/grüne Bereitstellung unterbrochen und der Switchover wird blockiert.
- Für Aurora MySQL kann der Quell-DB-Cluster keine Datenbanken mit dem Namen `tmp`enthalten. Datenbanken mit diesem Namen werden nicht in die grüne Umgebung kopiert.
- Für Aurora PostgreSQL werden nicht protokollierte Tabellen nicht in die grüne Umgebung repliziert, es sei denn, der `rds.logically_replicate_unlogged_tables`-Parameter ist in dem blauen DB-Cluster auf 1 gesetzt. Wir empfehlen, diesen Parameterwert nicht zu ändern, nachdem Sie eine Blau/Grün-Bereitstellung erstellt haben, um mögliche Replikationsfehler bei nicht protokollierten Tabellen zu vermeiden.
- Für Aurora PostgreSQL kann der Blue Environment keine selbstverwaltete logische Quelle (Herausgeber) oder Replik (Abonnent) sein. Für Aurora MySQL kann der blaue kein externes Binlog-Replikat sein.
- Während der Umstellung sind für die blauen und grünen Umgebungen keine Null-ETL-Integrationen mit Amazon Redshift möglich. Sie müssen zuerst die Integration löschen und umstellen. Anschließend erstellen Sie die Integration neu.
- Der Ereignisplaner (Parameter `event_scheduler`) muss in der grünen Umgebung deaktiviert werden, wenn Sie eine Blau/Grün-Bereitstellung erstellen. Dadurch wird verhindert, dass Ereignisse in der grünen Umgebung generiert werden und zu Inkonsistenzen führen.
- Alle Aurora Auto Scaling Scaling-Richtlinien, die auf dem blauen DB-Cluster definiert sind, werden nicht in die grüne Umgebung kopiert.

- Blaue/grüne Bereitstellungen unterstützen den AWS JDBC-Treiber für MySQL nicht. Weitere Informationen finden Sie unter Bekannte Einschränkungen von. GitHub
- Blau/Grün-Bereitstellungen werden für die folgenden Funktionen nicht unterstützt:
  - Amazon-RDS-Proxy
  - Regionsübergreifende Lesereplikate
  - Aurora Serverless v1-DB-Cluster
  - DB-Cluster, die Teil einer globalen Aurora-Datenbank sind
  - Babelfish für Aurora PostgreSQL
  - AWS CloudFormation

Einschränkungen der PostgreSQL-Erweiterung für Blue/Green-Bereitstellungen

Die folgenden Einschränkungen gelten für PostgreSQL-Erweiterungen:

- Die `pg_partman`-Erweiterung muss in der blauen Umgebung deaktiviert werden, wenn Sie eine Blau/Grün-Bereitstellung erstellen. Die Erweiterung führt DDL-Operationen wie etwa `CREATE TABLE` durch, die die logische Replikation von der blauen in die grüne Umgebung unterbrechen.
- Die `pg_cron`-Erweiterung muss in allen grünen Datenbanken deaktiviert bleiben, nachdem die Blau/Grün-Bereitstellung erstellt wurde. Die Erweiterung verfügt über Hintergrund-Worker, die als Superuser ausgeführt werden und die Schreibschutzeinstellung der grünen Umgebung umgehen, was zu Replikationskonflikten führen kann.
- Für die `apg_plan_mgmt`-Erweiterung muss der `apg_plan_mgmt.capture_plan_baselines`-Parameter für alle grünen Datenbanken auf `off` gesetzt sein, um Primärschlüsselkonflikte zu vermeiden, wenn ein identischer Plan in der blauen Umgebung erfasst wird. Weitere Informationen finden Sie unter the section called “Übersicht über die Abfrageplanverwaltung in Aurora PostgreSQL”.

  Wenn Sie Ausführungspläne in Aurora Replicas erfassen möchten, müssen Sie beim Aufrufen der `apg_plan_mgmt.create_replica_plan_capture`-Funktion den Endpunkt des blauen DB-Clusters angeben. Dadurch wird sichergestellt, dass die Planerfassungen nach der Umstellung weiterhin funktionieren. Weitere Informationen finden Sie unter the section called “Erfassung von Aurora-PostgreSQL-Ausführungsplänen”.
- Wenn der blaue DB-Cluster als fremder Server einer FDW-Erweiterung (Foreign Data Wrapper) konfiguriert ist, müssen Sie den Endpunktnamen des -Clusters anstelle von IP-Adressen verwenden. Dadurch kann die Konfiguration auch nach der Umstellung funktionsfähig bleiben.

- Die Erweiterungen `pglogical` und `pg_active` müssen in der blauen Umgebung deaktiviert werden, wenn Sie eine Blau/Grün-Bereitstellung erstellen. Nachdem Sie die grüne Umgebung zur neuen Produktionsumgebung erklärt haben, können Sie die Erweiterungen wieder aktivieren. Dazu kann die blaue Datenbank kein logischer Subscriber einer externen Instance sein.
- Wenn Sie die `pgAudit` Erweiterung verwenden, muss sie in den gemeinsam genutzten Bibliotheken (`shared_preload_libraries`) der benutzerdefinierten DB-Parametergruppen sowohl für die blaue als auch für die grüne DB-Instance verbleiben. Weitere Informationen finden Sie unter the section called “Einrichten der pgAudit-Erweiterung”.

Einschränkungen für Änderungen bei Blau/Grün-Bereitstellungen

Die folgenden Einschränkungen gelten für Änderungen in einer Blau/Grün-Bereitstellung:

- Sie können einen unverschlüsselten DB-Cluster nicht in einen verschlüsselten DB-Cluster ändern.
- Sie können einen verschlüsselten DB-Cluster nicht in einen unverschlüsselten DB-Cluster ändern.
- Sie können einen DB-Cluster in der blauen Umgebung nicht auf eine höhere Engine-Version als die des entsprechenden DB-Clusters in der grünen Umgebung ändern.
- Die Ressourcen in der blauen und der grünen Umgebung müssen sich in demselben AWS-Konto befinden.
- Wenn die blaue Umgebung Richtlinien für Aurora Auto Scaling enthält, werden diese Richtlinien nicht in die grüne Umgebung kopiert. Sie müssen die Richtlinien der grünen Umgebung manuell erneut hinzufügen.

Einschränkungen der logischen Replikation von PostgreSQL für Blau/Grün-Bereitstellungen

Blau/Grün-Bereitstellungen verwenden die logische Replikation, um die Staging-Umgebung mit der Produktionsumgebung synchron zu halten. PostgreSQL hat bestimmte Einschränkungen in Bezug auf die logische Replikation, die sich in Einschränkungen bei der Erstellung von Blau/Grün-Bereitstellungen für Aurora-PostgreSQL-DB-Cluster niederschlagen.

In der folgenden Tabelle werden die Einschränkungen der logischen Replikation beschrieben, die für Blau/Grün-Bereitstellungen für Aurora PostgreSQL gelten.

Einschränkung	Erklärung
Data Definition Language (DDL)-Anweisungen wie `CREATE TABLE` und `CREATE SCHEMA` werden nicht von der blauen in die grüne Umgebung repliziert.	Wenn Aurora eine DDL-Änderung in der blauen Umgebung erkennt, gehen die grünen Datenbanken in den Status Replikation herabgestuft über. Sie erhalten ein Ereignis, das Sie darüber informiert, dass DDL-Änderungen in der blauen Umgebung nicht in die grüne Umgebung repliziert werden können. Sie müssen die Blau/Grün-Bereitstellung und alle grünen Datenbanken löschen und dann neu erstellen. Andernfalls können Sie die Blau/Grün-Bereitstellung nicht umstellen.
`NEXTVAL`-Operationen an Sequenzobjekten werden nicht zwischen der blauen und der grünen Umgebung synchronisiert.	Während der Umstellung erhöht Aurora die Sequenzwerte in der grünen Umgebung so, dass sie denen in der blauen Umgebung entsprechen. Wenn Sie Tausende von Sequenzen haben, kann dies die Umstellung verzögern.
Die Erstellung oder Änderung großer Objekte in der blauen Umgebung wird nicht in die grüne Umgebung repliziert.	Wenn Aurora die Erstellung oder Änderung großer Objekte in der blauen Umgebung erkennt, die in der `pg_largeobject` -Systemtabelle gespeichert sind, gehen die grünen Datenbanken in den Status Replikation herabgestuft über. Aurora generiert ein Ereignis, das Sie darüber informiert, dass große Objektänderungen in der blauen Umgebung nicht in die grüne Umgebung repliziert werden können. Sie müssen die Blau/Grün-Bereitstellung und alle grünen Datenbanken löschen und dann neu erstellen. Andernfalls können Sie die Blau/Grün-Bereitstellung nicht umstellen.
Materialisierte Ansichten werden in der grünen	Durch das Aktualisieren materialisierter Ansichten in der blauen Umgebung werden sie in der grünen Umgebung nicht aktualisiert. Nach der Umstellung können Sie eine Aktualisierung der materialisierten Ansichten planen.

Einschränkung	Erklärung
Umgebung nicht automatisch aktualisiert.	
UPDATE- und DELETE-Operationen sind für Tabellen, die keinen Primärschlüssel haben, nicht zulässig.	Bevor Sie eine Blau/Grün-Bereitstellung erstellen, stellen Sie sicher, dass alle Tabellen in dem DB-Cluster über einen Primärschlüssel verfügen.

Weitere Informationen finden Sie in der Dokumentation zur logischen Replikation in PostgreSQL.

Erstellen einer Blau/Grün-Bereitstellung

Wenn Sie eine Blau/Grün-Bereitstellung erstellen, geben Sie den DB-Cluster an, der in die Bereitstellung kopiert werden soll. Der DB-Cluster, den Sie auswählen, ist der Produktions-DB-Cluster und wird in der blauen Umgebung zum DB-Cluster. RDS kopiert die Topologie der blauen Umgebung zusammen mit den konfigurierten Funktionen in einen Staging-Bereich. Der DB-Cluster wird in die grüne Umgebung kopiert und RDS konfiguriert die Replikation vom DB-Cluster in der blauen Umgebung zum DB-Cluster in der grünen Umgebung. RDS kopiert auch alle DB-Instances im DB-Cluster.

Themen

- Vorbereiten einer Blau-Grün-Bereitstellung
- Angeben von Änderungen bei der Erstellung einer Blau/Grün-Bereitstellung
- Erstellen einer Blau/Grün-Bereitstellung
- Einstellungen für die Erstellung von blauen/grünen Bereitstellungen

Vorbereiten einer Blau-Grün-Bereitstellung

Abhängig von der Engine, auf der Ihre ausgeführt wird, müssen Sie bestimmte Schritte ausführen, bevor Sie eine blaue/grüne Bereitstellung erstellen.

Themen

Vorbereitung eines Aurora MySQL-DB-Clusters für eine blaue/grüne Bereitstellung

Bevor Sie eine Blau/Grün-Bereitstellung für einen Aurora-MySQL-DB-Cluster erstellen, muss der Cluster mit einer benutzerdefinierten DB-Cluster-Parametergruppe verknüpft werden, bei der die binäre Protokollierung (`binlog_format`) aktiviert ist. Für die Replikation von der blauen Umgebung in die grüne Umgebung ist die binäre Protokollierung erforderlich. Obwohl jedes Binlog-Format funktioniert, empfehlen wir `ROW`, um das Risiko von Replikationsinkonsistenzen zu verringern. Weitere Informationen über das Erstellen einer benutzerdefinierten DB-Parametergruppe und das Festlegen von Parametern finden Sie unter the section called “Arbeiten mit DB-Cluster-Parametergruppen”.

> **Note**
>
> Durch die Aktivierung der binären Protokollierung wird die Anzahl der Write-Disk-I/O-Operationen für den DB-Cluster erhöht. Sie können die IOPS-Nutzung mit der `VolumeWriteIOPs` CloudWatch Metrik überwachen.

Nachdem Sie die binäre Protokollierung aktiviert haben, stellen Sie sicher, dass Sie den DB-Cluster neu starten, damit Ihre Änderungen wirksam werden. Blau/Grün-Bereitstellungen erfordern, dass die Writer-Instance mit der DB-Cluster-Parametergruppe synchronisiert ist, andernfalls schlägt die Erstellung fehl. Weitere Informationen finden Sie unter Neustarten einer DB-Instance in einem Aurora Cluster.

Darüber hinaus empfehlen wir, den Aufbewahrungszeitraum für Binärprotokolle auf einen anderen Wert zu ändern, als `NULL` zu verhindern, dass Binärprotokolldateien gelöscht werden. Weitere Informationen finden Sie unter the section called “Konfigurieren”.

Vorbereiten eines Aurora PostgreSQL-DB-Clusters für eine blaue/grüne Bereitstellung

Bevor Sie eine Blau/Grün-Bereitstellung für einen DB-Cluster von Aurora PostgreSQL erstellen, stellen Sie sicher, dass Sie die folgenden Schritte ausführen:

- Ordnen Sie den Cluster einer benutzerdefinierten DB-Cluster-Parametergruppe zu, für die die logische Replikation (`rds.logical_replication`) aktiviert ist. Für die Replikation von der blauen zur grünen Umgebung ist die logische Replikation erforderlich.

  Wenn Sie die logische Replikation aktivieren, müssen Sie auch bestimmte Cluster-Parameter wie`max_replication_slots`, `max_logical_replication_workers` und optimieren. `max_worker_processes` Anweisungen zum Aktivieren der logischen Replikation und zum Optimieren dieser Parameter finden Sie unterthe section called “Einrichten der logischen Replikation”.

  Stellen Sie außerdem sicher, dass der `synchronous_commit` Parameter auf eingestellt iston.

  Nachdem Sie die erforderlichen Parameter konfiguriert haben, stellen Sie sicher, dass Sie den DB-Cluster neu starten, damit Ihre Änderungen wirksam werden. Blau/Grün-Bereitstellungen erfordern, dass die Writer-Instance mit der DB-Cluster-Parametergruppe synchronisiert ist, andernfalls schlägt die Erstellung fehl. Weitere Informationen finden Sie unter Neustarten einer DB-Instance in einem Aurora Cluster.
- Stellen Sie sicher, dass Ihr DB-Cluster eine Version von Aurora PostgreSQL ausführt, die mit Blau/Grün-Bereitstellungen kompatibel ist. Eine Tabelle mit kompatiblen Versionen finden Sie unter the section called “Blau/Grün-Bereitstellungen mit Aurora PostgreSQL”.
- Stellen Sie sicher, dass alle Tabellen im DB-Cluster einen Primärschlüssel haben. Die logische PostgreSQL-Replikation lässt keine UPDATE- oder DELETE-Operationen mit Tabellen zu, die keinen Primärschlüssel haben.
- Wenn Sie Trigger verwenden, stellen Sie sicher, dass sie das Erstellen, Aktualisieren und Löschen von, und `pg_catalog.pg_replication_slots` Objekten `pg_catalog.pg_publicationpg_catalog.pg_subscription`, deren Namen mit 'rds' beginnen, nicht beeinträchtigen.

Angeben von Änderungen bei der Erstellung einer Blau/Grün-Bereitstellung

Sie können die folgenden Änderungen an dem DB-Cluster in der grünen Umgebung vornehmen, wenn Sie die Blau/Grün-Bereitstellung erstellen:

Sie können nach der Bereitstellung weitere Änderungen am DB-Cluster und seinen DB-Instances in der grünen Umgebung vornehmen. Sie können beispielsweise Schemaänderungen an Ihrer Datenbank vornehmen.

Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Angeben einer höheren Engine-Version

Sie können eine höhere Engine-Version angeben, wenn Sie ein DB-Engine-Upgrade testen möchten. Bei der Umstellung wird die Datenbank auf die von Ihnen angegebene Haupt- oder Unterversion der DB-Engine aktualisiert.

Geben Sie eine andere DB-Parametergruppe an

Sie können eine andere DB-Cluster-Parametergruppe angeben, als vom DB-Cluster verwendet wird. Sie können testen, wie sich Parameteränderungen auf den DB-Cluster in der grünen Umgebung auswirken, oder im Falle eines Upgrades eine Parametergruppe für eine neue Hauptversion der DB-Engine angeben.

Wenn Sie eine andere DB-Cluster-Parametergruppe festlegen, wird die angegebene DB-Parametergruppe dem DB-Cluster in der grünen Umgebung zugeordnet. Wenn Sie eine andere DB-Cluster-Parametergruppe festlegen, wird der DB-Cluster in der grünen Umgebung derselben Parametergruppe zugeordnet wie der blaue DB-Cluster.

Erstellen einer Blau/Grün-Bereitstellung

Sie können mit der, der oder der AWS Management Console RDS-API eine blaue/grüne Bereitstellung erstellen. AWS CLI

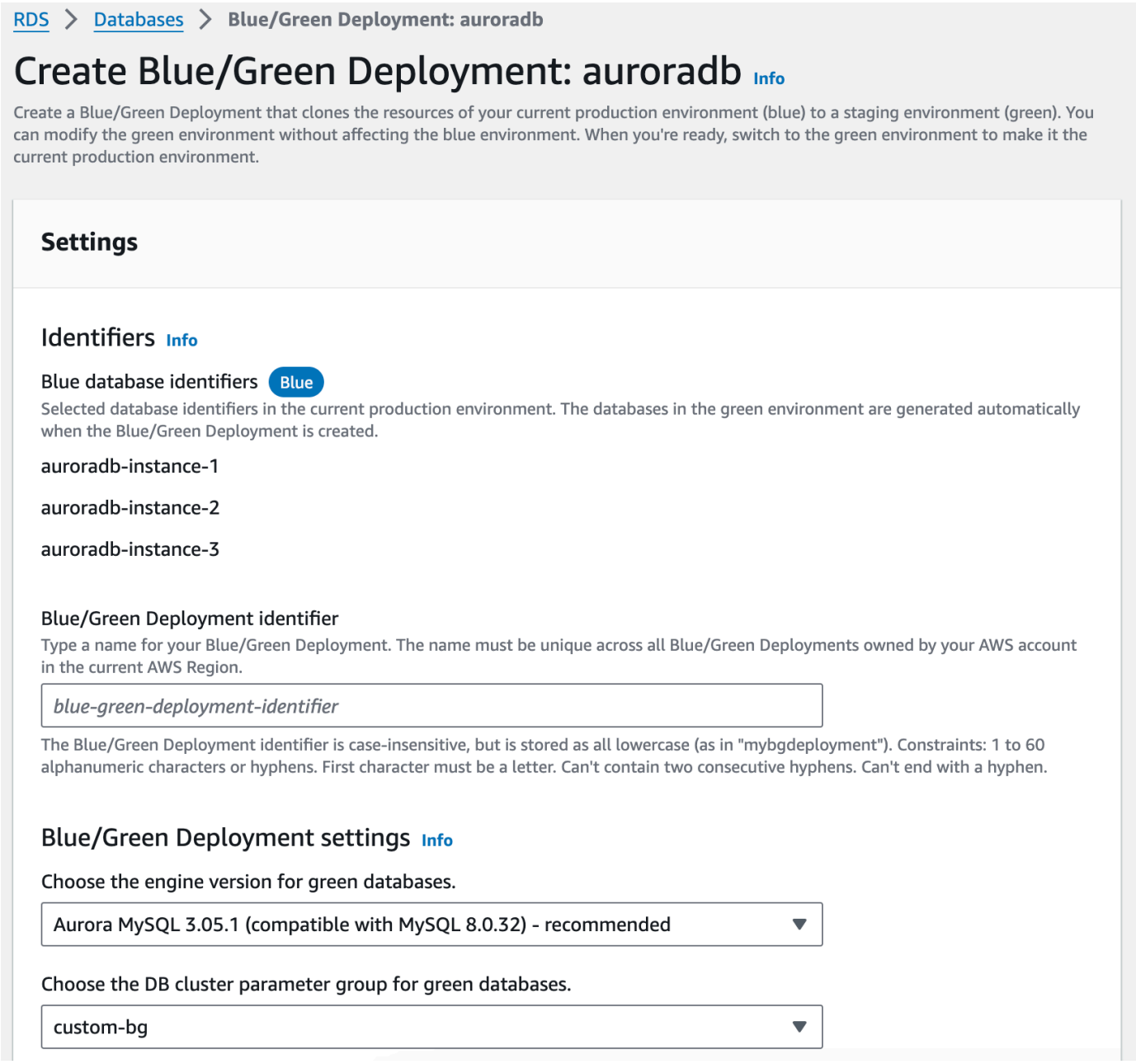
Konsole

So erstellen Sie eine Blau/Grün-Bereitstellung

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann den DB-Cluster zum Kopieren in eine grüne Umgebung aus.
3. Wählen Sie Actions, Create Blue/Green Deployment aus.

   Wenn Sie sich für einen Aurora-PostgreSQL-DB-Cluster entscheiden, überprüfen und bestätigen Sie die Einschränkungen der logischen Replikation. Weitere Informationen finden Sie unter the section called “Einschränkungen der logischen Replikation von PostgreSQL”.

Die Seite Create Blue/Green Deployment (Blau/Grün-Bereitstellung) wird angezeigt.



4. Überprüfen Sie die blauen Datenbankkennungen. Stellen Sie sicher, dass sie mit den DB-Instances übereinstimmen, die Sie in der blauen Umgebung erwarten. Wenn dies nicht der Fall ist, wählen Sie Cancel (Abbrechen) aus.
5. Geben Sie unter Blue/Green Deployment Identifier (Blau/Grün-Bereitstellungs-ID) einen Namen für Ihre Blau/Grün-Bereitstellung ein.

6. Geben Sie in den verbleibenden Abschnitten die Einstellungen für die grüne Umgebung an. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter the section called “Verfügbare Einstellungen”.

   Sie können nach der Bereitstellung weitere Änderungen an den Datenbanken in der grünen Umgebung vornehmen.

7. Wählen Sie Staging-Umgebung erstellen aus.

AWS CLI

Verwenden Sie den Befehl create-blue-green-deployment AWS CLI, um eine blaue/grüne Bereitstellung mit dem zu erstellen. Informationen zu den jeweiligen Optionen finden Sie unter the section called “Verfügbare Einstellungen”.

Example

Für LinuxmacOS, oderUnix:

```
aws rds create-blue-green-deployment \
    --blue-green-deployment-name aurora-blue-green-deployment \
    --source arn:aws:rds:us-east-2:123456789012:cluster:auroradb \
    --target-engine-version 8.0 \
    --target-db-cluster-parameter-group-name mydbclusterparametergroup
```

Windows:

```
aws rds create-blue-green-deployment ^
    --blue-green-deployment-name aurora-blue-green-deployment ^
    --source arn:aws:rds:us-east-2:123456789012:cluster:auroradb ^
    --target-engine-version 8.0 ^
    --target-db-cluster-parameter-group-name mydbclusterparametergroup
```

RDS-API

Verwenden Sie den `CreateBlueGreenDeployment`Vorgang, um mithilfe der Amazon RDS-API eine blaue/grüne Bereitstellung zu erstellen. Informationen zu den jeweiligen Optionen finden Sie unter the section called “Verfügbare Einstellungen”.

Einstellungen für die Erstellung von blauen/grünen Bereitstellungen

In der folgenden Tabelle werden die Einstellungen erläutert, die Sie wählen können, wenn Sie eine blaue/grüne Bereitstellung erstellen. Weitere Informationen zu den AWS CLI Optionen finden Sie unter create-blue-green-deployment. Weitere Informationen zu den RDS-API-Parametern finden Sie unter. CreateBlueGreenDeployment

Konsolene instellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter

Blaue/grüne Bereitstellungs-ID	Ein Name für die blaue/grüne Bereitstellung.	CLI-Option:
		`--blue-green-deployment-name`
		API-Parameter:
		`BlueGreenDeploymentName`

Blauer Datenbank bezeichner	Die ID des , den Sie in die grüne Umgebung kopieren möchten. Wenn Sie die CLI oder API verwenden, geben Sie den Amazon Resource Name (ARN) des an.	CLI-Option:
		`--source`
		API-Parameter:
		`Source`

DB-Cluster-Parametergruppe für grüne Datenbanken	Eine Parametergruppe, die den Datenbanken in der grünen Umgebung zugeordnet werden soll.	CLI-Option:
		`--target-db-cluster-parameter-group-name`
		API-Parameter:
		`TargetDBClusterParameterGroupName`

Konsolene instellung	Beschreibung der Einstellung	CLI-Option und RDS-API-Parameter

Engine-Version für grüne Datenbanken	Führen Sie ein Upgrade des in der grünen Umgebung auf die angegebene DB-Engine-Version durch.	CLI-Option:
		`--target-engine-version`
		RDS-API-Parameter:
		`TargetEngineVersion`

Anzeigen einer Blau/Grün-Bereitstellung

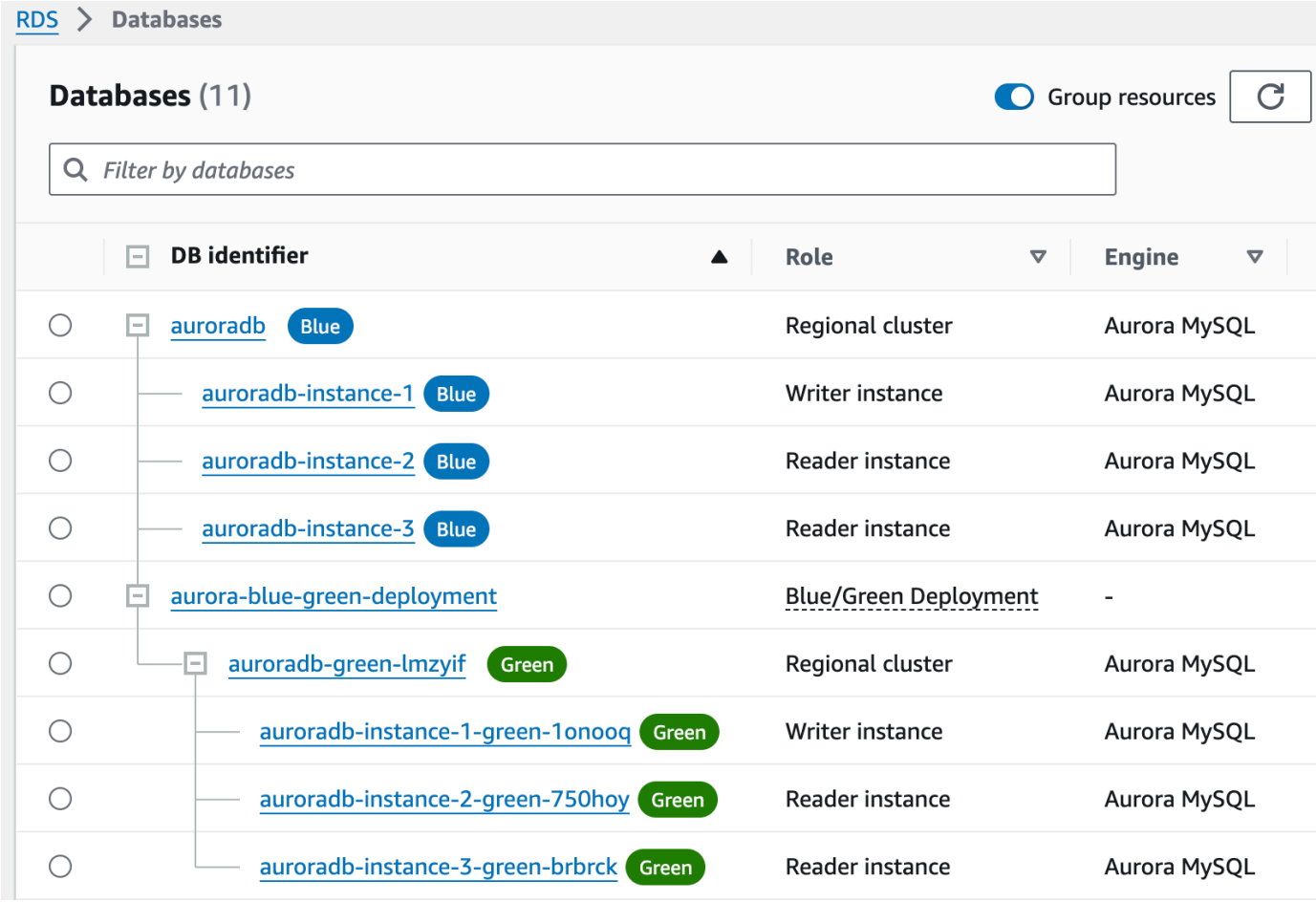
Sie können die Details einer Blau/Grün-Bereitstellung mithilfe der AWS Management Console, der AWS CLI oder der RDS-API anzeigen.

Außerdem können Sie Ereignisse anzeigen und abonnieren, um Informationen über eine Blau/Grün-Bereitstellung zu erhalten. Weitere Informationen finden Sie unter Blau/Grün-Bereitstellungsereignisse.

Konsole

So zeigen Sie Details über eine Blau/Grün-Bereitstellung an

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus und suchen Sie dann in der Liste nach der Blau/Grün-Bereitstellung.

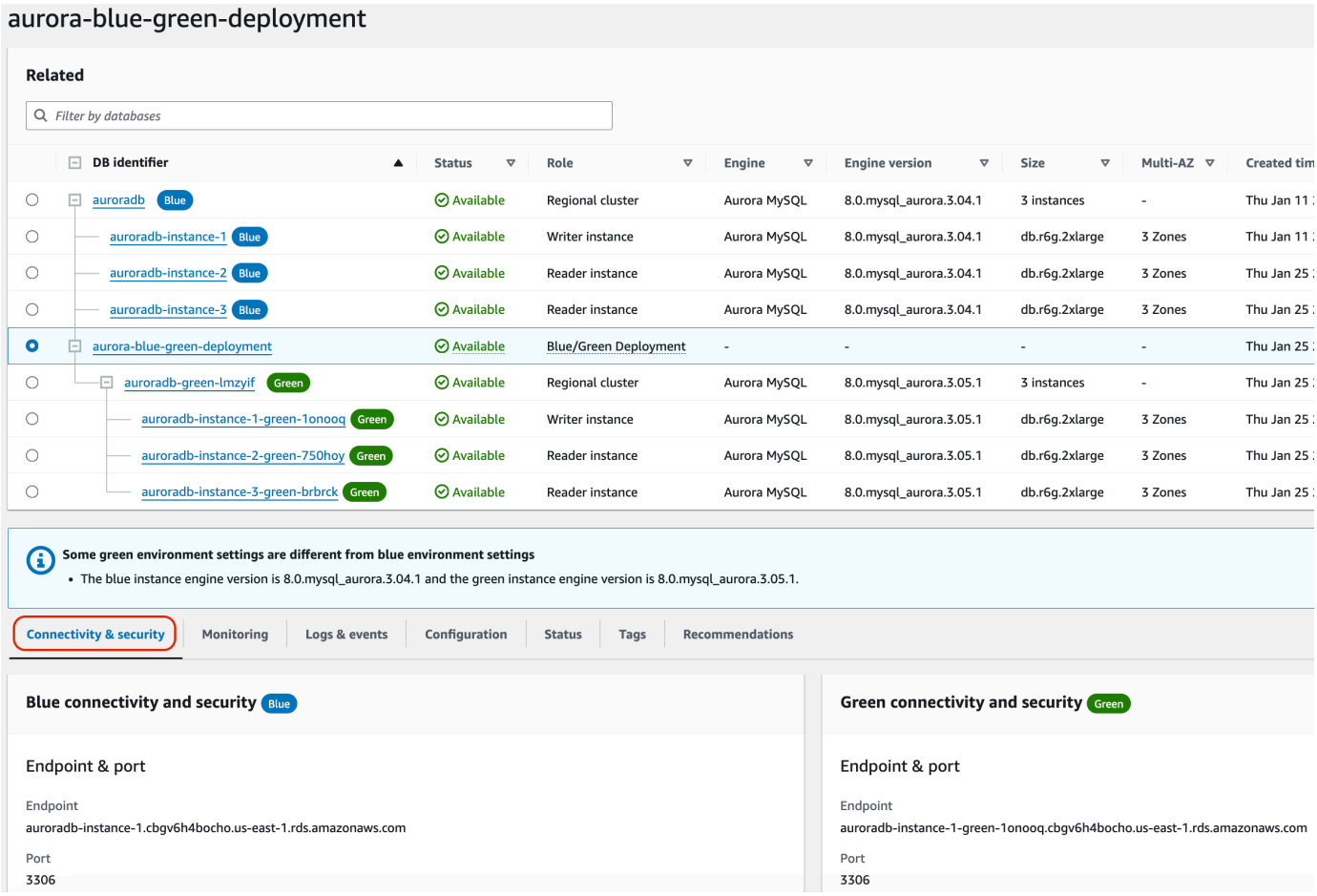


Der Wert Role (Rolle) für die Blau/Grün-Bereitstellung ist Blue/Green Deployment (Blau/Grün-Bereitstellung).

3. Wählen Sie den Namen der Blau/Grün-Bereitstellung aus, die Sie anzeigen möchten, um die Details anzeigen zu lassen.

   Jede Registerkarte verfügt über einen Abschnitt für die blaue und einen Abschnitt für die grüne Bereitstellung. Auf der Registerkarte Konfiguration kann sich die DB-Engine-Version beispielsweise in der blauen und in der grünen Umgebung unterscheiden, wenn Sie die DB-Engine-Version in der grünen Umgebung aktualisieren.

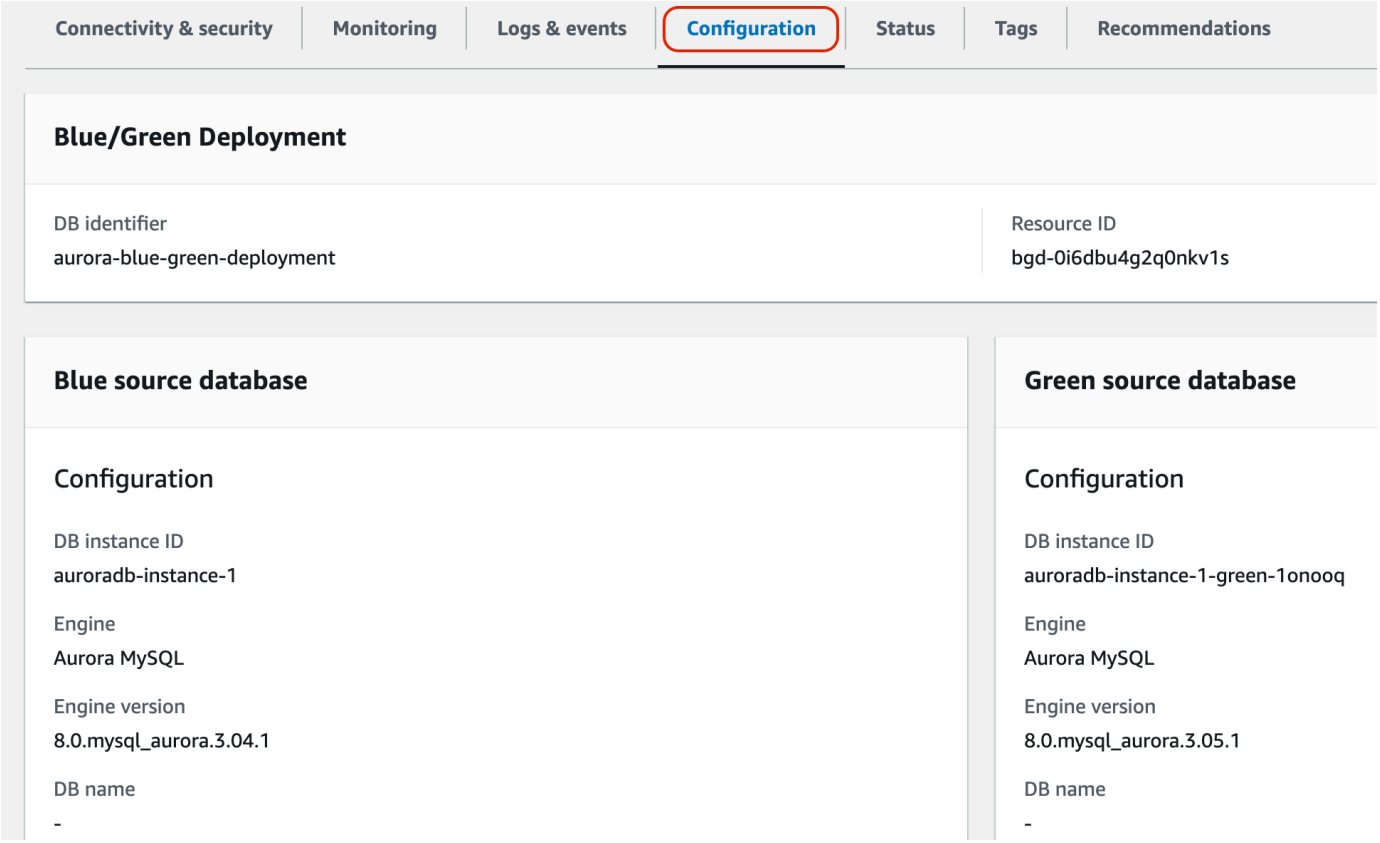
   Die folgende Abbildung zeigt ein Beispiel für die Registerkarte Konnektivität und Sicherheit:



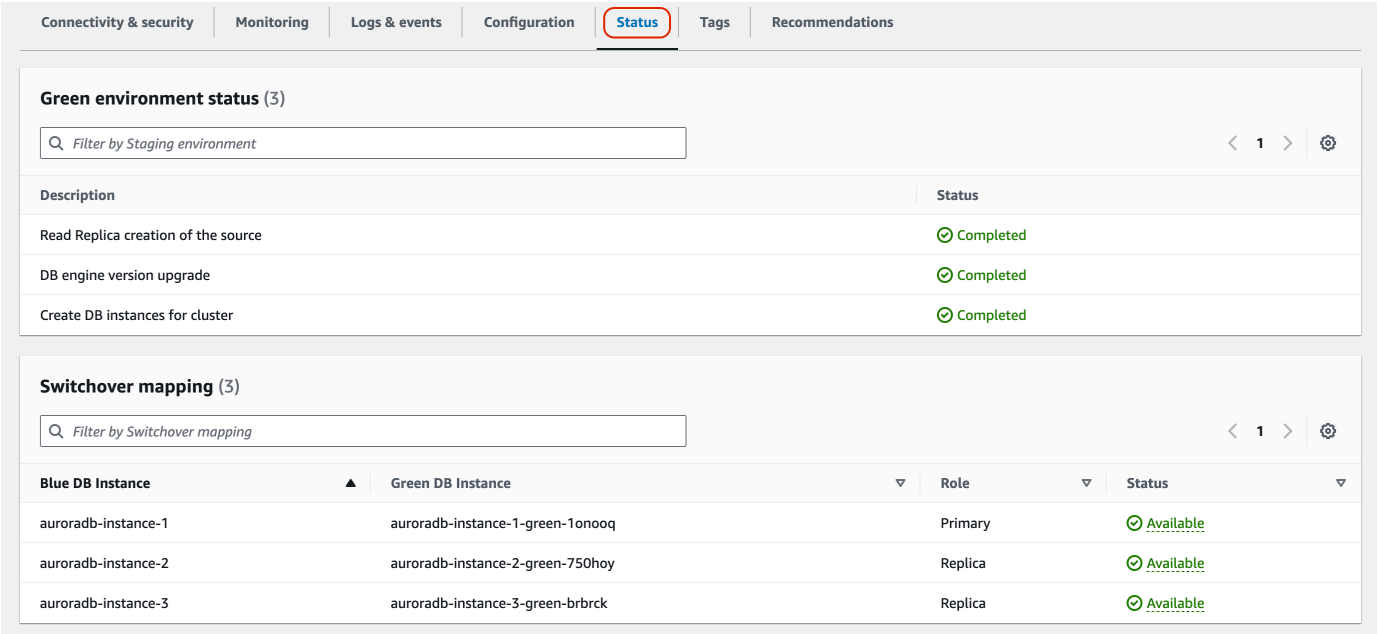
Die Registerkarte Konnektivität und Sicherheit enthält auch den Abschnitt Replikation, in dem der aktuelle Status der logischen Replikation und die Replikatverzögerung zwischen den blauen und grünen Umgebungen angezeigt werden. Wenn der Replikationsstatus `Replicating` lautet, wird die Blau/Grün-Bereitstellung erfolgreich repliziert.

Bei Blau/Grün-Bereitstellungen von Aurora PostgreSQL kann sich der Replikationsstatus in `Replication degraded` ändern, wenn Sie in der blauen Umgebung nicht unterstützte DDL-Änderungen vornehmen oder große Objekte ändern. Weitere Informationen finden Sie unter the section called “Einschränkungen der logischen Replikation von PostgreSQL”.

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte Konfiguration:



Die folgende Abbildung zeigt ein Beispiel für die Registerkarte Status:



AWS CLI

Um die Details zu einer Blau/Grün-Bereitstellung mithilfe der anzuzeigenAWS CLI, verwenden Sie den describe-blue-green-deployments Befehl .

Example Anzeigen der Details einer Blau/Grün-Bereitstellung durch Filtern nach ihrem Namen

Wenn Sie den describe-blue-green-deployments Befehl verwenden, können Sie nach der filtern`--blue-green-deployment-name`. Das folgende Beispiel zeigt die Details für eine Blau/Grün-Bereitstellung mit dem Namen *`my-blue-green-deployment`*.

```
aws rds describe-blue-green-deployments --filters Name=blue-green-deployment-
name,Values=my-blue-green-deployment
```

Example Anzeigen der Details einer Blau/Grün-Bereitstellung durch Angabe der entsprechenden ID

Wenn Sie den describe-blue-green-deployments Befehl verwenden, können Sie die angeben`--blue-green-deployment-identifier`. Das folgende Beispiel zeigt die Details für eine Blau/Grün-Bereitstellung mit der ID *`bgd-1234567890abcdef`*.

```
aws rds describe-blue-green-deployments --blue-green-deployment-
identifier bgd-1234567890abcdef
```

RDS-API

Wenn Sie die Details einer Blau/Grün-Bereitstellung mithilfe der Amazon-RDS-API anzeigen möchten, verwenden Sie den `DescribeBlueGreenDeployments`-Vorgang und geben Sie `BlueGreenDeploymentIdentifier` an.

Umstellen einer Blau/Grün-Bereitstellung

Bei einer Umstellung wird der DB-Cluster einschließlich seiner DB-Instances in der grünen Umgebung zum Produktions-DB-Cluster hochgestuft. Vor der Umstellung wird der Produktionsdatenverkehr an den Cluster in der blauen Umgebung weitergeleitet. Nach der Umstellung wird der Produktionsdatenverkehr an den DB-Cluster in der grünen Umgebung weitergeleitet.

Themen

Umstellungs-Timeout

Sie können einen Umstellungs-Timeout zwischen 30 Sekunden und 3 600 Sekunden (eine Stunde) festlegen. Wenn die Umstellung länger als angegeben dauert, werden alle Änderungen rückgängig gemacht und es werden keine Änderungen an einer der Umgebungen vorgenommen. Der Standardwert für den Timeout beträgt 300 Sekunden (fünf Minuten).

Integrationsschutz der Umstellung

Wenn Sie eine Umstellung starten, führt Amazon RDS einige grundlegende Prüfungen durch, um zu testen, ob die blaue und die grüne Umgebung für die Umstellung bereit sind. Diese Prüfungen werden als Integrationsschutz der Umstellung. Dieser Integrationsschutz verhindert eine Umstellung, wenn die Umgebungen dafür nicht bereit sind. Mit diesem Schutz werden längere Ausfallzeiten als erwartet vermieden und Datenverluste zwischen der blauen und der grünen Umgebung verhindern, die sich ergeben könnten, wenn die Umstellung gestartet wird.

Amazon RDS führt die folgenden Integrationsschutzprüfungen in der grünen Umgebung durch:

- Zustand der Replikation – Es wird geprüft, ob der Replikationsstatus des grünen DB-Clusters fehlerfrei ist. Der grüne DB-Cluster ist ein Replikat des blauen DB-Clusters.
- Replikationsverzögerung – Es wird geprüft, ob die Replikatverzögerung des grünen DB-Clusters innerhalb der für die Umstellung zulässigen Grenzwerte liegt. Die zulässigen Grenzwerte basieren auf dem angegebenen Timeout-Zeitraum. Die Replikatverzögerung gibt an, wie weit der grüne DB-Cluster hinter seinem blauen DB-Cluster zurückbleibt. Weitere Informationen finden Sie unter the section called “Diagnose und Lösung bei Verzögerungen zwischen Read Replicas (Lesereplikaten)” für Aurora MySQL und the section called “Überwachung einer -Replikation” für Aurora PostgreSQL.

- Aktive Schreibvorgänge – Es wird sichergestellt, dass es auf dem grünen DB-Cluster keine aktiven Schreibvorgänge gibt.

Amazon RDS führt die folgenden Integrationsschutzprüfungen in der blauen Umgebung durch:

- Externe Replikation — Stellt für Aurora PostgreSQL sicher, dass es sich bei der blauen Umgebung nicht um eine selbstverwaltete logische Quelle (Herausgeber) oder Replikat (Abonnent) handelt. Ist dies der Fall, empfehlen wir, die selbstverwalteten Replikations-Slots und Abonnements für alle Datenbanken in der blauen Umgebung zu löschen, mit dem Switchover fortzufahren und sie dann neu zu erstellen, um die Replikation fortzusetzen. Prüft für Aurora MySQL , ob es sich bei der Blue-Datenbank nicht um ein externes Binlog-Replikat handelt. Ist dies der Fall, stellen Sie sicher, dass sie nicht aktiv repliziert wird.
- Lang andauernde aktive Schreibvorgänge – Es wird sichergestellt, dass auf dem blauen DB-Cluster keine lang andauernden aktiven Schreibvorgänge vorhanden sind, da diese die Replikatverzögerung erhöhen können.
- Lang andauernde DDL-Anweisungen – Es wird sichergestellt, dass auf dem blauen DB-Cluster keine lang andauernden DDL-Anweisungen vorhanden sind, da diese die Replikatverzögerung erhöhen können.
- Nicht unterstützte PostgreSQL-Änderungen – Für DB-Cluster von Aurora PostgreSQL wird sichergestellt, dass in der blauen Umgebung keine DDL-Änderungen und keine Hinzufügungen oder Änderungen großer Objekte vorgenommen wurden. Weitere Informationen finden Sie unter the section called “Einschränkungen der logischen Replikation von PostgreSQL”.

  Wenn Amazon RDS nicht unterstützte PostgreSQL-Änderungen erkennt, wird der Replikationsstatus in `Replication degraded` geändert und Sie werden darüber informiert, dass eine Umstellung für die Blau/Grün-Bereitstellung nicht verfügbar ist. Um mit der Umstellung fortzufahren, empfehlen wir Ihnen, die Blau/Grün-Bereitstellung und alle grünen Datenbanken zu löschen und neu zu erstellen. Wählen Sie dazu Aktionen, Mit grünen Datenbanken löschen aus.

Umstellungsaktionen

Wenn Sie auf eine Blau/Grün-Bereitstellung umstellen, führt RDS die folgenden Aktionen aus:

1. Es führt Integritätsschutzprüfungen durch, um zu überprüfen, ob die blaue und die grüne Umgebung bereit für die Umstellung sind.
2. Es stoppt neue Schreibvorgänge auf dem DB-Cluster in beiden Umgebungen.

3. Es trennt Verbindungen mit den DB-Instances in beiden Umgebungen und erlaubt keine neuen Verbindungen.
4. Es wartet, bis die Replikation in der grünen Umgebung aufgeholt hat, sodass die grüne Umgebung mit der blauen Umgebung synchron ist.
5. Es benennt den DB-Cluster und die DB-Instances in beiden Umgebungen um.

   RDS benennt den DB-Cluster und die DB-Instances in der grünen Umgebung um, sodass sie dem jeweiligen DB-Cluster und den DB-Instances in der blauen Umgebung entsprechen. Angenommen, der Name einer DB-Instance in der blauen Umgebung lautet `mydb`. Nehmen wir außerdem an, dass der Name der entsprechenden DB-Instance in der grünen Umgebung `mydb-green-abc123` lautet. Während der Umstellung wird der Name der DB-Instance in der grünen Umgebung in `mydb` geändert.

   RDS benennt den DB-Cluster und die DB-Instances in der blauen Umgebung um, indem `-old`*n* an den aktuellen Namen angehängt wird, wobei *n* eine Zahl ist. Angenommen, der Name einer DB-Instance in der blauen Umgebung lautet `mydb`. Nach der Umstellung könnte der Name der DB-Instance `mydb-old1` lauten.

   RDS benennt auch die Endpunkte in der grünen Umgebung um, sodass sie mit den entsprechenden Endpunkten in der blauen Umgebung übereinstimmen und keine Anwendungsänderungen erforderlich sind.
6. Erlaubt Verbindungen mit Datenbanken in beiden Umgebungen.
7. Erlaubt neue Schreibvorgänge auf dem DB-Cluster in der neuen Produktionsumgebung.

   Nach dem Switchover erlaubt der DB-Cluster der vorherigen nur Lesevorgänge, . Selbst wenn Sie den `read_only` Parameter auf dem DB-Cluster deaktivieren, bleibt er schreibgeschützt, bis Sie die blaue/grüne Bereitstellung löschen.

Sie können den Status eines Switchovers mit Amazon EventBridge überwachen. Weitere Informationen finden Sie unter the section called “Blau/Grün-Bereitstellungsereignisse”.

Wenn Sie in der blauen Umgebung Tags konfiguriert haben, werden diese Tags während der Umstellung in die neue Produktionsumgebung verschoben. Die vorherige Produktionsumgebung behält diese Tags ebenfalls bei. Weitere Informationen zu Tags erhalten Sie unter Markieren von Amazon RDS-Ressourcen.

Wenn die Umstellung startet und aus irgendeinem Grund vorzeitig beendet wird, werden alle Änderungen rückgängig gemacht und es werden keine Änderungen an einer der Umgebungen vorgenommen.

Bewährte Methoden für die Umstellung

Wir empfehlen Ihnen dringend, sich an bewährte Methoden zu halten und vor der Umstellung die folgenden Aufgaben auszuführen:

- Testen Sie die Ressourcen in der grünen Umgebung gründlich. Stellen Sie sicher, dass sie ordnungsgemäß und effizient funktionieren.
- Überwachen Sie relevante CloudWatch Amazon-Metriken. Weitere Informationen finden Sie unter the section called “Überprüfung der CloudWatch Metriken vor dem Switchover”.
- Ermitteln Sie den besten Zeitpunkt für die Umstellung.

  Während der Umstellung werden Schreibvorgänge in beiden Umgebungen von den Datenbanken abgeschnitten. Ermitteln Sie einen Zeitpunkt, an dem der Datenverkehr in Ihrer Produktionsumgebung am niedrigsten ist. Lang andauernde Transaktionen, wie z. B. aktive DDLs, können die Dauer Ihrer Umstellung verlängern, was zu längeren Ausfallzeiten für Ihre Produktions-Workloads führt.

  Wenn Ihre DB-Cluster und DB-Instances über eine große Anzahl von Verbindungen verfügen, sollten Sie erwägen, diese manuell auf die für Ihre Anwendung erforderliche Mindestmenge zu reduzieren, bevor Sie auf die Blau/Grün-Bereitstellung umstellen. Dazu können Sie beispielsweise ein Skript erstellen, das den Status der Blau/Grün-Bereitstellung überwacht und mit der Bereinigung von Verbindungen beginnt, wenn es feststellt, dass sich der Status in `SWITCHOVER_IN_PROGRESS` geändert hat.
- Stellen Sie sicher, dass der DB-Cluster und die DB-Instances in beiden Umgebungen den Status `Available` aufweisen.
- Stellen Sie sicher, dass der DB-Cluster in der grünen Umgebung fehlerfrei ist und repliziert wird.
- Stellen Sie sicher, dass Ihre Netzwerk- und Client-Konfigurationen die Time To Live (TTL) des DNS-Caches nicht mehr als fünf Sekunden erhöhen, was die Standardeinstellung für DNS-Zonen von Aurora ist.
  Andernfalls senden Anwendungen nach der Umstellung weiterhin Schreibdatenverkehr an die blaue Umgebung.
- Gehen Sie für Aurora PostgreSQL-DB-Cluster wie folgt vor:

- Überprüfen Sie die Einschränkungen der logischen Replikation und ergreifen Sie vor dem Switchover alle erforderlichen Maßnahmen. Weitere Informationen finden Sie unter the section called “Einschränkungen der logischen Replikation von PostgreSQL”.
- Führen Sie die `ANALYZE`-Operation aus, um die Tabelle `pg_statistics` zu aktualisieren. Dadurch wird das Risiko von Leistungsproblemen nach dem Switchover reduziert.

> **Note**
>
> Während einer Umstellung können Sie keinen der DB-Cluster in der Umstellung ändern.

Überprüfung der CloudWatch Metriken vor dem Switchover

Bevor Sie zu einer blauen/grünen Bereitstellung wechseln, empfehlen wir Ihnen, die Werte der folgenden Kennzahlen bei Amazon CloudWatch zu überprüfen.

- `DatabaseConnections` – Verwenden Sie diese Metrik, um das Aktivitätsniveau in der Blau/Grün-Bereitstellung abzuschätzen, und stellen Sie sicher, dass der Wert für Ihre Bereitstellung auf einem akzeptablen Niveau liegt, bevor Sie umsteigen. Wenn Performance Insights aktiviert ist, ist `DBLoad` eine genauere Metrik.
- `ActiveTransactions` – Wenn `innodb_monitor_enable` in der DB-Parametergruppe für eine Ihrer DB-Instances auf `all` gesetzt ist, verwenden Sie diese Metrik, um festzustellen, ob es eine hohe Anzahl aktiver Transaktionen gibt, die die Umstellung blockieren könnten.

Weitere Informationen zu diesen Metriken finden Sie unter the section called “CloudWatch Metriken für Aurora”.

Überwachung der Replikatverzögerung vor dem Switchover

Bevor Sie zu einer blauen/grünen Bereitstellung wechseln, stellen Sie sicher, dass die Replikatverzögerung in der grünen Datenbank nahezu Null ist, um Ausfallzeiten zu reduzieren.

- Verwenden Sie für Aurora MySQL die `AuroraBinlogReplicaLag` CloudWatch Metrik, um die aktuelle Replikationsverzögerung in der grünen Umgebung zu identifizieren.
- Verwenden Sie für Aurora PostgreSQL die folgende SQL-Abfrage:

```
SELECT slot_name,
```

```
       confirmed_flush_lsn as flushed,
       pg_current_wal_lsn(),
       (pg_current_wal_lsn() - confirmed_flush_lsn) AS lsn_distance
FROM pg_catalog.pg_replication_slots
WHERE slot_type = 'logical';

slot_name        |    flushed    | pg_current_wal_lsn | lsn_distance
-----------------+---------------+--------------------+------------
logical_replica1 | 47D97/CF32980 | 47D97/CF3BAC8      | 37192
```

Die `confirmed_flush_lsn` steht für die letzte Log-Sequenznummer (LSN), die an das Replikat gesendet wurde. Die `pg_current_wal_lsn` stellt dar, wo sich die Datenbank jetzt befindet. Ein `lsn_distance` Wert von 0 bedeutet, dass das Replikat abgeholt wurde.

Umstellen einer Blau/Grün-Bereitstellung

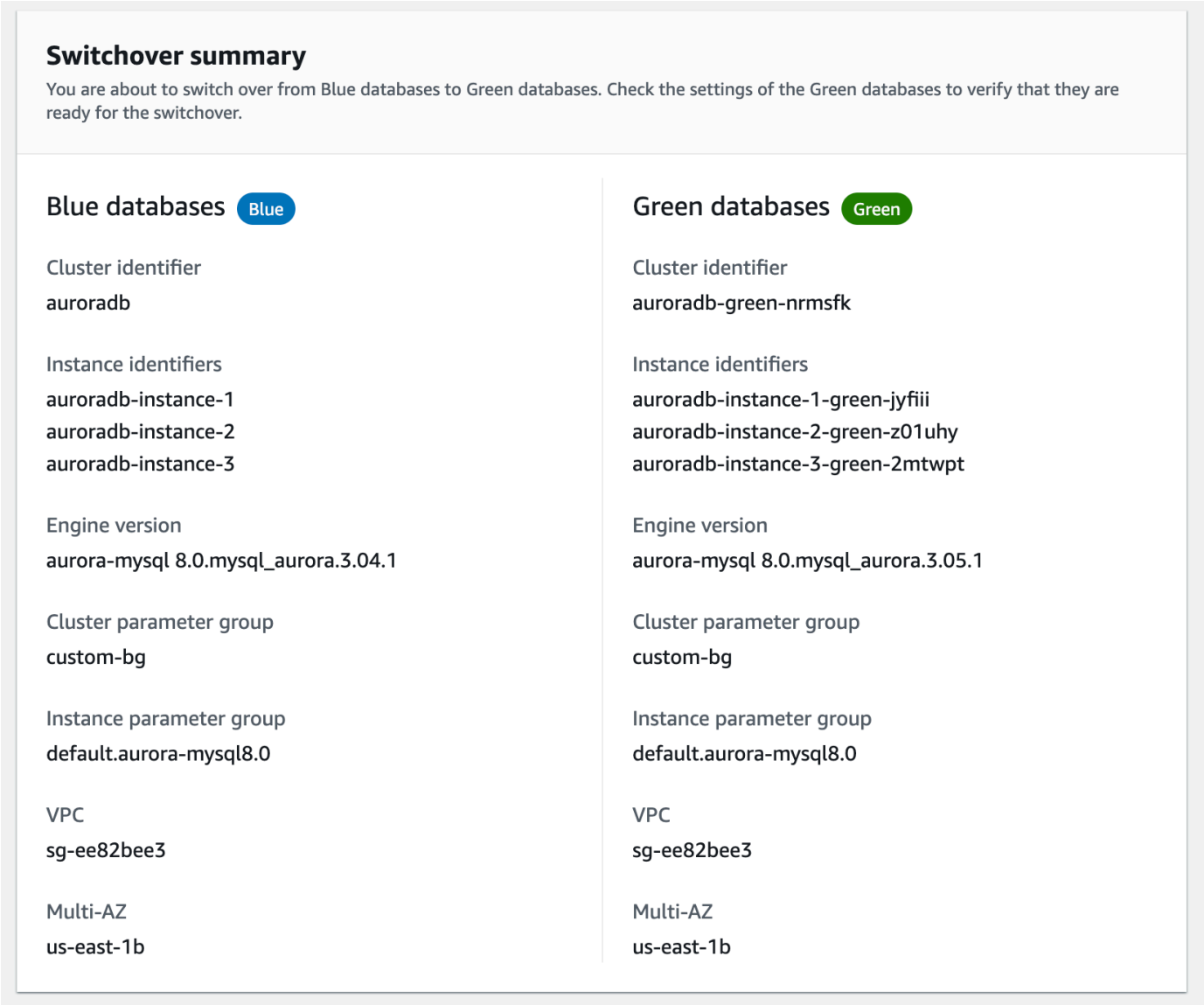
Sie können mit der, der oder der AWS Management Console RDS-API zu einer AWS CLI blauen/grünen Bereitstellung wechseln.

Konsole

So stellen Sie eine Blau/Grün-Bereitstellung um

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die Blau/Grün-Bereitstellung aus, die Sie umstellen möchten.
3. Wählen Sie unter Actions (Aktionen) die Option Switch over (Umstellen) aus.

   Die Seite Switch Over (Umstellen) wird angezeigt.



4. Sehen Sie sich auf der Seite Switchover (Umstellen) die Umstellungszusammenfassung an. Stellen Sie sicher, dass die Ressourcen in beiden Umgebungen Ihren Erwartungen entsprechen. Wenn dies nicht der Fall ist, wählen Sie Cancel (Abbrechen) aus.
5. Geben Sie unter Timeout-Einstellungen das Zeitlimit für die Umstellung ein.
6. Wenn auf Ihrem Cluster Aurora PostgreSQL ausgeführt wird, überprüfen und bestätigen Sie die vor der Umstellung zu berücksichtigenden Empfehlungen. Weitere Informationen finden Sie unter the section called “Einschränkungen der logischen Replikation von PostgreSQL”.
7. Wählen Sie Switch over (Umstellen) aus.

AWS CLI

Verwenden Sie den Befehl switchover-blue-green-deployment mit den folgenden Optionen AWS CLI, um eine blaue/grüne Bereitstellung mithilfe von umzuschalten:

- `--blue-green-deployment-identifier`— Geben Sie die Ressourcen-ID der blauen/grünen Bereitstellung an.
- `--switchover-timeout` – Geben Sie das Zeitlimit für die Umstellung in Sekunden an. Der Standardwert ist 300.

Example Umstellen einer Blau/Grün-Bereitstellung

Für LinuxmacOS, oderUnix:

```
aws rds switchover-blue-green-deployment \
    --blue-green-deployment-identifier bgd-1234567890abcdef \
    --switchover-timeout 600
```

Windows:

```
aws rds switchover-blue-green-deployment ^
    --blue-green-deployment-identifier bgd-1234567890abcdef ^
    --switchover-timeout 600
```

RDS-API

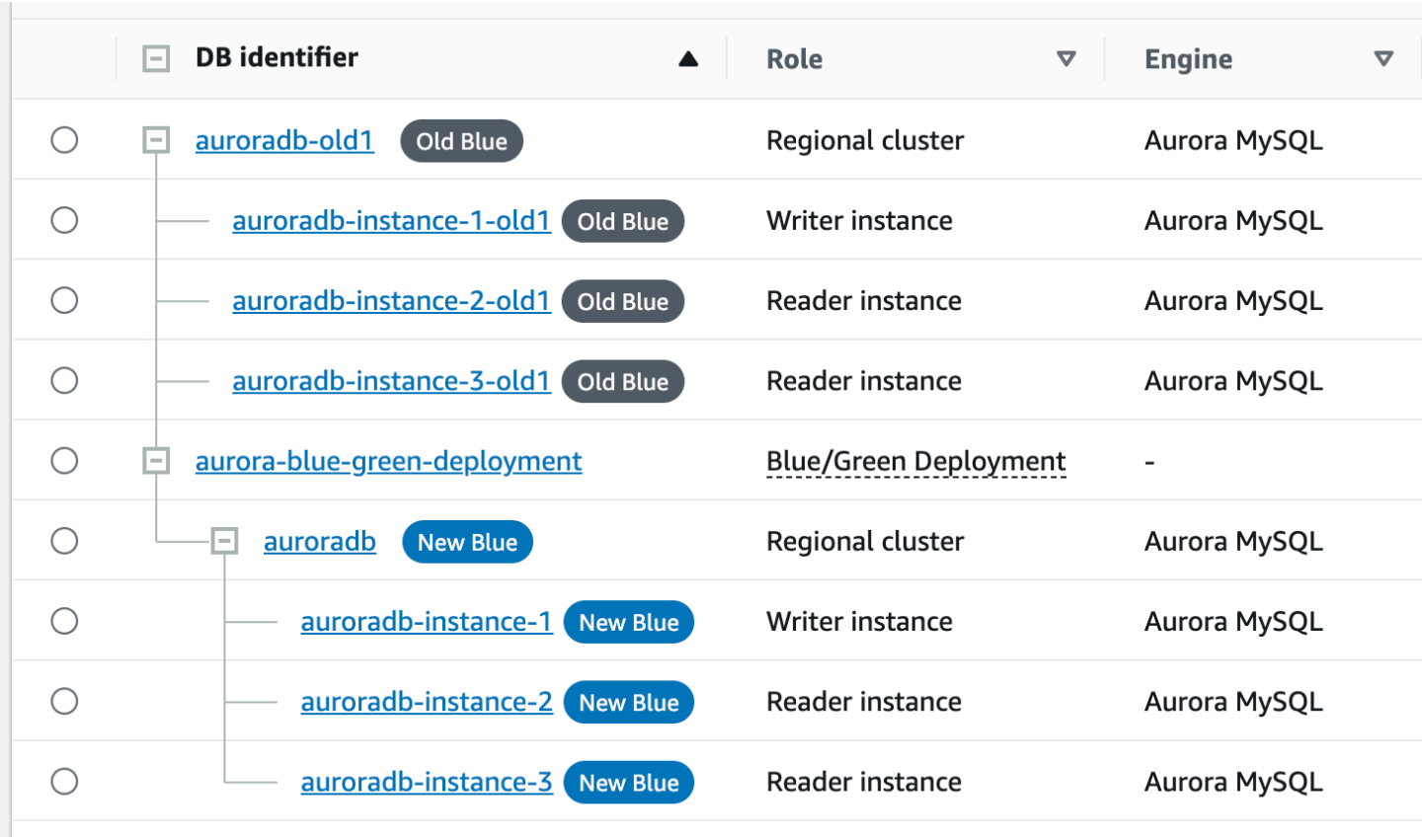
Verwenden Sie die `SwitchoverBlueGreenDeployment`-Operation mit den folgenden Parametern, um mithilfe der Amazon-RDS-API eine Blau/Grün-Bereitstellung umzustellen:

- `BlueGreenDeploymentIdentifier`— Geben Sie die Ressourcen-ID der blauen/grünen Bereitstellung an.
- `SwitchoverTimeout` – Geben Sie das Zeitlimit für die Umstellung in Sekunden an. Der Standardwert ist 300.

Nach der Umstellung

Nach einer Umstellung werden der DB-Cluster und die DB-Instances in der vorherigen blauen Umgebung beibehalten. Für diese Ressourcen fallen die Standardkosten an. Die Replikation und die binäre Protokollierung zwischen der blauen und der grünen Umgebung werden gestoppt.

RDS benennt den DB-Cluster und die DB-Instances in der blauen Umgebung um, indem `-old`*n* an den aktuellen Namen angehängt wird, wobei *n* eine Zahl ist. Der DB-Cluster wird in einen schreibgeschützten Zustand versetzt. Selbst wenn Sie den `read_only` Parameter auf dem DB-Cluster deaktivieren, bleibt er schreibgeschützt, bis Sie die blaue/grüne Bereitstellung löschen.



Aktualisierung des übergeordneten Knotens für Verbraucher

Wenn Sie eine blaue/grüne Bereitstellung von umgestellt haben und der blaue vor dem Switchover externe Replikate oder Binärprotokollverbraucher hatte, müssen Sie deren übergeordneten Knoten nach dem Switchover aktualisieren, um die Kontinuität der Replikation aufrechtzuerhalten.

Nach dem Switchover gibt die Writer-DB-Instance, die sich zuvor in der grünen Umgebung befand, ein Ereignis aus, das den Namen der Master-Log-Datei und die Master-Log-Position enthält. Beispielsweise:

```
aws rds describe-events --output json --source-type db-instance --source-identifier db-instance-identifier

{
    "Events": [
...
```

```
        {
            "SourceIdentifier": "db-instance-identifier",
            "SourceType": "db-instance",
            "Message": "Binary log coordinates in green environment after switchover:
             file mysql-bin-changelog.000003 and position 804",
            "EventCategories": [],
            "Date": "2023-11-10T01:33:41.911Z",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:db-instance-identifier"
        }
    ]
}
```

Stellen Sie zunächst sicher, dass der Verbraucher oder das Replikat alle Binärprotokolle aus der alten blauen Umgebung übernommen hat. Verwenden Sie dann die bereitgestellten Binärprotokollkoordinaten, um die Anwendung auf den Verbrauchern fortzusetzen. Wenn Sie beispielsweise eine MySQL-Replik auf EC2 ausführen, können Sie den `CHANGE MASTER TO` folgenden Befehl verwenden:

```
CHANGE MASTER TO MASTER_HOST='{new-writer-endpoint}', MASTER_LOG_FILE='mysql-bin-
changelog.000003', MASTER_LOG_POS=804;
```

Löschen einer Blau/Grün-Bereitstellung

Sie können eine Blau/Grün-Bereitstellung vor oder nach der Umstellung löschen.

Wenn Sie eine Blau/Grün-Bereitstellung löschen, bevor Sie sie umstellen, löscht Amazon RDS optional die/den Cluster in der Grün-Umgebung:

- Wenn Sie den DB-Cluster in der grünen Umgebung (`--delete-target`) löschen möchten, stellen Sie sicher, dass sein Löschschutz nicht aktiviert ist.
- Wenn Sie die/den DB- Cluster in der Grün-Umgebung (`--no-delete-target`) nicht löschen, werden/wird der Cluster beibehalten, er sind/ist jedoch nicht länger Teil einer Blau-/Grün-Bereitstellung. Die Replikation zwischen den Umgebungen wird fortgesetzt.

Die Option zum Löschen der grünen Datenbanken ist in der Konsole nach der Umstellung nicht verfügbar. Wenn Sie blaue/grüne Bereitstellungen mit dem löschen AWS CLI, können Sie die `--delete-target` Option nicht angeben, wenn der Bereitstellungsstatus lautet. `SWITCHOVER_COMPLETED`

> **Important**
>
> Das Löschen einer Blau/Grün-Bereitstellung wirkt sich nicht auf die blaue Umgebung aus.

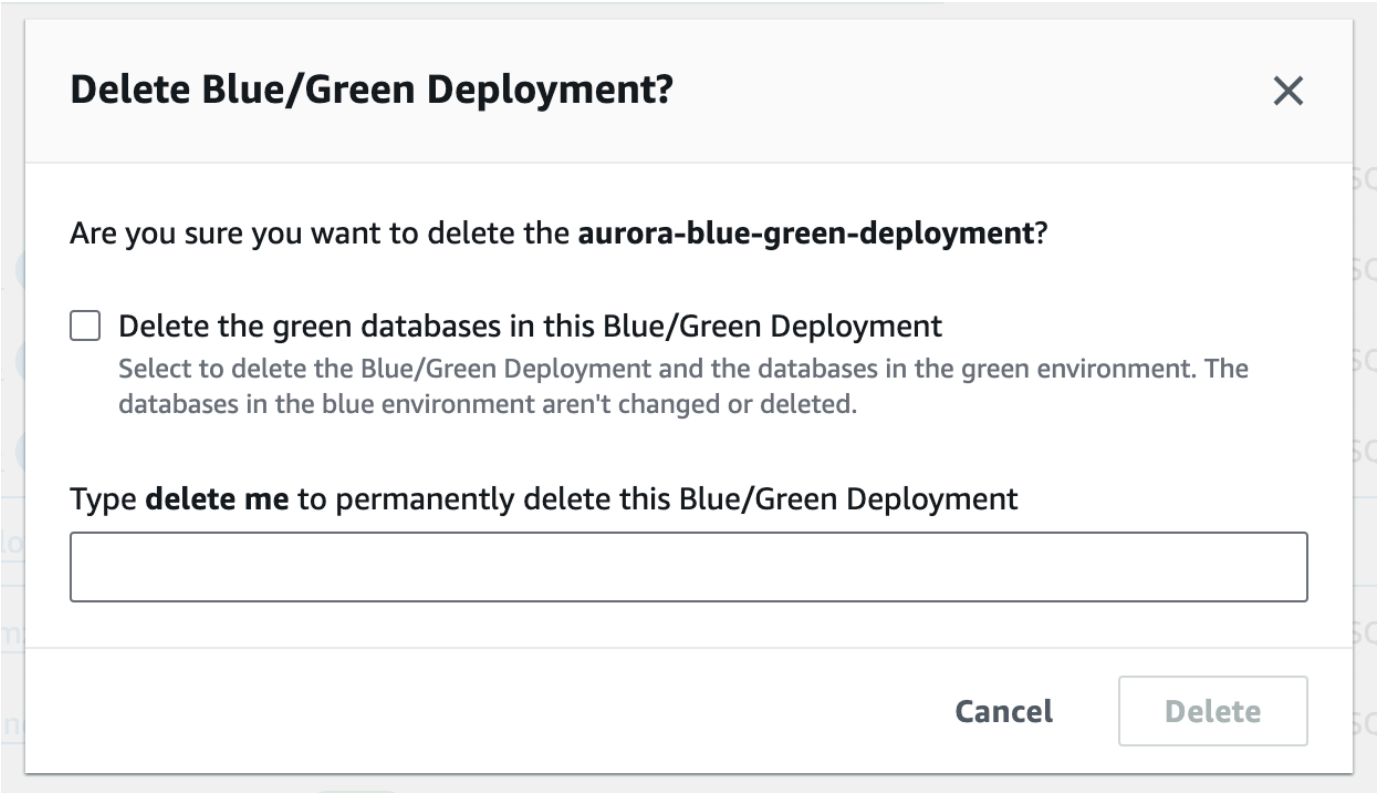
Sie können eine blaue/grüne Bereitstellung mithilfe der AWS Management Console, der oder der AWS CLI RDS-API löschen.

Konsole

So löschen Sie eine Blau/Grün-Bereitstellung

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die Blau/Grün-Bereitstellung aus, die Sie löschen möchten.
3. Klicken Sie bei Actions auf Delete.

   Das Fenster Delete Blue/Green Deployment? (Blau/Grün-Bereitstellung löschen?) wird angezeigt.



Um die grünen Datenbanken zu löschen, wählen Sie Delete the green databases in this Blue/Green Deployment (Die grünen Datenbanken in dieser Blau/Grün-Bereitstellung löschen) aus.

4. Geben Sie **`delete me`** in das Feld ein.
5. Wählen Sie Löschen aus.

AWS CLI

Um eine blaue/grüne Bereitstellung mithilfe von zu löschen AWS CLI, verwenden Sie den delete-blue-green-deploymentBefehl mit den folgenden Optionen:

- `--blue-green-deployment-identifier`— Die Ressourcen-ID der blauen/grünen Bereitstellung, die gelöscht werden soll.
- `--delete-target` – Gibt an, dass der DB-Cluster in der grünen Umgebung gelöscht wird. Sie können diese Option nicht angeben, wenn die Blau/Grün-Bereitstellung den Status `SWITCHOVER_COMPLETED` hat.
- `--no-delete-target` – Gibt an, dass der DB-Cluster in der grünen Umgebung beibehalten wird.

Example Löschen einer Blau/Grün-Bereitstellung und des DB-Clusters in der grünen Umgebung

Für LinuxmacOS, oderUnix:

```
aws rds delete-blue-green-deployment \
    --blue-green-deployment-identifier bgd-1234567890abcdef \
    --delete-target
```

Windows:

```
aws rds delete-blue-green-deployment ^
    --blue-green-deployment-identifier bgd-1234567890abcdef ^
    --delete-target
```

Example Löschen einer Blau/Grün-Bereitstellung unter Beibehaltung des DB-Clusters in der grünen Umgebung

Für LinuxmacOS, oderUnix:

```
aws rds delete-blue-green-deployment \
```

```
    --blue-green-deployment-identifier bgd-1234567890abcdef \
    --no-delete-target
```

Windows:

```
aws rds delete-blue-green-deployment ^
    --blue-green-deployment-identifier bgd-1234567890abcdef ^
    --no-delete-target
```

RDS-API

Verwenden Sie die `DeleteBlueGreenDeployment`-Operation mit den folgenden Parametern, um mithilfe der Amazon-RDS-API eine Blau/Grün-Bereitstellung zu löschen:

- `BlueGreenDeploymentIdentifier`— Die Ressourcen-ID der blauen/grünen Bereitstellung, die gelöscht werden soll.
- `DeleteTarget` – Geben Sie `TRUE` an, um den DB-Cluster in der grünen Umgebung zu löschen, oder `FALSE`, um ihn beizubehalten. Darf nicht `TRUE` sein, wenn die Blau/Grün-Bereitstellung den Status `SWITCHOVER_COMPLETED` hat.

Sichern und Wiederherstellen eines Amazon-Aurora-DB-Clusters

Diese Themen enthalten Informationen über Backup und Wiederherstellung von DB-Clustern von Amazon Aurora.

> **Tip**
>
> Die Hochverfügbarkeitsfunktionen und automatischen Sicherungsfunktionen von Aurora helfen, Ihre Daten zu schützen, ohne eine umfangreiche Einrichtung zu erfordern. Informieren Sie sich vor der Implementierung einer Sicherungsstrategie darüber, wie Aurora mehrere Kopien Ihrer Daten verwaltet und Ihnen hilft, über verschiedene DB-Instances und AWS-Regionen hinweg auf diese zuzugreifen. Details hierzu finden Sie unter Hohe Verfügbarkeit für Amazon Aurora.

Themen

Übersicht über das Sichern und Wiederherstellen eines Aurora-DB-Clusters

In den folgenden Themen werden Aurora-Backups und das Verfahren zum Wiederherstellen Ihres Aurora-DB-Clusters beschrieben.

Inhalt

Backups

Aurora sichert Ihr Cluster-Volume automatisch und bewahrt die Wiederherstellungsdaten für die Länge des Aufbewahrungszeitraums für Backups auf. Automatische Aurora-Backups sind kontinuierlich und inkrementell, sodass Sie schnell eine Wiederherstellung auf einen beliebigen Zeitpunkt im Aufbewahrungszeitraum für Backups durchführen können. Es gibt keine Auswirkungen auf die Leistungsfähigkeit oder Unterbrechung von Datenbank-Services, während Backup-Daten geschrieben werden. Sie können einen Aufbewahrungszeitraum für Backups von 1 bis 35 Tagen festlegen, wenn Sie einen DB-Cluster erstellen oder ändern. Automatische Aurora-Backups werden in Amazon S3 gespeichert.

Wenn Sie ein Backup nach dem eingestellten Aufbewahrungszeitraum behalten möchten, können Sie auch einen Snapshot der Daten Ihres Cluster-Volumes erstellen. Snapshots von Aurora-DB-Clustern

laufen nicht ab. Sie können ein neues DB-Cluster aus dem Snapshot erstellen. Weitere Informationen finden Sie unter Erstellen eines DB-Cluster-Snapshots.

> **Note**
>
> - Für Amazon Aurora-DB-Cluster beträgt der Standard-Aufbewahrungszeitraum für Backups einen Tag, unabhängig davon, wie der DB-Cluster erstellt wurde.
> - Automatisierte Sicherungen können in Aurora nicht deaktiviert werden. Die Aufbewahrungszeitraum von Sicherungen für Aurora wird vom DB-Cluster verwaltet.

Die Kosten für Sicherungsspeicher basieren auf dem Aufbewahrungszeitraum und der Menge der Aurora-Sicherungs- und -Snapshot-Daten. Weitere Informationen über den Speicher, der Aurora-Sicherungen und -Snapshots zugeordnet ist, finden Sie unter Grundlegendes zur Backup-Speicher-Nutzung in Amazon Aurora. Weitere Informationen zu den Preisen für Aurora-Sicherungsspeicher finden Sie unter Amazon RDS für Aurora: Preise. Nachdem der Aurora-Cluster, der einem Snapshot zugeordnet ist, gelöscht wurde, werden für die Speicherung dieses Snapshots die Standardgebühren für Sicherungsspeicher für Aurora berechnet.

Verwenden von AWS Backup

Sie können AWS Backup für die Verwaltung von Sicherungen von Amazon-Aurora-DB-Clustern verwenden.

Snapshots, die von AWS Backup verwaltet werden, gelten als manuelle DB-Cluster-Snapshots, werden jedoch nicht auf das DB-Cluster-Snapshot-Kontingent für Aurora angerechnet. Snapshots, die mit AWS Backup erstellt wurden, haben Namen mit `awsbackup:job-`*`AWS-Backup-job-number`*. Weitere Informationen zu AWS Backup finden Sie im AWS-Backup-Entwicklerhandbuch.

Sie können AWS Backup auch für die Verwaltung von Sicherungen von Amazon-Aurora-DB-Clustern verwenden. Wenn Ihr DB-Cluster mit einem Backup-Plan in verknüpft istAWS Backup, können Sie diesen Backup-Plan für die point-in-time Wiederherstellung verwenden. Automatisierte (kontinuierliche) Backups, die von AWS Backup verwaltet werden, haben Namen mit `continuous:cluster-`*`AWS-Backup-job-number`*. Weitere Informationen finden Sie unter Wiederherstellen eines DB-Clusters zu einem bestimmten Zeitpunkt mit AWS Backup.

Backup-Fenster

Automatisierte Backups werden täglich während des bevorzugten Zeitfensters für das Backup durchgeführt. Wenn die Sicherung mehr Zeit als im Zeitfenster angegeben benötigt, wird sie nach dem Ende des Fensters weiter ausgeführt, bis sie abgeschlossen ist. Das Backup-Fenster kann sich nicht mit dem wöchentlichen Wartungsfenster für den DB-Cluster überschneiden.

Automatische Aurora-Backups sind kontinuierlich und inkrementell. Das Backup-Fenster wird aber verwendet, um ein tägliches System-Backup zu erstellen, das innerhalb des Aufbewahrungszeitraums für Backups gespeichert wird. Sie können das Backup kopieren, um es über den Aufbewahrungszeitraum hinaus zu behalten.

> **Note**
>
> Wenn Sie einen DB-Cluster mit AWS Management Console erstellen, können Sie kein Backup-Fenster angeben. Sie können aber ein Backup-Fenster angeben, wenn Sie einen DB-Cluster mit der RDS-API oder AWS CLI erstellen.

Wenn Sie beim Erstellen des DB-Clusters kein bevorzugtes Backup-Fenster angeben, weist Aurora ein standardmäßiges 30-minütiges Backup-Fenster zu. Das Fenster wird zufällig aus einem 8-Stunden-Zeitraum für jede AWS-Region ausgewählt. In der folgenden Tabelle sind die Zeitblöcke für jede AWS-Region aufgeführt, in denen die Standard-Zeitfenster für das Backup zugewiesen werden.

Name der Region	Region	Zeitblock
US East (Ohio)	us-east-2	03:00 - 11:00 UTC
USA Ost (Nord-Virginia)	us-east-1	03:00 - 11:00 UTC
USA West (Nordkalifornien)	us-west-1	06:00 - 14:00 UTC
USA West (Oregon)	us-west-2	06:00 - 14:00 UTC
Africa (Cape Town)	af-south-1	03:00 - 11:00 UTC

Name der Region	Region	Zeitblock
Asia Pacific (Hong Kong)	ap-east-1	06:00 - 14:00 UTC
Asien-Pazifik (Hyderabad)	ap-south-2	06:30 – 14:30 Uhr UTC
Asien-Pazifik (Jakarta)	ap-southeast-3	08:00–16:00 Uhr UTC
Asien-Pazifik (Melbourne)	ap-southeast-4	11:00–19:00 Uhr UTC
Asien-Pazifik (Mumbai)	ap-south-1	16:30 - 00:30 UTC
Asia Pacific (Osaka)	ap-northeast-3	00:00 - 08:00 UTC
Asia Pacific (Seoul)	ap-northeast-2	13:00 - 21:00 UTC
Asien-Pazifik (Singapur)	ap-southeast-1	14:00 - 22:00 UTC
Asien-Pazifik (Sydney)	ap-southeast-2	12:00 - 20:00 UTC
Asien-Pazifik (Tokio)	ap-northeast-1	13:00 - 21:00 UTC
Canada (Central)	ca-central-1	03:00 bis 11:00 Uhr UTC
Kanada West (Calgary)	ca-west-1	18:00 - 02:00 UTC
China (Beijing)	cn-north-1	06:00 - 14:00 UTC
China (Ningxia)	cn-northwest-1	06:00 - 14:00 UTC
Europe (Frankfurt)	eu-central-1	20:00 - 04:00 UTC
Europa (Irland)	eu-west-1	22:00 - 06:00 UTC

Name der Region	Region	Zeitblock
Europe (London)	eu-west-2	22:00 bis 06:00 Uhr UTC
Europa (Mailand)	eu-south-1	02:00 - 10:00 UTC
Europa (Paris)	eu-west-3	07:29 - 14:29 UTC
Europa (Spanien)	eu-south-2	02:00 - 10:00 UTC
Europe (Stockholm)	eu-north-1	23:00 - 07:00 UTC
Europa (Zürich)	eu-central-2	02:00 - 10:00 UTC
Israel (Tel Aviv)	il-central-1	03:00 bis 11:00 Uhr UTC
Naher Osten (Bahrain)	me-south-1	06:00 - 14:00 UTC
Naher Osten (VAE)	me-central-1	05:00–13:00 UHR UTC
South America (São Paulo)	sa-east-1	23:00 - 07:00 UTC
AWS GovCloud (USA-Ost)	us-gov-east-1	17:00 - 01:00 UTC
AWS GovCloud (USA West)	us-gov-west-1	06:00 - 14:00 UTC

Aufbewahren automatisierter Backups

Wenn Sie einen bereitgestellten - oder Aurora Serverless v2 -DB-Cluster löschen, können Sie automatisierte Backups beibehalten. Auf diese Weise können Sie einen DB-Cluster zu einem bestimmten Zeitpunkt innerhalb des Backup-Aufbewahrungszeitraums wiederherstellen, auch nachdem der Cluster gelöscht wurde.

Beibehaltene, automatisierte Backups enthalten System-Snapshots und Transaktionsprotokolle aus einem DB-Cluster. Sie enthalten auch DB-Cluster-Eigenschaften wie die DB-Instance-Klasse, die für die Wiederherstellung in einen aktiven Cluster erforderlich sind.

Sie können aufbewahrte Backups mit der AWS Management Console, der RDS-API und der AWS CLI wiederherstellen oder entfernen.

> **Note**
>
> Sie können keine automatisierten Backups für Aurora Serverless v1 -DB-Cluster aufbewahren.

Themen

Aufbewahrungszeitraum

Die System-Snapshots und Transaktionsprotokolle in einem beibehaltenen, automatisierten Backup laufen auf dieselbe Art wie für den Quell-DB-Cluster ab. Die Einstellungen für den Aufbewahrungszeitraum des Quell-Clusters gelten auch für die automatisierten Backups. Da keine neuen Snapshots oder Protokolle für diesen Cluster erstellt wurden, laufen die beibehaltenen, automatisierten Backups letztendlich vollständig ab. Nach Ablauf der Beibehaltungsfrist behalten Sie weiterhin manuelle DB-Cluster-Snapshots bei, aber alle automatisierten Backups laufen ab.

Sie können beibehaltene, automatisierte Backups mit der Konsole, AWS CLI oder RDS-API entfernen. Weitere Informationen finden Sie unter Löschen aufbewahrter automatisierter Backups.

Im Gegensatz zu einem beibehaltenen, automatisierten Backup läuft ein endgültiger Snapshot nicht ab. Wir empfehlen dringend das Erstellen eines finalen Snapshots, selbst wenn Sie automatische Backups aufbewahren, da automatische Backups letztendlich ablaufen.

Anzeigen von beibehaltenen Backups

Um Ihre beibehaltenen, automatisierten Backups anzuzeigen, wählen Sie zuerst im Navigationsbereich Automatisierte Backups aus und dann Beibehalten aus. Um einzelne Snapshots anzuzeigen, die mit einem beibehaltenen automatisierten Backup verknüpft sind, wählen Sie im

Navigationsbereich Snapshot aus. Alternativ können Sie einzelne Snapshots beschreiben, die einem aufbewahrten automatischen Backup zugeordnet sind. Von da können Sie eine DB-Instance direkt aus einem dieser Snapshots wiederherstellen.

Zum Beschreiben Ihre gespeicherten automatisierten Backups mit AWS CLI, verwenden Sie einen der folgenden Befehle:

```
aws rds describe-db-cluster-automated-backups --db-cluster-resource-
id DB_cluster_resource_ID
```

Zum Beschreiben Ihrer automatischen Backups mit der RDS-API rufen Sie die `DescribeDBClusterAutomatedBackups`-Aktion mit einem der folgenden Parameter `DbClusterResourceId` auf:

Aufbewahrungskosten

Es fallen keine zusätzlichen Gebühren für Backup-Speicher von bis zu 100 % Ihres gesamten Aurora-Datenbankspeichers für jeden Aurora-DB-Cluster an. Außerdem fallen bis zu einem Tag keine zusätzlichen Kosten an, wenn Sie automatisierte Backups nach dem Löschen eines DB-Clusters beibehalten. Backups, die Sie länger als einen Tag beibehalten, werden in Rechnung gestellt.

Für Transaktionsprotokolle oder Instance-Metadaten wird keine zusätzliche Gebühr erhoben. Alle anderen Preisregeln für Backups gelten für wiederherstellbare Cluster. Weitere Informationen finden Sie auf der Seite Amazon-Aurora-Preise.

Einschränkungen

Die folgenden Einschränkungen gelten für aufbewahrte automatische Backups:

- Die maximale Anzahl der aufbewahrten automatischen Backups in einer AWS-Region ist 40. Dies ist nicht im Kontingent für DB-Cluster enthalten. Sie können bis zu 40 laufende DB-Cluster, 40 laufende DB-Instances und 40 beibehaltene, automatisierte Backups für DB-Cluster gleichzeitig haben.

  Weitere Informationen finden Sie unter Kontingente in Amazon Aurora.
- Aufbewahrte automatische Backups enthalten keine Informationen über Parameter oder Optionsgruppen.
- Sie können einen gelöschten Cluster zu jedem Zeitpunkt wiederherstellen, der zum Zeitpunkt des Löschens innerhalb der Beibehaltungsdauer liegt.

- Ein beibehaltener, automatisierter Backup kann nicht bearbeitet werden, da er aus System-Backups, Transaktionsprotokollen und den DB-Cluster-Eigenschaften besteht, die zum Zeitpunkt des Löschens des Quell-Clusters vorhanden waren.

Löschen aufbewahrter automatisierter Backups

Sie können aufbewahrte automatisierte Backups löschen, wenn sie nicht mehr benötigt werden.

Konsole

So löschen Sie eine aufbewahrte automatisierte Backup:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Automated backups (Automatisierte Backups) aus.
3. Wählen Sie die Registerkarte Beibehalten aus.

4. Wählen Sie die aufbewahrte automatisierte Sicherung, die Sie löschen möchten.
5. Klicken Sie bei Actions auf Delete.
6. Geben Sie auf der Bestätigungsseite **`delete me`** und wählen Sie Löschen aus.

AWS CLI

Sie können ein aufbewahrtes automatisiertes Backup löschen, indem Sie den AWS CLI Befehl delete-db-cluster-automated-backup mit der folgenden Option verwenden:

- `--db-cluster-resource-id` – Die Ressourcenkennung für den Quell-DB-Cluster.

  Sie finden die Ressourcenkennung für den Quell-DB-Cluster eines beibehaltenen automatisierten Backups, indem Sie den AWS CLI Befehl describe-db-cluster-automated-backups ausführen.

Example

In diesem Beispiel wird das beibehaltene, automatisierte Backup für den Quell-DB-Cluster gelöscht, das die Ressourcen-ID `cluster-123ABCEXAMPLE` hat.

Für Linux, macOSoder Unix:

```
aws rds delete-db-cluster-automated-backup \
    --db-cluster-resource-id cluster-123ABCEXAMPLE
```

Windows:

```
aws rds delete-db-cluster-automated-backup ^
    --db-cluster-resource-id cluster-123ABCEXAMPLE
```

RDS-API

Sie können ein aufbewahrtes automatisiertes Backup löschen, indem Sie die Amazon RDS-API-Operation DeleteDBClusterAutomatedBackup mit dem folgenden Parameter verwenden:

- `DbClusterResourceId` – Die Ressourcenkennung für den Quell-DB-Cluster.

  Sie finden die Ressourcenkennung für die Quell-DB-Instance eines aufbewahrten automatisierten Backups mithilfe der Amazon RDS-API-Operation DescribeDBClusterAutomatedBackups.

Wiederherstellen von Daten

Sie können Ihre Daten wiederherstellen, indem Sie einen neuen Aurora-DB-Cluster aus den von Aurora beibehaltenen Backup-Daten, aus einem von Ihnen gespeicherten DB-Cluster-Snapshot oder aus einem beibehaltenen, automatisierten Backup erstellen. Sie können schnell eine neue Kopie eines DB-Clusters wiederherstellen, die aus den Sicherungsdaten von irgendeinem Zeitpunkt der Aufbewahrungsfrist für Backups erstellt wurde. Da Aurora-Backups während des Aufbewahrungszeitraums für Backups fortlaufend und ansteigend sind, müssen Sie keine häufigen Snapshots Ihrer Daten machen, um die Wiederherstellungszeiten zu optimieren.

Der späteste wiederherstellbare Zeitpunkt für einen DB-Cluster ist der aktuelle Punkt, an dem Sie Ihr DB-Cluster wiederherstellen können. Dieser liegt im Normalfall 5 Minuten vor dem aktuellen Zeitpunkt für einen aktiven DB-Cluster oder 5 Minuten nach der Cluster-Löschzeit für ein beibehaltenes, automatisiertes Backup.

Der früheste wiederherstellbare Zeitpunkt gibt an, wie weit Sie zeitlich innerhalb des Aufbewahrungszeitraums für Backups zurückgehen können, um Ihr Cluster-Volume an einem vergangen Zeitpunkt wiederherstellen zu können.

Sehen Sie sich die Werte `Latest restorable time` oder `Earliest restorable time` in der RDS-Konsole an, um den spätesten und frühesten wiederherstellbaren Zeitpunkt für einen DB-Cluster zu bestimmen. Weitere Informationen zur Anzeige dieser Werte finden Sie unter Anzeigen von beibehaltenen Backups.

Sie können sehen, wann ein Wiederherstellungsvorgang eines DB-Clusters abgeschlossen ist, indem Sie `Latest restorable time` und `Earliest restorable time`-Werte überprüfen. Die Werte geben NULL zurück, bis der Wiederherstellungsvorgang abgeschlossen ist. Sie können kein Backup oder einen Wiederherstellungsvorgang anfordern, wenn `Latest restorable time` oder `Earliest restorable time` NULL zurückgibt.

Informationen zum Wiederherstellen eines DB-Clusters zu einem bestimmten Zeitpunkt finden Sie unter Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit.

Klonen von Datenbanken für Aurora

Sie können das Klonen von Datenbanken auch verwenden, um die Datenbanken Ihres Aurora DB-Clusters auf einen neuen DB-Cluster zu klonen, anstatt einen DB-Cluster-Snapshot wiederherzustellen. Die Klondatenbanken beanspruchen bei der Erstellung nur eine kleine Menge an zusätzlichem Speicherplatz. Die Daten werden nur als Datenänderungen entweder in den Quelldatenbanken oder in den Klondatenbanken kopiert. Sie können mehrere Klone vom selben DB-Cluster anfertigen oder zusätzliche Klone von anderen Klonen erstellen. Weitere Informationen finden Sie unter Klonen eines Volumes für einen Amazon-Aurora-DB-Cluster.

Backtrack

Aurora MySQL unterstützt jetzt das "Zurückspulen" eines DB-Clusters auf einen bestimmten Zeitpunkt, ohne dass die Daten aus einer Sicherung wiederhergestellt werden müssen. Weitere Informationen finden Sie unter Rückverfolgen eines Aurora-DB-Clusters.

Grundlegendes zur Backup-Speicher-Nutzung in Amazon Aurora

Amazon Aurora verwaltet zwei Arten von Backups: automatische (kontinuierliche) Backups und Snapshots.

Automatischer Backup-Speicher

Das automatische (kontinuierliche) Backup für einen Cluster speichert alle Datenbankänderungen innerhalb eines bestimmten Aufbewahrungszeitraums inkrementell, um sie auf jeden beliebigen Zeitpunkt innerhalb dieses Aufbewahrungszeitraums wiederherstellen zu können. Die Aufbewahrungszeiträume können zwischen 1 und 35 Tagen liegen. Automatische Backups erfolgen inkrementell und werden auf der Grundlage der Speichermenge berechnet, die für eine Wiederherstellung auf einen Zeitpunkt innerhalb des Aufbewahrungszeitraums erforderlich ist.

Aurora bietet außerdem ein kostenloses Kontingent für die Backup-Nutzung an. Dieses kostenlose Nutzungskontingent entspricht der aktuellen Cluster-Volume-Größe (wie durch die Amazon-CloudWatch-Metrik `VolumeBytesUsed` dargestellt). Dieses Kontingent wird von der berechneten Nutzung automatischer Backups abgezogen. Für automatische Backups mit einem Aufbewahrungszeitraum von nur 1 Tag fallen ebenfalls keine Gebühren an.

Beispiel: Ihr automatisches Backup hat einen Aufbewahrungszeitraum von 7 Tagen und Sie möchten Ihren Cluster auf den Status von vor vier Tagen zurücksetzen. Aurora verwendet die im automatischen Backup gespeicherten inkrementellen Daten, um den Status des Clusters zu genau diesem Zeitpunkt vor vier Tagen wiederherzustellen.

Das automatische Backup speichert alle erforderlichen Informationen, um den Cluster auf jeden Zeitpunkt innerhalb des Aufbewahrungszeitraums wiederherstellen zu können. Das bedeutet, dass alle Änderungen während des Aufbewahrungszeitraums gespeichert werden, einschließlich der Schreibvorgänge zu neuen Informationen oder des Löschens vorhandener Informationen. Bei Datenbanken, in denen viele Änderungen vorgenommen werden, nimmt die Größe des automatischen Backups mit der Zeit zu. Wenn an einer Datenbank keine Änderungen mehr vorgenommen werden, können Sie damit rechnen, dass sich die Größe des automatischen Backups verringert, da die zuvor gespeicherten Änderungen im Laufe der Zeit nicht mehr innerhalb des Aufbewahrungszeitraums liegen.

Die in Rechnung gestellte Gesamtnutzung für das automatische Backup übersteigt niemals die kumulative Cluster-Volume-Größe während des Aufbewahrungszeitraums. Wenn der Aufbewahrungszeitraum beispielsweise 7 Tage beträgt und das Cluster-Volumen 100 GB pro Tag

betrug, dann übersteigt die in Rechnung gestellte Nutzung automatischer Backups niemals 700 GB (100 GB * 7).

Snapshot-Speicher

DB-Cluster-Snapshots sind immer vollständige Backups, deren Größe der Größe des Cluster-Volumes zum Zeitpunkt der Snapshot-Erstellung entspricht. Snapshots, die entweder manuell vom Benutzer oder automatisch von einem AWS-Backups-Plan erstellt wurden, werden wie manuelle Snapshots behandelt. Aurora bietet unbegrenzten kostenlosen Speicherplatz für alle Snapshots, die innerhalb des Aufbewahrungszeitraums für automatische Backups liegen. Sobald ein manueller Snapshot außerhalb des Aufbewahrungszeitraums liegt, wird er in GB/Monat abgerechnet. Automatische System-Snapshots werden nur dann in Rechnung gestellt, wenn sie nach Ablauf des Aufbewahrungszeitraums kopiert und aufbewahrt werden.

Allgemeine Informationen zu Aurora-Sicherungen finden Sie unter Backups. Weitere Informationen zum Backup-Speicher von Aurora finden Sie auf der Webseite Amazon-Aurora-Preise.

Amazon-CloudWatch-Metriken für Aurora-Backup-Speicher

Sie können Ihre Aurora-Cluster überwachen und mit Amazon-CloudWatch-Metriken über die CloudWatch Konsole Berichte erstellen. Mit den folgenden CloudWatch-Metriken können Sie die Speicherkapazität Ihrer Aurora-Backups überprüfen und überwachen. Diese Metriken werden für jeden Aurora-DB-Cluster unabhängig voneinander berechnet.

- `BackupRetentionPeriodStorageUsed` – Stellt die Menge des Backup-Speichers in Bytes dar, die zurzeit zum Speichern automatischer Backups verwendet wird.
  - Der Wert hängt von der Größe des Cluster-Volumes und der Anzahl der Änderungen (Schreibvorgänge und Aktualisierungen) ab, die während des Aufbewahrungszeitraums am DB-Cluster vorgenommen werden. Dies liegt daran, dass das automatische Backup alle inkrementellen Änderungen am Cluster speichern muss, um eine Wiederherstellung auf einen beliebigen Zeitpunkt vornehmen zu können.
  - Diese Metrik zieht nicht das kostenlose Kontingent an Backup-Nutzung ab, das Aurora bereitstellt.
  - Diese Metrik gibt einen einzigen täglichen Datenpunkt für die an diesem Tag aufgezeichnete Nutzung automatischer Backups aus.
- `SnapshotStorageUsed` – Stellt die Menge des Backup-Speichers in Bytes dar, die zum Speichern manueller Snapshots über den Aufbewahrungszeitraum des automatischen Backups hinaus verwendet wird.

- Der Wert hängt von der Anzahl der Snapshots, die Sie über den Aufbewahrungszeitraum des automatischen Backups hinaus aufbewahren, und von der Größe der einzelnen Snapshots ab.
- Die Größe einzelner Snapshots entspricht der Größe des Cluster-Volumes zum Zeitpunkt der Snapshot-Erstellung.
- Snapshots sind vollständige Backups, keine inkrementellen.
- Diese Metrik gibt für jeden Snapshot, der in Rechnung gestellt wird, einen täglichen Datenpunkt aus. Verwenden Sie zum Abrufen Ihrer täglichen Gesamtnutzung von Snapshots die Summe dieser Metrik über einen Zeitraum von 1 Tag.

- `TotalBackupStorageBilled` – Stellt die Metriken für die gesamte in Rechnung gestellte Backup-Nutzung in Byte für den angegebenen Cluster dar:

  ```
  BackupRetentionPeriodStorageUsed + SnapshotStorageUsed - free tier
  ```

  - Diese Metrik gibt einen täglichen Datenpunkt für den Wert `BackupRetentionPeriodStorageUsed` abzüglich der von Aurora bereitgestellten kostenlosen Backup-Nutzungskontingente aus. Dieses kostenlose Kontingent entspricht der zuletzt aufgezeichneten Größe des DB-Cluster-Volumes. Dieser Datenpunkt stellt die tatsächlich in Rechnung gestellte Nutzung für das automatische Backup dar.
  - Diese Metrik gibt einzelne tägliche Datenpunkte für alle `SnapshotStorageUsed`-Werte aus.
  - Verwenden Sie zum Abrufen Ihrer täglich in Rechnung gestellten Backup-Nutzung die Summe dieser Metrik über einen Zeitraum von 1 Tag. Dadurch wird die gesamte in Rechnung gestellte Snapshot-Nutzung mit der in Rechnung gestellten automatischen Backup-Nutzung addiert, sodass sich Ihre gesamte in Rechnung gestellte Backup-Nutzung ergibt.

Weitere Informationen zur Verwendung der CloudWatch-Metriken finden Sie unter Verfügbarkeit von Aurora Metriken in der Amazon RDS Konsole.

Berechnung der Nutzung des Backup-Speichers

Die Nutzung für ein automatisches Backup wird anhand aller inkrementellen Datensätze berechnet, die gespeichert werden müssen, um eine Wiederherstellung auf einen beliebigen Zeitpunkt innerhalb des Aufbewahrungszeitraums des Backups vornehmen zu können.

Beispiel: Sie haben ein automatisches Backup mit einem Aufbewahrungszeitraum von 7 Tagen. Die Größe Ihres Cluster-Volumes unmittelbar vor dem Aufbewahrungszeitraum betrug 100 GB. Das ist also die geringste Menge, die Aurora speichern muss. Dann haben Sie die folgende Aktivität für die nächsten 7 Tage. Dabei ist die inkrementelle Datensatzgröße die Menge an Speicherplatz, die

zum Speichern der Änderungsdatensätze benötigt wird, die sich aus den Schreibvorgängen und Aktualisierungen Ihrer Datenbank ergeben.

Tag	Inkrementelle Datensatzgröße (GB)
1	10
2	15
3	25
4	20
5	10
6	25
7	30
Gesamtsumme	135

Diese Daten bedeuten, dass die berechnete automatische Backup-Nutzung für Ihr Backup wie folgt aussieht:

```
100 GB (volume size before retention period) + 135 GB (size of incremental records) =
 235 GB total backup usage
```

Von der in Rechnung gestellten Nutzung wird dann das kostenlose Nutzungskontingent abgezogen. Angenommen, die aktuelle Größe Ihres Volumes beträgt 200 GB:

```
235 GB total backup usage - 200 GB (latest volume size) = 35 GB billed backup usage
```

Häufig gestellte Fragen

Wann werden mir Snapshots in Rechnung gestellt?

Manuelle Snapshots, die außerhalb des Aufbewahrungszeitraums des automatisierten Backups liegen (d. h. älter sind), werden Ihnen in Rechnung gestellt.

Was ist ein manueller Snapshot?

Ein manueller Snapshot ist ein Snapshot, der eine der folgenden Bedingungen erfüllt:

- Manuelle Anforderung durch Sie
- Erstellung durch einen automatischen Backup-Service wie beispielsweise AWS Backup
- Kopiert aus einem automatischen System-Snapshot, um ihn über den Aufbewahrungszeitraum hinaus aufzubewahren

Was geschieht mit meinen manuellen Snapshots, wenn ich meinen DB-Cluster lösche?

Manuelle Snapshots laufen erst ab, wenn Sie sie löschen.

Wenn Sie Ihren DB-Cluster löschen, sind die zuvor erstellten manuellen Snapshots weiterhin vorhanden. Wenn diese Snapshots zuvor nicht in Rechnung gestellt wurden, da sie sich innerhalb des Aufbewahrungszeitraums für automatische Backups befanden, sind sie jetzt nicht mehr abgedeckt und die Nutzung wird voll in Rechnung gestellt.

Wie kann ich meine Backup-Speicherkosten senken?

Es gibt mehrere Möglichkeiten, die mit der Backup-Nutzung verbundenen Kosten zu senken:

- Löschen Sie manuelle Snapshots, die außerhalb des Aufbewahrungszeitraums Ihres automatischen Backups liegen. Dies umfasst die von Ihnen erstellten Snapshots sowie die Snapshots, die Ihr AWS-Backup-Plan möglicherweise erstellt hat. Überprüfen Sie unbedingt Ihren AWS-Backup-Plan, um sicherzustellen, dass nicht versehentlich Snapshots außerhalb des Aufbewahrungszeitraums aufbewahrt werden.
- Prüfen Sie Ihre Schreibvorgänge und Aktualisierungen an Ihrer Datenbank, um zu ermitteln, ob Sie die Anzahl der von Ihnen vorgenommenen Änderungen reduzieren können. Da das automatische Backup alle inkrementellen Änderungen innerhalb des Aufbewahrungszeitraums speichert, hat die Reduzierung der Anzahl der von Ihnen vorgenommenen Aktualisierungen auch geringere Kosten für automatische Backups zur Folge.
- Prüfen Sie, ob es sinnvoll wäre, die Aufbewahrungsdauer des automatischen Backups zu reduzieren. Ein kürzerer Aufbewahrungszeitraum bedeutet, dass das Backup weniger Tage an inkrementellen Daten speichert. Dies könnte geringere Gesamtkosten für das Backup zur Folge haben. Wenn Sie diesen Aufbewahrungszeitraum verkürzen, könnte dies jedoch auch dazu führen, dass einige Snapshots plötzlich in Rechnung gestellt werden, da sie sich jetzt außerhalb des Aufbewahrungszeitraums befinden. Überprüfen Sie unbedingt alle zusätzlichen Snapshot-Kosten, die möglicherweise anfallen, bevor Sie entscheiden, ob dies die richtige Option für Sie ist.

Wie wird Backup-Speicher abgerechnet?

Die Fakturierung für Backup-Speicher erfolgt nach GB/Monat.

Dies bedeutet, dass die Nutzung des Backup-Speichers als gewichteter Durchschnitt der Nutzung im angegebenen Monat berechnet wird. Im Folgenden finden Sie ein paar Beispiele für einen Monat mit 30 Tagen:

- Die in Rechnung gestellte Backup-Nutzung beträgt 100 GB für alle 30 Tage des Monats. Folgendes wird Ihnen in Rechnung gestellt:

```
(100 GB * 30) / 30 = 100 GB-month
```

- Die in Rechnung gestellte Backup-Nutzung beträgt 100 GB für die ersten 15 Tage des Monats, danach 0 GB für die restlichen 15 Tage. Folgendes wird Ihnen in Rechnung gestellt:

```
(100 GB * 15 + 0 GB * 15) / 30 = 50 GB-month
```

- Die in Rechnung gestellte Backup-Nutzung beträgt 50 GB für die ersten 10 Tage des Monats, 100 GB für die nächsten 10 Tage und 150 GB für die letzten 10 Tage. Folgendes wird Ihnen in Rechnung gestellt:

```
(50 GB * 10 + 100 GB * 10 + 150 GB * 10) / 30 = 100 GB-month
```

Wie wirkt sich die Rückverfolgungseinstellung für meinen DB-Cluster auf die Nutzung des Backup-Speichers aus?

Die Rückverfolgungseinstellung für einen Aurora-DB-Cluster wirkt sich nicht auf das Volumen der Sicherungsdaten für den entsprechenden Cluster aus. Der Speicher für Rückverfolgungsdaten wird von Amazon separat in Rechnung gestellt. Informationen zur Preisgestaltung von Aurora-Rückverfolgung finden Sie auf der Seite Amazon Aurora-Preisliste.

Inwiefern gelten die Speicherkosten für freigegebene Snapshots?

Wenn Sie einen Snapshot für einen anderen Benutzer freigeben, bleiben Sie der Besitzer dieses Snapshots. Die Speicherkosten gelten für den Snapshot-Besitzer. Wenn Sie einen freigegebenen Snapshot in Ihrem Besitz löschen, besteht kein Zugriff darauf mehr.

Um Zugriff auf einen freigegebenen Snapshot zu behalten, der im Besitz eines anderen Benutzers ist, können Sie den entsprechenden Snapshot kopieren. Dadurch werden Sie zum Besitzer des neuen Snapshots. Etwaige Speicherkosten für den kopierten Snapshot werden Ihrem Konto belastet.

Weitere Informationen zum Freigeben von Snapshots finden Sie unter Freigeben eines DB-Cluster-Snapshots. Weitere Informationen zum Kopieren von Snapshots finden Sie unter Kopieren eines DB-Cluster-Snapshots.

Erstellen eines DB-Cluster-Snapshots

Amazon RDS erstellt einen Snapshot für das Volume mit Ihrem DB-Cluster, damit der gesamte DB-Cluster gesichert wird und nicht nur einzelne Datenbanken. Beim Erstellen eines DB-Cluster-Snapshots wählen Sie den DB-Cluster aus, der gesichert werden soll, und benennen den DB-Cluster-Snapshot, damit Sie später mit diesem eine Wiederherstellung ausführen können. Die Zeit, die für die Erstellung eines DB-Cluster-Snapshots benötigt wird, hängt von der Größe Ihrer Datenbanken ab. Da der Snapshot das gesamte Speichervolume umfasst, wirkt sich die Größe von Dateien, wie z. B. temporäre Dateien, auch auf die Zeit aus, die zum Erstellen des Snapshots benötigt wird.

> **Note**
>
> Ihr DB-Cluster muss den Status `available` aufweisen, um einen DB-Cluster-Snapshot zu erstellen.

Im Gegensatz zu automatisierten Backups unterliegen manuelle Snapshots nicht dem Aufbewahrungszeitraum für Backups. Snapshots laufen nicht ab.

Für sehr langfristige Sicherungen empfehlen wir den Export von Snapshot-Daten in Amazon S3. Wenn die Hauptversion der DB-Engine nicht mehr unterstützt wird, können Sie diese Version nicht über einen Snapshot wiederherstellen. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Snapshot-Daten nach Amazon S3.

Sie können einen DB-Cluster-Snapshot mithilfe der AWS Management Console, der AWS CLIoder der RDS-API erstellen.

Konsole

So erstellen Sie einen DB-Cluster-Snapshot

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

   Die Liste manuellen Snapshots wird angezeigt.
3. Wählen Sie Take Snapshot (Snapshot erstellen) aus.

   Das Fenster Take DB Snapshot (DB-Snapshot erstellen) wird angezeigt.

4. Wählen Sie für Snapshot-Typ die Option DB-Cluster aus.
5. Wählen Sie den DB-Cluster aus, für den Sie einen Snapshot erstellen möchten.
6. Geben Sie den Snapshot-Namen ein.
7. Wählen Sie Take Snapshot (Snapshot erstellen) aus.

   Die Liste Manuelle Snapshots wird angezeigt, wobei der Status des neuen DB-Cluster-Snapshots als angezeigt wird`Creating`. Nachdem sein Status`Available`, können Sie die Erstellungszeit sehen.

AWS CLI

Wenn Sie einen DB-Cluster-Snapshot mit der erstellen AWS CLI, müssen Sie identifizieren, welcher DB-Cluster gesichert werden soll, und Ihrem DB-Cluster-Snapshot dann einen Namen geben, damit Sie ihn später wiederherstellen können. Verwenden Sie dazu den AWS CLI `create-db-cluster-snapshot` Befehl mit den folgenden Parametern:

- `--db-cluster-identifier`
- `--db-cluster-snapshot-identifier`

In diesem Beispiel erstellen Sie einen DB-Cluster-Snapshot mit dem Namen *`mydbclustersnapshot`* für einen DB-Cluster namens *`mydbcluster`*.

Example

Für Linux, macOSoder Unix:

```
aws rds create-db-cluster-snapshot \
    --db-cluster-identifier mydbcluster \
    --db-cluster-snapshot-identifier mydbclustersnapshot
```

Windows:

```
aws rds create-db-cluster-snapshot ^
    --db-cluster-identifier mydbcluster ^
    --db-cluster-snapshot-identifier mydbclustersnapshot
```

RDS-API

Beim Erstellen eines DB-Cluster-Snapshots mithilfe der Amazon RDS-API wählen Sie den DB-Cluster aus, der gesichert werden soll, und benennen den DB-Cluster-Snapshot, damit Sie später mit diesem eine Wiederherstellung ausführen können. Sie können dies tun, indem Sie den Amazon RDS API `CreateDBClusterSnapshot`-Befehl mit den folgenden Parametern verwenden:

- DBClusterIdentifier
- DBClusterSnapshotIdentifier

feststellen, ob der DB-Cluster-Snapshot verfügbar ist

Sie können überprüfen, ob der DB-Cluster-Snapshot verfügbar ist, indem Sie unter Snapshots auf der Registerkarte Wartung und Backups auf der Detailseite für den Cluster in der nachsehen AWS Management Console, indem Sie den `describe-db-cluster-snapshots` CLI-Befehl verwenden oder die API`DescribeDBClusterSnapshots`-Aktion verwenden.

Sie können den CLI-Befehl `wait db-cluster-snapshot-available` auch verwenden, um die API alle 30 Sekunden abzufragen, bis der Snapshot verfügbar ist.

Wiederherstellen aus einem DB-Cluster-Snapshot

Amazon RDS erstellt einen Snapshot für das Volume mit Ihrem DB-Cluster, damit der gesamte DB-Cluster gesichert wird und nicht nur einzelne Datenbanken. Sie können einen neuen DB-Cluster erstellen, indem Sie einen DB-Snapshot wiederherstellen. Sie geben den Namen des DB-Cluster-Snapshot an, aus dem die Wiederherstellung gestartet werden soll, und anschließend einen Namen für den neuen DB-Cluster, der bei dieser Wiederherstellung erstellt wird. Sie können keine Wiederherstellung aus einem DB-Cluster-Snapshot auf einem bestehenden DB-Cluster vornehmen. Bei der Wiederherstellung wird ein neuer DB-Cluster erstellt.

Important

Wenn Sie versuchen, einen Snapshot auf einer veralteten DB-Engine-Version wiederherzustellen, erfolgt ein sofortiges Upgrade auf die neueste Engine-Version. Darüber hinaus können Gebühren für erweiterten Support anfallen, wenn für die Version der erweiterte Support gilt oder der Standardsupport abgelaufen ist. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Extended Support.

Sie können den wiederhergestellten DB-Cluster nutzen, sobald sein Status `available` lautet.

Sie können AWS CloudFormation es verwenden, um einen DB-Cluster aus einem DB-Cluster-Snapshot wiederherzustellen. Weitere Informationen finden Sie unter AWS::RDS::DBCluster im AWS CloudFormation -Benutzerhandbuch.

Note

Durch die gemeinsame Nutzung eines manuellen DB-Cluster-Snapshots, ob verschlüsselt oder unverschlüsselt, können autorisierte AWS Konten einen DB-Cluster direkt aus dem Snapshot wiederherstellen, anstatt eine Kopie davon zu erstellen und von dort aus wiederherzustellen. Weitere Informationen finden Sie unter Freigeben eines DB-Cluster-Snapshots.

Informationen zur Wiederherstellung eines Aurora-DB-Clusters oder eines globalen Clusters mit einer RDS Extended Support-Version finden Sie unterWiederherstellung , eines Aurora-DB-Clusters oder eines globalen Clusters mit Amazon RDS Extended Support.

Überlegungen zu Parametergruppen

Wir empfehlen Ihnen, die DB-Parametergruppe und DB-Cluster-Parametergruppe für alle DB-Cluster-Snapshots aufzubewahren, die Sie erstellen, damit Sie Ihrem wiederhergestellten DB-Cluster die korrekte Parametergruppen zuordnen können.

Die Standard-DB-Parametergruppe und DB-Cluster-Parametergruppe sind dem wiederhergestellten Cluster zugeordnet, es sei denn, Sie wählen eine andere Instance aus. In den Standard-DB-Parametergruppen sind keine benutzerdefinierten Parametereinstellungen verfügbar.

Sie können die Parametergruppen angeben, wenn Sie den DB-Cluster wiederherstellen.

Weitere Informationen über DB-Parametergruppen und DB-Cluster-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Überlegungen zu Sicherheitsgruppen

Wenn Sie einen DB-Cluster wiederherstellen, werden die Standard-VPC (Virtual Private Cloud), DB-Subnetzgruppe und VPC-Sicherheitsgruppe mit der wiederhergestellten Instance verknüpft, wenn Sie keine anderen angeben.

- Wenn Sie die Amazon-RDS-Konsole verwenden, können Sie eine benutzerdefinierte VPC-Sicherheitsgruppe angeben, die dem Cluster zugeordnet werden soll, oder eine neue VPC-Sicherheitsgruppe erstellen.
- Wenn Sie die verwenden AWS CLI, können Sie eine benutzerdefinierte VPC-Sicherheitsgruppe angeben, die dem Cluster zugeordnet werden soll, indem Sie die `--vpc-security-group-ids` Option in den `restore-db-cluster-from-snapshot` Befehl aufnehmen.
- Wenn Sie die Amazon RDS-API verwenden, können sie den `VpcSecurityGroupIds.VpcSecurityGroupId.N`-Parameter in der Aktion `RestoreDBClusterFromSnapshot` einschließen.

Sobald die Wiederherstellung abgeschlossen ist und Ihr neuer DB-Cluster verfügbar ist, können Sie auch die VPC-Einstellungen ändern, indem Sie den DB-Cluster bearbeiten. Weitere Informationen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Überlegungen zu Amazon Aurora

Mit Aurora stellen Sie einen DB-Cluster-Snapshot in einem DB-Cluster wieder her.

Sie können sowohl mit Aurora MySQL als auch mit Aurora PostrgreSQL einen DB-Cluster-Snapshot in einem Aurora Serverless-DB-Cluster wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen eines Aurora Serverless v1-DB-Clusters.

Mit Aurora MySQL stellen Sie einen DB-Cluster-Snapshot von einem Cluster ohne parallele Abfrage auf einen Cluster mit paralleler Abfrage wieder her. Da die parallele Abfrage normalerweise bei sehr großen Tabellen verwendet wird, ist die Snapshot-Methode die schnellste Art, um große Datenmengen in einen parallelen und abfragefähigen Aurora MySQL-Cluster aufzunehmen. Weitere Informationen finden Sie unter Arbeiten mit Parallel Query für Amazon Aurora MySQL.

Wiederherstellung aus einem Snapshot

Sie können einen DB-Cluster aus einem DB-Cluster Snapshot wiederherstellen, indem Sie die AWS Management Console, die AWS CLI oder die RDS API verwenden.

Konsole

So stellen Sie einen DB-Cluster aus einem DB-Cluster-Snapshot wieder her

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den DB-Cluster-Snapshot für die Wiederherstellung aus.
4. Wählen Sie in Actions (Aktionen) die Option Restore Snapshot (Snapshot wiederherstellen) aus.

   Die Seite „Snapshot wiederherstellen“ wird angezeigt.
5. Wählen Sie die DB-Engine-Version, in der Sie den DB-Cluster wiederherstellen möchten.

   Standardmäßig wird der Snapshot in derselben DB-Engine-Version wie der Quell-DB-Cluster wiederhergestellt, sofern sie verfügbar ist.
6. Geben Sie für DB instance identifier (DB-Instance-Kennung) den Namen Ihres wiederhergestellten DB-Clusters ein.
7. Geben Sie andere Einstellungen an, z. B. die Speicherkonfiguration des DB-Clusters.

   Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.
8. Wählen Sie Restore DB Cluster (DB-Cluster wiederherstellen) aus.

AWS CLI

Um einen DB-Cluster aus einem DB-Cluster-Snapshot wiederherzustellen, verwenden Sie den AWS CLI Befehl restore-db-cluster-from-snapshot.

In diesem Beispiel führen Sie eine Wiederherstellung aus einem vorher erstellten DB-Cluster-Snapshot mit dem Namen durc `mydbclustersnapshot`. Sie stellen auf einen neuen DB-Cluster namens wieder he `mynewdbcluster`.

Sie können andere Einstellungen angeben, z. B. die DB-Engine-Version. Wenn Sie keine Engine-Version angeben, wird der DB-Cluster in der Standard-Engine-Version wiederhergestellt.

Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.

Example

Für LinuxmacOS, oderUnix:

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier mynewdbcluster \
    --snapshot-identifier mydbclustersnapshot \
    --engine aurora-mysql|aurora-postgresql
```

Windows:

```
aws rds restore-db-cluster-from-snapshot ^
    --db-cluster-identifier mynewdbcluster ^
    --snapshot-identifier mydbclustersnapshot ^
    --engine aurora-mysql|aurora-postgresql
```

Nachdem der DB-Cluster wiederhergestellt wurde, müssen Sie den DB-Cluster in der Sicherheitsgruppe hinzufügen, die von dem DB-Cluster verwendet wurde, um den DB-Snapshot zu erstellen, wenn Sie dieselbe Funktionalität wie in dem vorherigen DB-Cluster erhalten möchten.

> **Important**
>
> Wenn Sie die Konsole für das Wiederherstellen eines DB-Clusters verwenden, erstellt Amazon RDS automatisch die primäre DB-Instance (Writer) für Ihren DB-Cluster. Wenn Sie

AWS CLI für das Wiederherstellen eines DB-Clusters verwenden, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance. Wenn Sie die primäre DB-Instance nicht erstellen, bleiben die DB-Cluster-Endpunkte im Status `creating`.
Rufen Sie den create-db-instance AWS CLI Befehl auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Fügen Sie den Namen des DB-Clusters als `--db-cluster-identifier`-Optionswert ein.

RDS-API

Um einen DB-Cluster aus einem DB-Cluster-Snapshot wiederherzustellen, rufen Sie den RDS-API-Vorgang RestoreDB ClusterFromSnapshot mit den folgenden Parametern auf:

- `DBClusterIdentifier`
- `SnapshotIdentifier`

Important

Wenn Sie die Konsole für das Wiederherstellen eines DB-Clusters verwenden, erstellt Amazon RDS automatisch die primäre DB-Instance (Writer) für Ihren DB-Cluster. Wenn Sie die RDS-API für das Wiederherstellen eines DB-Clusters verwenden, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance. Wenn Sie die primäre DB-Instance nicht erstellen, bleiben die DB-Cluster-Endpunkte im Status `creating`.
Rufen Sie die RDS-API-Operation CreateDBInstance auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Beziehen Sie den Namen des DB-Clusters als `DBClusterIdentifier`-Parameterwert mit ein.

Kopieren eines DB-Cluster-Snapshots

Mit Amazon Aurora können Sie automatisierte Backups oder manuelle DB-Cluster-Snapshots kopieren. Nach dem Kopieren eines Snapshots ist die Kopie ein manueller Snapshot. Sie können mehrere Kopien eines automatisierten Backups oder eines manuellen Snapshots erstellen, aber jede Kopie muss über eine eindeutige Kennung verfügen.

Sie können einen Snapshot innerhalb desselben kopieren AWS-Region, Sie können einen Snapshot zwischen AWS-Regionen den anderen kopieren und Sie können gemeinsam genutzte Snapshots kopieren.

Einen DB-Cluster-Snapshot können Sie nicht mit nur einem Schritt regionsübergreifend oder über Konten hinweg kopieren. Führen Sie einen Schritt für jede dieser Kopieraktionen durch. Als Alternative zum Kopieren können Sie manuelle Snapshots auch mit anderen AWS Konten teilen. Weitere Informationen finden Sie unter Freigeben eines DB-Cluster-Snapshots.

> **Note**
>
> Amazon berechnet Ihnen die Kosten basierend auf dem Aufbewahrungszeitraum und der Menge der Amazon Aurora-Sicherungs- und -Snapshot-Daten. Weitere Informationen über den Speicher, der Aurora-Backups und -Snapshots zugeordnet ist, finden Sie unter Grundlegendes zur Backup-Speicher-Nutzung in Amazon Aurora. Weitere Informationen zu den Preisen für Aurora-Speicher finden Sie unter Amazon RDS for Aurora: Preise.

Themen

Einschränkungen

Im folgenden werden einige Einschränkungen beim Kopieren von Snapshots aufgeführt:

- Sie können einen Snapshot nicht in oder aus den folgenden AWS-Regionen Quellen kopieren:
  - China (Peking)
  - China (Ningxia)
- Sie können einen Snapshot zwischen AWS GovCloud (US-Ost) und AWS GovCloud (US-West) kopieren. Sie können jedoch keinen Snapshot zwischen diesen AWS GovCloud (US) Regionen und kommerziellen Regionen kopieren. AWS-Regionen
- Wenn Sie einen Quell-Snapshot löschen, bevor der Ziel-Snapshot verfügbar ist, kann das Kopieren des Snapshots fehlschlagen. Verifizieren Sie, dass der Ziel-Snapshot den Status `AVAILABLE` hat, bevor Sie einen Quell-Snapshot löschen.
- Pro Konto können bis zu fünf Snapshot-Kopieranforderungen an eine einzelne Zielregion aktiv sein.
- Wenn Sie mehrere Snapshot-Kopien für dieselbe Quell-DB-Instance anfordern, werden diese intern in die Warteschlange gestellt. Mit den später angeforderten Kopien wird erst begonnen, wenn die vorherigen Snapshot-Kopien fertiggestellt sind. Weitere Informationen finden Sie unter Warum ist die Erstellung meines EC2-AMI- oder EBS-Snapshots langsam? im AWS Knowledge Center.
- Je nach Umfang AWS-Regionen und Menge der zu kopierenden Daten kann eine regionsübergreifende Snapshot-Kopie Stunden in Anspruch nehmen. In einigen Fällen kann es eine große Anzahl von regionsübergreifenden Snapshot-Kopieranforderungen aus einer bestimmten -Region geben. In solchen Fällen stellt Amazon RDS neue regionsübergreifende Kopieranforderungen dieser -Quellregion gegebenenfalls in eine Warteschlange, bis aktive Kopiervorgänge abgeschlossen wurden. Zu Kopieranforderungen, die sich in der Warteschlange befinden, werden keine Fortschrittsinformationen angezeigt. Fortschrittsinformationen werden angezeigt, sobald der Kopiervorgang gestartet wird.

Snapshot-Aufbewahrung

Amazon RDS löscht automatisierte Backups in verschiedenen Situationen:

- Am Ende des Aufbewahrungszeitraums.
- Wenn Sie automatisierte Backups für einen DB-Cluster deaktivieren.
- Wenn Sie einen DB-Cluster löschen.

Soll ein automatisches Backup länger aufbewahrt werden, erstellen Sie durch Kopieren einen manuellen Snapshot, der aufbewahrt wird, bis Sie ihn löschen. Amazon-RDS-Speicherkosten können für manuelle Snapshots anfallen, wenn sie Ihren Standardspeicherplatz überschreiten.

Weitere Information zu Sicherungsspeicherkosten finden Sie unter Amazon RDS – Preise.

Kopieren freigegebener Snapshots

Sie können Snapshots kopieren, die Ihnen von anderen AWS Konten zur Verfügung gestellt wurden. In einigen Fällen können Sie einen verschlüsselten Snapshot kopieren, der von einem anderen AWS Konto aus geteilt wurde. In diesen Fällen müssen Sie Zugriff auf die Datei haben AWS KMS key , mit der der Snapshot verschlüsselt wurde.

Sie können einen freigegebenen DB-Cluster-Snapshot, ob verschlüsselt oder nicht, nur in dieselbe AWS-Region kopieren. Weitere Informationen finden Sie unter Freigeben verschlüsselter Snapshots.

Umgang mit Verschlüsselungen

Sie können einen Snapshot kopieren, der mit einem KMS-Schlüssel verschlüsselt wurde. Wenn Sie einen verschlüsselten Snapshot kopieren, muss auch die Kopie des Snapshots verschlüsselt werden. Wenn Sie einen verschlüsselten Snapshot innerhalb desselben kopieren AWS-Region, können Sie die Kopie mit demselben KMS-Schlüssel wie den ursprünglichen Snapshot verschlüsseln. Oder Sie können einen anderen KMS-Schlüssel angeben.

Wenn Sie einen verschlüsselten Snapshot in andere Regionen kopieren, müssen Sie einen gültigen KMS-Schlüssel für die Ziel- AWS-Region angeben. Es kann ein regionsspezifischer KMS-Schlüssel oder ein multiregionaler Schlüssel sein. Weitere Informationen über multiregionale Schlüssel finden Sie unter Verwenden von multiregionalen Schlüsseln in AWS KMS.

Der Quell-Snapshot bleibt den gesamten Kopiervorgang über verschlüsselt. Weitere Informationen finden Sie unter Einschränkungen von Amazon Aurora-verschlüsselten DB-Clustern.

> **Note**
>
> Bei Snapshots von Amazon Aurora-DB-Clustern können Sie einen unverschlüsselten DB-Cluster-Snapshot nicht verschlüsseln, wenn Sie den Snapshot kopieren.

Inkrementelles Kopieren von Snapshots

Aurora unterstützt kein inkrementelles Kopieren von Snapshots. Aurora DB-Cluster-Snapshot-Kopien sind immer Vollkopien. Eine vollständige Snapshot-Kopie enthält alle Daten und Metadaten, die zur Wiederherstellung der DB-Cluster erforderlich sind.

Regionsübergreifende Snapshot-Kopie

Sie können DB-Cluster-Snapshots über AWS-Regionen hinweg kopieren. Es gibt jedoch bestimmte Einschränkungen und Überlegungen für das Kopieren von regionsübergreifenden Snapshots.

Je nach Umfang und AWS-Regionen Menge der zu kopierenden Daten kann es Stunden dauern, bis eine regionsübergreifende Snapshot-Kopie abgeschlossen ist.

In einigen Fällen kann es eine große Anzahl von regionsübergreifenden Snapshot-Kopieranforderungen aus einer bestimmten AWS-Region geben. In solchen Fällen kann Amazon RDS neue regionsübergreifende Kopieranfragen von dieser Quelle AWS-Region in eine Warteschlange stellen, bis einige in Bearbeitung befindliche Kopien abgeschlossen sind. Zu Kopieranforderungen, die sich in der Warteschlange befinden, werden keine Fortschrittsinformationen angezeigt. Fortschrittsinformationen werden angezeigt, sobald das Kopieren beginnt.

Wenn Sie das regionsübergreifende Kopieren von Snapshots verwenden AWS Backup , obwohl es sich bei den Kopien um vollständige Kopien handelt, fallen die Datenübertragungsgebühren inkrementell an. Weitere Informationen finden Sie unter Backup-Kopien erstellen AWS-Regionen im AWS Backup Developer Guide.

Überlegungen zu Parametergruppen

Wenn Sie einen Snapshot regionsübergreifend kopieren, enthält die Kopie nicht die vom ursprünglichen DB-Cluster verwendete Parametergruppe. Wenn Sie einen Snapshot wiederherstellen, um einen neuen DB-Cluster zu erstellen, erhält dieser DB-Cluster die Standardparametergruppe für den, in dem AWS-Region er erstellt wurde. Soll der neue DB-Cluster die gleichen Parameter wie das Original erhalten, gehen Sie folgendermaßen vor:

1. Erstellen Sie im Ziel AWS-Region eine DB-Cluster-Parametergruppe mit denselben Einstellungen wie der ursprüngliche DB-Cluster. Wenn im neuen System bereits eine vorhanden ist AWS-Region, können Sie diese verwenden.

2. Nachdem Sie den Snapshot im Ziel wiederhergestellt haben AWS-Region, ändern Sie den neuen DB-Cluster und fügen Sie die neue oder vorhandene Parametergruppe aus dem vorherigen Schritt hinzu.

Kopieren eines DB-Cluster-Snapshots

Verwenden Sie zum Kopieren eines DB-Cluster-Snapshots die in diesem Thema beschriebenen Verfahren. Wenn es sich bei der Quell-Datenbank-Engine um Aurora handelt, ist der resultierende Snapshot ein DB-Cluster-Snapshot.

Für jedes AWS Konto können Sie bis zu fünf DB-Cluster-Snapshots gleichzeitig von einem AWS-Region zum anderen kopieren. Sie können sowohl verschlüsselte als auch unverschlüsselte DB-Cluster-Snapshots kopieren. Wenn Sie einen DB-Cluster-Snapshot in einen anderen kopieren AWS-Region, erstellen Sie einen manuellen DB-Cluster-Snapshot, der in diesem AWS-Region gespeichert wird. Beim Kopieren eines DB-Cluster-Snapshots aus der Quelle AWS-Region fallen Amazon RDS-Datenübertragungsgebühren an.

Weitere Informationen zu den Kosten von Datenübertragungen finden Sie unter Amazon RDS – Preise.

Nachdem die DB-Cluster-Snapshot-Kopie in der neuen Version erstellt wurde AWS-Region, verhält sich die DB-Cluster-Snapshot-Kopie genauso wie alle anderen DB-Cluster-Snapshots in dieser Version. AWS-Region

Konsole

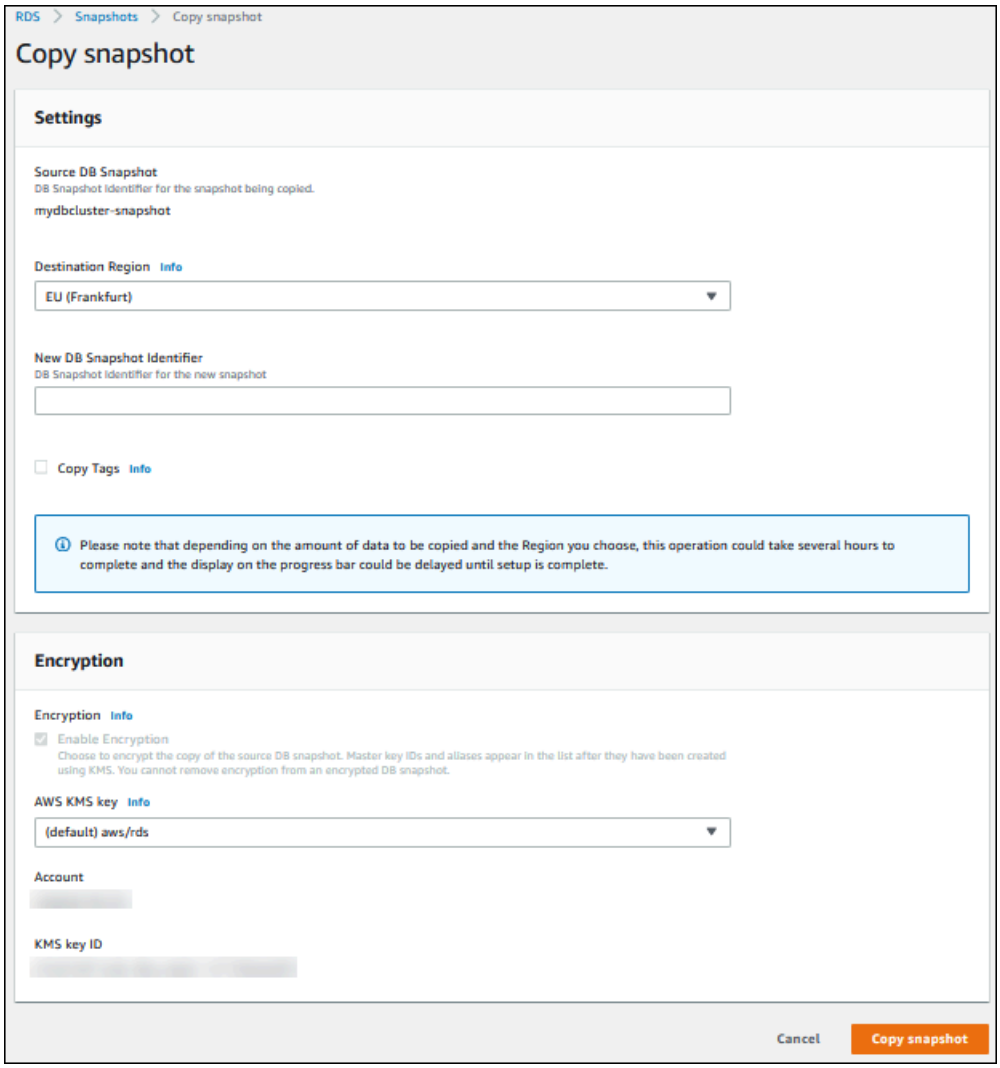
Mit diesem Verfahren kann ein verschlüsselter oder unverschlüsselter DB-Cluster-Snapshot in einer AWS-Region oder regionsübergreifend kopiert werden.

Um einen bereits laufenden Kopiervorgang abzubrechen, können Sie den DB-Cluster-Ziel-Snapshot löschen, während der DB-Cluster-Snapshot noch den Status copying hat.

So kopieren Sie einen DB-Cluster-Snapshot

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den DB-Cluster-Snapshot aus, den Sie kopieren möchten.

4. Wählen Sie für Actions (Aktionen) die Option Copy Snapshot (Snapshot kopieren). Die Seite Snapshot kopieren wird angezeigt.



5. (Optional) Um den DB-Cluster-Snapshot in eine andere zu kopieren AWS-Region, wählen Sie diese Option AWS-Region für Zielregion aus.
6. Geben Sie den Namen für die Kopie des DB-Cluster-Snapshots in das Feld New DB Snapshot Identifier (Neue DB-Snapshot-Kennung) ein.
7. Wählen Sie zum Kopieren von Tags und Werten aus dem Snapshot in die Kopie des Snapshots die Option Copy Tags (Tags kopieren).
8. Wählen Sie Copy Snapshot (Snapshot kopieren) aus.

Kopieren eines unverschlüsselten DB-Cluster-Snapshots mithilfe der AWS CLI oder Amazon RDS-API

Verwenden Sie die Verfahren in den folgenden Abschnitten, um einen unverschlüsselten DB-Cluster-Snapshot mithilfe der AWS CLI oder Amazon RDS-API zu kopieren.

Um einen bereits laufenden Kopiervorgang abzubrechen, können Sie den DB-Cluster-Ziel-Snapshot (`--target-db-cluster-snapshot-identifier` oder `TargetDBClusterSnapshotIdentifier`) löschen, während der DB-Cluster-Snapshot noch den Status copying hat.

AWS CLI

Verwenden Sie den AWS CLI copy-db-cluster-snapshotBefehl, um einen DB-Cluster-Snapshot zu kopieren. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, führen Sie den Befehl aus, in AWS-Region den der Snapshot kopiert werden soll.

Die folgenden Optionen werden zum Kopieren eines unverschlüsselten DB-Cluster-Snapshots verwendet:

- `--source-db-cluster-snapshot-identifier` – Der Bezeichner des zu kopierenden DB-Cluster-Snapshots. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, muss dieser Bezeichner das ARN-Format für die Quelle haben AWS-Region.
- `--target-db-cluster-snapshot-identifier` – Der Bezeichner für die neue Kopie des DB-Cluster-Snapshots.

Der folgende Code erstellt eine Kopie des DB-Cluster-Snapshots `arn:aws:rds:us-east-1:123456789012:cluster-snapshot:aurora-cluster1-snapshot-20130805` mit dem Namen`myclustersnapshotcopy`, AWS-Region in dem der Befehl ausgeführt wird. Beim Erstellen der Kopie werden alle Tags des ursprünglichen Snapshots in die Snapshot-Kopie übernommen.

Example

Für LinuxmacOS, oderUnix:

```
aws rds copy-db-cluster-snapshot \
  --source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:123456789012:cluster-snapshot:aurora-cluster1-snapshot-20130805 \
  --target-db-cluster-snapshot-identifier myclustersnapshotcopy \
```

```
  --copy-tags
```

Windows:

```
aws rds copy-db-cluster-snapshot ^
  --source-db-cluster-snapshot-identifier arn:aws:rds:us-east-1:123456789012:cluster-snapshot:aurora-cluster1-snapshot-20130805 ^
  --target-db-cluster-snapshot-identifier myclustersnapshotcopy ^
  --copy-tags
```

RDS-API

Verwenden Sie den Amazon ClusterSnapshot RDS-API-Vorgang CopyDB, um einen DB-Cluster-Snapshot zu kopieren. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, führen Sie die Aktion in dem aus, in den der Snapshot kopiert werden soll. AWS-Region

Die folgenden Parameter werden zum Kopieren eines unverschlüsselten DB-Cluster-Snapshots verwendet:

- `SourceDBClusterSnapshotIdentifier` – Der Bezeichner des zu kopierenden DB-Cluster-Snapshots. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, muss dieser Bezeichner das ARN-Format für die Quelle haben AWS-Region.
- `TargetDBClusterSnapshotIdentifier` – Der Bezeichner für die neue Kopie des DB-Cluster-Snapshots.

Der folgende Code erstellt eine Kopie eines Snapshots `arn:aws:rds:us-east-1:123456789012:cluster-snapshot:aurora-cluster1-snapshot-20130805` namens `myclustersnapshotcopy` in der USA West (Nordkalifornien)-Region . Beim Erstellen der Kopie werden alle Tags des ursprünglichen Snapshots in die Snapshot-Kopie übernommen.

Example

```
https://rds.us-west-1.amazonaws.com/
   ?Action=CopyDBClusterSnapshot
   &CopyTags=true
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &SourceDBSnapshotIdentifier=arn%3Aaws%3Ards%3Aus-east-1%3A123456789012%3Acluster-snapshot%3Aaurora-cluster1-snapshot-20130805
```

```
    &TargetDBSnapshotIdentifier=myclustersnapshotcopy
    &Version=2013-09-09
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20140429/us-west-1/rds/aws4_request
    &X-Amz-Date=20140429T175351Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddffed2
```

Kopieren eines verschlüsselten DB-Cluster-Snapshots mithilfe der AWS CLI oder Amazon RDS-API

Verwenden Sie die Verfahren in den folgenden Abschnitten, um einen verschlüsselten DB-Cluster-Snapshot mithilfe der AWS CLI oder Amazon RDS-API zu kopieren.

Um einen bereits laufenden Kopiervorgang abzubrechen, können Sie den DB-Cluster-Ziel-Snapshot (`--target-db-cluster-snapshot-identifier` oder `TargetDBClusterSnapshotIdentifier`) löschen, während der DB-Cluster-Snapshot noch den Status copying hat.

AWS CLI

Verwenden Sie den AWS CLI copy-db-cluster-snapshotBefehl, um einen DB-Cluster-Snapshot zu kopieren. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, führen Sie den Befehl aus, in AWS-Region den der Snapshot kopiert werden soll.

Die folgenden Optionen werden zum Kopieren eines verschlüsselten DB-Cluster-Snapshots verwendet:

- `--source-db-cluster-snapshot-identifier` – Der Bezeichner des zu kopierenden verschlüsselten DB-Cluster-Snapshots. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, muss dieser Bezeichner das ARN-Format für die Quelle haben AWS-Region.
- `--target-db-cluster-snapshot-identifier` – Der Bezeichner für die neue Kopie des verschlüsselten DB-Cluster-Snapshots.
- `--kms-key-id` - Die KMS-Schlüsselkennung für den Schlüssel, der für die Verschlüsselung der Kopie des DB-Cluster-Snapshots verwendet werden soll.

  Sie können diese Option optional verwenden, wenn der DB-Cluster-Snapshot verschlüsselt ist, Sie den Snapshot in denselben AWS-Region kopieren und einen neuen KMS-Schlüssel zum Verschlüsseln der Kopie angeben möchten. Andernfalls wird die Kopie des DB-Cluster-Snapshots mit demselben KMS-Schlüssel wie der ursprüngliche DB-Cluster-Snapshot verschlüsselt.

Sie müssen diese Option angeben, wenn der DB-Cluster-Snapshot verschlüsselt ist und Sie den Snapshot in eine andere AWS-Region kopieren. In diesem Fall müssen Sie einen KMS-Schlüssel für die Ziel- AWS-Region angeben.

Das folgende Codebeispiel kopiert den verschlüsselten DB-Cluster-Snapshot aus der Region USA West (Oregon) in die Region US East (N. Virginia). Der Befehl wird in der US East (N. Virginia)-Region aufgerufen.

Example

Für LinuxmacOS, oderUnix:

```
aws rds copy-db-cluster-snapshot \
  --source-db-cluster-snapshot-identifier arn:aws:rds:us-west-2:123456789012:cluster-snapshot:aurora-cluster1-snapshot-20161115 \
  --target-db-cluster-snapshot-identifier myclustersnapshotcopy \
  --kms-key-id my-us-east-1-key
```

Windows:

```
aws rds copy-db-cluster-snapshot ^
  --source-db-cluster-snapshot-identifier arn:aws:rds:us-west-2:123456789012:cluster-snapshot:aurora-cluster1-snapshot-20161115 ^
  --target-db-cluster-snapshot-identifier myclustersnapshotcopy ^
  --kms-key-id my-us-east-1-key
```

Der `--source-region` Parameter ist erforderlich, wenn Sie einen verschlüsselten DB-Cluster-Snapshot zwischen den Regionen AWS GovCloud (US-Ost) und AWS GovCloud (US-West) kopieren. Geben Sie für `--source-region` die AWS-Region Quell-DB-Instance an. Das AWS-Region angegebene in `source-db-cluster-snapshot-identifier` muss mit dem AWS-Region angegebenen für übereinstimmen`--source-region`.

Wenn `--source-region` nicht festgelegt ist, geben Sie einen `--pre-signed-url`-Wert an. Eine vorsignierte URL ist eine URL, die eine mit der Signaturversion 4 signierte Anforderung für den Befehl `copy-db-cluster-snapshot` enthält, die in der Quell- AWS-Region aufgerufen wird. Weitere Informationen zu dieser `pre-signed-url` Option finden Sie copy-db-cluster-snapshotin der AWS CLI Befehlsreferenz.

RDS-API

Verwenden Sie den Amazon ClusterSnapshot RDS-API-Vorgang CopyDB, um einen DB-Cluster-Snapshot zu kopieren. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, führen Sie die Aktion in dem aus, in den der Snapshot kopiert werden soll. AWS-Region

Die folgenden Parameter werden zum Kopieren eines verschlüsselten DB-Cluster-Snapshots verwendet:

- `SourceDBClusterSnapshotIdentifier` – Der Bezeichner des zu kopierenden verschlüsselten DB-Cluster-Snapshots. Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, muss dieser Bezeichner das ARN-Format für die Quelle haben AWS-Region.
- `TargetDBClusterSnapshotIdentifier` – Der Bezeichner für die neue Kopie des verschlüsselten DB-Cluster-Snapshots.
- `KmsKeyId` - Die KMS-Schlüsselkennung für den Schlüssel, der für die Verschlüsselung der Kopie des DB-Cluster-Snapshots verwendet werden soll.

  Sie können diesen Parameter optional verwenden, wenn der DB-Cluster-Snapshot verschlüsselt ist, Sie den Snapshot in denselben kopieren und einen neuen KMS-Schlüssel angeben AWS-Region, der zum Verschlüsseln der Kopie verwendet werden soll. Andernfalls wird die Kopie des DB-Cluster-Snapshots mit demselben KMS-Schlüssel wie der ursprüngliche DB-Cluster-Snapshot verschlüsselt.

  Sie müssen diesen Parameter angeben, wenn der DB-Cluster-Snapshot verschlüsselt ist und Sie den Snapshot in eine andere AWS-Region kopieren. In diesem Fall müssen Sie einen KMS-Schlüssel für die Ziel- AWS-Region angeben.
- `PreSignedUrl`— Wenn Sie den Snapshot in einen anderen kopieren AWS-Region, müssen Sie den `PreSignedUrl` Parameter angeben. Der `PreSignedUrl` Wert muss eine URL sein, die eine mit Signature Version 4 signierte Anforderung für den Aufruf der `CopyDBClusterSnapshot` Aktion in der Quelle AWS-Region enthält, aus der der DB-Cluster-Snapshot kopiert wurde. Weitere Informationen zur Verwendung einer vorsignierten URL finden Sie unter ClusterSnapshotCopyDB.

Das folgende Codebeispiel kopiert den verschlüsselten DB-Cluster-Snapshot aus der Region USA West (Oregon) in die Region US East (N. Virginia). Die Aktion wird in der US East (N. Virginia)-Region aufgerufen.

Example

```
https://rds.us-east-1.amazonaws.com/
    ?Action=CopyDBClusterSnapshot
    &KmsKeyId=my-us-east-1-key
    &PreSignedUrl=https%253A%252F%252Frds.us-west-2.amazonaws.com%252F
         %253FAction%253DCopyDBClusterSnapshot
         %2526DestinationRegion%253Dus-east-1
         %2526KmsKeyId%253Dmy-us-east-1-key
         %2526SourceDBClusterSnapshotIdentifier%253Darn%25253Aaws%25253Ards
%25253Aus-west-2%25253A123456789012%25253Acluster-snapshot%25253Aaurora-cluster1-
snapshot-20161115
         %2526SignatureMethod%253DHmacSHA256
         %2526SignatureVersion%253D4
         %2526Version%253D2014-10-31
         %2526X-Amz-Algorithm%253DAWS4-HMAC-SHA256
         %2526X-Amz-Credential%253DAKIADQKE4SARGYLE%252F20161117%252Fus-west-2%252Frds
%252Faws4_request
         %2526X-Amz-Date%253D20161117T215409Z
         %2526X-Amz-Expires%253D3600
         %2526X-Amz-SignedHeaders%253Dcontent-type%253Bhost%253Buser-agent%253Bx-amz-
content-sha256%253Bx-amz-date
         %2526X-Amz-Signature
%253D255a0f17b4e717d3b67fad163c3ec26573b882c03a65523522cf890a67fca613
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &SourceDBClusterSnapshotIdentifier=arn%3Aaws%3Ards%3Aus-
west-2%3A123456789012%3Acluster-snapshot%3Aaurora-cluster1-snapshot-20161115
    &TargetDBClusterSnapshotIdentifier=myclustersnapshotcopy
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20161117/us-east-1/rds/aws4_request
    &X-Amz-Date=20161117T221704Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=da4f2da66739d2e722c85fcfd225dc27bba7e2b8dbea8d8612434378e52adccf
```

Der `PreSignedUrl` Parameter ist erforderlich, wenn Sie einen verschlüsselten DB-Cluster-Snapshot zwischen den Regionen AWS GovCloud (US-Ost) und AWS GovCloud (US-West) kopieren. Der `PreSignedUrl` Wert muss eine URL sein, die eine mit Signature Version 4 signierte Anforderung enthält, damit der `CopyDBClusterSnapshot` Vorgang in der Quelle AWS-Region aufgerufen

wird, aus der der DB-Cluster-Snapshot kopiert wurde. Weitere Informationen zur Verwendung einer vorsignierten URL finden Sie unter CopyDB ClusterSnapshot in der Amazon RDS-API-Referenz.

Um eine vorsignierte URL automatisch und nicht manuell zu generieren, verwenden Sie stattdessen den AWS CLI copy-db-cluster-snapshotBefehl mit der `--source-region` Option.

Kopieren eines DB-Cluster-Snapshots in ein anderes Konto

Sie können anderen AWS Konten ermöglichen, von Ihnen angegebene DB-Cluster-Snapshots zu kopieren, indem Sie die Amazon RDS-API `ModifyDBClusterSnapshotAttribute` und `CopyDBClusterSnapshot` Aktionen verwenden. DB-Cluster-Snapshots können nur in der ursprünglichen AWS-Region in ein anderes Konto kopiert werden. Für das kontoübergreifende Kopieren macht Konto A den Snapshot zum Kopieren verfügbar und Konto B kopiert den Snapshot.

1. Rufen Sie unter Verwendung von Konto A `ModifyDBClusterSnapshotAttribute` auf und geben Sie **`restore`** für den Parameter `AttributeName` und die ID für Konto B für den Parameter `ValuesToAdd` an.
2. (Wenn der Snapshot verschlüsselt ist) Aktualisieren Sie unter Verwendung von Konto A die Schlüsselrichtlinie für den KMS-Schlüssel, fügen Sie den ARN von Konto B zuerst als `Principal` hinzu und erlauben Sie dann die Aktion `kms:CreateGrant`
3. (Wenn der Snapshot verschlüsselt ist) Verwenden Sie Konto B und wählen oder erstellen Sie einen Benutzer. Hängen Sie eine IAM-Richtlinie an den Benutzer an, die ihm das Kopieren eines verschlüsselten DB-Cluster-Snapshots unter Verwendung Ihres KMS-Schlüssels erlaubt.
4. Rufen Sie unter Verwendung von Konto B `CopyDBClusterSnapshot` auf und verwenden Sie den Parameter `SourceDBClusterSnapshotIdentifier`, um den ARN des zu kopierenden DB-Cluster-Snapshots anzugeben, der die ID für Konto A enthalten muss.

Verwenden Sie die API-Operation DescribeDB SnapshotAttributes oder DescribeDB, um alle AWS Konten aufzulisten, die zur Wiederherstellung eines DB-Cluster-Snapshots berechtigt sind. ClusterSnapshotAttributes

Um die Freigabeberechtigung für ein AWS Konto zu entfernen, verwenden Sie die `ModifyDBClusterSnapshotAttribute` Aktion `ModifyDBSnapshotAttribute` oder mit der `AttributeName` Einstellung auf `restore` und der ID des zu entfernenden Kontos im Parameter. `ValuesToRemove`

Kopieren eines unverschlüsselten DB-Cluster-Snapshots in ein anderes Konto

Verwenden Sie das folgende Verfahren, um einen unverschlüsselten DB-Cluster-Snapshot in ein anderes Konto in derselben AWS-Region zu kopieren.

1. Rufen Sie im Quellkonto für den DB-Cluster-Snapshot `ModifyDBClusterSnapshotAttribute` auf und geben Sie **`restore`** für den Parameter `AttributeName` und die ID für das Zielkonto für den Parameter `ValuesToAdd` an.

   Das Ausführen des folgenden Beispiels mit dem Konto `987654321` gewährt den beiden mit den Bezeichnern AWS und `123451234512` angegebenen `123456789012`-Konten das Recht zum Wiederherstellen des DB-Cluster-Snapshots mit dem Namen `manual-snapshot1`.

   ```
   https://rds.us-west-2.amazonaws.com/
    ?Action=ModifyDBClusterSnapshotAttribute
    &AttributeName=restore
    &DBClusterSnapshotIdentifier=manual-snapshot1
    &SignatureMethod=HmacSHA256&SignatureVersion=4
    &ValuesToAdd.member.1=123451234512
    &ValuesToAdd.member.2=123456789012
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20150922/us-west-2/rds/aws4_request
    &X-Amz-Date=20150922T220515Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=ef38f1ce3dab4e1dbf113d8d2a265c67d17ece1999ffd36be85714ed36dddbb3
   ```

2. Rufen Sie im Zielkonto `CopyDBClusterSnapshot` auf und verwenden Sie den Parameter `SourceDBClusterSnapshotIdentifier`, um den ARN des zu kopierenden DB-Cluster-Snapshots anzugeben, der die ID für das Quellkonto enthalten muss.

   Das Ausführen des folgenden Beispiels mit dem Konto `123451234512` kopiert den DB-Cluster-Snapshot `aurora-cluster1-snapshot-20130805` aus dem Konto `987654321` und erstellt einen DB-Cluster-Snapshot namens `dbclustersnapshot1`.

   ```
   https://rds.us-west-2.amazonaws.com/
      ?Action=CopyDBClusterSnapshot
      &CopyTags=true
      &SignatureMethod=HmacSHA256
      &SignatureVersion=4
      &SourceDBClusterSnapshotIdentifier=arn:aws:rds:us-west-2:987654321:cluster-
   snapshot:aurora-cluster1-snapshot-20130805
   ```

```
   &TargetDBClusterSnapshotIdentifier=dbclustersnapshot1
   &Version=2013-09-09
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20150922/us-west-2/rds/aws4_request
   &X-Amz-Date=20140429T175351Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-
date
   &X-Amz-
Signature=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddffed2
```

Kopieren eines verschlüsselten DB-Cluster-Snapshots in ein anderes Konto

Verwenden Sie das folgende Verfahren, um einen verschlüsselten DB-Cluster-Snapshot in ein anderes Konto in derselben AWS-Region zu kopieren.

1. Rufen Sie im Quellkonto für den DB-Cluster-Snapshot `ModifyDBClusterSnapshotAttribute` auf und geben Sie **`restore`** für den Parameter `AttributeName` und die ID für das Zielkonto für den Parameter `ValuesToAdd` an.

   Wenn Sie das folgende Beispiel mit dem Konto ausführen, `987654321` können zwei AWS Konto-IDs `123451234512` und `123456789012` der angegebene `manual-snapshot1` DB-Cluster-Snapshot wiederhergestellt werden.

   ```
   https://rds.us-west-2.amazonaws.com/
    ?Action=ModifyDBClusterSnapshotAttribute
    &AttributeName=restore
    &DBClusterSnapshotIdentifier=manual-snapshot1
    &SignatureMethod=HmacSHA256&SignatureVersion=4
    &ValuesToAdd.member.1=123451234512
    &ValuesToAdd.member.2=123456789012
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20150922/us-west-2/rds/aws4_request
    &X-Amz-Date=20150922T220515Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=ef38f1ce3dab4e1dbf113d8d2a265c67d17ece1999ffd36be85714ed36dddbb3
   ```

2. Erstellen Sie im Quellkonto für den DB-Cluster-Snapshot einen benutzerdefinierten KMS-Schlüssel, der dem verschlüsselten DB-Cluster-Snapshot entspricht AWS-Region . Bei der Erstellung des vom Kunden verwalteten Schlüssels gewähren Sie dem Ziel Zugriff darauf AWS-

Konto. Weitere Informationen finden Sie unter Erstellen Sie einen vom Kunden verwalteten Schlüssel und gewähren Sie Zugriff darauf.

3. Kopieren Sie den Snapshot und teilen Sie ihn für das Ziel AWS-Konto. Weitere Informationen finden Sie unter Kopieren Sie den Snapshot aus dem Quellkonto und teilen Sie ihn.
4. Rufen Sie im Zielkonto `CopyDBClusterSnapshot` auf und verwenden Sie den Parameter `SourceDBClusterSnapshotIdentifier`, um den ARN des zu kopierenden DB-Cluster-Snapshots anzugeben, der die ID für das Quellkonto enthalten muss.

   Das Ausführen des folgenden Beispiels mit dem Konto `123451234512` kopiert den DB-Cluster-Snapshot `aurora-cluster1-snapshot-20130805` aus dem Konto `987654321` und erstellt einen DB-Cluster-Snapshot namens `dbclustersnapshot1`.

```
https://rds.us-west-2.amazonaws.com/
   ?Action=CopyDBClusterSnapshot
   &CopyTags=true
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &SourceDBClusterSnapshotIdentifier=arn:aws:rds:us-west-2:987654321:cluster-
snapshot:aurora-cluster1-snapshot-20130805
   &TargetDBClusterSnapshotIdentifier=dbclustersnapshot1
   &Version=2013-09-09
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20150922/us-west-2/rds/aws4_request
   &X-Amz-Date=20140429T175351Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-
date
   &X-Amz-
Signature=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddffed2
```

Freigeben eines DB-Cluster-Snapshots

Mithilfe von Amazon RDS können Sie einen manuellen DB-Cluster-Snapshot wie folgt freigeben:

- Die Freigabe eines manuellen DB-Cluster-Snapshots, ob verschlüsselt oder nicht verschlüsselt, ermöglicht autorisierten AWS -Konten, den Snapshot zu kopieren.
- Die Freigabe eines manuellen DB-Cluster-Snapshots, ob verschlüsselt oder nicht verschlüsselt, ermöglicht autorisierten AWS -Konten die direkte Wiederherstellung eines DB-Clusters aus dem Snapshot, statt eine Kopie des DB-Clusters zu erstellen und es aus dieser Kopie wiederherzustellen.

> **Note**
>
> Um einen automatisierten DB-Cluster-Snapshot freizugeben, erstellen Sie einen manuellen DB-Cluster-Snapshot, indem Sie den automatisierten Snapshot kopieren und diese Kopie dann freigeben. Dieser Vorgang gilt auch für Ressourcen, die von AWS Backup generiert wurden.

Weitere Informationen zum Kopieren von Snapshots finden Sie unter Kopieren eines DB-Cluster-Snapshots. Weitere Informationen zum Wiederherstellen einer DB-Instance aus einem DB-Cluster-Snapshot finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.

Weitere Informationen zum Wiederherstellen eines DB-Clusters aus einem DB-Cluster-Snapshot finden Sie unter Übersicht über das Sichern und Wiederherstellen eines Aurora-DB-Clusters.

Sie können einen manuellen Snapshot mit bis zu 20 anderen teilen AWS-Konten.

Die folgende Einschränkung gilt, wenn Sie manuelle Schnappschüsse mit anderen AWS-Konten teilen:

- Wenn Sie einen DB-Cluster aus einem gemeinsam genutzten Snapshot mithilfe der AWS Command Line Interface (AWS CLI) oder der Amazon RDS-API wiederherstellen, müssen Sie den Amazon-Ressourcennamen (ARN) des gemeinsam genutzten Snapshots als Snapshot-ID angeben.

Inhalt

Freigeben eines Snapshots

Sie können einen DB-Cluster-Snapshot mit der AWS Management Console AWS CLI, oder der RDS-API teilen.

Konsole

Mithilfe der Amazon RDS-Konsole können Sie einen manuellen DB-Cluster-Snapshot mit bis zu 20 teilen AWS-Konten. Sie können die Konsole auch verwenden, um die Freigabe eines manuellen Snapshots für ein oder mehrere Konten zu beenden.

Freigeben eines manuellen DB-Cluster-Snapshots über die Amazon RDS-Konsole

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den manuellen Snapshot, den Sie freigeben möchten.
4. Wählen Sie unter Actions (Aktionen) die Option Share Snapshots (Snapshot freigeben).
5. Wählen Sie für DB Snapshot Visibility (Sichtbarkeit des DB-Snapshots) eine der folgenden Optionen.

   - Wenn die Quelle unverschlüsselt ist, wählen Sie Öffentlich, um allen AWS-Konten zu erlauben, einen DB-Cluster aus Ihrem manuellen DB-Cluster-Snapshot wiederherzustellen, oder wählen Sie Privat, um nur zu erlauben AWS-Konten , dass Sie einen DB-Cluster aus Ihrem manuellen DB-Cluster-Snapshot wiederherstellen dürfen.

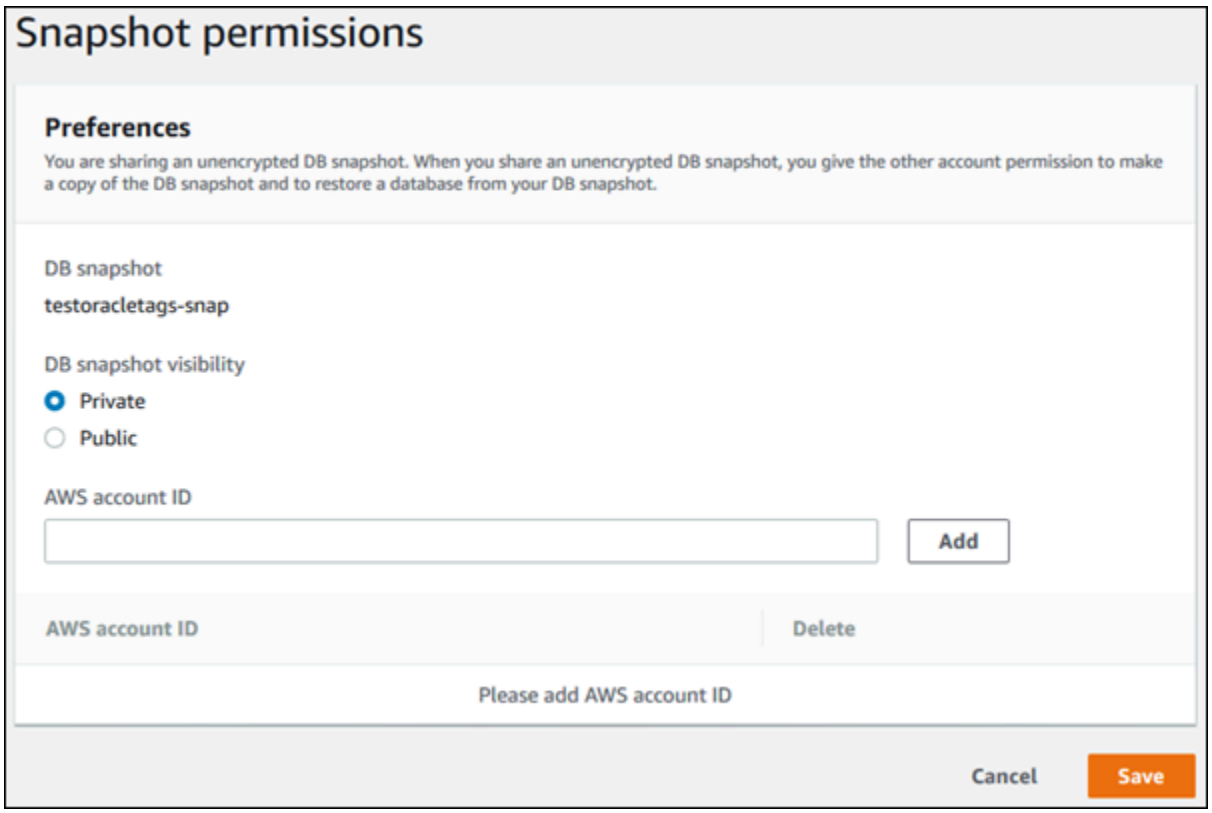
> **Warning**
>
> Wenn Sie die Sichtbarkeit von DB-Snapshots auf Öffentlich setzen, AWS-Konten können alle einen DB-Cluster aus Ihrem manuellen DB-Cluster-Snapshot wiederherstellen und haben Zugriff auf Ihre Daten. Geben Sie keine manuellen DB-Cluster-Snapshots als Public (Öffentlich) frei, die private Informationen enthalten. Weitere Informationen finden Sie unter Freigeben öffentlicher Snapshots.

- Ist die Quelle verschlüsselt, ist DB Snapshot Visibility (Sichtbarkeit des DB-Snapshots) auf Private (Privat) festgelegt, da verschlüsselte Snapshots nicht als öffentlich freigegeben werden können.

> **Note**
>
> Snapshots, die mit der Standardeinstellung verschlüsselt wurden, AWS KMS key können nicht geteilt werden. Informationen zur Umgehung dieses Problems finden Sie unterFreigeben verschlüsselter Snapshots.

6. Geben Sie AWS unter Konto-ID die AWS-Konto Kennung für ein Konto ein, dem Sie die Wiederherstellung eines DB-Clusters aus Ihrem manuellen Snapshot erlauben möchten, und wählen Sie dann Hinzufügen aus. Wiederholen Sie den Vorgang, um weitere AWS-Konto Identifikatoren (bis zu 20 AWS-Konten) hinzuzufügen.

   Wenn Ihnen beim Hinzufügen einer AWS-Konto Kennung zur Liste der zulässigen Konten ein Fehler unterläuft, können Sie sie aus der Liste löschen, indem Sie rechts neben der falschen AWS-Konto Kennung die Option Löschen wählen.



7. Nachdem Sie Kennungen für alle hinzugefügt haben AWS-Konten , denen Sie die Wiederherstellung des manuellen Snapshots erlauben möchten, wählen Sie Speichern, um Ihre Änderungen zu speichern.

AWS CLI

Verwenden Sie den Befehl `aws rds modify-db-cluster-snapshot-attribute`, um einen DB-Cluster-Snapshot freizugeben. Verwenden Sie den `--values-to-add` Parameter, um eine Liste der IDs für diejenigen hinzuzufügen AWS-Konten , die berechtigt sind, den manuellen Snapshot wiederherzustellen.

Example einen Snapshot mit einem einzigen Konto teilen

Im folgenden Beispiel wird AWS-Konto Identifier aktiviert`123456789012`, um den genannten DB-Cluster-Snapshot wiederherzustellen`cluster-3-snapshot`.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster-snapshot-attribute \
--db-cluster-snapshot-identifier cluster-3-snapshot \
--attribute-name restore \
```

```
--values-to-add 123456789012
```

Windows:

```
aws rds modify-db-cluster-snapshot-attribute ^
--db-cluster-snapshot-identifier cluster-3-snapshot ^
--attribute-name restore ^
--values-to-add 123456789012
```

Example einen Snapshot mit mehreren Konten teilen

Im folgenden Beispiel werden zwei AWS-Konto Identifikatoren aktiviert, `111122223333` und`444455556666`, um den genannten `manual-cluster-snapshot1` DB-Cluster-Snapshot wiederherzustellen.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster-snapshot-attribute \
--db-cluster-snapshot-identifier manual-cluster-snapshot1 \
--attribute-name restore \
--values-to-add {"111122223333","444455556666"}
```

Windows:

```
aws rds modify-db-cluster-snapshot-attribute ^
--db-cluster-snapshot-identifier manual-cluster-snapshot1 ^
--attribute-name restore ^
--values-to-add "[\"111122223333\",\"444455556666\"]"
```

> **Note**
>
> Bei Verwendung der Windows-Befehlszeile müssen doppelte Anführungszeichen (") im JSON-Code mit einem umgekehrten Schrägstrich (\) als Escape-Zeichen versehen werden.

Verwenden Sie den `describe-db-cluster-snapshot-attributes` AWS CLI Befehl, um die für die Wiederherstellung eines Snapshots AWS-Konten aktivierten Dateien aufzulisten.

RDS-API

Mithilfe der Amazon RDS-API können Sie auch einen manuellen DB-Cluster-Snapshot mit anderen AWS-Konten teilen. Rufen Sie dazu die Operation `ModifyDBClusterSnapshotAttribute` auf. Geben Sie `restore` für an und verwenden Sie den `ValuesToAdd` Parameter`AttributeName`, um eine Liste der IDs hinzuzufügen AWS-Konten , die berechtigt sind, den manuellen Snapshot wiederherzustellen.

Um einen manuellen Snapshot öffentlich und für alle wiederherstellbar zu machen AWS-Konten, verwenden Sie den Wert`all`. Achten Sie jedoch darauf, den `all` Wert nicht für manuelle Snapshots hinzuzufügen, die private Informationen enthalten, die nicht für alle verfügbar sein sollen. AWS-Konten Darüber hinaus sollten Sie `all` nicht für verschlüsselte Snapshots angeben, da die öffentliche Bereitstellung dieser Snapshots nicht unterstützt wird.

Verwenden Sie die `DescribeDBClusterSnapshotAttributes`API-Operation, um alle Dateien aufzulisten, die zur Wiederherstellung eines Snapshots AWS-Konten berechtigt sind.

Freigeben öffentlicher Snapshots

Sie können einen unverschlüsselten manuellen Snapshot als öffentlich freigeben, wodurch der Snapshot für alle AWS-Konten verfügbar ist. Achten Sie bei der Freigabe eines Snapshots als öffentlich darauf, dass in Ihren öffentlichen Snapshots keine privaten Informationen enthalten sind.

Wenn ein Snapshot öffentlich geteilt wird, gibt er allen die AWS-Konten Erlaubnis, den Snapshot zu kopieren und daraus DB-Cluster zu erstellen.

Die Speicherung von Backups öffentlicher Snapshots anderer Konten wird Ihnen nicht in Rechnung gestellt. Ihnen werden nur Ihre eigenen Snapshots berechnet.

Wenn Sie einen öffentlichen Snapshot kopieren, sind Sie der Eigentümer der Kopie. Ihnen wird die Speicherung von Backups Ihrer Snapshot-Kopie in Rechnung gestellt. Wenn Sie einen DB-Cluster aus einem öffentlichen Snapshot erstellen, wird Ihnen dieser DB-Cluster in Rechnung gestellt. Informationen zur Preisgestaltung von Amazon Aurora finden Sie in der Aurora-Preisliste.

Sie können nur Ihre eigenen öffentlichen Snapshots löschen. Um einen geteilten oder öffentlichen Snapshot zu löschen, stellen Sie sicher, dass Sie sich bei demjenigen anmelden AWS-Konto , dem der Snapshot gehört.

Öffentliche Snapshots anzeigen, die anderen gehören AWS-Konten

Sie können öffentliche Snapshots, die anderen Konten eines bestimmten Kontos gehören, AWS-Region auf der Registerkarte Öffentlich auf der Seite Snapshots in der Amazon RDS-Konsole anzeigen. Ihre Snapshots (die Ihrem Konto gehören) werden auf dieser Registerkarte nicht angezeigt.

So rufen Sie öffentliche Snapshots auf

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie die Registerkarte Public (Öffentlich).

   Die öffentlichen Snapshots werden angezeigt. Sie können in der Spalte Owner (Eigentümer) sehen, welches Konto einen öffentlichen Snapshot besitzt.

   > **Note**
   >
   > Möglicherweise müssen Sie die Seiteneinstellungen ändern, indem Sie das Zahnradsymbol oben rechts im Bereich Public Snapshots (Öffentliche Snapshots aufrufen, damit diese Spalte eingeblendet wird.

Aufrufen Ihrer eigenen öffentlichen Snapshots

Sie können den folgenden AWS CLI Befehl (nur Unix) verwenden, um die öffentlichen Snapshots anzuzeigen, die Ihnen AWS-Konto gehören. AWS-Region

```
aws rds describe-db-cluster-snapshots --snapshot-type public --include-public |
 grep account_number
```

Die zurückgegebene Ausgabe ähnelt bei öffentlichen Snapshots dem folgenden Beispiel.

```
"DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:myclustersnapshot1",
"DBClusterSnapshotArn": "arn:aws:rds:us-west-2:123456789012:cluster-
snapshot:myclustersnapshot2",
```

Teilen von öffentlichen Snapshots aus veralteten DB-Engine-Versionen

Das Wiederherstellen oder Kopieren von öffentlichen Snapshots aus veralteten DB-Engine-Versionen wird nicht unterstützt. Gehen Sie wie folgt vor, um Ihren vorhandenen öffentlichen Snapshot, der nicht unterstützt wird, zum Wiederherstellen oder Kopieren verfügbar zu machen:

1. Markieren Sie den Snapshot als privat.
2. Stellen Sie den Snapshot wieder her.
3. Führen Sie ein Upgrade des wiederhergestellten DB-Clusters auf eine unterstützte Engine-Version durch.
4. Erstellen Sie einen neuen Snapshot.
5. Teilen Sie den Snapshot erneut öffentlich.

Freigeben verschlüsselter Snapshots

Sie können DB-Cluster-Snapshots freigeben, die während der Speicherung mittels des AES-256-Verschlüsselungsalgorithmus verschlüsselt wurden, wie in Verschlüsseln von Amazon Aurora-Ressourcen beschrieben.

Die folgenden Einschränkungen gelten für die Freigabe verschlüsselter Snapshots:

- Sie können verschlüsselte Snapshots nicht als öffentlich freigeben.
- Sie können keinen Snapshot teilen, der mit dem Standard-KMS-Schlüssel desjenigen verschlüsselt wurde AWS-Konto , der den Snapshot geteilt hat.

Gehen Sie wie folgt vor, um das Problem mit dem standardmäßigen KMS-Schlüssel zu umgehen:

1. Erstellen Sie einen vom Kunden verwalteten Schlüssel und gewähren Sie Zugriff darauf.
2. Kopieren Sie den Snapshot aus dem Quellkonto und teilen Sie ihn.
3. Kopieren Sie den gemeinsam genutzten Snapshot in das Zielkonto.

Erstellen Sie einen vom Kunden verwalteten Schlüssel und gewähren Sie Zugriff darauf

Zunächst erstellen Sie einen benutzerdefinierten KMS-Schlüssel im selben Format AWS-Region wie der verschlüsselte DB-Cluster-Snapshot. Bei der Erstellung des vom Kunden verwalteten Schlüssels gewähren Sie einem anderen Benutzer Zugriff darauf AWS-Konto.

Um einen vom Kunden verwalteten Schlüssel zu erstellen und Zugriff darauf zu gewähren

1. Melden Sie sich AWS Management Console von der Quelle aus bei an AWS-Konto.
2. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.
3. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
4. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.
5. Klicken Sie auf Create key.
6. Gehen Sie auf der Seite „Schlüssel konfigurieren“ wie folgt vor:
    a. Wählen Sie als Schlüsseltyp die Option Symmetrisch aus.
    b. Wählen Sie unter Schlüsselverwendung die Option Verschlüsseln und entschlüsseln aus.
    c. Erweitern Sie Advanced options (Erweiterte Optionen).
    d. Wählen Sie für Herkunft des Schlüsselmaterials die Option KMS aus.
    e. Wählen Sie für Regionalität die Option Single Region Key aus.
    f. Wählen Sie Weiter aus.
7. Gehen Sie auf der Seite Labels hinzufügen wie folgt vor:
    a. Geben Sie für Alias einen Anzeigenamen für Ihren KMS-Schlüssel ein, z. **`share-snapshot`** B.
    b. (Optional) Geben Sie eine Beschreibung für Ihren KMS-Schlüssel ein.
    c. (Optional) Fügen Sie Ihrem KMS-Schlüssel Tags hinzu.
    d. Wählen Sie Weiter aus.
8. Klicken Sie auf der Seite Definieren wichtiger administrativer Berechtigungen auf Weiter.
9. Gehen Sie auf der Seite Schlüsselverwendungsberechtigungen definieren wie folgt vor:
    a. Wählen Sie für Andere AWS-Konten die Option Weitere hinzufügen aus AWS-Konto.
    b. Geben Sie die ID der Datei ein, AWS-Konto auf die Sie Zugriff gewähren möchten.

Sie können mehreren Zugriff gewähren AWS-Konten.

c. Wählen Sie Weiter aus.

10. Überprüfen Sie Ihren KMS-Schlüssel und wählen Sie dann Fertig stellen.

Kopieren Sie den Snapshot aus dem Quellkonto und teilen Sie ihn

Als Nächstes kopieren Sie den Quell-DB-Cluster-Snapshot mithilfe des vom Kunden verwalteten Schlüssels in einen neuen Snapshot. Dann teilen Sie ihn mit dem Ziel AWS-Konto.

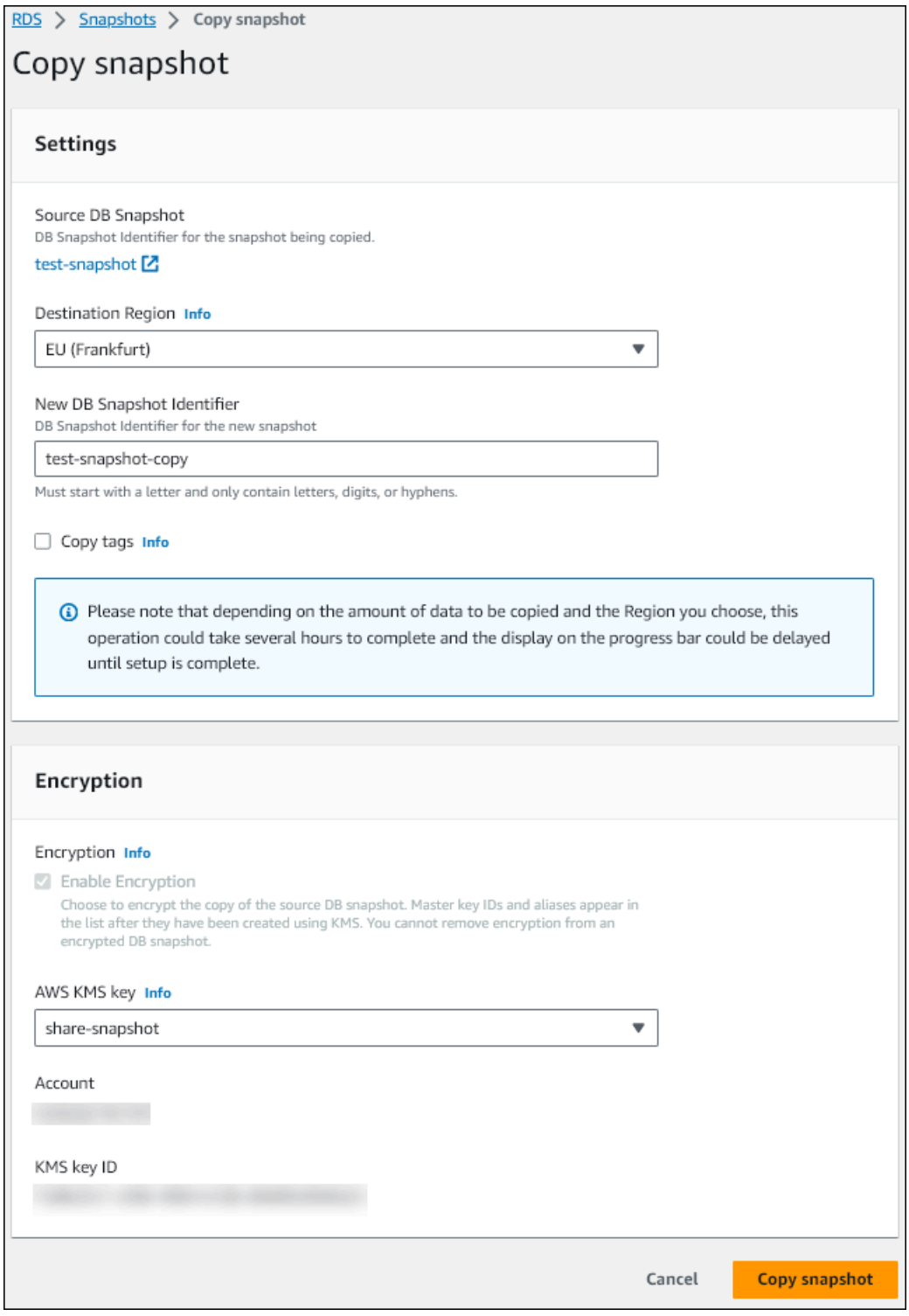
Um den Snapshot zu kopieren und zu teilen

1. Melden Sie sich bei der AWS Management Console von der Quelle aus an AWS-Konto.
2. Öffnen Sie die Amazon RDS-Konsole unter https://console.aws.amazon.com/rds/
3. Wählen Sie im Navigationsbereich die Option Snapshots.
4. Wählen Sie den DB-Cluster-Snapshot aus, den Sie kopieren möchten.
5. Wählen Sie für Actions (Aktionen) die Option Copy Snapshot (Snapshot kopieren).
6. Gehen Sie auf der Seite Snapshot kopieren wie folgt vor:

   a. Wählen Sie als Zielregion die Region aus, AWS-Region in der Sie den vom Kunden verwalteten Schlüssel im vorherigen Verfahren erstellt haben.

   b. Geben Sie den Namen für die Kopie des DB-Cluster-Snapshots in das Feld New DB Snapshot Identifier (Neue DB-Snapshot-Kennung) ein.

   c. Wählen Sie für AWS KMS keyden vom Kunden verwalteten Schlüssel aus, den Sie erstellt haben.



d. Wählen Sie Copy Snapshot (Snapshot kopieren) aus.

7. Wenn die Snapshot-Kopie verfügbar ist, wählen Sie sie aus.
8. Wählen Sie unter Actions (Aktionen) die Option Share Snapshots (Snapshot freigeben).
9. Gehen Sie auf der Seite Snapshot-Berechtigungen wie folgt vor:

a. Geben Sie die AWS-Konto ID ein, mit der Sie die Snapshot-Kopie teilen, und wählen Sie dann Hinzufügen.
b. Wählen Sie Speichern.

Der Snapshot wird geteilt.

Kopieren Sie den gemeinsam genutzten Snapshot in das Zielkonto

Jetzt können Sie den gemeinsam genutzten Snapshot in das Ziel kopieren AWS-Konto.

Um den gemeinsam genutzten Snapshot zu kopieren

1. Melden Sie sich vom Ziel AWS Management Console aus beim an AWS-Konto.
2. Öffnen Sie die Amazon RDS-Konsole unter https://console.aws.amazon.com/rds/
3. Wählen Sie im Navigationsbereich die Option Snapshots.
4. Wählen Sie den Tab Mit mir geteilt.
5. Wählen Sie den geteilten Snapshot aus.
6. Wählen Sie für Actions (Aktionen) die Option Copy Snapshot (Snapshot kopieren).
7. Wählen Sie Ihre Einstellungen für das Kopieren des Snapshots wie im vorherigen Verfahren, verwenden Sie jedoch eine AWS KMS key , die zum Zielkonto gehört.

   Wählen Sie Copy Snapshot (Snapshot kopieren) aus.

Das Teilen von Snapshots wird beendet

Um die gemeinsame Nutzung eines DB-Cluster-Snapshots zu beenden, entziehen Sie dem Ziel die Berechtigung AWS-Konto.

Konsole

Um die gemeinsame Nutzung eines manuellen DB-Cluster-Snapshots mit einem zu beenden AWS-Konto

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

3. Wählen Sie den manuellen Snapshot, für den Sie die Freigabe beenden möchten.
4. Wählen Sie die Option Actions (Aktionen) und anschließend Share Snapshot (Snapshot teilen) aus.
5. Um die Erlaubnis für ein zu entfernen AWS-Konto, wählen Sie Löschen als AWS Konto-ID für dieses Konto aus der Liste der autorisierten Konten.
6. Wählen Sie Speichern, um Ihre Änderungen zu speichern.

CLI

Verwenden Sie den `--values-to-remove` Parameter, um einen AWS-Konto Bezeichner aus der Liste zu entfernen.

Example das Stoppen der Snapshot-Freigabe

Das folgende Beispiel verhindert, dass AWS-Konto ID 444455556666 den Snapshot wiederherstellt.

LinuxmacOSUnixFür, oder:

```
aws rds modify-db-cluster-snapshot-attribute \
--db-cluster-snapshot-identifier manual-cluster-snapshot1 \
--attribute-name restore \
--values-to-remove 444455556666
```

Windows:

```
aws rds modify-db-cluster-snapshot-attribute ^
--db-cluster-snapshot-identifier manual-cluster-snapshot1 ^
--attribute-name restore ^
--values-to-remove 444455556666
```

RDS-API

Um die Freigabeberechtigung für eine zu entfernen AWS-Konto, verwenden Sie die `ModifyDBClusterSnapshotAttribute`Operation mit `AttributeName` set to `restore` und dem `ValuesToRemove` Parameter. Um einen manuellen Snapshot als privat zu markieren, entfernen Sie den Wert `all` aus der Liste der Werte für das Attribut `restore`.

Exportieren von DB-Cluster-Daten nach Amazon S3

Sie können Daten aus einem Live-DB-Cluster von Amazon Aurora in einen Amazon-S3-Bucket exportieren. Der Exportprozess läuft im Hintergrund und beeinträchtigt nicht die Leistung Ihres aktiven DB-Clusters.

Standardmäßig werden alle Daten im DB-Cluster exportiert. Sie können sich jedoch dafür entscheiden, bestimmte Sätze von Datenbanken, Schemata oder Tabellen zu exportieren.

Amazon Aurora klont den DB-Cluster, extrahiert Daten aus dem Klon und speichert die Daten in einem Amazon-S3-Bucket. Die Daten werden in einem Apache Parquet-Format gespeichert, das komprimiert und konsistent ist. Einzelne Parquet-Dateien sind normalerweise 1—10 MB groß.

Die schnellere Leistung, die Sie mit dem Export von Snapshot-Daten für Aurora MySQL Version 2 und Version 3 erzielen können, gilt nicht für den Export von DB-Cluster-Daten. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Snapshot-Daten nach Amazon S3.

Der Export des gesamten DB-Clusters wird Ihnen in Rechnung gestellt, unabhängig davon, ob Sie alle oder nur einen Teil der Daten exportieren. Weitere Informationen finden Sie auf der Seite Amazon-Aurora-Preise.

Nachdem die Daten exportiert wurden, können Sie die exportierten Daten direkt mit Tools wie Amazon Athena oder Amazon Redshift Spectrum analysieren. Weitere Informationen zur Verwendung von Athena zum Lesen von Parquet-Daten finden Sie unter Parquet SerDe im Amazon Athena Athena-Benutzerhandbuch. Weitere Informationen zur Verwendung von Redshift Spectrum zum Lesen von Parquet-Daten finden Sie unter COPY from columnar data formats im Amazon Redshift Database Developer Guide.

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen zur Versions- und Regionsverfügbarkeit beim Exportieren von DB-Cluster-Daten nach S3 finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für den Export von Clusterdaten nach Amazon S3.

Themen

- Überwachen von DB-Cluster-Exportaufgaben
- Abbrechen einer DB-Cluster-Exportaufgabe
- Fehlermeldungen für Amazon-S3-Exportaufgaben
- Fehlerbehebung bei PostgreSQL-Berechtigungsfehlern
- Benennungskonvention für Dateien
- Datenkonvertierung und Speicherformat

Einschränkungen

Das Exportieren von DB-Cluster-Daten nach Amazon S3 unterliegt folgenden Einschränkungen:

- Sie können nicht mehrere Exportaufgaben für denselben DB-Cluster gleichzeitig ausführen. Dies gilt sowohl für vollständige als auch Teilexporte.
- Pro Person können bis zu fünf DB-Snapshot-Exportaufgaben gleichzeitig ausgeführt werden. AWS-Konto
- DB-Cluster von Aurora Serverless v1 unterstützen keine Exporte nach S3.
- Aurora MySQL und Aurora PostgreSQL unterstützen Exporte nach S3 nur für den bereitgestellten Engine-Modus.
- Exporte nach S3 unterstützen keine S3-Präfixe, die einen Doppelpunkt (:) enthalten.
- Die folgenden Zeichen im S3-Dateipfad werden während des Exports in Unterstriche (_) konvertiert:

```
\ ` " (space)
```

- Wenn eine Datenbank, ein Schema oder eine Tabelle andere Zeichen als den folgenden enthält, wird ein teilweiser Export nicht unterstützt. Sie können jedoch den gesamten DB-Cluster exportieren.
  - Lateinische Buchstaben (A–Z)
  - Ziffern (0–9)
  - Dollar-Symbol ($)
  - Unterstrich (_)
- Leerzeichen ( ) und bestimmte andere Zeichen werden in den Spaltennamen von Datenbanktabellen nicht unterstützt. Tabellen mit den folgenden Zeichen in Spaltennamen werden beim Export übersprungen:

```
, ; { } ( ) \n \t = (space)
```

- Tabellen mit Schrägstrichen (/) im Namen werden beim Export übersprungen.
- Temporäre und nicht protokollierte Tabellen von Aurora PostgreSQL werden beim Export übersprungen.
- Wenn die Daten ein großes Objekt wie BLOB oder CLOB mit einer Größe von 500 MB oder mehr enthalten, schlägt der Export fehl.
- Wenn eine Zeile in einer Tabelle ca. 2 GB groß oder noch größer ist, wird die Tabelle beim Export übersprungen.
- Bei Teilexporten hat die `ExportOnly` Liste eine maximale Größe von 200 KB.
- Es wird dringend empfohlen, für jede Exportaufgabe einen eindeutigen Namen zu verwenden. Wenn Sie keinen eindeutigen Aufgabennamen verwenden, erhalten Sie möglicherweise die folgende Fehlermeldung:

  ExportTaskAlreadyExistsFehler: Beim Aufrufen des StartExportTask Vorgangs ist ein Fehler aufgetreten (ExportTaskAlreadyExists): Die Exportaufgabe mit der ID *xxxxx* ist bereits vorhanden.
- Da einige Tabellen möglicherweise übersprungen werden, empfehlen wir, nach dem Export die Anzahl der Zeilen und Tabellen in den Daten zu überprüfen.

Übersicht über das Exportieren von DB-Cluster-Daten

Sie verwenden den folgenden Prozess, um DB-Cluster-Daten in einen Amazon-S3-Bucket zu exportieren. Weitere Informationen finden Sie in den folgenden Abschnitten.

1. Identifizieren Sie den DB-Cluster, dessen Daten Sie exportieren möchten.
2. Richten Sie den Zugriff auf den Amazon S3-Bucket ein.

   Ein Bucket ist ein Container für Amazon S3-Objekte oder -Dateien. Um die Informationen für den Zugriff auf einen Bucket bereitzustellen, führen Sie die folgenden Schritte aus:

   a. Identifizieren Sie den S3-Bucket, in den die DB-Cluster-Daten exportiert werden soll. Der S3-Bucket muss sich in derselben AWS -Region wie der Cluster befinden. Weitere Informationen finden Sie unter Identifizieren des Amazon S3-Buckets, in den exportiert werden soll.

   b. Erstellen Sie eine AWS Identity and Access Management (IAM-) Rolle, die der Exportaufgabe des DB-Clusters Zugriff auf den S3-Bucket gewährt. Weitere Informationen finden Sie unter Bereitstellen des Zugriffs auf einen Amazon S3-Bucket mit einer IAM-Rolle.

3. Erstellen Sie eine symmetrische Verschlüsselung AWS KMS key für die serverseitige Verschlüsselung. Der KMS-Schlüssel wird von der Cluster-Exportaufgabe verwendet, um die AWS KMS serverseitige Verschlüsselung beim Schreiben der Exportdaten nach S3 einzurichten.

   Die KMS-Schlüsselrichtlinie muss die beiden Berechtigungen `kms:CreateGrant` und `kms:DescribeKey` enthalten. Weitere Informationen zur Verwendung von KMS-Schlüsseln in Amazon Aurora finden Sie unter AWS KMS key-Verwaltung.

   Wenn Ihre KMS-Schlüsselrichtlinie eine Deny-Anweisung enthält, stellen Sie sicher, dass Sie den AWS Dienstprinzipal `export.rds.amazonaws.com` explizit ausschließen.

   Sie können einen KMS-Schlüssel in Ihrem AWS Konto oder einen kontoübergreifenden KMS-Schlüssel verwenden. Weitere Informationen finden Sie unter Ein kontoübergreifendes Konto verwenden AWS KMS key.

4. Exportieren Sie den DB-Cluster mit der Konsole oder dem CLI-Befehl `start-export-task` nach Amazon S3. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Daten in einen Amazon-S3-Bucket.

5. Um auf Ihre exportierten Daten im Amazon S3-Bucket zuzugreifen, siehe Hochladen, Herunterladen und Verwalten von Objekten im Amazon Simple Storage Service User Guide.

Einrichten des Zugriffs auf einen Amazon S3-Bucket

Sie identifizieren den Amazon-S3-Bucket und gewähren der DB-Cluster-Exportaufgabe die Berechtigung, darauf zuzugreifen.

Themen

- Identifizieren des Amazon S3-Buckets, in den exportiert werden soll
- Bereitstellen des Zugriffs auf einen Amazon S3-Bucket mit einer IAM-Rolle
- Einen kontoübergreifenden Amazon-S3-Bucket verwenden

Identifizieren des Amazon S3-Buckets, in den exportiert werden soll

Identifizieren Sie den Amazon-S3-Bucket, in den die DB-Cluster-Daten exportiert werden sollen. Verwenden Sie einen vorhandenen S3-Bucket oder erstellen Sie einen neuen S3-Bucket.

> **Note**
>
> Der S3-Bucket muss sich in derselben AWS Region wie der DB-Cluster befinden.

Weitere Informationen zur Arbeit mit Amazon S3-Buckets finden Sie im Amazon Simple Storage Service User Guide:

- Wie zeige ich die Eigenschaften für einen S3-Bucket an?
- Wie aktiviere ich die Standardverschlüsselung für einen Amazon S3-Bucket?
- Wie erstelle ich einen S3-Bucket?

Bereitstellen des Zugriffs auf einen Amazon S3-Bucket mit einer IAM-Rolle

Bevor Sie DB-Cluster-Daten nach Amazon S3 exportieren, gewähren Sie den Exportaufgaben Schreibzugriff auf den Amazon-S3-Bucket.

Zum Gewähren dieser Berechtigung erstellen Sie eine IAM-Richtlinie, die Zugriff auf den Bucket ermöglicht. Erstellen Sie dann eine IAM-Rolle und fügen Sie der Rolle die Richtlinie an. Die IAM-Rolle können Sie später Ihrer DB-Cluster-Exportaufgabe zuweisen.

> **Important**
>
> Wenn Sie planen, den für den Export Ihres DB-Clusters AWS Management Console zu verwenden, können Sie festlegen, dass die IAM-Richtlinie und die Rolle automatisch erstellt werden, wenn Sie den DB-Cluster exportieren. Anweisungen finden Sie unter Exportieren von DB-Cluster-Daten in einen Amazon-S3-Bucket.

So erteilen Sie Aufgaben Zugriff auf Amazon S3

1. Erstellen Sie eine IAM-Richtlinie. Diese Richtlinie bietet dem Bucket und den Objekten Berechtigungen, die Ihrer DB-Cluster-Exportaufgabe Zugriff auf Amazon S3 erlauben.

Die Richtlinie muss die folgenden erforderlichen Aktionen enthalten, um die Übertragung von Dateien aus Amazon Aurora in einen S3-Bucket zu erlauben:

- `s3:PutObject*`
- `s3:GetObject*`
- `s3:ListBucket`
- `s3:DeleteObject*`
- `s3:GetBucketLocation`

Fügen Sie in die Richtlinie die folgenden Ressourcen zur Identifizierung des S3-Buckets und der Objekte im Bucket ein. Die folgende Liste von Ressourcen zeigt das ARN-Format (Amazon-Ressourcenname) für den Amazon S3-Zugriff.

- `arn:aws:s3:::DOC-EXAMPLE-BUCKET`
- `arn:aws:s3:::DOC-EXAMPLE-BUCKET/*`

Weitere Informationen zur Erstellung einer IAM-Richtlinie für Amazon Aurora finden Sie unter Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff. Siehe auch Tutorial: Erstellen und Anfügen Ihrer ersten vom Kunden verwalteten Richtlinie im IAM-Benutzerhandbuch.

Mit dem folgenden AWS CLI Befehl wird eine IAM-Richtlinie `ExportPolicy` mit diesen Optionen erstellt. Er gewährt Zugriff auf einen Bucket mit dem Namen *DOC-EXAMPLE-BUCKET*.

> **Note**
>
> Nachdem Sie die Richtlinie erstellt haben, notieren Sie den ARN der Richtlinie. Sie benötigen den ARN für einen nachfolgenden Schritt, in dem Sie die Richtlinie an eine IAM-Rolle anhängen.

```
aws iam create-policy  --policy-name ExportPolicy --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExportPolicy",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject*",
                "s3:ListBucket",
                "s3:GetObject*",
                "s3:DeleteObject*",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        }
    ]
}'
```

2. Erstellen Sie eine IAM-Rolle, damit Aurora diese IAM-Rolle in Ihrem Namen übernehmen kann, um auf Ihre Amazon-S3-Buckets zuzugreifen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer im IAM-Benutzerhandbuch.

   Das folgende Beispiel zeigt, wie der AWS CLI Befehl verwendet wird, um eine Rolle mit dem Namen zu erstellen. `rds-s3-export-role`

```
aws iam create-role  --role-name rds-s3-export-role  --assume-role-policy-document
 '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "export.rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole"
       }
     ]
   }'
```

3. Fügen Sie die erstellte IAM-Richtlinie der IAM-Rolle an, die Sie erstellt haben.

Mit dem folgenden AWS CLI Befehl wird die zuvor erstellte Richtlinie an die angegebene `rds-s3-export-role` Rolle angehängt. Ersetzen Sie *`your-policy-arn`* durch den Richtlinien-ARN, den Sie in einem früheren Schritt notiert haben.

```
aws iam attach-role-policy  --policy-arn your-policy-arn  --role-name rds-s3-export-role
```

Einen kontoübergreifenden Amazon-S3-Bucket verwenden

Sie können S3-Buckets kontenübergreifend AWS verwenden. Weitere Informationen finden Sie unter Einen kontoübergreifenden Amazon-S3-Bucket verwenden.

Exportieren von DB-Cluster-Daten in einen Amazon-S3-Bucket

Sie können bis zu fünf gleichzeitige DB-Cluster-Exportaufgaben pro AWS-Konto durchführen.

> **Note**
>
> Das Exportieren von DB-Cluster-Daten kann je nach Datenbanktyp und -größe eine Weile dauern. Die Exportaufgabe klont zuerst die gesamte Datenbank und skaliert sie, bevor die Daten in Amazon S3 extrahiert werden. Der Fortschritt des Vorgangs während dieser Phase wird als Starting (Startet) angezeigt. Wenn die Aufgabe zum Exportieren von Daten zu S3 wechselt, wird der Fortschritt als In progress (In Bearbeitung) angezeigt.
> Die Zeit, die für den Export benötigt wird, hängt von den in der Datenbank gespeicherten Daten ab. Beispielsweise exportieren Tabellen mit gut verteilten numerischen Primärschlüssel- oder Indexspalten am schnellsten. Bei Tabellen, die keine Spalte enthalten, die für die Partitionierung geeignet ist, und bei Tabellen mit nur einem Index für eine auf Zeichenfolgen basierende Spalte, dauert dies länger, da der Export einen langsameren Single-Thread-Prozess verwendet.

Sie können DB-Cluster-Daten mit der AWS Management Console, der oder der RDS-API nach Amazon S3 exportieren. AWS CLI

Wenn Sie eine Lambda-Funktion zum Exportieren der DB-Cluster-Daten verwenden, fügen Sie die Aktion `kms:DescribeKey` der Lambda-Funktionsrichtlinie hinzu. Weitere Informationen finden Sie unter AWS Lambda Berechtigungen.

Konsole

Die Konsolenoption Export to Amazon S3 (Nach Amazon S3 exportieren) wird nur für DB-Cluster angezeigt, die nach Amazon S3 exportiert werden können. Ein DB-Cluster ist aus folgenden Gründen möglicherweise nicht für den Export verfügbar:

- Die DB-Engine wird für den S3-Export nicht unterstützt.
- Die DB-Cluster-Version wird für den S3-Export nicht unterstützt.
- Der S3-Export wird in der AWS Region, in der der DB-Cluster erstellt wurde, nicht unterstützt.

So exportieren Sie DB-Cluster-Daten

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den DB-Cluster aus, dessen Daten Sie exportieren möchten.
4. Wählen Sie für Actions (Aktionen) die Option Export to Amazon S3 (Nach Amazon S3 exportieren) aus.

   Das Fenster Export to Amazon S3 (Nach Amazon S3 exportieren) erscheint.
5. Geben Sie für Export identifier (Export-ID) einen Namen ein, um die Exportaufgabe zu identifizieren. Dieser Wert wird auch für den Namen der im S3-Bucket erstellten Datei verwendet.
6. Wählen Sie die zu exportierenden Daten aus:

   - Wählen Sie All (Alle) aus, um alle Daten im DB-Cluster zu exportieren.
   - Wählen Sie Partial (Teilweise) aus, um bestimmte Teile des DB-Clusters zu exportieren. Um zu ermitteln, welche Teile des Clusters exportiert werden sollen, geben Sie eine oder mehrere Datenbanken, Schemas oder Tabellen für Bezeichner ein, getrennt durch Leerzeichen.

     Verwenden Sie das folgende Format:

     ```
     database[.schema][.table] database2[.schema2][.table2] ... databasen[.schemaN]
     [.tablen]
     ```

     Zum Beispiel:

```
mydatabase mydatabase2.myschema1 mydatabase2.myschema2.mytable1
 mydatabase2.myschema2.mytable2
```

7. Wählen Sie für S3 bucket (S3-Bucket) den Bucket aus, in den exportiert werden soll.

   Um die exportierten Daten einem Ordnerpfad im S3-Bucket zuzuordnen, geben Sie den optionalen Pfad für S3 prefix (S3-Präfix) ein.

8. Wählen Sie für die IAM-Rolle entweder eine Rolle, die Ihnen Schreibzugriff auf den gewählten S3-Bucket gewährt, oder erstellen Sie eine neue Rolle.

   - Wenn Sie eine Rolle durch Befolgen der Schritte in Bereitstellen des Zugriffs auf einen Amazon S3-Bucket mit einer IAM-Rolle erstellt haben, wählen Sie diese Rolle.
   - Wenn Sie keine Rolle erstellt haben, die Ihnen Schreibzugriff auf den von Ihnen gewählten S3-Bucket gewährt, wählen Sie Create a new role (Neue Rolle erstellen) aus, um die Rolle automatisch zu erstellen. Geben Sie dann unter IAM role name (IAM-Rollenname) einen Namen für die Rolle ein.

9. Geben Sie für KMS key (KMS-Schlüssel) den ARN für den Schlüssel ein, der für die Verschlüsselung der exportierten Daten verwendet werden soll.
10. Wählen Sie Export to Amazon S3 (Nach Amazon S3 exportieren) aus.

AWS CLI

Um DB-Cluster-Daten mit dem nach Amazon S3 zu exportieren AWS CLI, verwenden Sie den Befehl start-export-task mit den folgenden erforderlichen Optionen:

- `--export-task-identifier`
- `--source-arn` – Der Amazon-Ressourcenname (ARN) des DB-Clusters.
- `--s3-bucket-name`
- `--iam-role-arn`
- `--kms-key-id`

In den folgenden Beispielen heißt die Exportaufgabe my-cluster-export, wodurch die Daten in einen S3-Bucket mit dem Namen DOC-EXAMPLE-DESTINATION-BUCKET exportiert werden.

Example

LinuxmacOSFürUnix, oder:

```
aws rds start-export-task \
    --export-task-identifier my-cluster-export \
    --source-arn arn:aws:rds:us-west-2:123456789012:cluster:my-cluster \
    --s3-bucket-name DOC-EXAMPLE-DESTINATION-BUCKET \
    --iam-role-arn iam-role \
    --kms-key-id my-key
```

Windows:

```
aws rds start-export-task ^
    --export-task-identifier my-DB-cluster-export ^
    --source-arn arn:aws:rds:us-west-2:123456789012:cluster:my-cluster ^
    --s3-bucket-name DOC-EXAMPLE-DESTINATION-BUCKET ^
    --iam-role-arn iam-role ^
    --kms-key-id my-key
```

Beispiel für eine Ausgabe folgt.

```
{
    "ExportTaskIdentifier": "my-cluster-export",
    "SourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:my-cluster",
    "S3Bucket": "DOC-EXAMPLE-DESTINATION-BUCKET",
    "IamRoleArn": "arn:aws:iam:123456789012:role/ExportTest",
    "KmsKeyId": "my-key",
    "Status": "STARTING",
    "PercentProgress": 0,
    "TotalExtractedDataInGB": 0,
}
```

Wenn Sie einen Ordnerpfad im S3-Bucket für den DB-Cluster-Export bereitstellen möchten, nehmen Sie die Option `--s3-prefix` in den Befehl start-export-task auf.

RDS-API

Um DB-Cluster-Daten mithilfe der Amazon RDS-API nach Amazon S3 zu exportieren, verwenden Sie den StartExportTask-Vorgang mit den folgenden erforderlichen Parametern:

- `ExportTaskIdentifier`

- `SourceArn` – der ARN des DB-Clusters
- `S3BucketName`
- `IamRoleArn`
- `KmsKeyId`

Überwachen von DB-Cluster-Exportaufgaben

Sie können DB-Cluster-Exporte mithilfe der AWS Management Console AWS CLI, der oder der RDS-API überwachen.

Konsole

So überwachen Sie DB-Cluster-Exporte

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Exports in Amazon S3 (Exporte in Amazon S3) aus.

   DB-Cluster-Exporte werden in der Spalte Source type (Quelltyp) angegeben. Der Exportstatus wird in der Spalte Status angezeigt.
3. Um ausführliche Informationen über einen bestimmten DB-Cluster-Export anzuzeigen, wählen Sie die Exportaufgabe aus.

AWS CLI

Verwenden Sie den describe-export-tasksBefehl AWS CLI, um DB-Cluster-Exportaufgaben mithilfe von zu überwachen.

Das folgende Beispiel zeigt, wie Sie aktuelle Informationen über alle Ihre DB-Cluster-Exporte anzeigen können.

Example

```
aws rds describe-export-tasks

{
    "ExportTasks": [
        {
```

```
            "Status": "CANCELED",
            "TaskEndTime": "2022-11-01T17:36:46.961Z",
            "S3Prefix": "something",
            "S3Bucket": "DOC-EXAMPLE-BUCKET",
            "PercentProgress": 0,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/K7MDENG/
bPxRfiCYEXAMPLEKEY",
            "ExportTaskIdentifier": "anewtest",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 0,
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:parameter-groups-
test"
        },
{
            "Status": "COMPLETE",
            "TaskStartTime": "2022-10-31T20:58:06.998Z",
            "TaskEndTime": "2022-10-31T21:37:28.312Z",
            "WarningMessage": "{\"skippedTables\":[],\"skippedObjectives\":[],\"general
\":[{\"reason\":\"FAILED_TO_EXTRACT_TABLES_LIST_FOR_DATABASE\"}]}",
            "S3Prefix": "",
            "S3Bucket": "DOC-EXAMPLE-BUCKET1",
            "PercentProgress": 100,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/2Zp9Utk/
h3yCo8nvbEXAMPLEKEY",
            "ExportTaskIdentifier": "thursday-events-test",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 263,
            "SourceArn": "arn:aws:rds:us-
west-2:123456789012:cluster:example-1-2019-10-31-06-44"
        },
        {
            "Status": "FAILED",
            "TaskEndTime": "2022-10-31T02:12:36.409Z",
            "FailureCause": "The S3 bucket DOC-EXAMPLE-BUCKET2 isn't located in the
 current AWS Region. Please, review your S3 bucket name and retry the export.",
            "S3Prefix": "",
            "S3Bucket": "DOC-EXAMPLE-BUCKET2",
            "PercentProgress": 0,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/2Zp9Utk/
h3yCo8nvbEXAMPLEKEY",
            "ExportTaskIdentifier": "wednesday-afternoon-test",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 0,
```

```
            "SourceArn": "arn:aws:rds:us-
west-2:123456789012:cluster:example-1-2019-10-30-06-45"
        }
    ]
}
```

Wenn Sie Informationen über eine bestimmte Exportaufgabe anzeigen möchten, nehmen Sie die Option `--export-task-identifier` in den Befehl `describe-export-tasks` auf. Um die Ausgabe zu filtern, fügen Sie die Option `--Filters` ein. Weitere Optionen finden Sie im describe-export-tasksBefehl.

RDS-API

Verwenden Sie den Vorgang DescribeExportTasks, um Informationen zu DB-Cluster-Exporten mithilfe der Amazon RDS-API anzuzeigen.

Um den Abschluss des Exportworkflows zu verfolgen oder einen anderen Workflow zu initiieren, können Sie Themen von Amazon Simple Notification Service abonnieren. Weitere Informationen zu Amazon SNS finden Sie unter Arbeiten mit Amazon-RDS-Ereignisbenachrichtigungen.

Abbrechen einer DB-Cluster-Exportaufgabe

Sie können eine DB-Cluster-Exportaufgabe mithilfe der AWS Management Console AWS CLI, der oder der RDS-API abbrechen.

> **Note**
>
> Durch das Abbrechen einer Exportaufgabe werden keine Daten entfernt, die nach Amazon S3 exportiert wurden. Informationen zum Löschen der Daten über die Konsole finden Sie unter Wie lösche ich Objekte aus einem S3-Bucket?. Um die Daten mit der CLI zu löschen, verwenden Sie den Befehl delete-object.

Konsole

So brechen Sie eine DB-Cluster-Exportaufgabe ab

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich die Option Exports in Amazon S3 (Exporte in Amazon S3) aus.

   DB-Cluster-Exporte werden in der Spalte Source type (Quelltyp) angegeben. Der Exportstatus wird in der Spalte Status angezeigt.
3. Wählen Sie die Exportaufgabe aus, die Sie abbrechen möchten.
4. Klicken Sie auf Abbrechen.
5. Wählen Sie die Bestätigungsseite Cancel export task (Exportaufgabe abbrechen) aus.

AWS CLI

Um eine Exportaufgabe mit dem abzubrechen AWS CLI, verwenden Sie den Befehl cancel-export-task. Der Befehl erfordert die Option `--export-task-identifier`.

Example

```
aws rds cancel-export-task --export-task-identifier my-export
{
    "Status": "CANCELING",
    "S3Prefix": "",
    "S3Bucket": "DOC-EXAMPLE-BUCKET",
    "PercentProgress": 0,
    "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/K7MDENG/bPxRfiCYEXAMPLEKEY",
    "ExportTaskIdentifier": "my-export",
    "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
    "TotalExtractedDataInGB": 0,
    "SourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:export-example-1"
}
```

RDS-API

Um eine Exportaufgabe mithilfe der Amazon RDS-API abzubrechen, verwenden Sie den Vorgang CancelExportTask mit dem `ExportTaskIdentifier` Parameter.

Fehlermeldungen für Amazon-S3-Exportaufgaben

In der folgenden Tabelle werden die Nachrichten beschrieben, die zurückgegeben werden, wenn Amazon-S3-Exportaufgaben fehlschlagen.

Fehlernachricht	Beschreibung
Der Quell-DB-Cluster konnte nicht gefunden werden oder es konnte nicht darauf zugegriffen werden: [Clustername]	Der Quell-DB-Cluster kann nicht geklont werden.
Ein unbekannter interner Fehler ist aufgetreten.	Die Aufgabe ist fehlgeschlagen, da eine unbekannte Störung, eine Ausnahme oder ein Fehler aufgetreten ist.
Beim Schreiben der Metadaten der Exportaufgabe in den S3-Bucket [Bucket-Name] ist ein unbekannter interner Fehler aufgetreten.	Die Aufgabe ist fehlgeschlagen, da eine unbekannte Störung, eine Ausnahme oder ein Fehler aufgetreten ist.
Der RDS-Export konnte die Metadaten der Exportaufgabe nicht schreiben, da er die IAM-Rolle [Rolle ARN] nicht übernehmen kann.	Die Exportaufgabe geht davon aus, dass Ihre IAM-Rolle überprüft, ob es erlaubt ist Metadaten in Ihren S3-Bucket zu schreiben Wenn die Aufgabe Ihre IAM-Rolle nicht übernehmen kann, schlägt sie fehl.
Der RDS-Export konnte die Metadaten der Exportaufgabe nicht in den S3-Bucket [Bucket-Name] mit der IAM-Rolle [Rolle ARN] mit dem KMS-Schlüssel [Schlüssel-ID] schreiben. Fehlercode: [Fehlercode]	Eine oder mehrere Berechtigungen fehlen, sodass die Exportaufgabe nicht auf den S3-Bucket zugreifen kann. Diese Fehlermeldung wird ausgelöst, wenn einer der folgenden Fehlercodes empfangen wird: • `AWSSecurityTokenServiceException` mit dem Fehlercode `AccessDenied` • `AmazonS3Exception` mit dem Fehlercode `NoSuchBucket` , `AccessDenied` , `KMS.KMSInvalidStateException` , `403 Forbidden` , oder `KMS.DisabledException` Diese Fehlercodes weisen darauf hin, dass für die IAM-Rolle, den S3-Bucket oder den KMS-Schlüssel Einstellungen falsch konfiguriert sind.

Fehlernachricht	Beschreibung
Die IAM-Rolle [Rolle ARN] ist nicht berechtigt, [S3-Aktion] im S3-Bucket [Bucket-Name] aufzurufen. Überprüfen Sie Ihre Berechtigungen und versuchen Sie den Export erneut.	Die IAM-Richtlinie ist falsch konfiguriert. Die Berechtigung für die spezifische S3-Aktion für den S3-Bucket fehlt, was zu einem Fehler der Exportaufgabe führt.
Fehler bei der Überprüfung des KMS-Schlüssels. Überprüfen Sie die Anmeldeinformation Ihres KMS-Schlüssels und versuchen Sie es erneut.	Die Überprüfung der KMS-Schlüsselanmeldeinformationen ist fehlgeschlagen.
Die Überprüfung der S3-Anmeldeinformation ist fehlgeschlagen. Überprüfen Sie die Berechtigungen für Ihren S3-Bucket und Ihre IAM-Richtlinie.	Die Überprüfung der S3-Anmeldeinformation ist fehlgeschlagen.
Der S3-Bucket [Bucket-Name] ist ungültig. Entweder befindet sie sich nicht in der aktuellen AWS-Region oder es gibt sie nicht. Überprüfen Sie Ihren S3-Bucket-Namen und versuchen Sie den Export erneut.	Der S3-Bucket ist ungültig.
Der S3-Bucket [Bucket-Name] befindet sich nicht in der aktuellen AWS-Region. Überprüfen Sie Ihren S3-Bucket-Namen und versuchen Sie den Export erneut.	Der S3-Bucket ist falsch AWS-Region.

Fehlerbehebung bei PostgreSQL-Berechtigungsfehlern

Beim Exportieren von PostgreSQL-Datenbanken in Amazon S3 wird möglicherweise ein `PERMISSIONS_DO_NOT_EXIST`-Fehler angezeigt, der besagt, dass bestimmte Tabellen übersprungen wurden. Dieser Fehler tritt normalerweise auf, wenn der Superuser, den Sie beim Erstellen des DB-Clusters angegeben haben, keine Berechtigungen für den Zugriff auf diese Tabellen besitzt.

Führen Sie den folgenden Befehl aus, um diesen Fehler zu beheben:

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA schema_name TO superuser_name
```

Weitere Informationen zu Superuser-Berechtigungen finden Sie unter Berechtigungen von Hauptbenutzerkonten.

Benennungskonvention für Dateien

Exportierte Daten für bestimmte Tabellen werden im Format *base_prefix*/*files* gespeichert, wobei das Basispräfix folgendes ist:

```
export_identifier/database_name/schema_name.table_name/
```

Beispielsweise:

```
export-1234567890123-459/rdststcluster/mycluster.DataInsert_7ADB5D19965123A2/
```

Ausgabedateien verwenden die folgende Benennungskonvention, wobei *partition_index* alphanumerisch ist:

```
partition_index/part-00000-random_uuid.format-based_extension
```

Beispielsweise:

```
1/part-00000-c5a881bb-58ff-4ee6-1111-b41ecff340a3-c000.gz.parquet
a/part-00000-d7a881cc-88cc-5ab7-2222-c41ecab340a4-c000.gz.parquet
```

Die Namenskonvention für Dateien kann geändert werden. Daher empfehlen wir beim Lesen von Zieltabellen, dass Sie alles innerhalb des Basispräfixes für die Tabelle lesen.

Datenkonvertierung und Speicherformat

Wenn Sie einen DB-Cluster in einen Amazon-S3-Bucket exportieren, konvertiert Amazon Aurora Daten in das Parquet-Format, exportiert Daten darin und speichert Daten im Parquet-Format. Weitere Informationen finden Sie unter Datenkonvertierung beim Exportieren in einen Amazon S3-Bucket.

Exportieren von DB-Cluster-Snapshot-Daten nach Amazon S3

Sie können DB-Cluster-Snapshot-Daten in einen Amazon-S3-Bucket exportieren. Der Exportprozess läuft im Hintergrund und beeinträchtigt nicht die Leistung Ihres aktiven DB-Clusters.

Wenn Sie einen DB-Cluster-Snapshot exportieren, extrahiert Amazon Aurora Daten aus dem Snapshot und speichert sie in einem Amazon-S3-Bucket. Sie können manuelle Snapshots und automatisierte System-Snapshots exportieren. Standardmäßig werden alle Daten im Snapshot exportiert. Sie können sich jedoch dafür entscheiden, bestimmte Sätze von Datenbanken, Schemata oder Tabellen zu exportieren.

Die Daten werden in einem Apache Parquet-Format gespeichert, das komprimiert und konsistent ist. Einzelne Parquet-Dateien sind normalerweise 1—10 MB groß.

Nachdem die Daten exportiert wurden, können Sie die exportierten Daten direkt mit Tools wie Amazon Athena oder Amazon Redshift Spectrum analysieren. Weitere Informationen zur Verwendung von Athena zum Lesen von Parquet-Daten finden Sie unter Parquet SerDe im Amazon Athena Athena-Benutzerhandbuch. Weitere Informationen zur Verwendung von Redshift Spectrum zum Lesen von Parquet-Daten finden Sie unter COPY from columnar data formats im Amazon Redshift Database Developer Guide.

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen zur Versions- und Regionsverfügbarkeit beim Exportieren von Snapshot-Daten von DB-Cluster nach S3 finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für den Export von Snapshot-Daten nach Amazon S3.

Themen

- Datenkonvertierung beim Exportieren in einen Amazon S3-Bucket

Einschränkungen

Das Exportieren von DB-Snapshot-Daten nach Amazon S3 hat die folgenden Einschränkungen:

- Sie können nicht mehrere Exportaufgaben für denselben DB-Cluster-Snapshot gleichzeitig ausführen. Dies gilt sowohl für vollständige als auch Teilexporte.
- Pro Person können bis zu fünf DB-Snapshot-Exportaufgaben gleichzeitig ausgeführt werden. AWS-Konto
- Sie können keine Snapshot-Daten aus Aurora Serverless v1 DB-Clustern nach S3 exportieren.
- Exporte nach S3 unterstützen keine S3-Präfixe, die einen Doppelpunkt (:) enthalten.
- Die folgenden Zeichen im S3-Dateipfad werden während des Exports in Unterstriche (_) konvertiert:

```
\ ` " (space)
```

- Wenn eine Datenbank, ein Schema oder eine Tabelle andere Zeichen als den folgenden enthält, wird ein teilweiser Export nicht unterstützt. Sie können jedoch den gesamten DB-Snapshot exportieren.
  - Lateinische Buchstaben (A–Z)
  - Ziffern (0–9)
  - Dollar-Symbol ($)
  - Unterstrich (_)
- Leerzeichen ( ) und bestimmte andere Zeichen werden in den Spaltennamen von Datenbanktabellen nicht unterstützt. Tabellen mit den folgenden Zeichen in Spaltennamen werden beim Export übersprungen:

```
, ; { } ( ) \n \t = (space)
```

- Tabellen mit Schrägstrichen (/) im Namen werden beim Export übersprungen.
- Temporäre und nicht protokollierte Tabellen von Aurora PostgreSQL werden beim Export übersprungen.
- Wenn die Daten ein großes Objekt wie BLOB oder CLOB mit einer Größe von 500 MB oder mehr enthalten, schlägt der Export fehl.

- Wenn eine Zeile in einer Tabelle ca. 2 GB groß oder noch größer ist, wird die Tabelle beim Export übersprungen.
- Bei Teilexporten hat die `ExportOnly` Liste eine maximale Größe von 200 KB.
- Es wird dringend empfohlen, für jede Exportaufgabe einen eindeutigen Namen zu verwenden. Wenn Sie keinen eindeutigen Aufgabennamen verwenden, erhalten Sie möglicherweise die folgende Fehlermeldung:

  ExportTaskAlreadyExistsFehler: Beim Aufrufen des StartExportTask Vorgangs ist ein Fehler aufgetreten (ExportTaskAlreadyExists): Die Exportaufgabe mit der ID *xxxxx* ist bereits vorhanden.
- Sie können einen Snapshot löschen, während Sie seine Daten nach S3 exportieren, aber die Speicherkosten für diesen Snapshot werden Ihnen so lange in Rechnung gestellt, bis die Exportaufgabe abgeschlossen ist.
- Sie können exportierte Snapshot-Daten aus S3 nicht in einem neuen DB-Cluster wiederherstellen.

Übersicht über das Exportieren von Snapshot-Daten

Sie verwenden den folgenden Prozess, um DB-Snapshot-Daten in eine Amazon S3 einen Bucket zu exportieren. Weitere Informationen finden Sie in den folgenden Abschnitten.

1. Identifizieren Sie den zu exportierenden Snapshot.

   Verwenden Sie einen vorhandenen automatischen oder manuellen Snapshot oder erstellen Sie einen manuellen Snapshot einer DB-Instance.
2. Richten Sie den Zugriff auf den Amazon S3-Bucket ein.

   Ein Bucket ist ein Container für Amazon S3-Objekte oder -Dateien. Um die Informationen für den Zugriff auf einen Bucket bereitzustellen, führen Sie die folgenden Schritte aus:

   a. Identifizieren Sie den S3-Bucket, in den der Snapshot exportiert werden soll. Der S3-Bucket muss sich in derselben AWS Region wie der Snapshot befinden. Weitere Informationen finden Sie unter Identifizieren des Amazon S3-Buckets, in den exportiert werden soll.

   b. Erstellen Sie eine AWS Identity and Access Management (IAM-) Rolle, die der Snapshot-Exportaufgabe Zugriff auf den S3-Bucket gewährt. Weitere Informationen finden Sie unter Bereitstellen des Zugriffs auf einen Amazon S3-Bucket mit einer IAM-Rolle.
3. Erstellen Sie eine symmetrische Verschlüsselung AWS KMS key für die serverseitige Verschlüsselung. Der KMS-Schlüssel wird von der Snapshot-Exportaufgabe verwendet, um die AWS KMS serverseitige Verschlüsselung beim Schreiben der Exportdaten nach S3 einzurichten.

Die KMS-Schlüsselrichtlinie muss die beiden Berechtigungen `kms:CreateGrant` und `kms:DescribeKey` enthalten. Weitere Informationen zur Verwendung von KMS-Schlüsseln in Amazon Aurora finden Sie unter AWS KMS key-Verwaltung.

Wenn Ihre KMS-Schlüsselrichtlinie eine Deny-Anweisung enthält, stellen Sie sicher, dass Sie den AWS Dienstprinzipal `export.rds.amazonaws.com` explizit ausschließen.

Sie können einen KMS-Schlüssel in Ihrem AWS Konto oder einen kontoübergreifenden KMS-Schlüssel verwenden. Weitere Informationen finden Sie unter Ein kontoübergreifendes Konto verwenden AWS KMS key.

4. Exportieren Sie den Snapshot mit der Konsole oder dem CLI-Befehl `start-export-task` nach Amazon S3. Weitere Informationen finden Sie unter Exportieren eines Snapshots in einen Amazon S3-Bucket.
5. Um auf Ihre exportierten Daten im Amazon S3-Bucket zuzugreifen, siehe Hochladen, Herunterladen und Verwalten von Objekten im Amazon Simple Storage Service User Guide.

Einrichten des Zugriffs auf einen Amazon S3-Bucket

Sie identifizieren den Amazon-S3-Bucket und gewähren dem Snapshot die Berechtigung, auf den Bucket zuzugreifen.

Themen

- Identifizieren des Amazon S3-Buckets, in den exportiert werden soll
- Bereitstellen des Zugriffs auf einen Amazon S3-Bucket mit einer IAM-Rolle
- Einen kontoübergreifenden Amazon-S3-Bucket verwenden
- Ein kontoübergreifendes Konto verwenden AWS KMS key

Identifizieren des Amazon S3-Buckets, in den exportiert werden soll

Identifizieren Sie den Amazon S3-Bucket, in den der DB-Snapshot exportiert werden soll. Verwenden Sie einen vorhandenen S3-Bucket oder erstellen Sie einen neuen S3-Bucket.

> **Note**
>
> Der S3-Bucket, in den exportiert werden soll, muss sich in derselben AWS Region wie der Snapshot befinden.

Weitere Informationen zur Arbeit mit Amazon S3-Buckets finden Sie im Amazon Simple Storage Service User Guide:

- Wie zeige ich die Eigenschaften für einen S3-Bucket an?
- Wie aktiviere ich die Standardverschlüsselung für einen Amazon S3-Bucket?
- Wie erstelle ich einen S3-Bucket?

Bereitstellen des Zugriffs auf einen Amazon S3-Bucket mit einer IAM-Rolle

Bevor Sie DB-Snapshot-Daten nach Amazon S3 exportieren, geben Sie den Snapshot-Exportaufgaben Schreibzugriffsrechte auf den Amazon S3-Bucket.

Zum Gewähren dieser Berechtigung erstellen Sie erstellen Sie eine IAM-Richtlinie, die Zugriff auf den Bucket ermöglicht. Erstellen Sie dann eine IAM-Rolle und fügen Sie der Rolle die Richtlinie an. Die IAM-Rolle können Sie später Ihrer Snapshot-Exportaufgabe zuweisen.

> **Important**
>
> Wenn Sie planen, den zum Exportieren Ihres Snapshots AWS Management Console zu verwenden, können Sie festlegen, dass die IAM-Richtlinie und die Rolle beim Exportieren des Snapshots automatisch erstellt werden. Anweisungen finden Sie unter Exportieren eines Snapshots in einen Amazon S3-Bucket.

So geben Sie DB-Snapshot-Aufgaben Zugriff auf Amazon S3

1. Erstellen Sie eine IAM-Richtlinie. Diese Richtlinie bietet die Berechtigungen für den Bucket und die Objekte, die den Zugriff auf Ihre Snapshot-Exportaufgabe ermöglichen Amazon S3.

   Die Richtlinie muss die folgenden erforderlichen Aktionen enthalten, um die Übertragung von Dateien aus Amazon Aurora in einen S3-Bucket zu ermöglichen:

   - `s3:PutObject*`

- `s3:GetObject*`
- `s3:ListBucket`
- `s3:DeleteObject*`
- `s3:GetBucketLocation`

Fügen Sie in die Richtlinie die folgenden Ressourcen zur Identifizierung des S3-Buckets und der Objekte im Bucket ein. Die folgende Liste von Ressourcen zeigt das ARN-Format (Amazon-Ressourcenname) für den Amazon S3-Zugriff.

- `arn:aws:s3:::DOC-EXAMPLE-BUCKET`
- `arn:aws:s3:::DOC-EXAMPLE-BUCKET/*`

Weitere Informationen zur Erstellung einer IAM-Richtlinie für Amazon Aurora finden Sie unter Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff. Siehe auch Tutorial: Erstellen und Anfügen Ihrer ersten vom Kunden verwalteten Richtlinie im IAM-Benutzerhandbuch.

Mit dem folgenden AWS CLI Befehl wird eine IAM-Richtlinie `ExportPolicy` mit diesen Optionen erstellt. Er gewährt Zugriff auf einen Bucket mit dem Namen *DOC-EXAMPLE-BUCKET*.

> **Note**
>
> Nachdem Sie die Richtlinie erstellt haben, notieren Sie den ARN der Richtlinie. Sie benötigen den ARN für einen nachfolgenden Schritt, in dem Sie die Richtlinie an eine IAM-Rolle anhängen.

```
aws iam create-policy  --policy-name ExportPolicy --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExportPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject*",
                "s3:ListBucket",
                "s3:GetObject*",
```

```
                "s3:DeleteObject*",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        }
    ]
}'
```

2. Erstellen Sie eine IAM-Rolle, damit Aurora diese IAM-Rolle in Ihrem Namen übernehmen kann, um auf Ihre Amazon-S3-Buckets zuzugreifen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer im IAM-Benutzerhandbuch.

   Das folgende Beispiel zeigt, wie der AWS CLI Befehl verwendet wird, um eine Rolle mit dem Namen zu erstellen. `rds-s3-export-role`

```
aws iam create-role  --role-name rds-s3-export-role  --assume-role-policy-document
 '{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
           "Service": "export.rds.amazonaws.com"
         },
        "Action": "sts:AssumeRole"
      }
    ]
  }'
```

3. Fügen Sie die erstellte IAM-Richtlinie der IAM-Rolle an, die Sie erstellt haben.

   Mit dem folgenden AWS CLI Befehl wird die zuvor erstellte Richtlinie an die angegebene `rds-s3-export-role` Rolle angehängt. Ersetzen Sie *`your-policy-arn`* durch den Richtlinien-ARN, den Sie in einem früheren Schritt notiert haben.

```
aws iam attach-role-policy  --policy-arn your-policy-arn  --role-name rds-s3-
export-role
```

Einen kontoübergreifenden Amazon-S3-Bucket verwenden

Sie können Amazon S3 S3-Buckets AWS kontenübergreifend verwenden. Um einen kontoübergreifenden Bucket zu verwenden, fügen Sie eine Bucket-Richtlinie hinzu, um den Zugriff auf die IAM-Rolle zu erlauben, die Sie für die S3-Exporte verwenden. Weitere Informationen finden Sie unter Beispiel 2: Bucket-Eigentümer erteilt kontoübergreifende Bucket-Berechtigungen.

- Fügen Sie eine Bucket-Richtlinie an Ihren Bucket an, wie im folgenden Beispiel gezeigt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/Admin"
            },
            "Action": [
                "s3:PutObject*",
                "s3:ListBucket",
                "s3:GetObject*",
                "s3:DeleteObject*",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ]
        }
    ]
}
```

Ein kontoübergreifendes Konto verwenden AWS KMS key

Sie können ein Cross-Konto verwenden AWS KMS key , um Amazon S3 S3-Exporte zu verschlüsseln. Zuerst fügen Sie dem lokalen Konto eine Schlüsselrichtlinie hinzu und fügen dann IAM-Richtlinien im externen Konto hinzu. Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben.

So verwenden Sie einen kontoübergreifenden KMS-Schlüssel

1. Fügen Sie dem lokalen Konto eine Schlüsselrichtlinie hinzu.

   Das folgende Beispiel gibt `ExampleRole` und `ExampleUser` im externen Konto 444455556666 Berechtigungen im lokalen Konto 123456789012.

```
{
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::444455556666:role/ExampleRole",
            "arn:aws:iam::444455556666:user/ExampleUser"
        ]
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant"
    ],
    "Resource": "*"
}
```

2. Fügen Sie IAM-Richtlinien im externen Konto hinzu.

   Die folgende IAM-Richtlinie erlaubt es dem Prinzipal, den KMS-Schlüssel im Konto 123456789012 für kryptografische Operationen zu erlauben. Um diese Berechtigung an `ExampleRole` und `ExampleUser` zu erteilen, fügen Sie die Richtlinie zu ihnen im Konto 444455556666 an.

```
{
    "Sid": "Allow use of KMS key in account 123456789012",
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
```

```
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant"
    ],
    "Resource": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Exportieren eines Snapshots in einen Amazon S3-Bucket

Pro Person können bis zu fünf DB-Snapshot-Exportaufgaben gleichzeitig ausgeführt werden. AWS-Konto

> **Note**
>
> Das Exportieren von RDS-Snapshots kann je nach Datenbanktyp und -größe eine Weile dauern. Die Exportaufgabe stellt zuerst die gesamte Datenbank wieder her und skaliert sie, bevor die Daten in Amazon S3 extrahiert werden. Der Fortschritt des Vorgangs während dieser Phase wird als Starting (Startet) angezeigt. Wenn die Aufgabe zum Exportieren von Daten zu S3 wechselt, wird der Fortschritt als In progress (In Bearbeitung) angezeigt.
> Die Zeit, die für den Export benötigt wird, hängt von den in der Datenbank gespeicherten Daten ab. Beispielsweise exportieren Tabellen mit gut verteilten numerischen Primärschlüssel- oder Indexspalten am schnellsten. Bei Tabellen, die keine Spalte enthalten, die für die Partitionierung geeignet ist, und bei Tabellen mit nur einem Index für eine auf Zeichenfolgen basierende Spalte, dauert dies länger, da der Export einen langsameren Single-Thread-Prozess verwendet. Diese längere Exportzeit tritt auf, da der Export einen langsameren Single-Thread-Prozess verwendet.

Sie können einen DB-Snapshot mit der AWS Management Console, der oder der RDS-API nach Amazon S3 exportieren. AWS CLI

Wenn Sie eine Lambda-Funktion zum Exportieren eines Snapshots verwenden, fügen Sie die Aktion `kms:DescribeKey` der Lambda-Funktionsrichtlinie hinzu. Weitere Informationen finden Sie unter AWS Lambda Berechtigungen.

Konsole

Die Konsolenoption Export to Amazon S3 (Zu Amazon S3-Konsole exportieren) wird nur für Snapshots angezeigt, die zu Amazon S3 exportiert werden können. Ein Snapshot ist aus folgenden Gründen möglicherweise nicht für den Export verfügbar:

- Die DB-Engine wird für den S3-Export nicht unterstützt.
- Die DB-Instance-Version wird für den S3-Export nicht unterstützt.
- Der S3-Export wird in der AWS Region, in der der Snapshot erstellt wurde, nicht unterstützt.

So exportieren Sie einen DB-Snapshot:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie auf den Registerkarten die Art des Snapshots aus, den Sie exportieren möchten.
4. Wählen Sie in der Liste der Snapshots den Snapshot aus, den Sie exportieren möchten.
5. Wählen Sie für Actions (Aktionen) die Option Export to Amazon S3 (Nach Amazon S3 exportieren) aus.

   Das Fenster Export to Amazon S3 (Nach Amazon S3 exportieren) erscheint.
6. Geben Sie für Export identifier (Export-ID) einen Namen ein, um die Exportaufgabe zu identifizieren. Dieser Wert wird auch für den Namen der im S3-Bucket erstellten Datei verwendet.
7. Wählen Sie die zu exportierenden Daten aus:

   - Wählen Sie All (Alle), um alle Daten im Snapshot zu exportieren.
   - Wählen Sie Partial (Teilweise), um bestimmte Teile des Snapshots zu exportieren. Um zu ermitteln, welche Teile des Snapshots exportiert werden sollen, geben Sie eine oder mehrere Datenbanken, Schemas oder Tabellen für Bezeichner ein, getrennt durch Leerzeichen.

     Verwenden Sie das folgende Format:

     ```
     database[.schema][.table] database2[.schema2][.table2] ... databasen[.schemaN]
     [.tablen]
     ```

     Zum Beispiel:

```
mydatabase mydatabase2.myschema1 mydatabase2.myschema2.mytable1
 mydatabase2.myschema2.mytable2
```

8. Wählen Sie für S3 bucket (S3-Bucket) den Bucket aus, in den exportiert werden soll.

   Um die exportierten Daten einem Ordnerpfad im S3-Bucket zuzuordnen, geben Sie den optionalen Pfad für S3 prefix (S3-Präfix) ein.

9. Wählen Sie für die IAM-Rolle entweder eine Rolle, die Ihnen Schreibzugriff auf den gewählten S3-Bucket gewährt, oder erstellen Sie eine neue Rolle.

   - Wenn Sie eine Rolle durch Befolgen der Schritte in Bereitstellen des Zugriffs auf einen Amazon S3-Bucket mit einer IAM-Rolle erstellt haben, wählen Sie diese Rolle.
   - Wenn Sie keine Rolle erstellt haben, die Ihnen Schreibzugriff auf den von Ihnen gewählten S3-Bucket gewährt, wählen Sie Create a new role (Neue Rolle erstellen) aus, um die Rolle automatisch zu erstellen. Geben Sie dann unter IAM role name (IAM-Rollenname) einen Namen für die Rolle ein.

10. Für AWS KMS key geben Sie den ARN für den Schlüssel ein, der für die Verschlüsselung der exportierten Daten verwendet werden soll.
11. Wählen Sie Export to Amazon S3 (Nach Amazon S3 exportieren) aus.

AWS CLI

Um einen DB-Snapshot mit dem nach Amazon S3 zu exportieren AWS CLI, verwenden Sie den Befehl start-export-task mit den folgenden erforderlichen Optionen:

- `--export-task-identifier`
- `--source-arn`
- `--s3-bucket-name`
- `--iam-role-arn`
- `--kms-key-id`

In den folgenden Beispielen heißt die Snapshot-Exportaufgabe my-snapshot-export, wodurch ein Snapshot in einen S3-Bucket mit dem Namen DOC-EXAMPLE-DESTINATION-BUCKET exportiert wird.

Example

LinuxmacOSFürUnix, oder:

```
aws rds start-export-task \
    --export-task-identifier my-snapshot-export \
    --source-arn arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name \
    --s3-bucket-name DOC-EXAMPLE-DESTINATION-BUCKET \
    --iam-role-arn iam-role \
    --kms-key-id my-key
```

Windows:

```
aws rds start-export-task ^
    --export-task-identifier my-snapshot-export ^
    --source-arn arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name ^
    --s3-bucket-name DOC-EXAMPLE-DESTINATION-BUCKET ^
    --iam-role-arn iam-role ^
    --kms-key-id my-key
```

Beispiel für eine Ausgabe folgt.

```
{
    "Status": "STARTING",
    "IamRoleArn": "iam-role",
    "ExportTime": "2019-08-12T01:23:53.109Z",
    "S3Bucket": "DOC-EXAMPLE-DESTINATION-BUCKET",
    "PercentProgress": 0,
    "KmsKeyId": "my-key",
    "ExportTaskIdentifier": "my-snapshot-export",
    "TotalExtractedDataInGB": 0,
    "TaskStartTime": "2019-11-13T19:46:00.173Z",
    "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name"
}
```

Um einen Ordnerpfad im S3-Bucket für den Snapshot-Export bereitzustellen, fügen Sie die Option `--s3-prefix` im Befehl start-export-task hinzu.

RDS-API

Um einen DB-Snapshot mithilfe der Amazon RDS-API nach Amazon S3 zu exportieren, verwenden Sie den StartExportTask-Vorgang mit den folgenden erforderlichen Parametern:

- `ExportTaskIdentifier`
- `SourceArn`
- `S3BucketName`
- `IamRoleArn`
- `KmsKeyId`

Exportleistung in Aurora MySQL

Die DB-Cluster-Snapshots der Versionen 2 und 3 von Aurora MySQL verwenden einen fortschrittlichen Exportmechanismus, um die Leistung zu verbessern und die Exportzeit zu verkürzen. Der Mechanismus umfasst Optimierungen wie mehrere Export-Threads und Parallelabfragen von Aurora MySQL, um die Vorteile der gemeinsamen Speicherarchitektur von Aurora zu nutzen. Die Optimierungen werden adaptiv angewendet, abhängig von der Größe und Struktur des Datensatzes.

Sie müssen die Parallelabfragen nicht aktivieren, um den schnelleren Exportvorgang zu verwenden, aber der Prozess hat dieselben Einschränkungen wie die Parallelabfragen. Darüber hinaus werden einige Datenwerte nicht unterstützt, z. B. Daten, an denen der Tag des Monats `0` oder das Jahr `0000` lautet. Weitere Informationen finden Sie unter Arbeiten mit Parallel Query für Amazon Aurora MySQL.

Wenn Leistungsoptimierungen angewendet werden, sehen Sie möglicherweise auch viel größere (~200 GB) Parquet-Dateien für Exporte von Aurora MySQL Version 2 und 3.

Wenn der schnellere Exportvorgang nicht verwendet werden kann, beispielsweise aufgrund inkompatibler Datentypen oder Werte, wechselt Aurora automatisch in einen Single-Thread-Exportmodus ohne Parallelabfrage. Je nachdem, welcher Prozess verwendet wird und wie viel Daten exportiert werden sollen, kann die Exportleistung variieren.

Überwachung von Snapshot-Exporten

Sie können DB-Snapshot-Exporte mithilfe der AWS Management Console AWS CLI, der oder der RDS-API überwachen.

Konsole

So überwachen Sie DB-Snapshot-Exporte:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich die Option Exports in Amazon S3 (Exporte in Amazon S3) aus.

   DB-Snapshot-Exporte werden in der Spalte Source type (Quelltyp) angegeben. Der Exportstatus wird in der Spalte Status angezeigt.

3. Um ausführliche Informationen über einen bestimmten Snapshot-Export anzuzeigen, wählen Sie die Exportaufgabe aus.

AWS CLI

Verwenden Sie den Befehl describe-export-tasks AWS CLI, um DB-Snapshot-Exporte mithilfe von zu überwachen.

Das folgende Beispiel zeigt, wie Sie aktuelle Informationen über alle Ihre Snapshot-Exporte anzeigen können.

Example

```
aws rds describe-export-tasks

{
    "ExportTasks": [
        {
            "Status": "CANCELED",
            "TaskEndTime": "2019-11-01T17:36:46.961Z",
            "S3Prefix": "something",
            "ExportTime": "2019-10-24T20:23:48.364Z",
            "S3Bucket": "DOC-EXAMPLE-BUCKET",
            "PercentProgress": 0,
            "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/K7MDENG/
bPxRfiCYEXAMPLEKEY",
            "ExportTaskIdentifier": "anewtest",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 0,
            "TaskStartTime": "2019-10-25T19:10:58.885Z",
            "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:parameter-
groups-test"
        },
{
            "Status": "COMPLETE",
            "TaskEndTime": "2019-10-31T21:37:28.312Z",
```

```
            "WarningMessage": "{\"skippedTables\":[],\"skippedObjectives\":[],\"general
\":[{\"reason\":\"FAILED_TO_EXTRACT_TABLES_LIST_FOR_DATABASE\"}]}",
            "S3Prefix": "",
            "ExportTime": "2019-10-31T06:44:53.452Z",
            "S3Bucket": "DOC-EXAMPLE-BUCKET1",
            "PercentProgress": 100,
            "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/2Zp9Utk/
h3yCo8nvbEXAMPLEKEY",
            "ExportTaskIdentifier": "thursday-events-test",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 263,
            "TaskStartTime": "2019-10-31T20:58:06.998Z",
            "SourceArn":
 "arn:aws:rds:AWS_Region:123456789012:snapshot:rds:example-1-2019-10-31-06-44"
        },
        {
            "Status": "FAILED",
            "TaskEndTime": "2019-10-31T02:12:36.409Z",
            "FailureCause": "The S3 bucket my-exports isn't located in the current AWS
 Region. Please, review your S3 bucket name and retry the export.",
            "S3Prefix": "",
            "ExportTime": "2019-10-30T06:45:04.526Z",
            "S3Bucket": "DOC-EXAMPLE-BUCKET2",
            "PercentProgress": 0,
            "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/2Zp9Utk/
h3yCo8nvbEXAMPLEKEY",
            "ExportTaskIdentifier": "wednesday-afternoon-test",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 0,
            "TaskStartTime": "2019-10-30T22:43:40.034Z",
            "SourceArn":
 "arn:aws:rds:AWS_Region:123456789012:snapshot:rds:example-1-2019-10-30-06-45"
        }
    ]
}
```

Um Informationen über einen bestimmten Snapshot-Export anzuzeigen, fügen Sie die Option `--export-task-identifier` mit dem Befehl `describe-export-tasks` ein. Um die Ausgabe zu filtern, fügen Sie die Option `--Filters` ein. Weitere Optionen finden Sie beim describe-export-tasks-Befehl.

RDS-API

Verwenden Sie den Vorgang DescribeExportTasks, um Informationen zu DB-Snapshot-Exporten mithilfe der Amazon RDS-API anzuzeigen.

Um den Abschluss des Exportworkflows zu verfolgen oder einen anderen Workflow zu initiieren, können Sie Themen von Amazon Simple Notification Service abonnieren. Weitere Informationen zu Amazon SNS finden Sie unter Arbeiten mit Amazon-RDS-Ereignisbenachrichtigungen.

Abbrechen einer Snapshot-Exportaufgabe

Sie können eine Aufgabe zum Exportieren von DB-Snapshots mithilfe der AWS Management Console AWS CLI, der oder der RDS-API abbrechen.

> **Note**
>
> Das Abbrechen einer Snapshot-Exportaufgabe entfernt keine Daten, die nach Amazon S3 exportiert wurden. Informationen zum Löschen der Daten über die Konsole finden Sie unter Wie lösche ich Objekte aus einem S3-Bucket?. Um die Daten mit der CLI zu löschen, verwenden Sie den Befehl delete-object.

Konsole

So brechen Sie eine Aufgabe zum Export von Snapshots ab:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Exports in Amazon S3 (Exporte in Amazon S3) aus.

   DB-Snapshot-Exporte werden in der Spalte Source type (Quelltyp) angegeben. Der Exportstatus wird in der Spalte Status angezeigt.
3. Wählen Sie die Snapshot-Exportaufgabe aus, die Sie abbrechen möchten.
4. Klicken Sie auf Abbrechen.
5. Wählen Sie die Bestätigungsseite Cancel export task (Exportaufgabe abbrechen) aus.

AWS CLI

Um eine Snapshot-Exportaufgabe mit dem abzubrechen AWS CLI, verwenden Sie den Befehl cancel-export-task. Der Befehl erfordert die Option `--export-task-identifier`.

Example

```
aws rds cancel-export-task --export-task-identifier my_export
{
    "Status": "CANCELING",
    "S3Prefix": "",
    "ExportTime": "2019-08-12T01:23:53.109Z",
    "S3Bucket": "DOC-EXAMPLE-BUCKET",
    "PercentProgress": 0,
    "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/K7MDENG/bPxRfiCYEXAMPLEKEY",
    "ExportTaskIdentifier": "my_export",
    "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
    "TotalExtractedDataInGB": 0,
    "TaskStartTime": "2019-11-13T19:46:00.173Z",
    "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:export-example-1"
}
```

RDS-API

Um eine Snapshot-Exportaufgabe mithilfe der Amazon RDS-API abzubrechen, verwenden Sie den CancelExportTask-Vorgang mit dem `ExportTaskIdentifier` Parameter.

Fehlermeldungen für Amazon-S3-Exportaufgaben

In der folgenden Tabelle werden die Nachrichten beschrieben, die zurückgegeben werden, wenn Amazon-S3-Exportaufgaben fehlschlagen.

Fehlernachricht	Beschreibung
Ein unbekannter interner Fehler ist aufgetreten.	Die Aufgabe ist fehlgeschlagen, da eine unbekannte Störung, eine Ausnahme oder ein Fehler aufgetreten ist.
Beim Schreiben der Metadaten der Exportaufgabe in den S3-Bucket	Die Aufgabe ist fehlgeschlagen, da eine unbekannte Störung, eine Ausnahme oder ein Fehler aufgetreten ist.

Fehlernachricht	Beschreibung
[Bucket-Name] ist ein unbekannter interner Fehler aufgetreten.	
Der RDS-Export konnte die Metadaten der Exportaufgabe nicht schreiben, da er die IAM-Rolle [Rolle ARN] nicht übernehmen kann.	Die Exportaufgabe geht davon aus, dass Ihre IAM-Rolle überprüft, ob es erlaubt ist Metadaten in Ihren S3-Bucket zu schreiben Wenn die Aufgabe Ihre IAM-Rolle nicht übernehmen kann, schlägt sie fehl.
Der RDS-Export konnte die Metadaten der Exportaufgabe nicht in den S3-Bucket [Bucket-Name] mit der IAM-Rolle [Rolle ARN] mit dem KMS-Schlüssel [Schlüssel-ID] schreiben. Fehlercode: [Fehlercode]	Eine oder mehrere Berechtigungen fehlen, sodass die Exportaufgabe nicht auf den S3-Bucket zugreifen kann. Diese Fehlermeldung wird ausgelöst, wenn einer der folgenden Fehlercodes empfangen wird: • `AWSSecurityTokenServiceException` mit dem Fehlercode `AccessDenied` • `AmazonS3Exception` mit dem Fehlercode `NoSuchBucket` , `AccessDenied` , `KMS.KMSInvalidStateException` , `403 Forbidden` , oder `KMS.DisabledException` Diese Fehlercodes weisen darauf hin, dass für die IAM-Rolle, den S3-Bucket oder den KMS-Schlüssel Einstellungen falsch konfiguriert sind.
Die IAM-Rolle [Rolle ARN] ist nicht berechtigt, [S3-Aktion] im S3-Bucket [Bucket-Name] aufzurufen. Überprüfen Sie Ihre Berechtigungen und versuchen Sie den Export erneut.	Die IAM-Richtlinie ist falsch konfiguriert. Die Berechtigung für die spezifische S3-Aktion für den S3-Bucket fehlt, was zu einem Fehler der Exportaufgabe führt.
Fehler bei der Überprüfung des KMS-Schlüssels. Überprüfen Sie die Anmeldeinformation Ihres KMS-Schlüssels und versuchen Sie es erneut.	Die Überprüfung der KMS-Schlüsselanmeldeinformationen ist fehlgeschlagen.

Fehlernachricht	Beschreibung
Die Überprüfung der S3-Anmeld einformation ist fehlgeschlagen. Überprüfen Sie die Berechtigungen für Ihren S3-Bucket und Ihre IAM-Richtlinie.	Die Überprüfung der S3-Anmeldeinformation ist fehlgeschlagen.
Der S3-Bucket [Bucket-Name] ist ungültig. Entweder befindet sie sich nicht in der aktuellen AWS-Region oder es gibt sie nicht. Überprüfen Sie Ihren S3-Bucket-Namen und versuchen Sie den Export erneut.	Der S3-Bucket ist ungültig.
Der S3-Bucket [Bucket-Name] befindet sich nicht in der aktuellen AWS-Region. Überprüfen Sie Ihren S3-Bucket-Namen und versuchen Sie den Export erneut.	Der S3-Bucket ist falsch AWS-Region.

Fehlerbehebung bei PostgreSQL-Berechtigungsfehlern

Beim Exportieren von PostgreSQL-Datenbanken in Amazon S3 wird möglicherweise ein `PERMISSIONS_DO_NOT_EXIST`-Fehler angezeigt, der besagt, dass bestimmte Tabellen übersprungen wurden. Dieser Fehler tritt normalerweise auf, wenn der Superuser, den Sie beim Erstellen der DB-Instance angegeben haben, keine Berechtigungen für den Zugriff auf diese Tabellen besitzt.

Führen Sie den folgenden Befehl aus, um diesen Fehler zu beheben:

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA schema_name TO superuser_name
```

Weitere Informationen zu Superuser-Berechtigungen finden Sie unter Berechtigungen von Hauptbenutzerkonten.

Benennungskonvention für Dateien

Exportierte Daten für bestimmte Tabellen werden im Format *base_prefix*/*files* gespeichert, wobei das Basispräfix folgendes ist:

```
export_identifier/database_name/schema_name.table_name/
```

Zum Beispiel:

```
export-1234567890123-459/rdststdb/rdststdb.DataInsert_7ADB5D19965123A2/
```

Es gibt zwei Konventionen für die Benennung von Dateien.

- Aktuelle Konvention:

  ```
  batch_index/part-partition_index-random_uuid.format-based_extension
  ```

  Der Batchindex ist eine Sequenznummer, die einen aus der Tabelle gelesenen Datenstapel darstellt. Wenn wir Ihre Tabelle nicht in kleine Teile partitionieren können, die parallel exportiert werden sollen, wird es mehrere Batch-Indizes geben. Das Gleiche passiert, wenn Ihre Tabelle in mehrere Tabellen partitioniert ist. Es wird mehrere Batch-Indizes geben, einen für jede der Tabellenpartitionen Ihrer Haupttabelle.

  Wenn wir Ihre Tabelle in kleine Teile partitionieren können, die parallel gelesen werden sollen, wird es nur den 1 Batch-Index-Ordner geben.

  Im Batch-Index-Ordner befinden sich eine oder mehrere Parquet-Dateien, die die Daten Ihrer Tabelle enthalten. Das Präfix des Parquet-Dateinamens ist`part-`*`partition_index`*. Wenn Ihre Tabelle partitioniert ist, gibt es mehrere Dateien, die mit dem Partitionsindex `00000` beginnen.

  Es kann Lücken in der Reihenfolge des Partitionsindexes geben. Dies liegt daran, dass jede Partition aus einer Bereichsabfrage in Ihrer Tabelle abgerufen wird. Wenn sich im Bereich dieser Partition keine Daten befinden, wird diese Sequenznummer übersprungen.

  Nehmen wir beispielsweise an, dass die `id` Spalte der Primärschlüssel der Tabelle ist und ihre Minimal- und Maximalwerte `100` und `1000` sind. Wenn wir versuchen, diese Tabelle mit neun Partitionen zu exportieren, lesen wir sie mit parallel Abfragen wie den folgenden:

  ```
  SELECT * FROM table WHERE id <= 100 AND id < 200
  SELECT * FROM table WHERE id <= 200 AND id < 300
  ```

  Dies sollte neun Dateien von `part-00000-`*`random_uuid`*`.gz.parquet` bis erzeugen`part-00008-`*`random_uuid`*`.gz.parquet`. Wenn es jedoch keine Zeilen mit IDs

zwischen 200 und gibt350, ist eine der fertigen Partitionen leer und es wird keine Datei dafür erstellt. Im vorherigen Beispiel wurde `part-00001-random_uuid.gz.parquet` nicht erstellt.

- Ältere Konvention:

```
part-partition_index-random_uuid.format-based_extension
```

Dies entspricht der aktuellen Konvention, jedoch ohne das *batch_index* Präfix, zum Beispiel:

```
part-00000-c5a881bb-58ff-4ee6-1111-b41ecff340a3-c000.gz.parquet
part-00001-d7a881cc-88cc-5ab7-2222-c41ecab340a4-c000.gz.parquet
part-00002-f5a991ab-59aa-7fa6-3333-d41eccd340a7-c000.gz.parquet
```

Die Namenskonvention für Dateien kann geändert werden. Daher empfehlen wir beim Lesen von Zieltabellen, dass Sie alles innerhalb des Basispräfixes für die Tabelle lesen.

Datenkonvertierung beim Exportieren in einen Amazon S3-Bucket

Wenn Sie einen DB-Snapshot in einen Amazon-S3-Bucket exportieren, konvertiert Amazon Aurora Daten in das Parquet-Format, exportiert Daten darin und speichert Daten im Parquet-Format. Weitere Informationen über Parquet finden Sie auf der Website Apache Parquet.

Parquet speichert alle Daten als einen der folgenden primitiven Typen:

- BOOLEAN
- INT32
- INT64
- INT96
- FLOAT
- DOUBLE
- BYTE_ARRAY – Ein Byte-Array mit variabler Länge, auch bekannt als Binary
- FIXED_LEN_BYTE_ARRAY – Ein Byte-Array fester Länge, das verwendet wird, wenn die Werte eine konstante Größe haben

Es gibt nur wenige Parquet-Datentypen, um die Komplexität beim Lesen und Schreiben des Formats zu reduzieren. Parquet bietet logische Typen zur Erweiterung primitiver Typen. Ein logischer Typ ist

als Annotation, bei der Daten in einem `LogicalType`-Metadatenfeld implementiert sind. Die logische Typannotation beschreibt, wie der primitive Typ zu interpretieren ist.

Wenn der logische Typ `STRING` einen `BYTE_ARRAY`-Typ annotiert, gibt er an, dass das Byte-Array als UTF-8-kodierte Zeichenfolge interpretiert werden soll. Nach Abschluss einer Exportaufgabe informiert Sie Amazon Aurora, wenn eine Zeichenfolgenkonvertierung stattgefunden hat. Die zugrunde liegenden exportierten Daten entsprechen immer den Daten aus der Quelle. Aufgrund des Kodierungsunterschieds in UTF-8 können jedoch einige Zeichen beim Einlesen von Tools wie Athena anders als in der Quelle erscheinen.

Weitere Informationen finden Sie unter Logische Typdefinitionen für Parquet in der Parquet-Dokumentation.

Themen

- MySQL-Datentypzuordnung zu Parquet
- PostgreSQL-Datentyp-Mapping zu Parquet

MySQL-Datentypzuordnung zu Parquet

Die folgende Tabelle zeigt die Zuordnung von MySQL-Datentypen zu Parquet-Datentypen, wenn die Daten konvertiert und nach Amazon S3 exportiert werden.

Quelldatentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zur Konvertierung
Numerische Datentypen			
BIGINT	INT64		
BIGINT UNSIGNED	FIXED_LEN_BYTE_ARRAY(9)	DECIMAL(20,0)	Parquet unterstützt nur signierte Typen, daher erfordert das Mapping ein zusätzliches Byte (8 plus 1), um den Typ BIGINT_UNSIGNED zu speichern.

Quelldatentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zur Konvertierung
BIT	BYTE_ARRAY		
DECIMAL	INT32	DECIMAL (p,s)	Wenn der Quellwert kleiner als 2^{31} ist, wird er als INT32 gespeichert.
	INT64	DECIMAL (p,s)	Wenn der Quellwert 2^{31} oder größer ist, aber kleiner als 2^{63} ist, wird er als INT64 gespeichert.
	FIX_LEN_BYTE_ARRAY(N)	DECIMAL (p,s)	Wenn der Quellwert 2^{63} oder größer ist, wird er als FIXED_LEN_BYTE_ARRAY(N) gespeichert.
	BYTE_ARRAY	STRING	Parquet unterstützt maximal 38 Dezimalstellen. Der Dezimalwert wird in eine Zeichenfolge vom Typ BYTE_ARRAY konvertiert und als UTF8 kodiert.
DOUBLE	DOUBLE		
FLOAT	DOUBLE		
INT	INT32		
INT UNSIGNED	INT64		

Quelldatentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zur Konvertierung
MEDIUMINT	INT32		
MEDIUMINT UNSIGNED	INT64		
NUMERIC	INT32	DECIMAL (p,s)	Wenn der Quellwert kleiner als 2^{31} ist, wird er als INT32 gespeichert.
	INT64	DECIMAL (p,s)	Wenn der Quellwert 2^{31} oder größer ist, aber kleiner als 2^{63} ist, wird er als INT64 gespeichert.
	FIXED_LEN _ARRAY(N)	DECIMAL (p,s)	Wenn der Quellwert 2^{63} oder größer ist, wird er als FIXED_LEN _BYTE_ARRAY(N) gespeichert.
	BYTE_ARRAY	STRING	Parquet unterstützt keine numerische Genauigkeit größer als 38. Der Numeric-Wert wird in eine Zeichenfolge vom Typ BYTE_ARRAY konvertiert und als UTF8 kodiert.
SMALLINT	INT32		

Quelldatentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zur Konvertierung
SMALLINT UNSIGNED	INT32		
TINYINT	INT32		
TINYINT UNSIGNED	INT32		
Zeichenfolgen-Datentypen			
BINARY	BYTE_ARRAY		
BLOB	BYTE_ARRAY		
CHAR	BYTE_ARRAY		
ENUM	BYTE_ARRAY	STRING	
LINESTRING	BYTE_ARRAY		
LONGBLOB	BYTE_ARRAY		
LONGTEXT	BYTE_ARRAY	STRING	
MEDIUMBLOB	BYTE_ARRAY		
MEDIUMTEXT	BYTE_ARRAY	STRING	
MULTILINESTRING	BYTE_ARRAY		
SET	BYTE_ARRAY	STRING	
TEXT	BYTE_ARRAY	STRING	
TINYBLOB	BYTE_ARRAY		
TINYTEXT	BYTE_ARRAY	STRING	
VARBINARY	BYTE_ARRAY		

Quelldatentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zur Konvertierung
VARCHAR	BYTE_ARRAY	STRING	
Datums- und Uhrzeit-Datentypen			
DATUM	BYTE_ARRAY	STRING	Ein Datum wird in eine Zeichenfolge vom Typ BYTE_ARRAY konvertiert und als UTF8 kodiert.
DATETIME	INT64	TIMESTAMP_MICROS	
TIME	BYTE_ARRAY	STRING	Ein TIME-Typ wird in einem BYTE_ARRAY in eine Zeichenfolge konvertiert und als UTF8 kodiert.
TIMESTAMP	INT64	TIMESTAMP_MICROS	
YEAR	INT32		
Geometrische Datentypen			
GEOMETRY	BYTE_ARRAY		
GEOMETRYCOLLECTION	BYTE_ARRAY		
MULTIPOINT	BYTE_ARRAY		
MULTIPOLYGON	BYTE_ARRAY		
POINT	BYTE_ARRAY		

Quelldatentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zur Konvertierung
POLYGON	BYTE_ARRAY		
JSON-Datentyp			
JSON	BYTE_ARRAY	STRING	

PostgreSQL-Datentyp-Mapping zu Parquet

Die folgende Tabelle zeigt das Mapping von PostgreSQL-Datentypen zu Parquet-Datentypen, wenn Daten konvertiert und nach Amazon S3 exportiert werden.

PostgreSQL-Datentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zum Mapping
Numerische Datentypen			
BIGINT	INT64		
BIGSERIAL	INT64		
DECIMAL	BYTE_ARRAY	STRING	Ein DECIMAL-Typ wird in eine Zeichenfolge in einem BYTE_ARRAY-Typ konvertiert und als UTF8 kodiert. Diese Konvertierung soll Komplikationen aufgrund von Datengenauigkeit und Datenwerten, die keine Zahlen sind (NaN), vermeiden.

PostgreSQL-Datentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zum Mapping
DOUBLE PRECISION	DOUBLE		
INTEGER	INT32		
MONEY	BYTE_ARRAY	STRING	
REAL	FLOAT		
SERIAL	INT32		
SMALLINT	INT32	INT_16	
SMALLSERIAL	INT32	INT_16	
Zeichenfolgen- und verwandte Datentypen			
ARRAY	BYTE_ARRAY	STRING	Ein Array wird in eine Zeichenfolge konvertiert und als BINARY (UTF8) kodiert. Diese Konvertierung dient dazu, Komplikationen aufgrund von Datengenauigkeit, Datenwerten, die keine Zahl sind (NaN), und Zeitdatenwerten zu vermeiden.
BIT	BYTE_ARRAY	STRING	
BIT VARYING	BYTE_ARRAY	STRING	
BYTEA	BINARY		

PostgreSQL-Datentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zum Mapping
CHAR	BYTE_ARRAY	STRING	
CHAR(N)	BYTE_ARRAY	STRING	
ENUM	BYTE_ARRAY	STRING	
NAME	BYTE_ARRAY	STRING	
TEXT	BYTE_ARRAY	STRING	
TEXT SEARCH	BYTE_ARRAY	STRING	
VARCHAR(N)	BYTE_ARRAY	STRING	
XML	BYTE_ARRAY	STRING	
Datums- und Uhrzeit-Datentypen			
DATUM	BYTE_ARRAY	STRING	
INTERVAL	BYTE_ARRAY	STRING	
TIME	BYTE_ARRAY	STRING	
TIME WITH TIME ZONE	BYTE_ARRAY	STRING	
TIMESTAMP	BYTE_ARRAY	STRING	
TIMESTAMP WITH TIME ZONE	BYTE_ARRAY	STRING	
Geometrische Datentypen			
BOX	BYTE_ARRAY	STRING	
CIRCLE	BYTE_ARRAY	STRING	
LINE	BYTE_ARRAY	STRING	

PostgreSQL-Datentyp	Parquet-Primitiv-Typ	Logische Typannotation	Anmerkungen zum Mapping
LINESEGMENT	BYTE_ARRAY	STRING	
PATH	BYTE_ARRAY	STRING	
POINT	BYTE_ARRAY	STRING	
POLYGON	BYTE_ARRAY	STRING	
JSON-Datentypen			
JSON	BYTE_ARRAY	STRING	
JSONB	BYTE_ARRAY	STRING	
Weitere Datentypen			
BOOLEAN	BOOLEAN		
CIDR	BYTE_ARRAY	STRING	Network-Datentyp
COMPOSITE	BYTE_ARRAY	STRING	
DOMAIN	BYTE_ARRAY	STRING	
INET	BYTE_ARRAY	STRING	Network-Datentyp
MACADDR	BYTE_ARRAY	STRING	
OBJECT IDENTIFIER	–		
PG_LSN	BYTE_ARRAY	STRING	
RANGE	BYTE_ARRAY	STRING	
UUID	BYTE_ARRAY	STRING	

Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit

Sie können einen DB-Cluster auf einen bestimmten Zeitpunkt wiederherstellen, wodurch ein neuer DB-Cluster erstellt wird.

Wenn Sie einen DB-Cluster zu einem bestimmten Zeitpunkt wiederherstellen, können Sie die Standard-VPC-Sicherheitsgruppe (Virtual Private Cloud) auswählen. Oder Sie können eine benutzerdefinierte VPC-Sicherheitsgruppe auf Ihren DB-Cluster anwenden.

Wiederhergestellte DB-Cluster werden automatisch dem Standard-DB-Cluster und DB-Parametergruppen zugeordnet. Sie können jedoch eine benutzerdefinierte Parametergruppe anwenden, indem Sie diese während einer Wiederherstellung angeben.

Amazon Aurora lädt Protokolldatensätze für DB-Cluster laufend nach Amazon S3 hoch. Um den letzten wiederherstellbaren Zeitpunkt für einen DB-Cluster zu ermitteln, verwenden Sie den AWS CLI describe-db-clustersBefehl und sehen Sie sich den Wert an, der im `LatestRestorableTime` Feld für den DB-Cluster zurückgegeben wurde.

Sie können die Backup auf jeden beliebigen Zeitpunkt innerhalb des Aufbewahrungszeitraums für Backups vornehmen. Um den frühesten wiederherstellbaren Zeitpunkt für einen DB-Cluster zu ermitteln, verwenden Sie den AWS CLI describe-db-clustersBefehl und sehen Sie sich den Wert an, der im `EarliestRestorableTime` Feld für den DB-Cluster zurückgegeben wird.

Der Backup-Aufbewahrungszeitraum des wiederhergestellten DB-Clusters entspricht dem des Quell-DB-Clusters.

> **Note**
>
> Informationen in diesem Thema gelten für Amazon Aurora. Weitere Informationen zum Wiederherstellen einer Amazon-RDS-DB-Instance finden Sie unter Wiederherstellen einer DB-Instance zu einer bestimmten Zeit.
> Weitere Informationen zum Sichern und Wiederherstellen eines Aurora-DB-Clusters finden Sie unter Übersicht über das Sichern und Wiederherstellen eines Aurora-DB-Clusters.
> Für Aurora MySQL können Sie einen bereitgestellten DB-Cluster als Aurora Serverless-DB-Cluster wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen eines Aurora Serverless v1-DB-Clusters.
> Sie können es auch verwenden AWS Backup , um Backups von Amazon Aurora Aurora-DB-Clustern zu verwalten. Wenn Ihr DB-Cluster mit einem Backup-Plan verknüpft ist AWS Backup, wird dieser Backup-Plan für die point-in-time Wiederherstellung verwendet. Weitere

Informationen finden Sie unter Wiederherstellen eines DB-Clusters zu einem bestimmten Zeitpunkt mit AWS Backup.

Informationen zur Wiederherstellung eines Aurora-DB-Clusters oder eines globalen Clusters mit einer RDS Extended Support-Version finden Sie unterWiederherstellung , eines Aurora-DB-Clusters oder eines globalen Clusters mit Amazon RDS Extended Support.

Sie können einen DB-Cluster mithilfe der AWS Management Console, der oder der RDS-API auf einen bestimmten Zeitpunkt zurücksetzen. AWS CLI

Konsole

Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Automated backups (Automatisierte Backups) aus.

   Die automatisierten Backups werden auf der Registerkarte Current Region (Aktuelle Region) angezeigt.

3. Wählen Sie den -DB-Cluster aus, den Sie wiederherstellen möchten.
4. Wählen Sie unter Aktionen die Option Restore to point in time (Zu einem bestimmten Zeitpunkt wiederherstellen) aus.

   Anschließend wird das Fenster Restore to point in time (Zu einem bestimmten Zeitpunkt wiederherstellen) angezeigt.
5. Wählen Sie Späteste Wiederherstellungszeit, um auf den spätesten möglichen Zeitpunkt wiederherzustellen oder wählen Sie Benutzerdefiniert, um eine Zeit auszuwählen.

   Wenn Sie Benutzerdefiniert wählen, geben Sie das Datum und die Uhrzeit ein, auf die Sie den Cluster wiederherstellen möchten.

> **Note**
>
> Zeiten werden in Ihrer lokalen Zeitzone angezeigt, die durch einen Offset von Coordinated Universal Time (UTC) angezeigt wird. Beispiel: UTC-5 ist Ost Standardzeit/ Zentral Sommerzeit.

6. Geben Sie für DB-Cluster-Kennung den Namen des wiederhergestellten DB-Ziel-Clusters ein. Der Name muss eindeutig sein.
7. Wählen Sie bei Bedarf andere Optionen aus, z. B. die DB-Instance-Klasse und die DB-Cluster-Speicherkonfiguration.

   Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.
8. Wählen Sie Restore to point in time (Zu einem bestimmten Zeitpunkt wiederherstellen) aus.

AWS CLI

Um einen DB-Cluster zu einem bestimmten Zeitpunkt wiederherzustellen, verwenden Sie den AWS CLI Befehl restore-db-cluster-to-, point-in-time um einen neuen DB-Cluster zu erstellen.

Sie können andere Einstellungen festlegen. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.

Das Tagging von Ressourcen wird für diesen Vorgang unterstützt. Wenn Sie die Option `--tags` verwenden, werden die Tags des Quell-DB-Clusters ignoriert und die bereitgestellten verwendet. Andernfalls werden die neuesten Tags aus dem Quell-Cluster verwendet.

Example

Für LinuxmacOS, oderUnix:

```
aws rds restore-db-cluster-to-point-in-time \
    --source-db-cluster-identifier mysourcedbcluster \
    --db-cluster-identifier mytargetdbcluster \
    --restore-to-time 2017-10-14T23:45:00.000Z
```

Windows:

```
aws rds restore-db-cluster-to-point-in-time ^
    --source-db-cluster-identifier mysourcedbcluster ^
    --db-cluster-identifier mytargetdbcluster ^
    --restore-to-time 2017-10-14T23:45:00.000Z
```

Important

Wenn Sie die Konsole für das Wiederherstellen eines DB-Clusters zu einer bestimmen Zeit verwenden, erstellt Amazon RDS automatisch die primäre Instance (Writer) für Ihren DB-Cluster. Wenn Sie den verwenden AWS CLI , um einen DB-Cluster auf einen bestimmten Zeitpunkt wiederherzustellen, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance.
Rufen Sie den create-db-instance AWS CLI Befehl auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Fügen Sie den Namen des DB-Clusters als `--db-cluster-identifier`-Optionswert ein.

RDS-API

Zum Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit rufen Sie den Amazon RDS-API `RestoreDBClusterToPointInTime`-Betrieb mit den folgenden Parametern auf:

- `SourceDBClusterIdentifier`
- `DBClusterIdentifier`
- `RestoreToTime`

Important

Wenn Sie die Konsole für das Wiederherstellen eines DB-Clusters zu einer bestimmen Zeit verwenden, erstellt Amazon RDS automatisch die primäre Instance (Writer) für Ihren DB-Cluster. Wenn Sie RDS API für das Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit verwenden, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance.
Rufen Sie die RDS-API-Operation CreateDBInstance auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Beziehen Sie den Namen des DB-Clusters als `DBClusterIdentifier`-Parameterwert mit ein.

Wiederherstellen eines DB-Clusters zu einem bestimmten Zeitpunkt aus einem beibehaltenen, automatisierten Backup

Sie können einen DB-Cluster aus einem beibehaltenen, automatisierten Backup wiederherstellen, nachdem Sie den Quell-DB-Cluster gelöscht haben, wenn sich das Backup innerhalb des Aufbewahrungszeitraums des Quell-Clusters befindet. Der Vorgang ähnelt dem Wiederherstellen eines DB-Clusters aus einem automatisierten Backup.

> **Note**
>
> Mit diesem Verfahren können Sie einen Aurora Serverless v1 DB-Cluster nicht wiederherstellen, da automatische Backups für Aurora Serverless v1 Cluster nicht aufbewahrt werden.

Konsole

Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Automated backups (Automatisierte Backups) aus.
3. Wählen Sie die Registerkarte Beibehalten aus.

4. Wählen Sie den -DB-Cluster aus, den Sie wiederherstellen möchten.
5. Wählen Sie unter Aktionen die Option Restore to point in time (Zu einem bestimmten Zeitpunkt wiederherstellen) aus.

   Anschließend wird das Fenster Restore to point in time (Zu einem bestimmten Zeitpunkt wiederherstellen) angezeigt.
6. Wählen Sie Späteste Wiederherstellungszeit, um auf den spätesten möglichen Zeitpunkt wiederherzustellen oder wählen Sie Benutzerdefiniert, um eine Zeit auszuwählen.

Wenn Sie Benutzerdefiniert wählen, geben Sie das Datum und die Uhrzeit ein, auf die Sie den Cluster wiederherstellen möchten.

> **Note**
>
> Zeiten werden in Ihrer lokalen Zeitzone angezeigt, die durch einen Offset von Coordinated Universal Time (UTC) angezeigt wird. Beispiel: UTC-5 ist Ost Standardzeit/ Zentral Sommerzeit.

7. Geben Sie für DB-Cluster-Kennung den Namen des wiederhergestellten DB-Ziel-Clusters ein. Der Name muss eindeutig sein.
8. Wählen Sie bei Bedarf andere Optionen aus, z. B. DB-Instance-Class.

   Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.
9. Wählen Sie Restore to point in time (Zu einem bestimmten Zeitpunkt wiederherstellen) aus.

AWS CLI

Um einen DB-Cluster zu einem bestimmten Zeitpunkt wiederherzustellen, verwenden Sie den AWS CLI Befehl restore-db-cluster-to-, point-in-time um einen neuen DB-Cluster zu erstellen.

Sie können andere Einstellungen festlegen. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.

Das Tagging von Ressourcen wird für diesen Vorgang unterstützt. Wenn Sie die Option `--tags` verwenden, werden die Tags des Quell-DB-Clusters ignoriert und die bereitgestellten verwendet. Andernfalls werden die neuesten Tags aus dem Quell-Cluster verwendet.

Example

Für LinuxmacOS, oderUnix:

```
aws rds restore-db-cluster-to-point-in-time \
    --source-db-cluster-resource-id cluster-123ABCEXAMPLE \
    --db-cluster-identifier mytargetdbcluster \
    --restore-to-time 2017-10-14T23:45:00.000Z
```

Windows:

```
aws rds restore-db-cluster-to-point-in-time ^
    --source-db-cluster-resource-id cluster-123ABCEXAMPLE ^
    --db-cluster-identifier mytargetdbcluster ^
    --restore-to-time 2017-10-14T23:45:00.000Z
```

Important

Wenn Sie die Konsole für das Wiederherstellen eines DB-Clusters zu einer bestimmen Zeit verwenden, erstellt Amazon RDS automatisch die primäre Instance (Writer) für Ihren DB-Cluster. Wenn Sie den verwenden AWS CLI , um einen DB-Cluster auf einen bestimmten Zeitpunkt wiederherzustellen, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance.
Rufen Sie den create-db-instance AWS CLI Befehl auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Fügen Sie den Namen des DB-Clusters als `--db-cluster-identifier`-Optionswert ein.

RDS-API

Zum Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit rufen Sie den Amazon RDS-API `RestoreDBClusterToPointInTime`-Betrieb mit den folgenden Parametern auf:

- `SourceDbClusterResourceId`
- `DBClusterIdentifier`
- `RestoreToTime`

Important

Wenn Sie die Konsole für das Wiederherstellen eines DB-Clusters zu einer bestimmen Zeit verwenden, erstellt Amazon RDS automatisch die primäre Instance (Writer) für Ihren DB-Cluster. Wenn Sie RDS API für das Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit verwenden, müssen Sie die primäre Instance für Ihren DB-Cluster explizit erstellen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance.
Rufen Sie die RDS-API-Operation CreateDBInstance auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Beziehen Sie den Namen des DB-Clusters als `DBClusterIdentifier`-Parameterwert mit ein.

Wiederherstellen eines DB-Clusters zu einem bestimmten Zeitpunkt mit AWS Backup

Sie können es verwenden, AWS Backup um Ihre automatisierten Backups zu verwalten und sie dann zu einem bestimmten Zeitpunkt wiederherzustellen. Dazu erstellen Sie einen Backup-Plan in AWS Backup und weisen Ihren DB-Cluster als Ressource zu. Anschließend aktivieren Sie in der Backup-Regel kontinuierliche Backups für PITR. Weitere Informationen zu Backup-Plänen und Backup-Regeln finden Sie im AWS Backup-Leitfaden für Entwickler.

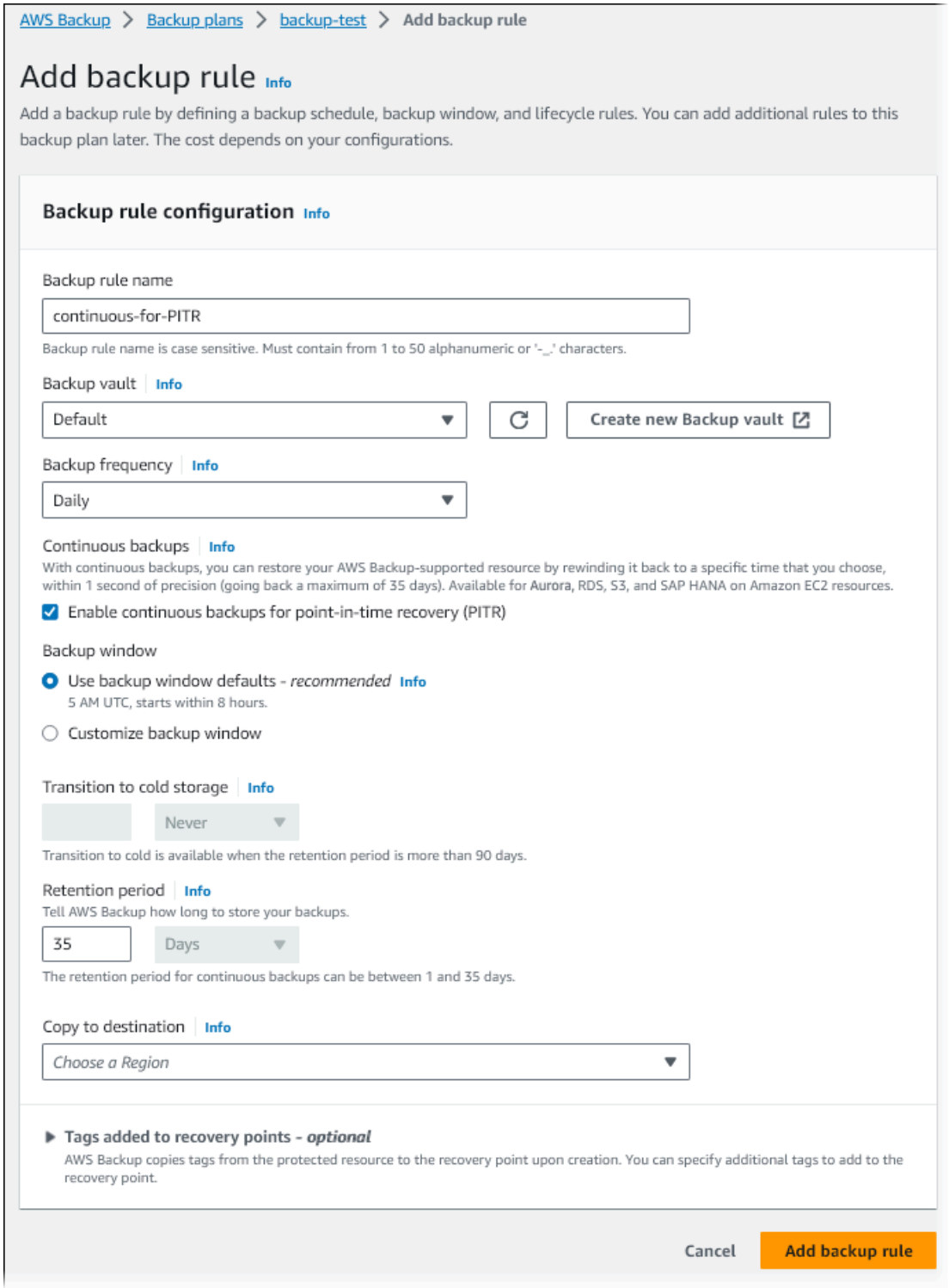
Aktivierung kontinuierlicher Backups in AWS Backup

Sie aktivieren kontinuierliche Backups in den Backup-Regeln.

So aktivieren Sie kontinuierliche Backups für PITR

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup-Pläne aus.
3. Unter Name des Backup-Plans wählen Sie den Backup-Plan aus, den Sie für die Sicherung Ihres DB-Clusters verwenden.
4. Wählen Sie im Abschnitt Konfiguration der Sicherungsregel die Option Sicherungsregel hinzufügen aus.

   Die Seite Sicherungsregel hinzufügen wird angezeigt.
5. Aktivieren Sie das Kontrollkästchen Kontinuierliche Backups für die point-in-time Wiederherstellung (PITR) aktivieren.



6. Wählen Sie nach Bedarf andere Einstellungen, und wählen Sie dann Sicherungsregel hinzufügen.

Wiederherstellung aus einem kontinuierlichen Backup in AWS Backup

Verwenden Sie einen Backup-Tresor, um die Wiederherstellung zu einem bestimmten Zeitpunkt zu erstellen.

Konsole

Sie können den verwenden AWS Management Console , um einen DB-Cluster auf einen bestimmten Zeitpunkt wiederherzustellen.

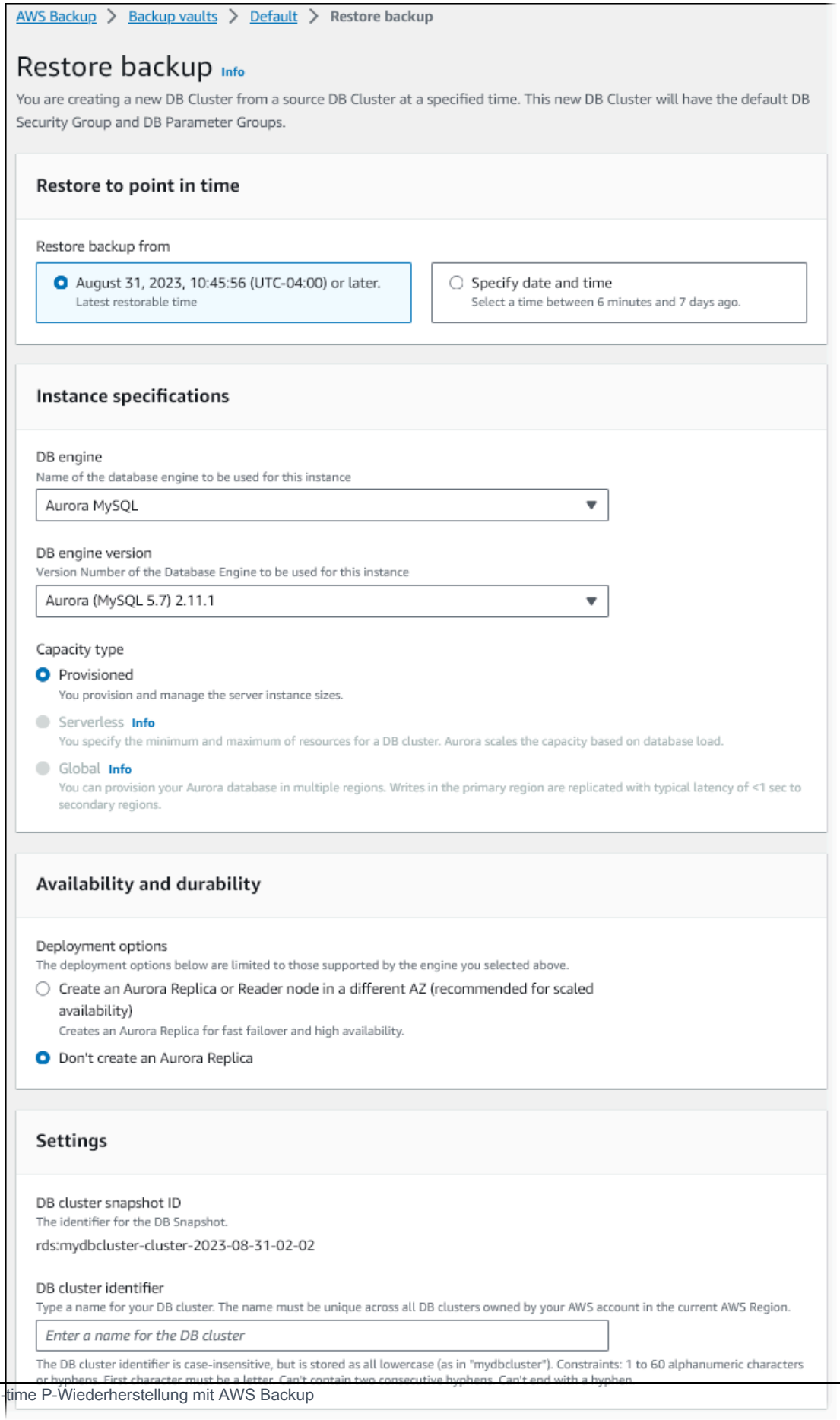
Zur Wiederherstellung aus einem kontinuierlichen Backup in AWS Backup

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Backup Konsole unter https://console.aws.amazon.com/backup.
2. Wählen Sie im Navigationsbereich Backup vaults (Sicherungstresore) aus.
3. Wählen Sie den Backup-Tresor aus, der Ihr kontinuierliches Backup enthält, zum Beispiel Standard.

   Die Seite mit den Details zum Backup-Tresor wird angezeigt.
4. Unter Wiederherstellungspunkte wählen Sie den Wiederherstellungspunkt für die automatische Sicherung aus.

   Der Sicherungstyp ist Kontinuierlich und der Name ist `continuous:cluster-`*`AWS-Backup-job-number`*.
5. Wählen Sie unter Aktionen die Option Wiederherstellen aus.

   Die Seite Sicherung wiederherstellen wird angezeigt.


AWS Backup > Backup vaults > Default > Restore backup
Restore backup Info
You are creating a new DB Cluster from a source DB Cluster at a specified time. This new DB Cluster will have the default DB Security Group and DB Parameter Groups.
Restore to point in time
Restore backup from
August 31, 2023, 10:45:56 (UTC-04:00) or later.
Latest restorable time
Specify date and time
Select a time between 6 minutes and 7 days ago.
Instance specifications
DB engine
Name of the database engine to be used for this instance
Aurora MySQL
DB engine version
Version Number of the Database Engine to be used for this instance
Aurora (MySQL 5.7) 2.11.1
Capacity type
Provisioned
You provision and manage the server instance sizes.
Serverless Info
You specify the minimum and maximum of resources for a DB cluster. Aurora scales the capacity based on database load.
Global Info
You can provision your Aurora database in multiple regions. Writes in the primary region are replicated with typical latency of <1 sec to secondary regions.
Availability and durability
Deployment options
The deployment options below are limited to those supported by the engine you selected above.
Create an Aurora Replica or Reader node in a different AZ (recommended for scaled availability)
Creates an Aurora Replica for fast failover and high availability.
Don't create an Aurora Replica
Settings
DB cluster snapshot ID
The identifier for the DB Snapshot.
rds:mydbcluster-cluster-2023-08-31-02-02
DB cluster identifier
Type a name for your DB cluster. The name must be unique across all DB clusters owned by your AWS account in the current AWS Region.
Enter a name for the DB cluster
The DB cluster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

6. Wählen Sie unter Zum gewünschten Zeitpunkt wiederherstellen Datum und Uhrzeit angeben, um zu einem bestimmten Zeitpunkt wiederherzustellen.
7. Wählen Sie je nach Bedarf weitere Einstellungen für die Wiederherstellung des DB-Clusters, und wählen Sie dann Sicherung wiederherstellen.

   Die Seite Jobs wird angezeigt und zeigt das Fenster Wiederherstellungsjobs an. Eine Meldung am Anfang der Seite enthält Informationen zu dem Wiederherstellungsjob.

Nach der Wiederherstellung des DB-Clusters müssen Sie diesem die primäre (Writer)-DB-Instance hinzufügen. Rufen Sie den create-db-instance AWS CLI Befehl auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Beziehen Sie den Namen des DB-Clusters als `--db-cluster-identifier`-Parameterwert mit ein.

CLI

Sie verwenden den start-restore-job AWS CLI Befehl, um den DB-Cluster auf eine bestimmte Zeit zurückzusetzen. Die folgenden Parameter sind erforderlich:

- `--recovery-point-arn` – Der Amazon-Ressourcenname (ARN) für den Wiederherstellungspunkt, von dem aus die Wiederherstellung durchgeführt werden soll.
- `--resource-type` – verwenden Sie `Aurora`.
- `--iam-role-arn`— Der ARN für die IAM-Rolle, die Sie für AWS Backup Operationen verwenden.
- `--metadata` – Die Metadaten, die Sie zur Wiederherstellung des DB-Clusters verwenden. Die folgenden Parameter sind erforderlich:
  - `DBClusterIdentifier`
  - `Engine`
  - `RestoreToTime` oder `UseLatestRestorableTime`

Das folgende Beispiel zeigt, wie ein DB-Cluster zu einem bestimmten Zeitpunkt wiederhergestellt wird.

```
aws backup start-restore-job \
--recovery-point-arn arn:aws:backup:eu-central-1:123456789012:recovery-
point:continuous:cluster-itsreallyjustanexample1234567890-487278c2 \
--resource-type Aurora \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/AWSBackupDefaultServiceRole
 \
```

```
--metadata '{"DBClusterIdentifier":"backup-pitr-test","Engine":"aurora-
mysql","RestoreToTime":"2023-09-01T17:00:00.000Z"}'
```

Das folgende Beispiel zeigt, wie ein DB-Cluster zum letzten wiederherstellbaren Zeitpunkt wiederhergestellt wird.

```
aws backup start-restore-job \
--recovery-point-arn arn:aws:backup:eu-central-1:123456789012:recovery-
point:continuous:cluster-itsreallyjustanexample1234567890-487278c2 \
--resource-type Aurora \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/AWSBackupDefaultServiceRole
 \
--metadata '{"DBClusterIdentifier":"backup-pitr-latest","Engine":"aurora-
mysql","UseLatestRestorableTime":"true"}'
```

Nach der Wiederherstellung des DB-Clusters müssen Sie diesem die primäre (Writer)-DB-Instance hinzufügen. Rufen Sie den create-db-instance AWS CLI Befehl auf, um die primäre Instance für Ihren DB-Cluster zu erstellen. Beziehen Sie den Namen des DB-Clusters als `--db-cluster-identifier`-Parameterwert mit ein.

Löschen eines DB-Cluster-Snapshots

Sie können DB-Cluster-Snapshots löschen, die mit Amazon RDS verwaltet werden, wenn Sie sie nicht mehr benötigen.

> **Note**
>
> Um mit AWS Backup verwaltete Backups zu löschen, verwenden Sie die AWS Backup-Konsole. Informationen zu AWS Backup finden Sie im AWS Backup-Developer-Handbuch.

Löschen eines DB-Cluster-Snapshots

Sie können einen DB-Cluster-Snapshot mit der Konsole, der AWS CLI oder der RDS-API löschen.

Um einen freigegebenen oder öffentlichen Snapshot zu löschen, müssen Sie sich bei dem AWS-Konto anmelden, in dessen Besitz sich der Snapshot befindet.

Konsole

So löschen Sie einen DB-Cluster-Snapshot

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den DB-Cluster-Snapshot aus, den Sie löschen möchten.
4. Wählen Sie unter Actions (Aktionen) die Option Delete Snapshot (Snapshot löschen) aus.
5. Wählen Sie auf der Bestätigungsseite die Option Delete (Löschen) aus.

AWS CLI

Sie können einen DB-Cluster-Snapshot mit dem AWS CLI Befehl löschendelete-db-cluster-snapshot.

Zum Löschen eines DB-Cluster-Snapshots werden die folgenden Optionen verwendet.

- `--db-cluster-snapshot-identifier` – Der Bezeichner des DB-Cluster-Snapshots.

Example

Der folgende Code löscht den DB-Cluster-Snapshot `mydbclustersnapshot`.

Für Linux, macOSoder Unix:

```
aws rds delete-db-cluster-snapshot \
    --db-cluster-snapshot-identifier mydbclustersnapshot
```

Windows:

```
aws rds delete-db-cluster-snapshot ^
    --db-cluster-snapshot-identifier mydbclustersnapshot
```

RDS-API

Sie können einen DB-Cluster-Snapshot mithilfe der Amazon RDS-API-Operation DeleteDBClusterSnapshot löschen.

Zum Löschen eines DB-Cluster-Snapshots werden die folgenden Parameter verwendet.

- `DBClusterSnapshotIdentifier` – Der Bezeichner des DB-Cluster-Snapshots.

Tutorial: Wiederherstellen eines DB-Clusters von Amazon Aurora aus einem DB-Cluster-Snapshot

Bei der Arbeit mit Amazon Aurora ist häufig eine DB-Instance vorhanden, mit der Sie gelegentlich arbeiten, aber die Sie nicht ständig brauchen. Sie können beispielsweise einen DB-Cluster verwenden, um die Daten für einen Bericht zu speichern, den Sie nur vierteljährlich erstellen. Eine Möglichkeit, in einem solchen Szenario Geld zu sparen, besteht darin, nach Abschluss des Berichts einen DB-Cluster-Snapshot des DB-Clusters zu verwenden. Anschließend löschen Sie den DB-Cluster und stellen ihn wieder her, wenn Sie neue Daten hochladen und den Bericht im nächsten Quartal erstellen müssen.

Wenn Sie einen DB-Cluster wiederherstellen, können Sie den Namen des DB-Cluster-Snapshots für die Wiederherstellung angeben. Anschließend vergeben Sie einen Namen für den neuen DB-Cluster, der durch den Wiederherstellungsvorgang erstellt wird. Weitere Informationen zum Wiederherstellen von DB-Cluster aus Snapshots finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.

In diesem Tutorial führen wir ein Upgrade des wiederhergestellten DB-Clusters von Aurora MySQL Version 2 (mit MySQL 5.7 kompatibel) auf Aurora MySQL Version 3 (mit MySQL 8.0 kompatibel) durch.

Wiederherstellen eines DB-Clusters aus einem DB-Cluster-Snapshot über die Amazon-RDS-Konsole

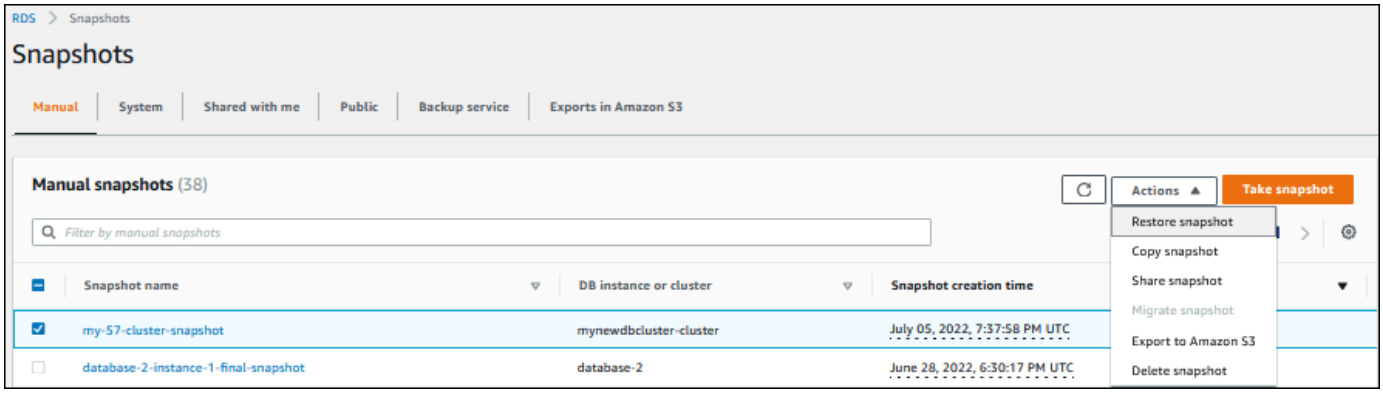
Wenn Sie einen DB-Cluster aus einem Snapshot über die AWS Management Console wiederherstellen, wird auch die primäre (Writer-)DB-Instance erstellt.

> **Note**
>
> Während die primäre DB-Instance erstellt wird, erscheint sie als Reader-Instance, wird aber nach der Erstellung zur Writer-Instance.

So stellen Sie einen DB-Cluster aus einem DB-Cluster-Snapshot wieder her

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

3. Wählen Sie den DB-Cluster-Snapshot für die Wiederherstellung aus.
4. Wählen Sie in Actions (Aktionen) die Option Restore Snapshot (Snapshot wiederherstellen) aus.

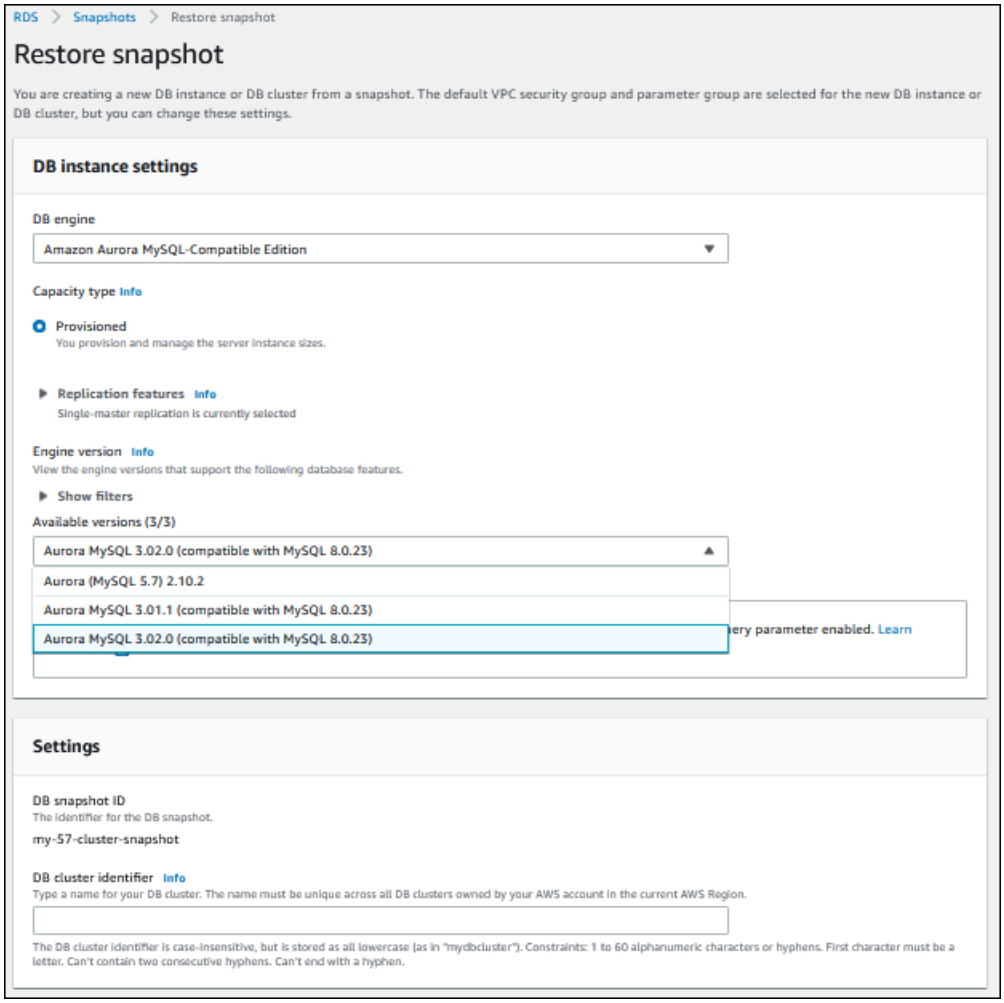


Anschließend wird die Seite Restore snapshot (Snapshot wiederherstellen) angezeigt.

5. Führen Sie unter DB instance settings (DB-Instance-Einstellungen) folgende Schritte aus:

   a. Verwenden Sie die Standardeinstellung für DB engine (DB-Engine).

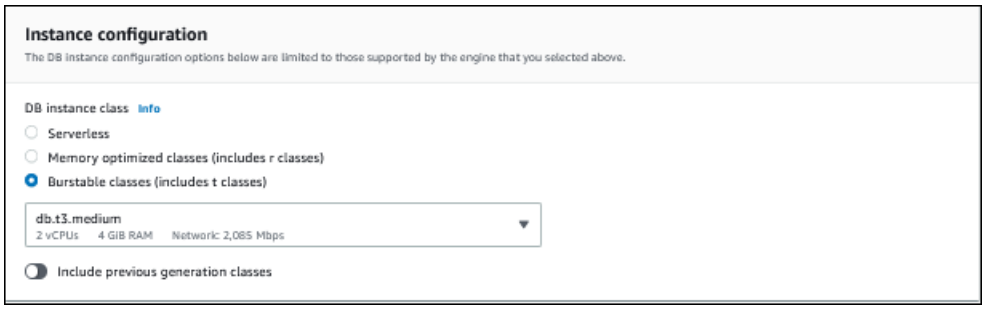
   b. Wählen Sie für Available versions (Verfügbare Versionen) eine mit MySQL 8.0 kompatible Version aus, z. B. Aurora MySQL 3.02.0 (compatible with MySQL 8.0.23) (Aurora MySQL 3.02.0 (mit MySQL 8.0.23 kompatibel).



6. Geben Sie unter Settings (Einstellungen) für DB cluster identifier (DB-Cluster-Kennung) den eindeutigen Namen ein, den Sie für den wiederhergestellten DB-Cluster verwenden möchten, zum Beispiel **`my-80-cluster`**.
7. Verwenden Sie unter Connectivity (Konnektivität) die Standardeinstellungen für folgende Optionen:
   - Virtual Private Cloud (VPC)
   - DB subnet group (DB-Subnetzgruppe)
   - Öffentlicher Zugriff
   - VPC security group (firewall) (VPC-Sicherheitsgruppe (Firewall))
8. Wählen Sie die DB instance class (DB-Instance-Klasse) aus.

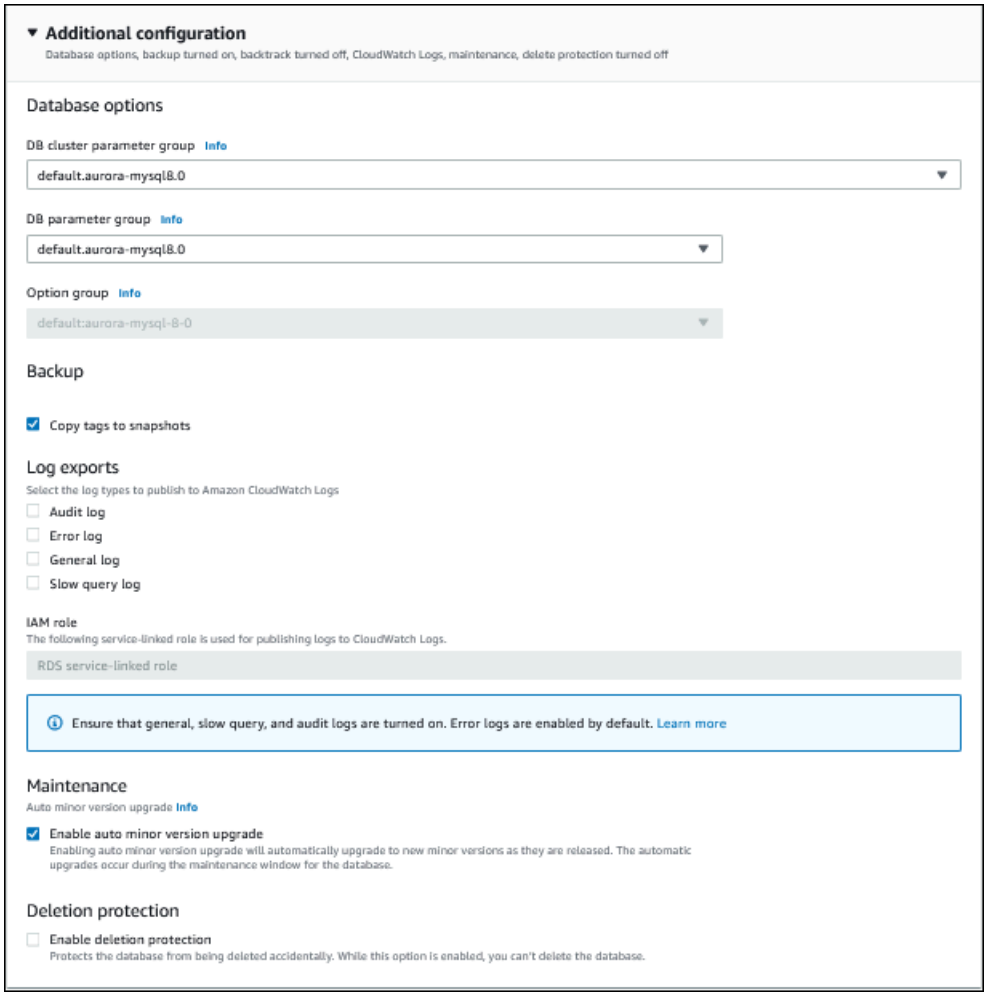
Wählen Sie für dieses Tutorial Burstable classes (includes t classes) (Burst-fähige Klassen (einschließlich t-Klassen)) und dann db.t3.medium aus.

> **Note**
>
> Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter DB-Instance-Klassenarten.



9. Verwenden Sie für Database authentication (Datenbankauthentifizierung) die Standardeinstellung.
10. Für Encryption (Verschlüsselung) verwenden Sie die Standardeinstellungen.

    Wenn der Quell-DB-Cluster für den Snapshot verschlüsselt wurde, wird der wiederhergestellte DB-Cluster ebenfalls verschlüsselt. Die Verschlüsselung kann nicht aufgehoben werden.
11. Erweitern Sie Additional configuration (Zusätzliche Konfiguration) unten auf der Seite.



12. Nehmen Sie die folgenden Einstellungen vor:

    a. Verwenden Sie für dieses Tutorial den Standardwert für DB cluster parameter group (DB-Cluster-Parametergruppe).

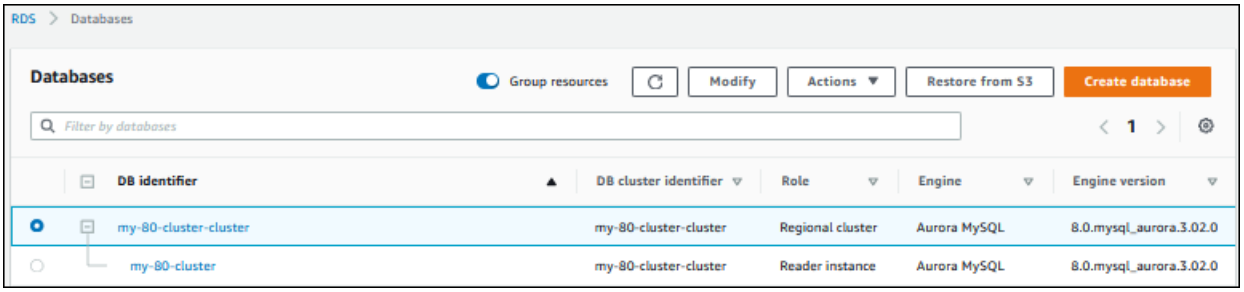
    b. Verwenden Sie für dieses Tutorial den Standardwert für DB parameter group (DB-Parametergruppe).

    c. Aktivieren Sie für Log exports (Protokollexporte) alle Kontrollkästchen.

    d. Aktivieren Sie für Deletion protection (Löschschutz) das Kontrollkästchen Enable deletion protection (Löschschutz aktivieren).

13. Klicken Sie auf Restore DB Instance (DB-Instance wiederherstellen).

Auf der Seite Databases (Datenbanken) wird der wiederhergestellte DB-Cluster mit dem Status `Creating` angezeigt.



Während die primäre DB-Instance erstellt wird, erscheint sie als Reader-Instance, wird aber nach der Erstellung zur Writer-Instance.

Wiederherstellen eines DB-Clusters aus einem DB-Cluster-Snapshot mithilfe der AWS CLI

Das Wiederherstellen eines DB-Clusters aus einem Snapshot mithilfe der AWS CLI erfolgt in zwei Schritten:

1. Wiederherstellen eines DB-Clusters mit dem restore-db-cluster-from-snapshot-Befehl
2. Erstellen der primären (Writer-)DB-Instance mit dem create-db-instance Befehl

Wiederherstellen eines DB-Clusters

Verwenden Sie den Befehl `restore-db-cluster-from-snapshot`. Die folgenden Optionen sind erforderlich:

- `--db-cluster-identifier` – Der Name des wiederhergestellten DB-Clusters.
- `--snapshot-identifier` – Der Name des DB-Snapshots, der für die Wiederherstellung verwendet wird.
- `--engine` – Die Datenbank-Engine des wiederhergestellten DB-Clusters. Sie muss mit der Datenbank-Engine des Quell-DB-Clusters kompatibel sein.

  Es stehen folgende Optionen zur Verfügung:

  - `aurora-mysql` – mit Aurora MySQL 5.7 und 8.0 kompatibel
  - `aurora-postgresql` – mit Aurora PostgreSQL kompatibel

  In diesem Beispiel verwenden wir `aurora-mysql`.
- `--engine-version` – die Version des zu erstellenden DB-Clusters In diesem Beispiel verwenden wir eine mit MySQL 8.0 kompatible Version.

Im folgenden Beispiel wird ein mit Aurora MySQL 8.0 kompatibler DB-Cluster mit dem Namen `my-new-80-cluster` aus einem DB-Cluster-Snapshot namens `my-57-cluster-snapshot` wiederhergestellt.

So stellen Sie den DB-Cluster wieder her

- Verwenden Sie einen der folgenden Befehle.

  Für Linux, macOSoder Unix:

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier my-new-80-cluster \
    --snapshot-identifier my-57-cluster-snapshot \
    --engine aurora-mysql \
    --engine-version 8.0.mysql_aurora.3.02.0
```

  Windows:

```
aws rds restore-db-cluster-from-snapshot ^
    --db-cluster-identifier my-new-80-cluster ^
    --snapshot-identifier my-57-cluster-snapshot ^
    --engine aurora-mysql ^
    --engine-version 8.0.mysql_aurora.3.02.0
```

Die Ausgabe sieht in etwa folgendermaßen aus.

```
{
    "DBCluster": {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "eu-central-1b",
            "eu-central-1c",
            "eu-central-1a"
        ],
        "BackupRetentionPeriod": 14,
        "DatabaseName": "",
        "DBClusterIdentifier": "my-new-80-cluster",
        "DBClusterParameterGroup": "default.aurora-mysql8.0",
        "DBSubnetGroup": "default",
        "Status": "creating",
```

```
        "Endpoint": "my-new-80-cluster.cluster-############.eu-
central-1.rds.amazonaws.com",
        "ReaderEndpoint": "my-new-80-cluster.cluster-ro-############.eu-
central-1.rds.amazonaws.com",
        "MultiAZ": false,
        "Engine": "aurora-mysql",
        "EngineVersion": "8.0.mysql_aurora.3.02.0",
        "Port": 3306,
        "MasterUsername": "admin",
        "PreferredBackupWindow": "01:55-02:25",
        "PreferredMaintenanceWindow": "thu:21:14-thu:21:44",
        "ReadReplicaIdentifiers": [],
        "DBClusterMembers": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-########",
                "Status": "active"
            }
        ],
        "HostedZoneId": "Z1RLNU0EXAMPLE",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:eu-central-1:123456789012:key/#######-5ccc-49cc-8aaa-
############",
        "DbClusterResourceId": "cluster-ZZ12345678ITSJUSTANEXAMPLE",
        "DBClusterArn": "arn:aws:rds:eu-central-1:123456789012:cluster:my-new-80-
cluster",
        "AssociatedRoles": [],
        "IAMDatabaseAuthenticationEnabled": false,
        "ClusterCreateTime": "2022-07-05T20:45:42.171000+00:00",
        "EngineMode": "provisioned",
        "DeletionProtection": false,
        "HttpEndpointEnabled": false,
        "CopyTagsToSnapshot": false,
        "CrossAccountClone": false,
        "DomainMemberships": [],
        "TagList": []
    }
}
```

Erstellen der primären (Writer-)DB-Instance

Verwenden Sie den Befehl `create-db-instance`, um die primäre (Writer-)DB-Instance zu erstellen. Die folgenden Optionen sind erforderlich:

- `--db-cluster-identifier` – Der Name des wiederhergestellten DB-Clusters.
- `--db-instance-identifier` – Der Name der primären DB-Instance.
- `--db-instance-class` – Die Instance-Klasse der primären DB-Instance. In diesem Beispiel verwenden wir `db.t3.medium`.

  > **Note**
  >
  > Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter DB-Instance-Klassenarten.

- `--engine` – Die Datenbank-Engine der primären DB-Instance. Es muss dieselbe Datenbank-Engine sein, die der wiederhergestellte DB-Cluster verwendet.

  Es stehen folgende Optionen zur Verfügung:

  - `aurora-mysql` – mit Aurora MySQL 5.7 und 8.0 kompatibel
  - `aurora-postgresql` – mit Aurora PostgreSQL kompatibel

  In diesem Beispiel verwenden wir `aurora-mysql`.

Im folgenden Beispiel wird eine primäre (Writer-)DB-Instance mit dem Namen `my-new-80-cluster-instance` im wiederhergestellten DB-Cluster, der mit Aurora MySQL 8.0 kompatibel ist, namens `my-new-80-cluster` erstellt.

So erstellen Sie die primäre DB-Instance

- Verwenden Sie einen der folgenden Befehle.

  Für Linux, macOSoder Unix:

  ```
  aws rds create-db-instance \
      --db-cluster-identifier my-new-80-cluster \
      --db-instance-identifier my-new-80-cluster-instance \
      --db-instance-class db.t3.medium \
      --engine aurora-mysql
  ```

  Windows:

```
aws rds create-db-instance ^
    --db-cluster-identifier my-new-80-cluster ^
    --db-instance-identifier my-new-80-cluster-instance ^
    --db-instance-class db.t3.medium ^
    --engine aurora-mysql
```

Die Ausgabe sieht in etwa folgendermaßen aus.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "my-new-80-cluster-instance",
        "DBInstanceClass": "db.t3.medium",
        "Engine": "aurora-mysql",
        "DBInstanceStatus": "creating",
        "MasterUsername": "admin",
        "AllocatedStorage": 1,
        "PreferredBackupWindow": "01:55-02:25",
        "BackupRetentionPeriod": 14,
        "DBSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-########",
                "Status": "active"
            }
        ],
        "DBParameterGroups": [
            {
                "DBParameterGroupName": "default.aurora-mysql8.0",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-2305ca49",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "eu-central-1a"
```

```
                    },
                    "SubnetOutpost": {},
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "eu-central-1b"
                    },
                    "SubnetOutpost": {},
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "eu-central-1c"
                    },
                    "SubnetOutpost": {},
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sat:02:41-sat:03:11",
        "PendingModifiedValues": {},
        "MultiAZ": false,
        "EngineVersion": "8.0.mysql_aurora.3.02.0",
        "AutoMinorVersionUpgrade": true,
        "ReadReplicaDBInstanceIdentifiers": [],
        "LicenseModel": "general-public-license",
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "default:aurora-mysql-8-0",
                "Status": "in-sync"
            }
        ],
        "PubliclyAccessible": false,
        "StorageType": "aurora",
        "DbInstancePort": 0,
        "DBClusterIdentifier": "my-new-80-cluster",
        "StorageEncrypted": true,
        "KmsKeyId": "arn:aws:kms:eu-central-1:534026745191:key/#######-5ccc-49cc-8aaa-
############",
        "DbiResourceId": "db-5C6UT5PU0YETANOTHEREXAMPLE",
        "CACertificateIdentifier": "rds-ca-2019",
```

```
        "DomainMemberships": [],
        "CopyTagsToSnapshot": false,
        "MonitoringInterval": 0,
        "PromotionTier": 1,
        "DBInstanceArn": "arn:aws:rds:eu-central-1:123456789012:db:my-new-80-cluster-
instance",
        "IAMDatabaseAuthenticationEnabled": false,
        "PerformanceInsightsEnabled": false,
        "DeletionProtection": false,
        "AssociatedRoles": [],
        "TagList": []
    }
}
```

Überwachung von Metriken in einem Amazon-Aurora-Cluster

Amazon Aurora verwendet einen Cluster replizierter Datenbankserver. Das Überwachen eines Aurora-Clusters erfordert in der Regel die Überprüfung des Zustands mehrerer DB-Instances. Die Instances haben möglicherweise spezielle Rollen, die hauptsächlich Schreiboperationen, nur Lesevorgänge oder eine Kombination verarbeiten. Sie überwachen auch den Gesamtzustand des Clusters, indem Sie die Replikationsverzögerung messen. Dabei handelt es sich um die Zeitspanne, in der Änderungen, die von einer DB-Instance vorgenommen wurden, für die anderen Instances verfügbar sind.

Themen

Übersicht über die Überwachung von Metriken in Amazon Aurora

Die Überwachung ist ein wichtiger Teil der Aufrechterhaltung von Zuverlässigkeit, Verfügbarkeit und Performance von Amazon Aurora und Ihren AWS-Lösungen. Um Mehrpunktfehler einfacher zu debuggen, empfehlen wir, Überwachungsdaten aus allen Teilen Ihrer AWS-Lösung zu erfassen.

Themen

Überwachungsplan

Bevor Sie mit der Überwachung von Amazon Aurora beginnen, sollten Sie einen Überwachungsplan erstellen. Dieser Plan sollte die folgenden Fragen beantworten:

- Was sind Ihre Ziele bei der Überwachung?
- Welche Ressourcen möchten Sie überwachen?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungs-Tools möchten Sie verwenden?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Leistungsbasislinie

Um Ihre Überwachungsziele zu erreichen, müssen Sie eine Basislinie erstellen. Messen Sie dazu die Leistung unter unterschiedlichen Lastbedingungen zu verschiedenen Zeiten in Ihrer Amazon Aurora-Umgebung. Sie können Metriken wie die folgenden überwachen:

- Netzwerkdurchsatz
- Client-Verbindungen
- I/O für Lese-, Schreib- oder Metadatenoperationen
- Burst-Guthaben für Ihre DB-Instances

Es wird empfohlen, historische Leistungsdaten für Amazon Aurora zu speichern.. Mithilfe der gespeicherten Daten können Sie die aktuelle Leistung mit früheren Trends vergleichen. Sie können so auch normale Leistungsmuster von Anomalien unterscheiden und Methoden zur Behebung von Problemen entwickeln.

Richtlinien zur Leistung

Die zulässigen Werte für Leistungsmetriken sind im Allgemeinen davon abhängig, wie die Basislinie aussieht, und wofür die Anwendung gedacht ist. Prüfen Sie, ob dauerhafte oder tendenzielle Abweichungen von Ihrer Ausgangsbasis vorliegen. Die folgenden Metriken sind häufig die Ursache von Leistungsproblemen:

- Hohe CPU- oder RAM-Nutzung – Hohe Werte für die CPU- oder RAM-Nutzung können angemessen sein, wenn sie der Zielsetzung Ihrer Anwendung entsprechen (z. B. in Bezug auf Durchsatz oder Gleichzeitigkeit) und erwartet werden.
- Nutzung des Datenträgerplatzes – Überprüfen Sie die Nutzung des Datenträgerplatzes, wenn konsistent 85 Prozent oder mehr des gesamten Datenträgerplatzes belegt werden. Prüfen Sie, ob Daten in der Instance gelöscht oder auf einem anderen System archiviert werden können, um Speicherplatz freizugeben.
- Netzwerkdatenverkehr – Wenden Sie sich an Ihren Systemadministrator, um zu erfahren, welcher Durchsatz für Ihr Domänennetzwerk und Ihre Internetverbindung erwartet wird. Überprüfen Sie den Netzwerkdatenverkehr, wenn der Durchsatz dauerhaft unter dem erwarteten Wert liegt.
- Datenbankverbindungen – Sie sollten eine Einschränkung der Datenbankverbindungen in Betracht ziehen, wenn eine große Anzahl von Benutzerverbindungen sowie auch eine Abnahme der Instance-Leistung und -Reaktionszeit zu erkennen sind. Die optimale Anzahl der Benutzerverbindungen für Ihre DB-Instance ist von der Instance-Klasse und der Komplexität der ausgeführten Operationen abhängig. Um die Anzahl der Datenbankverbindungen zu bestimmen, ordnen Sie Ihre DB-Instance einer Parametergruppe zu, für die der Parameter `User Connections` auf einen anderen Wert als „0“ (unbegrenzt) gesetzt ist. Sie können eine entweder eine vorhandene Parametergruppe verwenden oder eine neue erstellen. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen.
- IOPS-Metriken – Die erwarteten Werte für IOPS-Metriken sind von der Datenträgerspezifikation und der Serverkonfiguration abhängig. Verwenden Sie die Basiswerte als typische Werte. Prüfen Sie, ob dauerhafte Abweichungen von den Werten Ihrer Ausgangsbasis vorliegen. Für eine optimale IOPS-Leistung stellen Sie sicher, dass Ihr typisches Working Set in den Speicher passt, um Lese- und Schreibvorgänge zu minimieren.

Wenn die Leistung außerhalb der festgelegten Baseline liegt, müssen Sie möglicherweise Änderungen vornehmen, um die Datenbankverfügbarkeit für Ihre Workload zu optimieren. Beispielsweise müssen Sie möglicherweise die Instance-Klasse Ihrer DB-Instance ändern. Oder Sie müssen möglicherweise die Anzahl der DB-Instance und Read Replicas ändern, die für Clients verfügbar sind.

Überwachungstools

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Aurora und Ihren anderen AWS-Lösungen. AWS bietet verschiedene Überwachungswerkzeuge, um Amazon Aurora zu beobachten, Probleme zu melden und ggf. automatisch Maßnahmen ergreifen zu können.

Themen

Automatisierte Überwachungstools

Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

Themen

Amazon-Aurora-Cluster-Status und Empfehlungen

Sie können die folgenden automatisierten Tools zur Überwachung von Amazon Aurora verwenden und auftretende Probleme melden:

- Amazon Aurora--Cluster-Status – Zeigen Sie über die Amazon-RDS-Konsole, den AWS CLI oder die RDS-API-Details zum aktuellen Status Ihres -Clusters an.
- Amazon Aurora Empfehlungen — Reagieren Sie auf automatisierte Empfehlungen für Datenbankressourcen wie DB-Instances, DB-Cluster, und DB-Cluster-Parametergruppen. Weitere Informationen finden Sie unter Anzeigen und Beantworten von Amazon-Aurora-Empfehlungen.

Amazon- CloudWatch Metriken für Amazon Aurora

Amazon Aurora lässt sich CloudWatch für zusätzliche Überwachungsfunktionen in Amazon integrieren.

- Amazon CloudWatch – Dieser Service überwacht Ihre -AWSRessourcen und die Anwendungen, auf denen Sie ausgeführt werden, AWS in Echtzeit. Sie können die folgenden Amazon-CloudWatch Funktionen mit Amazon Aurora verwenden:
  - Amazon- CloudWatch Metriken – Amazon Aurora sendet CloudWatch automatisch jede Minute Metriken für jede aktive Datenbank an . Sie erhalten keine zusätzlichen Gebühren für Amazon-RDS-Metriken in CloudWatch. Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora.
  - Amazon- CloudWatch Alarme – Sie können eine einzelne Amazon-Aurora-Metrik über einen bestimmten Zeitraum überwachen. Anschließend können Sie eine oder mehrere Aktionen basierend auf dem Wert der Metrik relativ zu einem von Ihnen festgelegten Schwellenwert ausführen.

Amazon RDS Performance Insights und Betriebssystemüberwachung

Sie können die folgenden automatisierten Tools zum Überwachen der Amazon Aurora-Leistung verwenden:

- Amazon RDS Performance Insights – Bewerten Sie die Belastung Ihrer Datenbank und bestimmen Sie, wann und wo Maßnahmen ergriffen werden sollen. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .
- Amazon RDS Enhanced Monitoring – Sehen Sie sich in Echtzeit Metriken für das Betriebssystem an. Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).

Integrierte Services

Die folgenden AWS-Services sind in Amazon Aurora integriert:

- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen einfach mit Daten aus einer Vielzahl von Quellen verbinden können. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora-Ereignissen.

- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von -Amazon-Aurora-Instances, und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. Weitere Informationen finden Sie unter Überwachen von Amazon Aurora-Protokolldateien.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Konto-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora-API-Aufrufen in AWS CloudTrail.
- Database Activity Streams ist eine Amazon-Aurora-Funktion, die einen near-real-time Stream der Aktivität in Ihrer -DB-Cluster bereitstellt. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.
- DevOpsGuru für RDS ist eine Funktion von Amazon DevOpsGuru, die Machine Learning auf Performance-Insights-Metriken für Amazon-Aurora-Datenbanken anwendet. Weitere Informationen finden Sie unter Analysieren von Aurora-Leistungsanomalien mit Amazon DevOps Guru für Amazon RDS.

Manuelle Überwachungstools

Sie müssen die Elemente, die die CloudWatch Alarme nicht abdecken, manuell überwachen. Amazon RDS CloudWatch AWS Trusted Advisor und andere AWSKonsolen-Dashboards bieten einen at-a-glance Überblick über den Zustand Ihrer AWS Umgebung. Wir empfehlen, auch die Protokolldateien auf Ihrer DB-Instance zu überprüfen.

- In der Amazon RDS-Konsole können Sie die folgenden Elemente für Ihre Ressourcen überwachen:
  - Die Anzahl der Verbindungen zu einer DB-Instance
  - Die Anzahl der Lese- und Schreibvorgänge in einer DB-Instance
  - Der von einer DB-Instance aktuell verwendete Speicherplatz
  - Der aktuell verwendete Arbeitsspeicher und die aktuelle CPU-Nutzung einer DB-Instance
  - Der Netzwerkdatenverkehr von und zu einer DB-Instance
- Über das Trusted Advisor-Dashboard können Sie die folgenden Prüfungen in Bezug auf die Kostenoptimierung, Sicherheit, Fehlertoleranz und Leistungssteigerung einsehen:
  - Amazon RDS-DB-Instances im Leerlauf
  - Zugriffsrisiko für Amazon RDS-Sicherheitsgruppen
  - Amazon RDS-Backups
  - Amazon RDS-Multi-AZ

- Barrierefreiheit von Aurora-DB-Instances

  Weitere Informationen zu diesen Prüfungen finden Sie unter Trusted Advisor – bewährte Methoden (Prüfungen).

- CloudWatch Die -Startseite zeigt:
  - Aktuelle Alarme und Status
  - Diagramme mit Alarmen und Ressourcen
  - Servicestatus

  Darüber hinaus können Sie mit Folgendes CloudWatch tun:

  - Erstellen Sie benutzerdefinierte Dashboards zur Überwachung der Services, die Ihnen wichtig sind.
  - Aufzeichnen von Metrikdaten, um Probleme zu beheben und Trends zu erkennen.
  - Suchen und durchsuchen aller AWS-Ressourcenmetriken
  - Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden.

Status der anzeigen

Mit der Amazon RDS-Konsole können Sie schnell auf den Status Ihrer zugreifen.

Themen

Anzeigen eines Amazon Aurora-DB-Clusters

Es gibt mehrere Möglichkeiten, Informationen zu Ihren Amazon Aurora-DB-Clustern und DB-Instances in Ihren DB-Clustern anzuzeigen.

- Sie können DB-Cluster und DB-Instances in der Amazon RDS-Konsole durch Auswahl von Databases (Datenbanken) in der Navigationsebene anzeigen.
- Sie können DB-Cluster- und DB-Instance-Informationen mit AWS Command Line Interface (AWS CLI) abrufen.
- Sie können Informationen über DB-Cluster und DB-Instances mit der Amazon RDS-API abrufen.

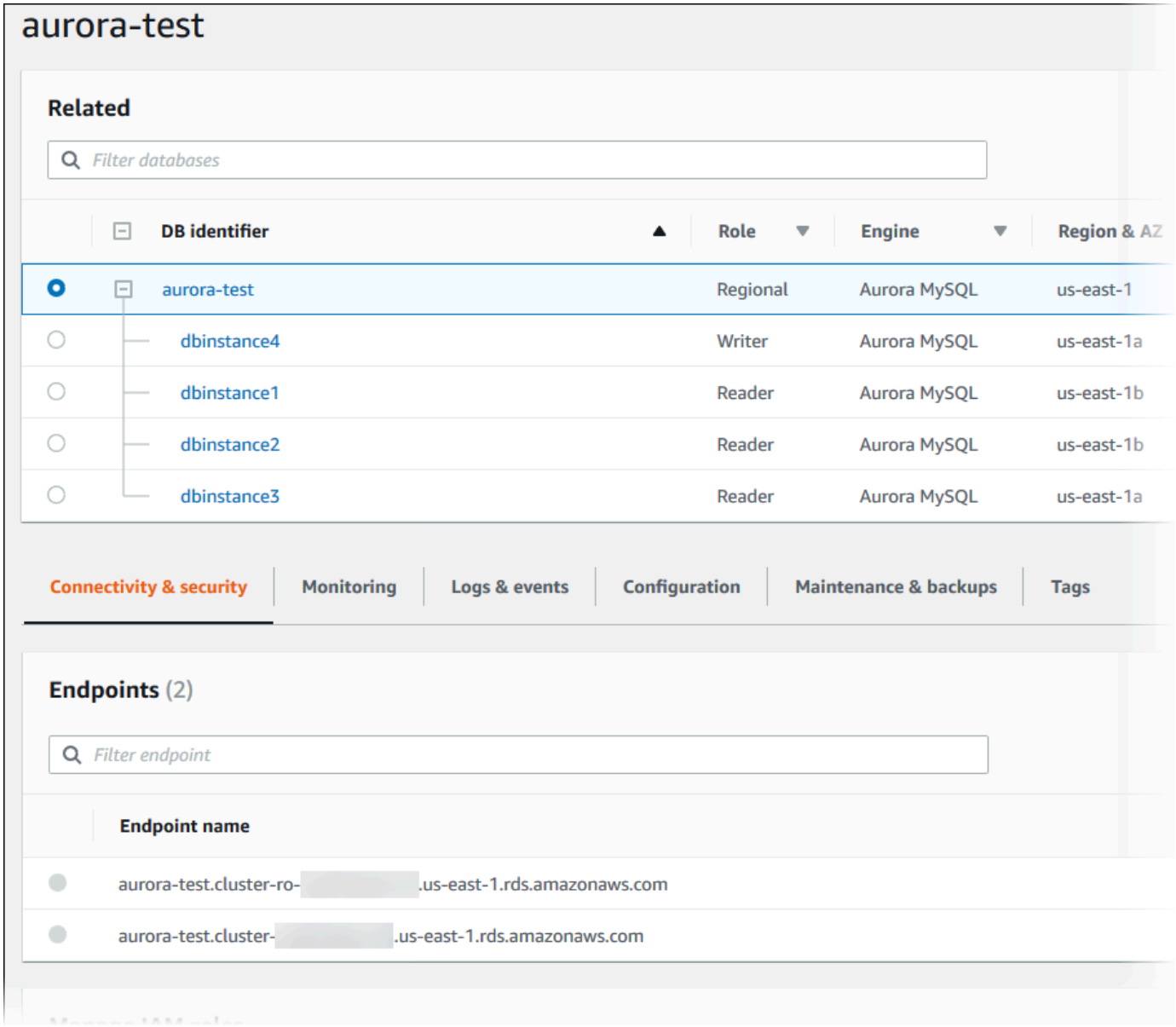
Konsole

In der Amazon RDS Konsole können Sie Details zu einem DB-Cluster anzeigen, indem Sie im Navigationsbereich der Konsole die Option Datenbanken auswählen. Details zu DB-Instances, die einem Amazon Aurora-DB-Cluster angehören, können Sie auch anzeigen.

So zeigen Sie DB-Cluster in der Amazon-RDS-Konsole an bzw. ändern sie

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie in der Liste den Namen des Aurora-DB-Clusters aus, den Sie anzeigen möchten.

   In der folgenden Abbildung wird beispielsweise die Detailseite für den DB-Cluster mit der Bezeichnung `aurora-test` angezeigt. Für den DB-Cluster werden in der Liste DB identifier (DB-Kennung) vier DB-Instances angezeigt. Die Writer-DB-Instance, `dbinstance4`, ist die primäre DB-Instance für den DB-Cluster.



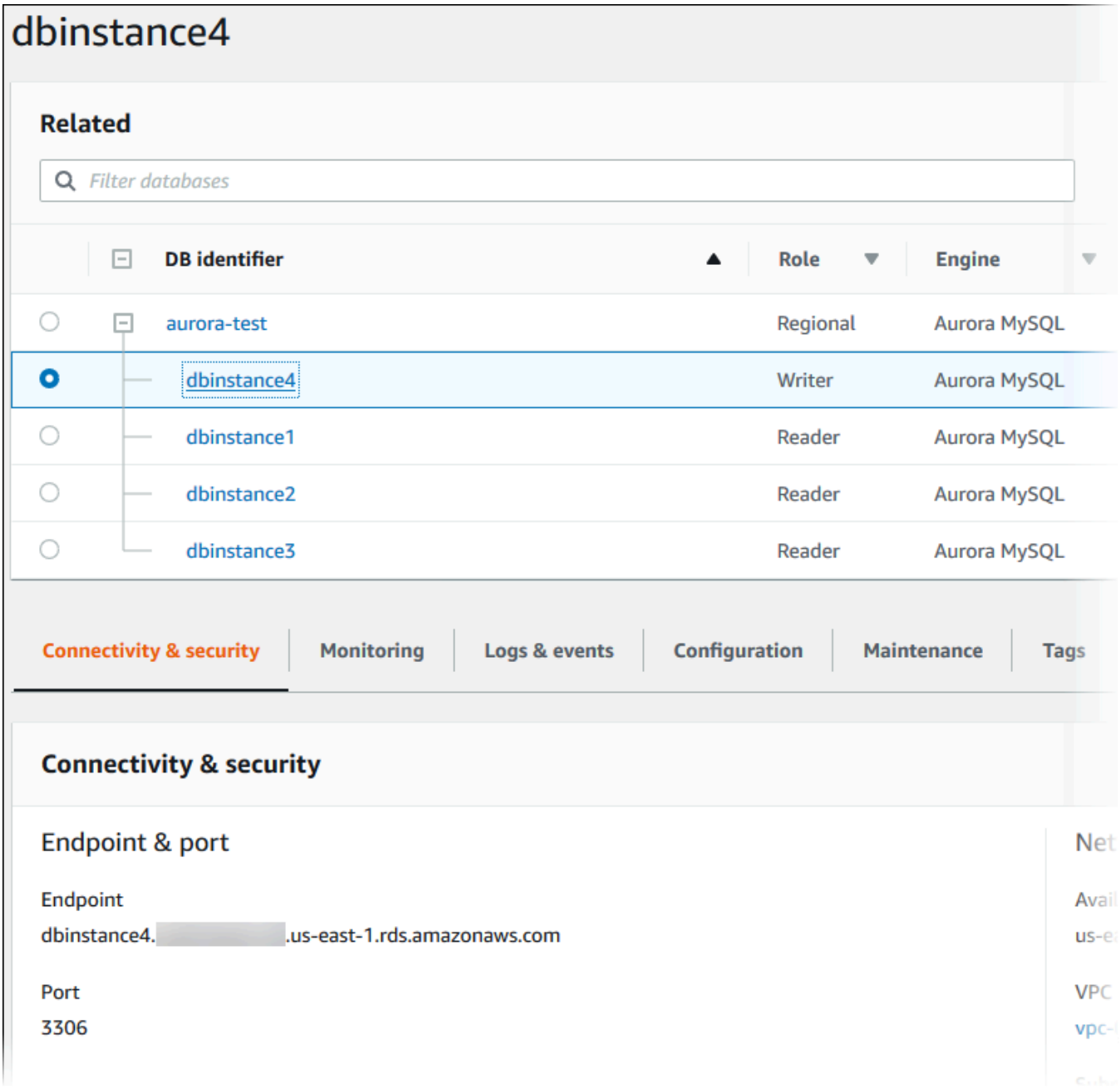
4. Um einen DB-Cluster zu ändern, wählen Sie ihn in der Liste aus gefolgt von Modify (Ändern).

So zeigen Sie DB-Instances eines DB-Clusters in der Amazon-RDS-Konsole an bzw. ändern sie

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Führen Sie eine der folgenden Aktionen aus:

   - Um eine DB-Instance anzuzeigen, wählen Sie eine aus der Liste aus, die Mitglied des Aurora-DB-Clusters ist.

Wenn Sie zum Beispiel auf die `dbinstance4` DB-Instance-Kennung klicken, zeigt die Konsole die Detailseite für die `dbinstance4` DB-Instance an, wie in der folgenden Abbildung dargestellt.



- Um eine DB-Instance zu ändern, wählen Sie die DB-Instance aus der Liste und Modify (Ändern) aus. Weitere Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

AWS CLI

Um DB-Cluster-Informationen mithilfe von anzuzeigen AWS CLI, verwenden Sie den Befehl describe-db-clusters. Der folgende AWS CLI Befehl listet beispielsweise die DB-Clusterinformationen für alle DB-Cluster in der `us-east-1` Änderungsregion für das konfigurierte Konto auf. AWS

```
aws rds describe-db-clusters --region us-east-1
```

Der Befehl gibt die folgende Ausgabe zurück, wenn Ihre für die JSON-Ausgabe konfiguriert AWS CLI ist.

```
{
    "DBClusters": [
        {
            "Status": "available",
            "Engine": "aurora-mysql",
            "Endpoint": "sample-cluster1.cluster-123456789012.us-
east-1.rds.amazonaws.com"
            "AllocatedStorage": 1,
            "DBClusterIdentifier": "sample-cluster1",
            "MasterUsername": "mymasteruser",
            "EarliestRestorableTime": "2023-03-30T03:35:42.563Z",
            "DBClusterMembers": [
                {
                    "IsClusterWriter": false,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "DBInstanceIdentifier": "sample-replica"
                },
                {
                    "IsClusterWriter": true,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "DBInstanceIdentifier": "sample-primary"
                }
            ],
            "Port": 3306,
            "PreferredBackupWindow": "03:34-04:04",
            "VpcSecurityGroups": [
                {
                    "Status": "active",
                    "VpcSecurityGroupId": "sg-ddb65fec"
                }
            ],
            "DBSubnetGroup": "default",
```

```
            "StorageEncrypted": false,
            "DatabaseName": "sample",
            "EngineVersion": "5.7.mysql_aurora.2.11.0",
            "DBClusterParameterGroup": "default.aurora-mysql5.7",
            "BackupRetentionPeriod": 1,
            "AvailabilityZones": [
                "us-east-1b",
                "us-east-1c",
                "us-east-1d"
            ],
            "LatestRestorableTime": "2023-03-31T20:06:08.903Z",
            "PreferredMaintenanceWindow": "wed:08:15-wed:08:45"
        },
        {
            "Status": "available",
            "Engine": "aurora-mysql",
            "Endpoint": "aurora-sample.cluster-123456789012.us-
east-1.rds.amazonaws.com",
            "AllocatedStorage": 1,
            "DBClusterIdentifier": "aurora-sample-cluster",
            "MasterUsername": "mymasteruser",
            "EarliestRestorableTime": "2023-03-30T10:21:34.826Z",
            "DBClusterMembers": [
                {
                    "IsClusterWriter": false,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "DBInstanceIdentifier": "aurora-replica-sample"
                },
                {
                    "IsClusterWriter": true,
                    "DBClusterParameterGroupStatus": "in-sync",
                    "DBInstanceIdentifier": "aurora-sample"
                }
            ],
            "Port": 3306,
            "PreferredBackupWindow": "10:20-10:50",
            "VpcSecurityGroups": [
                {
                    "Status": "active",
                    "VpcSecurityGroupId": "sg-55da224b"
                }
            ],
            "DBSubnetGroup": "default",
            "StorageEncrypted": false,
```

```
            "DatabaseName": "sample",
            "EngineVersion": "5.7.mysql_aurora.2.11.0",
            "DBClusterParameterGroup": "default.aurora-mysql5.7",
            "BackupRetentionPeriod": 1,
            "AvailabilityZones": [
                "us-east-1b",
                "us-east-1c",
                "us-east-1d"
            ],
            "LatestRestorableTime": "2023-03-31T20:00:11.491Z",
            "PreferredMaintenanceWindow": "sun:03:53-sun:04:23"
        }
    ]
}
```


RDS-API

Um Informationen zu DB-Clustern über die Amazon RDS-API anzuzeigen, verwenden Sie die Aktion DescribeDBClusters.

Anzeigen des DB-Clusterstatus

Der Status eines DB-Clusters zeigt seinen Zustand an. Sie können den Status eines DB-Clusters und der Cluster-Instances mithilfe der Amazon RDS-Konsole AWS CLI, der oder der API anzeigen.

> **Note**
>
> Aurora führt daneben noch einen anderen Statuswert, der als Wartungsstatus bezeichnet wird, und der in der Spalte Wartung in der Amazon RDS-Konsole angezeigt wird. Dieser Wert gibt den Status der Wartungspatches an, die auf dem DB-Cluster installiert werden müssen. Der Wartungsstatus ist von dem Status des DB-Clusters unabhängig. Weitere Informationen zum Wartungsstatus finden Sie unter Anwenden von Updates für eine DB-einen DB-Cluster.

Die möglichen Statuswerte für DB-Cluster sind in der folgenden Tabelle aufgeführt.

DB-Cluster-Status	Berechnet	Beschreibung
Verfügbar	Berechnet	Der DB-Cluster ist stabil und verfügbar. Wenn ein Aurora Serverless Cluster verfügbar und angehalten ist, wird Ihnen nur der Speicher berechnet.
Backing-up	Berechnet	Der DB-Cluster wird derzeit gesichert.
backtracking	Berechnet	Der DB-Cluster wird derzeit rückverfolgt. Dieser Status gilt nur für Aurora MySQL.
Cloning-failed	Nicht berechnet	Das Klonen eines DB-Clusters ist fehlgesch lagen.
Erstellen	Nicht berechnet	Der DB-Cluster wird gerade erstellt. Während der DB-Cluster erstellt wird, kann nicht darauf zugegriffen werden.
Wird gelöscht	Nicht berechnet	Der DB-Cluster wird gerade gelöscht.
Failing-over	Berechnet	Es wird gerade ein Failover von der primären Instance in ein Aurora-Replica durchgeführt.

DB-Cluster-Status	Berechnet	Beschreibung
Inaccessible-encryption-credentials	Nicht berechnet	Auf die zum Verschlüsseln oder Entschlüsseln des DB-Clusters AWS KMS key verwendeten Dateien kann nicht zugegriffen oder diese wiederhergestellt werden.
Inaccessible-encryption-credentials-recoverable	Berechnet für Speicher	Es ist kein Zugriff auf den KMS-Schlüssel möglich, der zum Ver- oder Entschlüsseln des DB-Clusters verwendet wird. Wenn der KMS-Schlüssel jedoch aktiv ist, kann ein Neustart des DB-Clusters ihn wiederherstellen. Weitere Informationen finden Sie unter Verschlüsseln eines Amazon-Aurora-DB-Clusters.
Wartung	Berechnet	Amazon RDS installiert auf dem DB-Cluster ein Wartungsupdate. Dieser Status wird bei Wartungen auf der Ebene des DB-Clusters verwendet, die von RDS lange im Voraus geplant werden.
Migrating	Berechnet	Es wird gerade ein DB-Cluster-Snapshot in einen DB-Cluster wiederhergestellt.
Migration-failed	Nicht berechnet	Eine Migration ist fehlgeschlagen.
Ändern	Berechnet	Der DB-Cluster wird aufgrund einer Kundenanfrage, den DB-Cluster zu ändern, geändert.
Promoting	Berechnet	Ein Lesereplikat wird gerade zu einem eigenständigen DB-Cluster hochgestuft.
Vorbereitung der Datenmigration	Berechnet	Amazon RDS bereitet die Migration von Daten nach Aurora vor.
Wird umbenannt	Berechnet	Der DB-Cluster wird aufgrund einer Kundenanfrage auf Instance-Umbenennung umbenannt.

DB-Cluster-Status	Berechnet	Beschreibung
Resetting-master-credentials	Berechnet	Die Master-Anmeldeinformationen für den DB-Cluster werden auf eine Kundenanfrage auf Zurücksetzung hin zurückgesetzt.
Wird gestartet	Berechnet für Speicher	Der DB-Cluster wird gestartet.
Angehalten	Berechnet für Speicher	Der DB-Cluster wird gestoppt.
Wird angehalten	Berechnet für Speicher	Der DB-Cluster wird gerade angehalten.
Storage-optimization	Berechnet	Ihre DB-Instance wird modifiziert, um die Speichergröße oder den Speichertyp zu ändern. Die DB-Instance ist voll funktionsfähig. Während sich die DB-Instance aber im Zustand der Speicheroptimierung befindet, können Sie keine Änderungen am Speicher der DB-Instance anfordern. Der Prozess der Speicheroptimierung ist in der Regel kurz, kann aber manchmal bis zu und sogar über 24 Stunden dauern.
Update-iam-db-auth	Berechnet	Die IAM-Autorisierung für den DB-Cluster wird gerade aktualisiert.
Wird upgegradet	Berechnet	Die DB-Cluster-Engine wird auf eine neue Version aktualisiert.

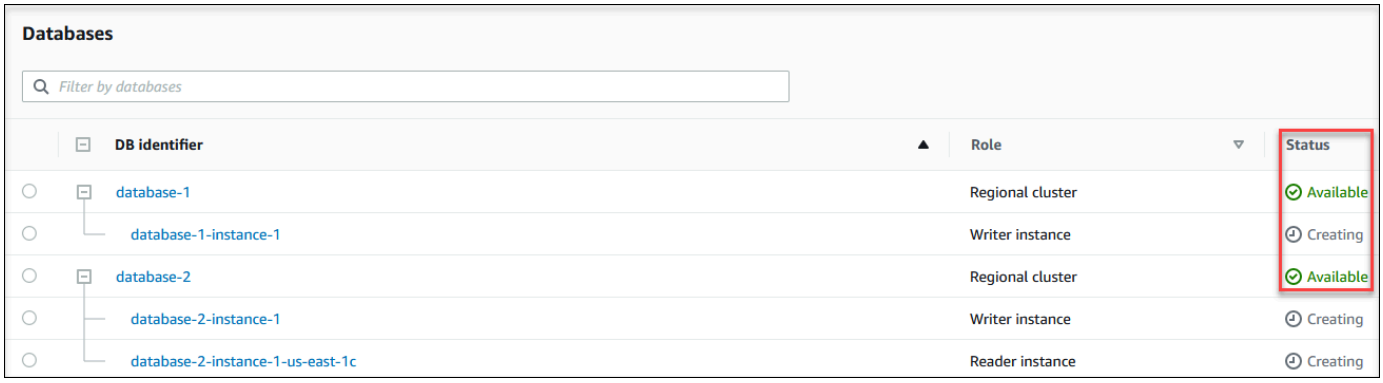
Konsole

So zeigen Sie den Status eines DB-Clusters an

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Datenbanken aus.

   Die Seite „Datenbanken“ wird zusammen mit der Liste der DB-Cluster angezeigt. Für die einzelnen DB-Cluster wird der Statuswert angezeigt.



CLI

Um nur den Status der DB-Cluster anzuzeigen, verwenden Sie die folgende Abfrage unter AWS CLI.

```
aws rds describe-db-clusters --query 'DBClusters[*].[DBClusterIdentifier,Status]' --
output table
```

Anzeigen von DB-Instance-Status in einem Aurora-Cluster

Der Status einer DB-Instance in einem Aurora Cluster zeigt den Zustand der DB-Instance an. Sie können die folgenden Verfahren verwenden, um den DB-Instance-Status eines Clusters in der Amazon RDS-Konsole, im AWS CLI Befehl oder im API-Vorgang anzuzeigen.

> **Note**
>
> Amazon RDS führt daneben noch einen anderen Statuswert, der als Wartungsstatus bezeichnet wird, und der in der Spalte Wartung in der Amazon RDS-Konsole angezeigt wird. Dieser Wert gibt den Status der Wartungspatches an, die auf der DB-Instance installiert werden müssen. Der Wartungsstatus ist von dem Status der DB-Instance unabhängig. Weitere Informationen zum Wartungsstatus finden Sie unter Anwenden von Updates für eine DB-einen DB-Cluster.

In der folgenden Tabelle finden Sie die möglichen Statuswerte für DB-Instances. Diese Tabelle zeigt auch, ob Ihnen die DB-Instance und der Speicher in Rechnung gestellt werden, die nur für Speicher in Rechnung gestellt oder nicht in Rechnung gestellt werden. Für alle DB-Instance-Status wird immer die Sicherungsnutzung berechnet.

DB-Instance-Status	Berech	Beschreibung
Verfügbar	Berech	Die DB-Instance ist fehlerfrei und verfügbar.
Backing-up	Berech	Die DB-Instance wird derzeit gesichert.
backtracking	Berech	Die DB-Instance wird derzeit rückverfolgt. Dieser Status gilt nur für Aurora MySQL.
Configuring-enhanced-monitoring	Berech	Für diese DB-Instance wird „Enhanced Monitoring“ (Erweiterte Überwachung) aktiviert oder deaktiviert.
Configuring-iam-database-auth	Berech	AWS Identity and Access Management Die (IAM-) Datenbank authentifizierung wird für diese DB-Instance aktiviert oder deaktiviert.
Configuring-log-exports	Berech	Das Veröffentlichen von Protokolldateien in Amazon CloudWatch Logs wird für diese DB-Instance aktiviert oder deaktiviert.

DB-Instance-Status	Berech	Beschreibung
Converting-to-vpc	Berech	Die sich nicht in einer Amazon Virtual Private Cloud (Amazon VPC) befindliche DB-Instance wird in eine DB-Instance umgewandelt, die sich in einer Amazon VPC befindet.
Erstellen	Nicht berechı	Die DB-Instance wird gerade erstellt. Während die DB-Instance erstellt wird, kann nicht auf sie zugegriffen werden.
Delete-precheck	Nicht berechı	Amazon RDS überprüft, ob Lesereplikate fehlerfrei sind und sicher gelöscht werden können.
Wird gelöscht	Nicht berechı	Die DB-Instance wird gerade gelöscht.
Fehlgeschlagen	Nicht berechı	Die DB-Instance befindet sich im Fehlerzustand und Amazon RDS kann sie nicht wiederherstellen. Führen Sie eine point-in-time Wiederherstellung zum letzten wiederherstellbaren Zeitpunkt der DB-Instance durch, um die Daten wiederher zustellen.
Inaccessible-encryption-credentials	Nicht berechı	Die zum Verschlüsseln oder Entschlüsseln der DB-Instance AWS KMS key verwendete Datei kann nicht abgerufen oder wiederhergestellt werden.
Inaccessible-encryption-credentials-recoverable	Berech für Speiche	Es ist kein Zugriff auf den KMS-Schlüssel möglich, der zum Ver- oder Entschlüsseln der DB-Instance verwendet wird. Wenn der KMS-Schlüssel jedoch aktiv ist, kann ein Neustart der DB-Instance ihn wiederherstellen. Weitere Informationen finden Sie unter Verschlüsseln eines Amazon-Aurora-DB-Clusters.
Incompatible-network	Nicht berechı	Amazon RDS versucht, auf der DB-Instance eine Wiederher stellungsaktion durchzuführen, was bislang gescheitert ist, weil der Status der VPC die Durchführung der Aktion verhinder t. Dieser Status kann beispielsweise eintreten, wenn alle IP-Adressen in einem Subnetz belegt sind und Amazon RDS keine IP-Adresse für die DB-Instance abrufen kann.

DB-Instance-Status	Berech	Beschreibung
Incompatible-option-group	Berech	Amazon RDS hat versucht, eine Optionsgruppenänderung zu übernehmen, konnte den Vorgang jedoch nicht abschließen, und Amazon RDS kann keinen Rollback auf den vorherige n Optionsgruppenstatus durchführen. Weitere Informationen enthält die Liste Recent Events (Aktuelle Ereignisse) für die DB-Instance. Dieser Status kann beispielsweise eintreten, wenn eine Optionsgruppe eine Option wie TDE und die DB-Instance keine verschlüsselten Daten enthält.
Incompatible-param eters	Berech	Amazon RDS kann die DB-Instance nicht hochfahren, weil in der DB-Parametergruppe der DB-Instance angegebene Parameter nicht mit der DB-Instance kompatibel sind. Machen Sie die letzten Änderungen an den Parametern der DB-Instan ce rückgängig, um wieder auf die DB-Instance zugreifen zu können. Beachten Sie für weitere Informationen zu den inkompatiblen Parametern die Liste Recent Events (Aktuelle Ereignisse) für die DB-Instance.
Incompatible-restore	Nicht berechı	Amazon RDS kann keine point-in-time Wiederherstellung durchführen.
Insufficient-capacity	Nicht berechı	Amazon RDS kann Ihre Instance nicht erstellen, da derzeit keine ausreichende Kapazität verfügbar ist. Um Ihre DB-Instan ce in derselben AZ mit demselben Instance-Typ zu erstellen , löschen Sie Ihre DB-Instance, warten Sie ein paar Stunden und versuchen Sie erneut zu erstellen. Alternativ können Sie eine neue Instance mit einer anderen Instance-Klasse oder AZ erstellen.
Wartung	Berech	Amazon RDS installiert auf der DB-Instance ein Wartungsu pdate. Dieser Status wird bei Wartungen auf der Ebene der Instance verwendet, die von RDS lange im Voraus geplant werden.
Ändern	Berech	Die DB-Instance wird aufgrund einer Kundenanfrage geändert.

DB-Instance-Status	Berech	Beschreibung
Moving-to-vpc	Berech	Die DB-Instance wird in eine neue Amazon Virtual Private Cloud (Amazon VPC) verschoben.
Rebooting	Berech	Die DB-Instance wird aufgrund einer Kundenanfrage oder eines Amazon RDS-Prozesses neu gestartet.
Resetting-master-credentials	Berech	Die Masteranmeldeinformationen für die DB-Instance werden auf eine Kundenanfrage hin zurückgesetzt.
Wird umbenannt	Berech	Die DB-Instance wird aufgrund einer Kundenanfrage umbenannt.
Restore-error	Berech	Bei dem Versuch, einen Snapshot point-in-time oder aus einem Snapshot wiederherzustellen, ist bei der DB-Instance ein Fehler aufgetreten.
Wird gestartet	Berech für Speich	Die DB-Instance wird gestartet.
Angehalten	Berech für Speich	Die DB-Instance ist angehalten.
Wird angehalten	Berech für Speich	Die DB-Instance wird gestoppt.
Storage-config-upgrade	Berech	Die Konfiguration des Speicherdateisystems der DB-Instance wird aktualisiert. Dieser Status gilt nur für grüne Datenbanken innerhalb einer Blau/Grün-Bereitstellung oder für DB-Instance-Lesereplikate.

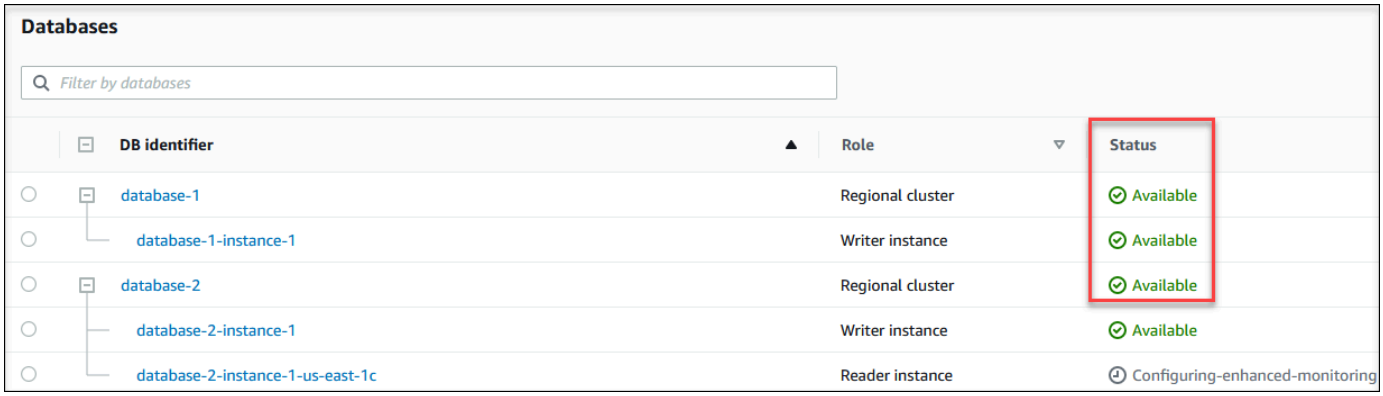
DB-Instance-Status	Berech	Beschreibung
Storage-full	Berech	Die DB-Instance hat die Speicherkapazitätszuteilung erreicht. Dies ist ein kritischer Status, wir empfehlen deshalb eine umgehende Behebung dieses Problems. Vergrößern Sie zu diesem Zweck den verfügbaren Speicher, indem Sie die DB-Instance ändern. Um diese Situation zu vermeiden, stellen Sie CloudWatch Amazon-Alarme so ein, dass Sie gewarnt werden, wenn der Speicherplatz knapp wird.
Storage-optimization	Berech	Amazon RDS optimiert den Speicher Ihrer DB-Instance. Der Prozess der Speicheroptimierung ist in der Regel kurz, kann aber manchmal bis zu und sogar über 24 Stunden dauern. Während der Speicheroptimierung bleibt die DB-Instance verfügbar. Die Speicheroptimierung ist ein Hintergrundprozess, der die Verfügbarkeit der Instance nicht beeinträchtigt.
Wird upgegradet	Berech	Die Datenbank-Engine wird auf eine neue Version aktualisiert.

Konsole

So zeigen Sie den Status einer DB-Instance an

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.

   Die Seite „Datenbanken“ wird zusammen mit der Liste der DB-Instances angezeigt. Für jede DB-Instance in einem Cluster wird der Statuswert angezeigt.



CLI

Um die DB-Instance und ihre Statusinformationen mithilfe von anzuzeigen AWS CLI, verwenden Sie den Befehl describe-db-instances. Der folgende AWS CLI Befehl listet beispielsweise alle Informationen zu DB-Instances auf.

```
aws rds describe-db-instances
```

Zum Anzeigen einer bestimmten DB-Instance und deren Status rufen Sie den Befehl describe-db-instances mit der folgenden Option auf:

- `DBInstanceIdentifier` – der Name der DB-Instance

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

Um nur den Status aller DB-Instances anzuzeigen, verwenden Sie die folgende Abfrage in AWS CLI.

```
aws rds describe-db-instances --query 'DBInstances[*].
[DBInstanceIdentifier,DBInstanceStatus]' --output table
```

API

Um den Status der DB-Instance mithilfe der Amazon-RDS-API anzuzeigen, rufen Sie die Operation DescribeDBInstances auf.

Anzeigen und Beantworten von Amazon-Aurora-Empfehlungen

Amazon Aurora bietet automatisierte Empfehlungen für Datenbankressourcen wie DB-Instances, DB-Cluster, und DB-Parametergruppen. Diese Empfehlungen bieten Anleitungen nach bewährten Methoden, indem sie die DB-Cluster-Konfiguration, DB-Instance-Konfiguration, die Nutzung und die Leistungsdaten analysieren.

Amazon RDS Performance Insights überwacht bestimmte Metriken und erstellt automatisch Schwellenwerte, indem analysiert wird, welche Stufen für eine bestimmte Ressource als potenziell problematisch angesehen werden. Wenn neue Metrikwerte über einen bestimmten Zeitraum einen vordefinierten Schwellenwert überschreiten, generiert Performance Insights eine proaktive Empfehlung. Diese Empfehlung trägt dazu bei, zukünftige Auswirkungen auf die Datenbankleistung zu vermeiden. Beispielsweise wird die Empfehlung „Leerlauf in Transaktion“ für Aurora-PostgreSQL-Instances von generiert, wenn die mit der Datenbank verbundenen Sitzungen keine aktive Arbeit ausführen, aber Datenbankressourcen blockiert lassen können. Um proaktive Empfehlungen zu erhalten, müssen Sie Performance Insights mit einem Aufbewahrungszeitraum für kostenpflichtige Stufen aktivieren. Informationen zum Aktivieren von Performance Insights finden Sie unter Performance Insights für Aurora ein- und ausschalten. Informationen zu Preisen und zur Datenspeicherung für Performance Insights finden Sie unter Preisgestaltung und Datenaufbewahrung für Performance-Insights.

DevOpsGuru für RDS überwacht bestimmte Metriken, um zu erkennen, wann das Verhalten der Metrik sehr ungewöhnlich oder ungewöhnlich wird. Diese Anomalien werden als reaktive Erkenntnisse mit Empfehlungen gemeldet. Beispielsweise DevOpskönnteGuru für RDS Ihnen empfehlen, eine Erhöhung der CPU-Kapazität in Betracht zu ziehen oder Warteereignisse zu untersuchen, die zur DB-Last beitragen. DevOpsGuru für RDS bietet auch schwellenwertbasierte proaktive Empfehlungen. Für diese Empfehlungen müssen Sie DevOpsGuru für RDS aktivieren. Informationen zum Aktivieren von DevOpsGuru für RDS finden Sie unter DevOpsGuru einschalten und die Ressourcenabdeckung angeben.

Empfehlungen haben einen der folgenden Status: aktiv, verworfen, ausstehend oder gelöst. Gelöste Empfehlungen sind 365 Tage lang verfügbar.

Sie können die Empfehlungen anzeigen oder verwerfen. Sie können eine konfigurationsbasierte aktive Empfehlung sofort anwenden, im nächsten Wartungsfenster planen oder sie verwerfen. Für schwellenwertbasierte proaktive und auf Machine Learning basierende reaktive Empfehlungen müssen Sie die vorgeschlagene Ursache des Problems überprüfen und dann die empfohlenen Maßnahmen zur Behebung des Problems durchführen.

Themen

Anzeige der Empfehlungen von Amazon Aurora

Amazon Aurora erstellt Empfehlungen für eine Ressource, wenn die Ressource erstellt oder geändert wird.

Die konfigurationsbasierten Empfehlungen werden in den folgenden Regionen unterstützt:

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europe (Frankfurt)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Südamerika (São Paulo)

In der folgenden Tabelle finden Sie Beispiele für konfigurationsbasierte Empfehlungen.

Typ	Beschreibung	Empfehlung	Ausfall: it erforde ich	Zusätzliche Informati onen
Automatis ierte Ressourcen-	Automatisierte Backups sind für Ihre DB-Instances nicht aktiviert. Automatis	Aktivieren Sie automatische Backups mit einer	Ja	Übersicht über das Sichern und Wiederherstellen

Typ	Beschreibung	Empfehlung	Ausfall: it erforde ich	Zusätzliche Informati onen
Backups sind deaktiviert	ierte Backups werden empfohlen, da sie die point-in-time Wiederherstellung Ihrer DB-Instances ermöglichen.	Aufbewahrungsfrist von bis zu 14 Tagen.		eines Aurora-DB-Clusters Entmystifizierung der Amazon RDS-Backup-Speicherkosten im Datenbank-Blog AWS
Ein Upgrade der Engine-Nebenversion ist erforderlich	Auf Ihren Datenbankressourcen wird nicht die neueste Nebenversion der DB-Engine ausgeführt. Die neueste Nebenversion enthält die neuesten Sicherheitsupdates und andere Verbesserungen.	Führen Sie ein Upgrade auf die neueste Engine-Version durch.	Ja	Warten eines Amazon Aurora-DB-Clusters
Enhanced Monitoring ist ausgeschaltet	Für Ihre Datenbankressourcen ist Enhanced Monitoring nicht aktiviert. Erweiterte Überwachung bietet Echtzeit-Betriebssystemmetriken für die Überwachung und Fehlerbehebung.	Aktivieren Sie die erweiterte Überwachung.	Nein	Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung)

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
Die Speicherverschlüsselung ist ausgeschaltet	Amazon RDS unterstützt Verschlüsselung im Ruhezustand für alle Datenbank-Engines mithilfe der Schlüssel, die Sie im AWS Key Management Service (AWS KMS) verwalten. Auf einer aktiven DB-Instance mit Amazon RDS-Verschlüsselung werden die im Speicher gespeicherten Daten verschlüsselt, ähnlich wie bei automatisierten Backups, Read Replicas und Snapshots. Wenn die Verschlüsselung beim Erstellen eines Aurora-DB-Clusters nicht aktiviert ist, müssen Sie einen entschlüsselten Snapshot in einem verschlüsselten DB-Cluster wiederherstellen.	Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand für Ihren DB-Cluster.	Ja	Sicherheit in Amazon Aurora

Typ	Beschreibung	Empfehlung	Ausfall: it erforde ich	Zusätzliche Informati onen
DB-Cluste r mit allen Instances in derselben Availability Zone	Die DB-Cluster befinden sich derzeit in einer einzigen Availability Zone. Verwenden Sie mehrere Availabil ity Zones, um die Verfügbarkeit zu verbessern.	Fügen Sie die DB-Instances mehreren Availability Zones in Ihrem DB-Cluster hinzu.	Nein	Hohe Verfügbarkeit für Amazon Aurora
DB-Instan ces in den Clustern mit heterogen en Instance-Größen	Wir empfehlen, dass Sie dieselbe DB-Instance-Klasse und Größe für alle DB-Instances in Ihrem DB-Cluster verwenden.	Verwenden Sie dieselbe Instance-Klasse und Größe für alle DB-Instances in Ihrem DB-Cluster.	Ja	Replikation mit Amazon Aurora
DB-Instan ces in den Clustern mit heterogen en Instance-Klassen	Wir empfehlen, dass Sie dieselbe DB-Instance-Klasse und Größe für alle DB-Instances in Ihrem DB-Cluster verwenden.	Verwenden Sie dieselbe Instance-Klasse und Größe für alle DB-Instances in Ihrem DB-Cluster.	Ja	Replikation mit Amazon Aurora

Typ	Beschreibung	Empfehlung	Ausfall: it erforde ich	Zusätzliche Informati onen
DB-Instan ces in den Clustern mit heterogenen Parameter gruppen	Wir empfehlen, dass alle DB-Instances im DB-Cluster dieselbe DB-Parametergruppe verwenden.	Ordnen Sie die DB-Instance der DB-Parametergruppe zu, die der Writer-In stance in Ihrem DB-Cluster zugeordnet ist.	Nein	Arbeiten mit Parametergruppen
Amazon RDS-DB-Cl uster haben eine DB-Instance	Fügen Sie Ihrem DB-Cluster mindesten s eine weitere DB-Instance hinzu, um die Verfügbarkeit und Leistung zu verbesser n.	Fügen Sie Ihrem DB-Cluster eine Reader-DB-Instance hinzu.	Nein	Hohe Verfügbarkeit für Amazon Aurora
Performance Insights ist ausgeschaltet	Performance Insights überwacht die Auslastung Ihrer DB-Instance, um Sie bei der Analyse und Lösung von Datenbankleistungs problemen zu unterstützen. Wir empfehlen, Performan ce Insights zu aktivieren.	Aktivieren Sie Performance Insights.	Nein	Überwachung mit Performance Insights auf

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
Die Aktualisierung der Hauptversionen von RDS-Ressourcen ist erforderlich	Datenbanken mit der aktuellen Hauptversion für die DB-Engine werden nicht unterstützt. Wir empfehlen Ihnen, auf die neueste Hauptversion zu aktualisieren, die neue Funktionen und Verbesserungen enthält.	Führen Sie ein Upgrade auf die neueste Hauptversion für die DB-Engine durch.	Ja	Amazon-Aurora-Updates Erstellen einer Blau/Grün-Bereitstellung
DB-Cluster unterstützen nur ein Volumen von bis zu 64 TiB	Ihre DB-Cluster unterstützen Volumes bis zu 64 TiB. Die neuesten Engine-Versionen unterstützen Volumes bis zu 128 TiB für Ihren DB-Cluster. Wir empfehlen, dass Sie die Engine-Version Ihres DB-Clusters auf die neuesten Versionen aktualisieren, um Volumes bis zu 128 TiB zu unterstützen.	Aktualisieren Sie die Engine-Version Ihrer DB-Cluster, um Volumes bis zu 128 TiB zu unterstützen.	Ja	Amazon Aurora-Größenbeschränkungen

Typ	Beschreibung	Empfehlung	Ausfall: it erforde ich	Zusätzliche Informati onen
DB-Cluste r mit allen Reader-In stances in derselben Availability Zone	Availability Zones (AZs) sind Standorte , die sich voneinander unterscheiden, um bei Ausfällen innerhalb der einzelnen AWS Regionen für Isolation zu sorgen. Wir empfehlen, dass Sie die primäre Instance und die Reader-In stances in Ihrem DB-Cluster auf mehrere AZs verteilen, um die Verfügbarkeit Ihres DB-Clusters zu verbessern. Sie können einen Multi-AZ-Cluster mithilfe der AWS Managemen t Console, der AWS CLI oder der Amazon RDS-API erstellen, wenn Sie den Cluster erstellen. Sie können den vorhandenen Aurora-Cluster in einen Multi-AZ-Cluster ändern, indem Sie eine neue Reader-Instance hinzufügen	Ihr DB-Cluster hat alle seine Read-Inst ances in derselben Availability Zone. Wir empfehlen, dass Sie die Reader-Instances auf mehrere Availabil ity Zones verteilen. Die Verteilung erhöht die Verfügbarkeit und verbessert die Reaktionszeit, indem die Netzwerklatenz zwischen den Clients und der Datenbank reduziert wird.	Nein	Hohe Verfügbarkeit für Amazon Aurora

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
	und eine andere AZ angeben.			
Die DB-Speicherparameter weichen vom Standard ab	Die Speicherparameter der DB-Instances unterscheiden sich erheblich von den Standardwerten. Diese Einstellungen können sich auf die Leistung auswirken und zu Fehlern führen. Wir empfehlen, die benutzerdefinierten Speicherparameter für die DB-Instance auf ihre Standardwerte in der DB-Parametergruppe zurückzusetzen.	Setzen Sie die Speicherparameter auf ihre Standardwerte zurück.	Nein	Arbeiten mit Parametergruppen

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
Der Abfrage-Cache-Parameter ist aktiviert	Wenn Änderungen erfordern, dass Ihr Abfrage-Cache gelöscht wird, scheint Ihre DB-Instance zum Stillstand zu kommen. Die meisten Workloads profitieren nicht von einem Abfrage-Cache. Der Abfrage-Cache wurde aus der MySQL-Version 8 entfernt. Wir empfehlen, den Parameter query_cache_type auf 0 zu setzen.	Setzen Sie den `query_cache_type` Parameterwert `0` in Ihren DB-Parametergruppen auf.	Ja	Arbeiten mit Parametergruppen

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
`log_output` Der Parameter ist auf Tabelle eingestellt	Wenn auf gesetzt `log_output` ist`TABLE`, wird mehr Speicherplatz verwendet als wenn auf eingestellt `log_output` ist`FILE`. Wir empfehlen, den Parameter auf zu setzen`FILE`, um zu verhindern, dass die Speichergrößenbeschränkung erreicht wird.	Stellen Sie den `log_output` Parameterwert `FILE` in Ihren DB-Parametergruppen auf ein.	Nein	Aurora-MySQL-Datenbank-Protokolldateien
`autovacuum` Der Parameter ist ausgeschaltet	Der Autovacuum-Parameter ist für die DB-Cluster Ihrer ausgeschaltet. Wenn Sie die automatische Bereinigung deaktivieren, werden Tabelle und Index größer und die Leistung beeinträchtigt. Wir empfehlen, dass Sie Autovacuum in Ihren DB-Parametergruppen aktivieren.	Aktivieren Sie den Autovacuum-Parameter in Ihren DB-Cluster-Parametergruppen.	Nein	Grundlegendes zum Thema Autovacuum in Amazon RDS for PostgreSQL PostgreSQL-Umgebungen im Datenbank-Blog AWS

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
`synchronous_commit` Der Parameter ist ausgeschaltet	Wenn der `synchronous_commit` Parameter ausgeschaltet ist, können Daten bei einem Datenbankabsturz verloren gehen. Die Haltbarkeit der Datenbank ist gefährdet. Wir empfehlen Ihnen, den `synchronous_commit` -Parameter zu aktivieren.	Aktivieren Sie `synchronous_commit` Parameter in Ihren DB-Parametergruppen.	Ja	Amazon Aurora PostgreSQL-Parameter: Replikation, Sicherheit und Protokollierung im AWS Datenbank-Blog
`track_counts` Der Parameter ist ausgeschaltet	Wenn der `track_counts` Parameter ausgeschaltet ist, sammelt die Datenbank keine Statistiken zur Datenbankaktivität. Autovacuum erfordert, dass diese Statistiken korrekt funktionieren. Wir empfehlen , den Parameter `track_counts` auf 1 zu setzen.	Setzen Sie `track_counts` den Parameter auf1.	Nein	Laufzeitstatistiken für PostgreSQL

Typ	Beschreibung	Empfehlung	Ausfall: it erforde ich	Zusätzliche Informati onen
`enable_in dexonlysc an` Der Parameter ist ausgeschaltet	Der Abfrageplaner oder Optimierer kann den Plantyp „Nur Index“ für den Scanplan nicht verwenden, wenn er deaktiviert ist. Es wird empfohlen , den `enable_in dexonlyscan` Parameterwert auf festzulegen. 1	Stellen Sie den `enable_in dexonlyscan` Parameterwert auf ein1.	Nein	Planner-Methodenko nfiguration für PostgreSQL
`enable_in dexscan` Der Parameter ist ausgeschaltet	Der Abfrageplaner oder Optimierer kann den Plantyp Indexscan nicht verwenden, wenn er ausgeschaltet ist. Wir empfehlen, den `enable_in dexscan` Wert auf festzulegen. 1	Setzen Sie den `enable_in dexscan` Parameter wert auf1.	Nein	Planner-Methodenko nfiguration für PostgreSQL

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
`innodb_flush_log_at_trx` Der Parameter ist ausgeschaltet	Der Wert des `innodb_flush_log_at_trx` Parameters Ihrer DB-Instance ist kein sicherer Wert. Dieser Parameter steuert die Persistenz von Commit-Operationen auf der Festplatte. Wir empfehlen, den Parameter `innodb_flush_log_at_trx` auf 1 zu setzen.	Setzen Sie den `innodb_flush_log_at_trx` Parameterwert auf1.	Nein	Konfigurieren, wie oft der Protokollpuffer geleert wird

Typ	Beschreibung	Empfehlung	Ausfall: it erforde ich	Zusätzliche Informati onen
`innodb_st ats_persi stent` Der Parameter ist ausgeschaltet	Ihre DB-Instan ce ist nicht dafür konfiguriert, die InnoDB-Statistiken auf der Festplatte zu speichern. Wenn die Statistiken nicht gespeichert werden, werden sie bei jedem Neustart der Instanz und jedem Zugriff auf die Tabelle neu berechnet. Dies führt zu Abweichungen im Abfrageausführungs plan. Sie können den Wert dieses globalen Parameter s auf Tabellenebene ändern. Es wird empfohlen , den `innodb_st ats_persistent` Parameterwert auf festzulegen`0N`.	Stellen Sie den `innodb_st ats_persistent` Parameterwert auf ein`0N`.	Nein	Arbeiten mit Parametergruppen

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
`innodb_open_files` Der Parameter ist niedrig	Der `innodb_open_files` Parameter steuert die Anzahl der Dateien, die InnoDB gleichzeitig öffnen kann. InnoDB öffnet alle Protokoll- und System-Tablespace-Dateien, wenn mysqld läuft. Ihre DB-Instance hat einen niedrigen Wert für die maximale Anzahl von Dateien, die InnoDB gleichzeitig öffnen kann. Wir empfehlen, den Parameter `innodb_open_files` auf einen Mindestwert von 65 zu setzen.	Setzen Sie den `innodb_open_files` Parameter auf einen Mindestwert von. 65	Ja	InnoDB öffnet Dateien für MySQL

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
`max_user_connections` Der Parameter ist niedrig	Ihre DB-Instance hat einen niedrigen Wert für die maximale Anzahl gleichzeitiger Verbindungen für jedes Datenbankkonto. Wir empfehlen, den `max_user_connections` Parameter auf eine Zahl größer als zu setzen`5`.	Erhöhen Sie den Wert des `max_user_connections` Parameters auf eine Zahl größer als`5`.	Ja	Kontoressourcenlimits für MySQL festlegen
Read Replicas sind im schreibbaren Modus geöffnet	Ihre DB-Instance verfügt über eine Read Replica im schreibbaren Modus, der Updates von Clients ermöglicht. Wir empfehlen, den `read_only` Parameter auf zu setzen, `TrueIfReplica` damit sich die Read Replicas nicht im schreibbaren Modus befinden.	Setzen Sie den `read_only` Parameterwert auf. `TrueIfReplica`	Nein	Arbeiten mit Parametergruppen

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
`innodb_default_row_format` Die Parametereinstellung ist unsicher	Bei Ihrer DB-Instance tritt ein bekanntes Problem auf: Eine Tabelle, die in einer MySQL-Version vor 8.0.26 mit der `row_format` Einstellung auf `COMPACT` oder `REDUNDANT` erstellt wurde, ist nicht zugänglich und kann nicht wiederhergestellt werden, wenn der Index 767 Byte überschreitet. Wir empfehlen, den Parameterwert auf zu setzen. `innodb_default_row_format` `DYNAMIC`	Stellen Sie den `innodb_default_row_format` Parameterwert auf ein`DYNAMIC`.	Nein	Änderungen in MySQL 8.0.26

Typ	Beschreibung	Empfehlung	Ausfall: it erforde ich	Zusätzliche Informati onen
`general_l ogging` Der Parameter ist aktiviert	Die allgemeine Protokollierung ist für Ihre DB-Instan ce aktiviert. Diese Einstellung ist nützlich bei der Behebung von Datenbankproblemen . Das Aktivieren der allgemeinen Protokoll ierung erhöht jedoch die Anzahl der I/O-Operationen und den zugewiesenen Speicherplatz, was zu Konflikten und Leistungseinbußen führen kann. Prüfen Sie Ihre Anforderungen für die allgemeine Nutzung der Protokollierung. Wir empfehlen, den `general_logging` Parameterwert auf zu setzen`0`.	Prüfen Sie Ihre Anforderungen für die allgemeine Nutzung der Protokollierung. Wenn dies nicht verpflichtend ist, empfehlen wir Ihnen, den `general_l ogging` Parameter wert auf zu setzen`0`.	Nein	Überblick über Aurora-MySQL-Datenbankprotokolle

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
Der DB-Cluster ist für Lese-Workloads nicht ausreichend bereitgestellt	Wir empfehlen, dass Sie Ihrem DB-Cluster eine Reader-DB-Instance mit derselben Instance-Klasse und Größe wie die Writer-DB-Instance im Cluster hinzufügen. Die aktuelle Konfiguration umfasst eine DB-Instance mit einer kontinuierlich hohen Datenbanklast, die hauptsächlich durch Lesevorgänge verursacht wird. Verteilen Sie diese Operationen, indem Sie dem Cluster eine weitere DB-Instance hinzufügen und die Lese-Arbeitslast an den schreibgeschützten Endpunkt des DB-Clusters weiterleiten.	Fügen Sie dem Cluster eine Reader-DB-Instance hinzu.	Nein	Hinzufügen von Aurora-Replicas zu einem DB-Cluster Verwalten von Performance und Skalierung für einen Aurora-DB-Cluster Amazon-RDS-Preise

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
Die RDS-Instance ist in Bezug auf die Systemspeicherkapazität nicht ausreichend ausgestattet	Wir empfehlen, dass Sie Ihre Abfragen so anpassen, dass sie weniger Speicher verwenden oder einen DB-Instance-Typ mit mehr zugewiesenem Speicher verwenden. Wenn der Instance nur noch wenig Arbeitsspeicher zur Verfügung steht, wird die Datenbankleistung beeinträchtigt.	Verwenden Sie eine DB-Instance mit höherer Speicherkapazität	Ja	Vertikale und horizontale Skalierung Ihrer Amazon RDS-Instance im AWS Datenbank-Blog Amazon RDS-Instance-Typen Amazon-RDS-Preise
Die RDS-Instance ist im Hinblick auf die CPU-Kapazität des Systems nicht ausreichend bereitgestellt	Wir empfehlen Ihnen, Ihre Abfragen so zu optimieren, dass sie weniger CPU verbrauchen, oder Ihre DB-Instance so zu ändern, dass sie eine DB-Instance-Klasse mit höher zugewiesenen vCPUs verwendet. Die Datenbankleistung kann sinken, wenn die CPU-Auslastung einer DB-Instance knapp wird.	Verwenden Sie eine DB-Instance mit höherer CPU-Kapazität	Ja	Vertikale und horizontale Skalierung Ihrer Amazon RDS-Instance im AWS Datenbank-Blog Amazon RDS-Instance-Typen Amazon-RDS-Preise

Typ	Beschreibung	Empfehlung	Ausfallzeit erforderlich	Zusätzliche Informationen
RDS-Ressourcen nutzen das Verbindungspooling nicht korrekt	Wir empfehlen Ihnen, Amazon RDS Proxy zu aktivieren, um bestehende Datenbankverbindungen effizient zu bündeln und gemeinsam zu nutzen. Wenn Sie bereits einen Proxy für Ihre Datenbank verwenden, konfigurieren Sie ihn korrekt, um das Verbindungspooling und den Lastenausgleich über mehrere DB-Instances hinweg zu verbessern. RDS Proxy kann dazu beitragen, das Risiko von Verbindungsausfällen und Ausfallzeiten zu verringern und gleichzeitig die Verfügbarkeit und Skalierbarkeit zu verbessern.	Aktivieren Sie RDS Proxy oder ändern Sie Ihre bestehende Proxykonfiguration	Nein	Vertikale und horizontale Skalierung Ihrer Amazon RDS-Instance im AWS Datenbank-Blog Verwenden von Amazon RDS Proxy für Aurora Amazon RDS Proxy — Preise

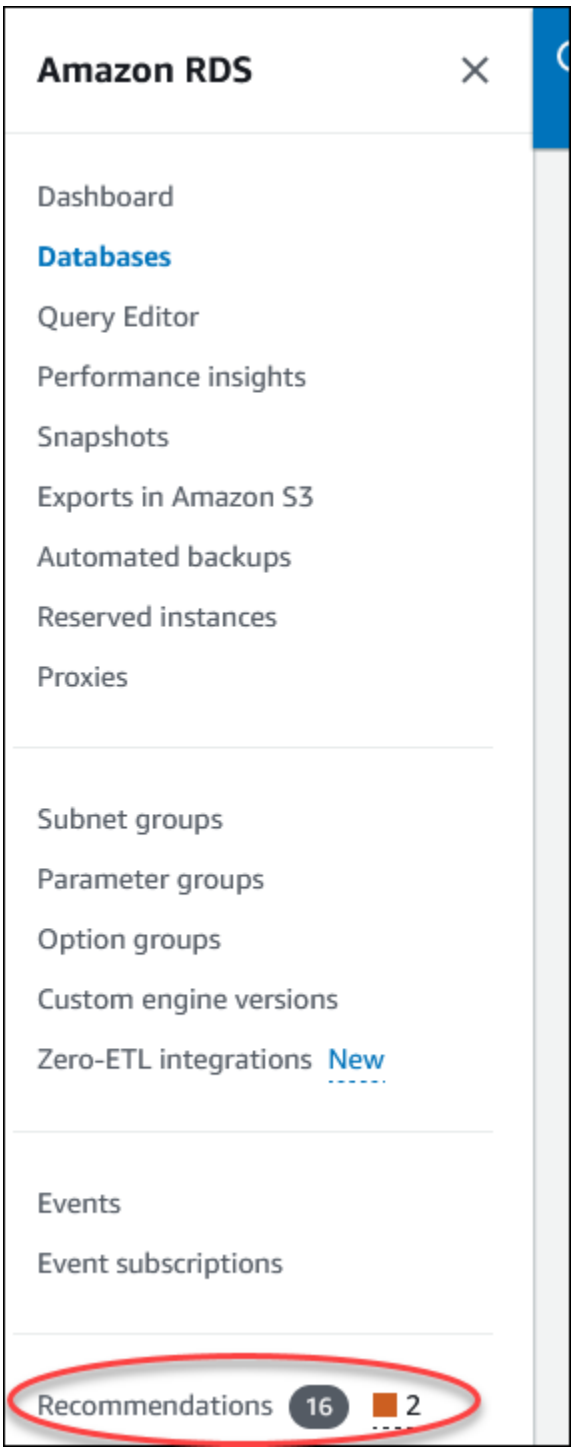
Mithilfe der Amazon RDS-Konsole können Sie Amazon Aurora-Empfehlungen für Amazon für Ihre Datenbankressourcen einsehen. Für einen DB-Cluster werden die Empfehlungen für den DB-Cluster und seine Instances angezeigt.

Konsole

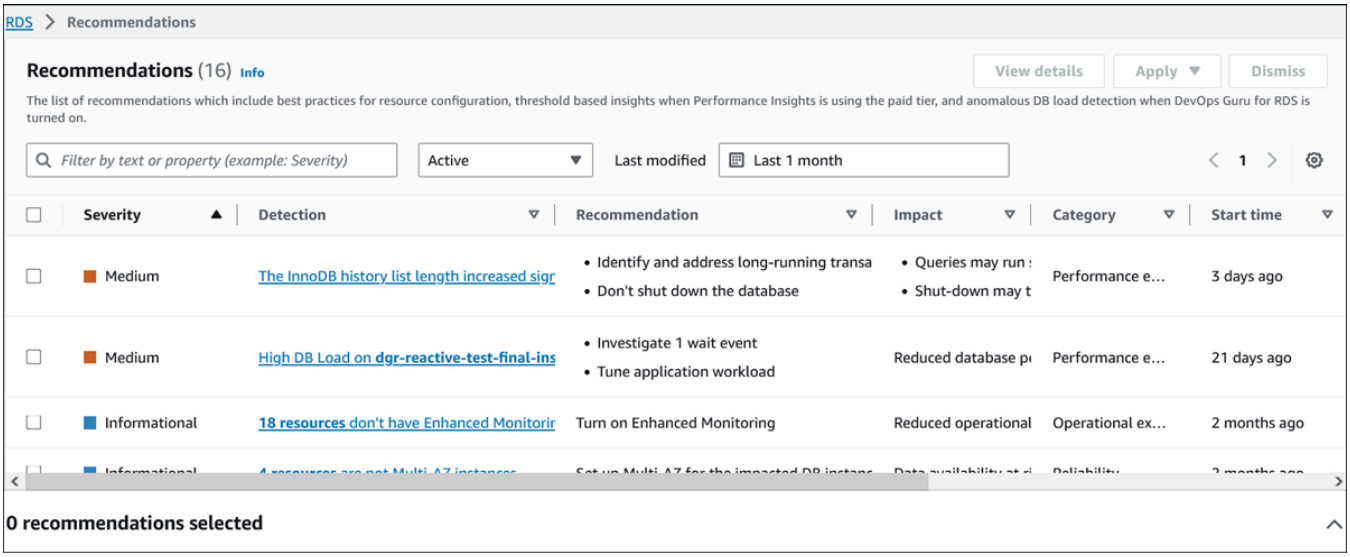
Um die Aurora-Empfehlungen einzusehen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus:

    - Wählen Sie Empfehlungen aus. Die Anzahl der aktiven Empfehlungen für Ihre Ressourcen und die Anzahl der Empfehlungen mit dem höchsten Schweregrad, die im letzten Monat generiert wurden, sind neben Empfehlungen verfügbar. Um die Anzahl der aktiven Empfehlungen für jeden Schweregrad zu ermitteln, wählen Sie die Zahl aus, die den höchsten Schweregrad anzeigt.

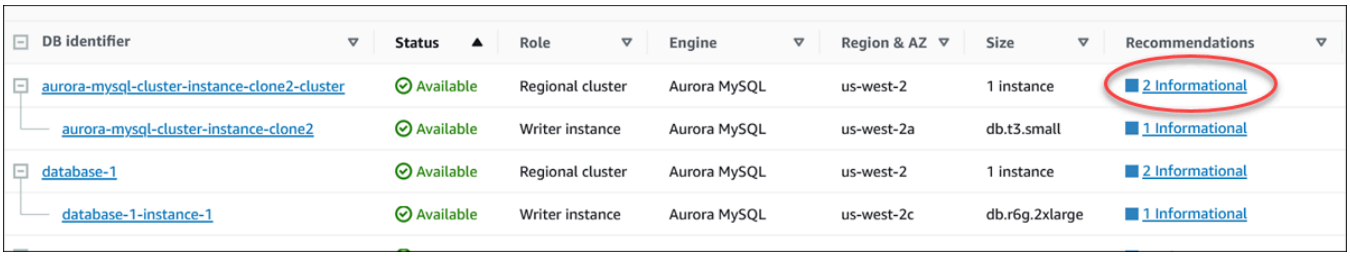


Standardmäßig wird auf der Seite „Empfehlungen“ eine Liste der neuen Empfehlungen des letzten Monats angezeigt. Amazon Aurora gibt Empfehlungen für alle Ressourcen in Ihrem Konto und sortiert die Empfehlungen nach ihrem Schweregrad.

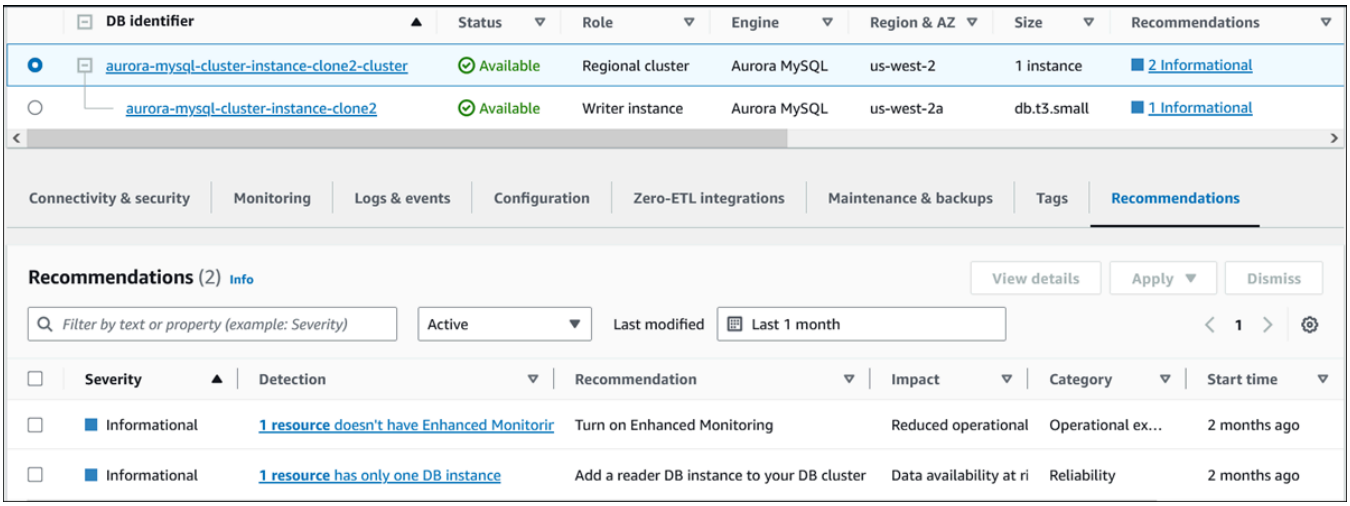


Sie können eine Empfehlung auswählen, um unten auf der Seite einen Abschnitt zu sehen, der die betroffenen Ressourcen und Einzelheiten zur Umsetzung der Empfehlung enthält.

- Wählen Sie auf der Seite Datenbanken die Option Empfehlungen für eine Ressource aus.



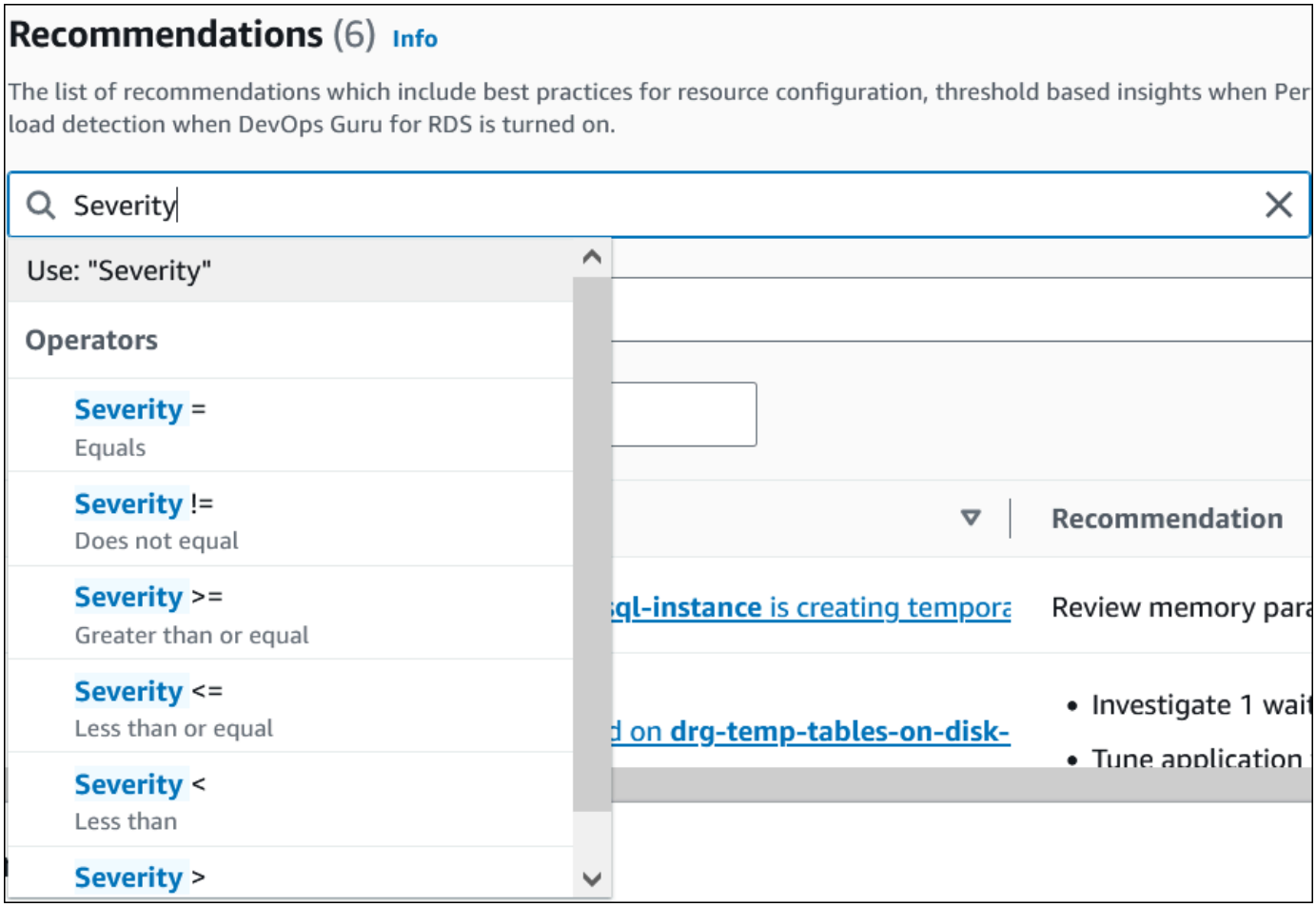
Auf der Registerkarte Empfehlungen werden die Empfehlungen und ihre Details für die ausgewählte Ressource angezeigt.



Die folgenden Informationen sind für die Empfehlungen verfügbar:

- Schweregrad — Das Ausmaß der Auswirkungen des Problems. Die Schweregrade lauten „Hoch“, „Mittel“, „Niedrig“ und „Informativ“.
- Erkennung — Die Anzahl der betroffenen Ressourcen und eine kurze Beschreibung des Problems. Wählen Sie diesen Link, um die Empfehlung und die Analysedetails anzuzeigen.
- Empfehlung — Eine kurze Beschreibung der empfohlenen Maßnahme, die angewendet werden soll.
- Auswirkung — Eine kurze Beschreibung der möglichen Auswirkungen, wenn die Empfehlung nicht angewendet wird.
- Kategorie — Die Art der Empfehlung. Die Kategorien sind Leistungseffizienz, Sicherheit, Zuverlässigkeit, Kostenoptimierung, betriebliche Exzellenz und Nachhaltigkeit.
- Status — Der aktuelle Status der Empfehlung. Die möglichen Status sind Alle, Aktiv, Abgelehnt, Gelöst und Ausstehend.
- Startzeit — Die Zeit, zu der das Problem begann. Zum Beispiel vor 18 Stunden.
- Letzte Änderung — Der Zeitpunkt, zu dem die Empfehlung aufgrund einer Änderung des Schweregrads zuletzt vom System aktualisiert wurde, oder der Zeitpunkt, zu dem Sie auf die Empfehlung geantwortet haben. Zum Beispiel vor 10 Stunden.
- Endzeit — Der Zeitpunkt, zu dem das Problem beendet wurde. Bei anhaltenden Problemen wird die Uhrzeit nicht angezeigt.
- Ressourcen-ID — Der Name einer oder mehrerer Ressourcen.

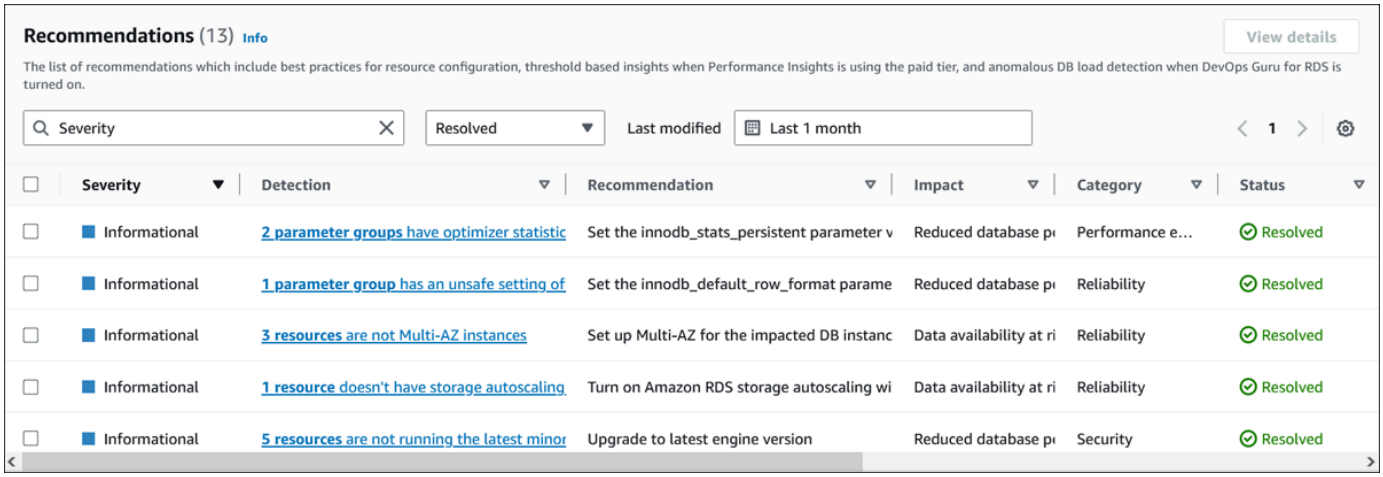
3. (Optional) Wählen Sie in dem Feld die Operatoren Schweregrad oder Kategorie aus, um die Liste der Empfehlungen zu filtern.



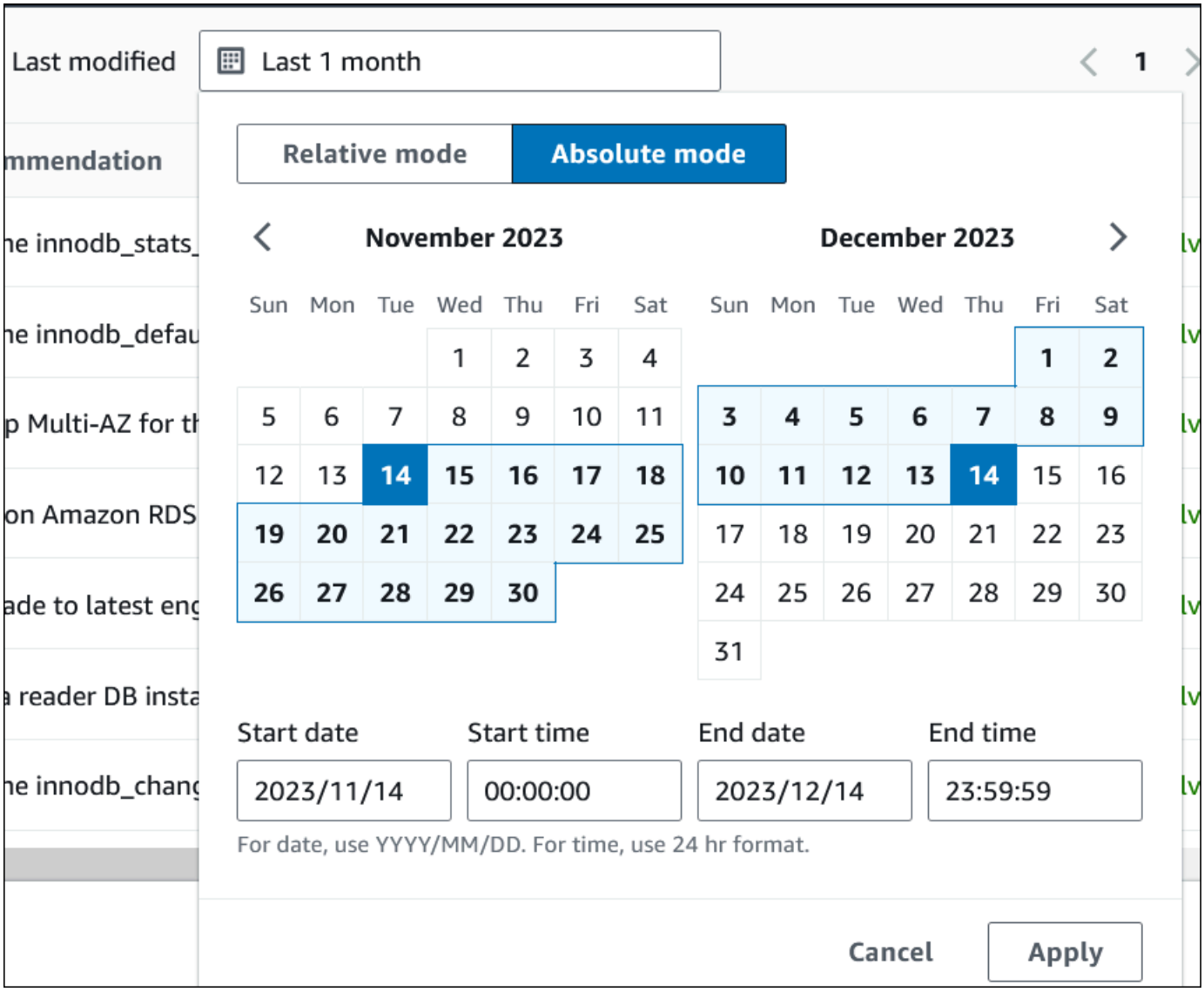
Die Empfehlungen für den ausgewählten Vorgang werden angezeigt.

4. (Optional) Wählen Sie einen der folgenden Empfehlungsstatus:

   - Aktiv (Standard) — Zeigt die aktuellen Empfehlungen an, die Sie anwenden, für das nächste Wartungsfenster planen oder ablehnen können.
   - Alle — Zeigt alle Empfehlungen mit dem aktuellen Status an.
   - Abgelehnt — Zeigt die abgelehnten Empfehlungen an.
   - Gelöst — Zeigt die Empfehlungen an, die gelöst wurden.
   - Ausstehend — Zeigt die Empfehlungen an, deren empfohlene Maßnahmen derzeit ausgeführt werden oder für das nächste Wartungsfenster geplant sind.



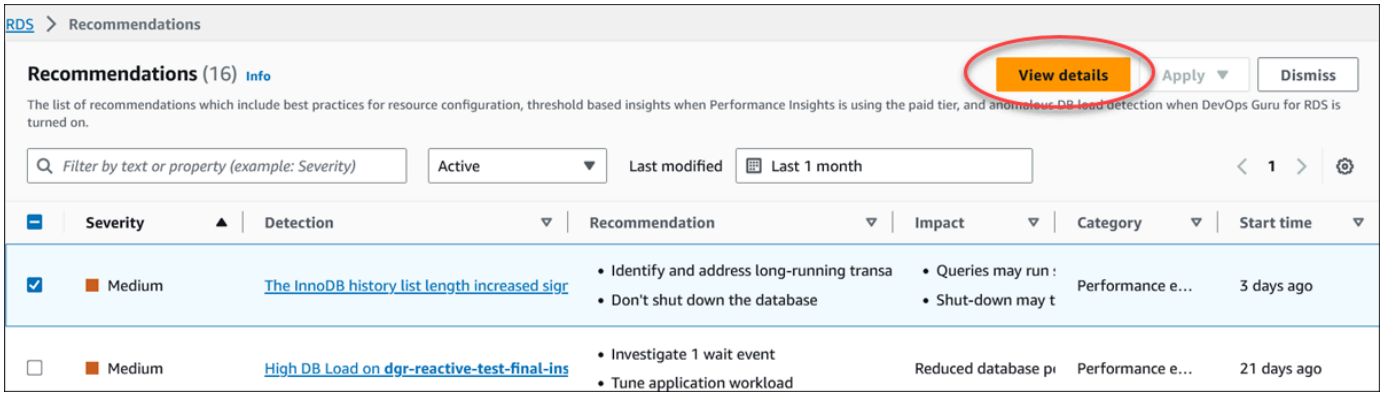
5. (Optional) Wählen Sie unter Letzte Änderung den relativen Modus oder den absoluten Modus, um den Zeitraum zu ändern. Auf der Seite „Empfehlungen“ werden die Empfehlungen angezeigt, die in dem Zeitraum generiert wurden. Der Standardzeitraum ist der letzte Monat. Im Modus Absolut können Sie den Zeitraum wählen oder die Uhrzeit in die Felder Startdatum und Enddatum eingeben.



Die Empfehlungen für den eingestellten Zeitraum werden angezeigt.

Beachten Sie, dass Sie alle Empfehlungen für Ressourcen in Ihrem Konto sehen können, indem Sie den Bereich auf Alle setzen.

6. (Optional) Wählen Sie auf der rechten Seite Einstellungen aus, um die anzuzeigenden Details anzupassen. Sie können ein Seitenformat wählen, die Textzeilen umbrechen und die Spalten zulassen oder ausblenden.
7. (Optional) Wählen Sie eine Empfehlung und dann Details anzeigen aus.



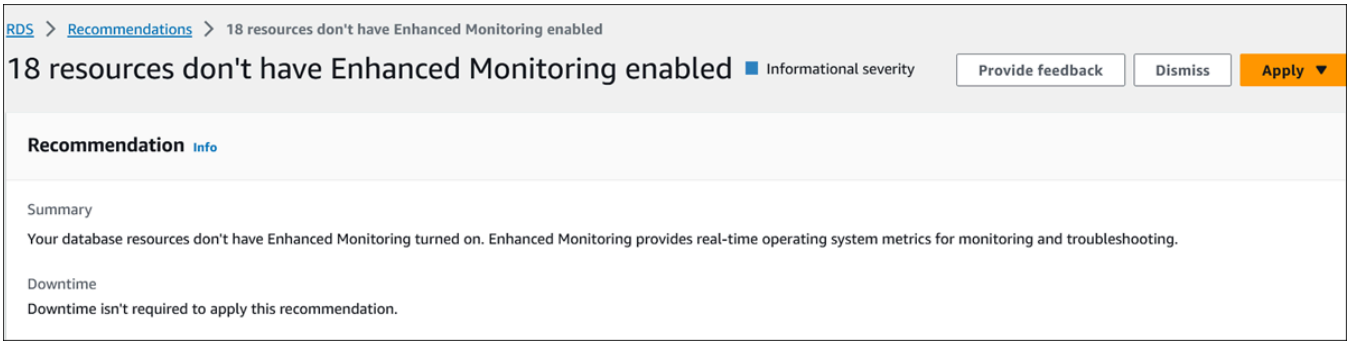
Die Seite mit den Empfehlungsdetails wird angezeigt. Der Titel gibt die Gesamtzahl der Ressourcen an, bei denen das Problem erkannt wurde, und den Schweregrad.

Informationen zu den Komponenten auf der Detailseite für eine auf Anomalien basierende reaktive Empfehlung finden Sie unter Reaktive Anomalien anzeigen im Amazon DevOps Guru-Benutzerhandbuch.

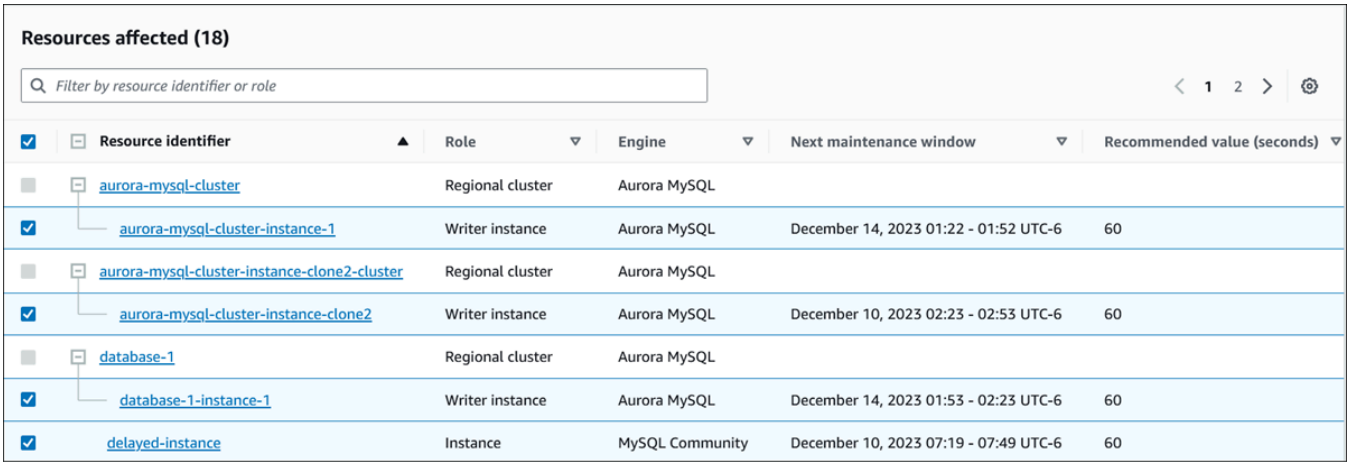
Informationen zu den Komponenten auf der Detailseite für eine auf Schwellenwerten basierende proaktive Empfehlung finden Sie unter. Anzeigen proaktiver Empfehlungen für Performance Insights

Bei den anderen automatisierten Empfehlungen werden auf der Seite mit den Empfehlungsdetails die folgenden Komponenten angezeigt:

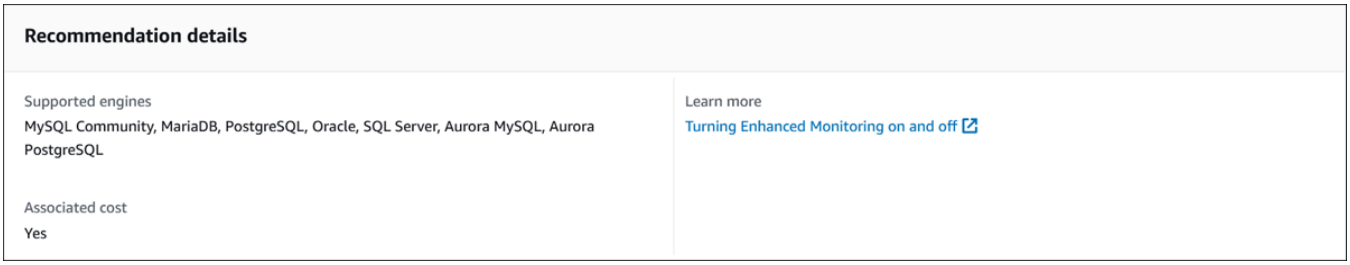
- Empfehlung — Eine Zusammenfassung der Empfehlung und der Angabe, ob Ausfallzeiten erforderlich sind, um die Empfehlung umzusetzen.



- Betroffene Ressourcen — Einzelheiten zu den betroffenen Ressourcen.



- Einzelheiten zur Empfehlung — Informationen zum unterstützten Modul, alle erforderlichen Kosten für die Umsetzung der Empfehlung und Link zur Dokumentation mit weiteren Informationen.



CLI

Um die Amazon RDS-Empfehlungen der DB-Instances oder DB-Cluster anzuzeigen, verwenden Sie den folgenden Befehl in AWS CLI.

```
aws rds describe-db-recommendations
```

RDS-API

Verwenden Sie den Vorgang DescribedbRecommendations, um Amazon RDS-Empfehlungen mithilfe der Amazon RDS-API anzuzeigen.

Reagieren auf Amazon Aurora-Empfehlungen

In der Liste der -Aurora-Empfehlungen können Sie:

- Wenden Sie sofort eine konfigurationsbasierte Empfehlung an oder verschieben Sie sie bis zum nächsten Wartungsfenster.

- Verwerfen Sie eine oder mehrere Empfehlungen.
- Verschieben Sie eine oder mehrere verworfene Empfehlungen in aktive Empfehlungen.

Anwenden einer Amazon-Aurora-Empfehlung

Wählen Sie mithilfe der Amazon-RDS-Konsole auf der Detailseite eine konfigurationsbasierte Empfehlung oder eine betroffene Ressource aus und wenden Sie die Empfehlung sofort an oder planen Sie sie für das nächste Wartungsfenster. Die Ressource muss möglicherweise neu gestartet werden, damit die Änderung wirksam wird. Für einige Empfehlungen für DB-Parametergruppen müssen Sie die Ressourcen möglicherweise neu starten.

Die schwellenwertbasierten proaktiven oder anomaliebasierten reaktiven Empfehlungen haben nicht die Option „anwenden“ und erfordern möglicherweise eine zusätzliche Überprüfung.

Konsole

So wenden Sie eine konfigurationsbasierte Empfehlung an

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus:

   - Wählen Sie Empfehlungen aus.

     Die Seite Empfehlungen wird mit der Liste aller Empfehlungen angezeigt.
   - Wählen Sie Datenbanken und dann Empfehlungen für eine Ressource auf der Datenbankseite aus.

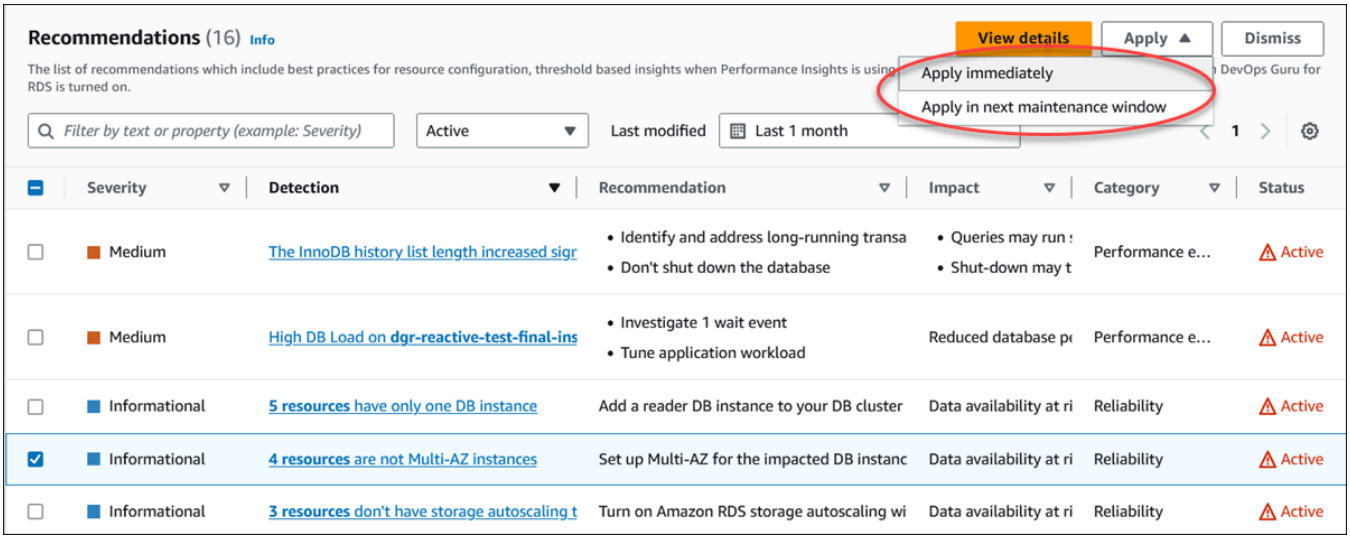
     Die Details werden auf der Registerkarte Empfehlungen für die ausgewählte Empfehlung angezeigt.
   - Wählen Sie auf der Seite Empfehlungen die Option Erkennung für eine aktive Empfehlung oder auf der Seite Datenbanken die Registerkarte Empfehlungen aus.

     Die Seite mit den Empfehlungsdetails wird angezeigt.
3. Wählen Sie auf der Seite mit den Empfehlungsdetails eine Empfehlung oder eine oder mehrere betroffene Ressourcen aus und führen Sie einen der folgenden Schritte aus:

   - Wählen Sie Anwenden und dann Sofort anwenden aus, um die Empfehlung sofort anzuwenden.

- Wählen Sie Anwenden und dann Im nächsten Wartungsfenster anwenden aus, um im nächsten Wartungsfenster zu planen.

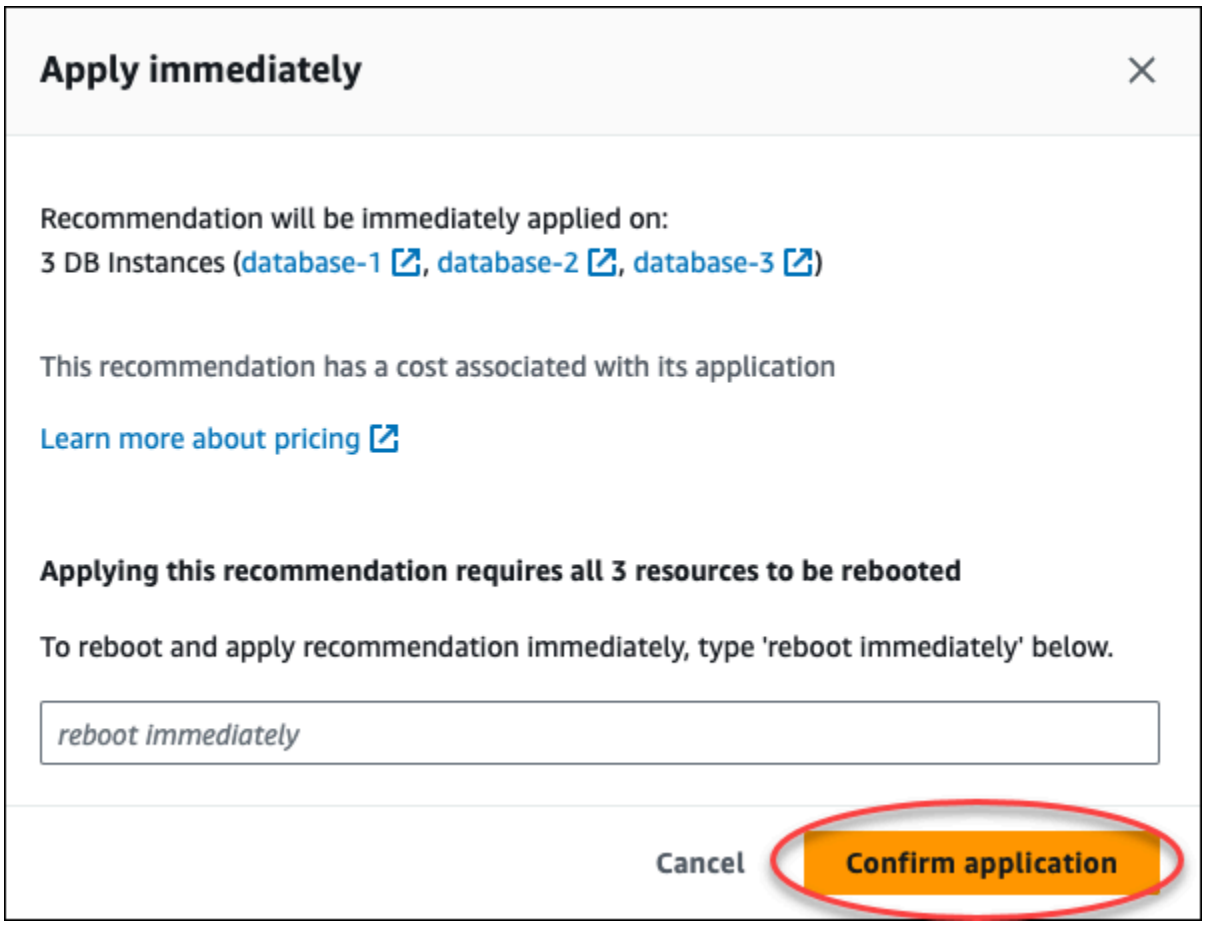
  Der ausgewählte Empfehlungsstatus wird bis zum nächsten Wartungsfenster auf Ausstehend aktualisiert.



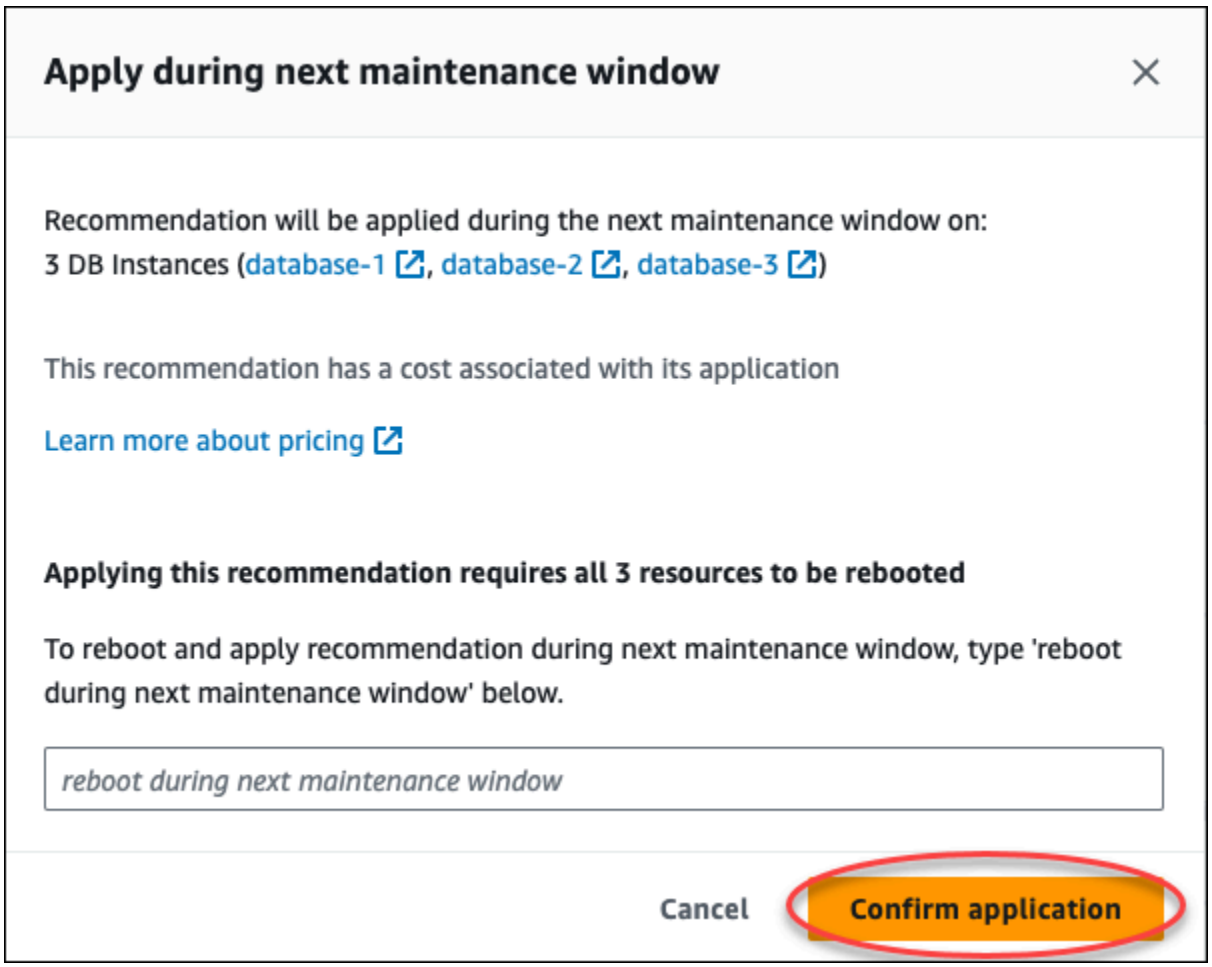
Ein Bestätigungsfenster wird angezeigt.

4. Wählen Sie Anwendung bestätigen, um die Empfehlung anzuwenden. Dieses Fenster bestätigt, ob die Ressourcen einen automatischen oder manuellen Neustart erfordern, damit die Änderungen wirksam werden.

   Das folgende Beispiel zeigt das Bestätigungsfenster, um die Empfehlung sofort anzuwenden.



Das folgende Beispiel zeigt das Bestätigungsfenster, in dem die Anwendung der Empfehlung im nächsten Wartungsfenster geplant wird.



Ein Banner zeigt eine Meldung an, wenn die angewendete Empfehlung erfolgreich ist oder fehlgeschlagen ist.

Das folgende Beispiel zeigt das Banner mit der erfolgreichen Nachricht.

Das folgende Beispiel zeigt das Banner mit der Fehlermeldung.

RDS-API

So wenden Sie eine konfigurationsbasierte -Aurora-Empfehlung mit der Amazon-RDS-API an

1. Verwenden Sie die Produktion DescribeDBRecommendations. Die `RecommendedActions` in der Ausgabe kann eine oder mehrere empfohlene Aktionen enthalten.
2. Verwenden Sie das -RecommendedActionObjekt für jede empfohlene Aktion aus Schritt 1. Die Ausgabe enthält `Operation` und `Parameters`.

   Das folgende Beispiel zeigt die Ausgabe mit einer empfohlenen Aktion.

```
   "RecommendedActions": [
       {
           "ActionId": "0b19ed15-840f-463c-a200-b10af1b552e3",
           "Title": "Turn on auto backup", // localized
           "Description": "Turn on auto backup for my-mysql-instance-1", //
localized
           "Operation": "ModifyDbInstance",
           "Parameters": [
               {
                   "Key": "DbInstanceIdentifier",
                   "Value": "my-mysql-instance-1"
               },
               {
                   "Key": "BackupRetentionPeriod",
                   "Value": "7"
               }
           ],
           "ApplyModes": ["immediately", "next-maintenance-window"],
           "Status": "applied"
       },
       ... // several others
   ],
```

3. Verwenden Sie `operation` für jede empfohlene Aktion aus der Ausgabe in Schritt 2 und geben Sie die `Parameters` Werte ein.
4. Nachdem der Vorgang in Schritt 2 erfolgreich war, verwenden Sie den Vorgang ModifyDBRecommendation, um den Empfehlungsstatus zu ändern.

Verwerfen der Amazon-Aurora-Empfehlungen

Sie können eine oder mehrere Empfehlungen verwerfen.

Konsole

So verwerfen Sie eine oder mehrere Empfehlungen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus:

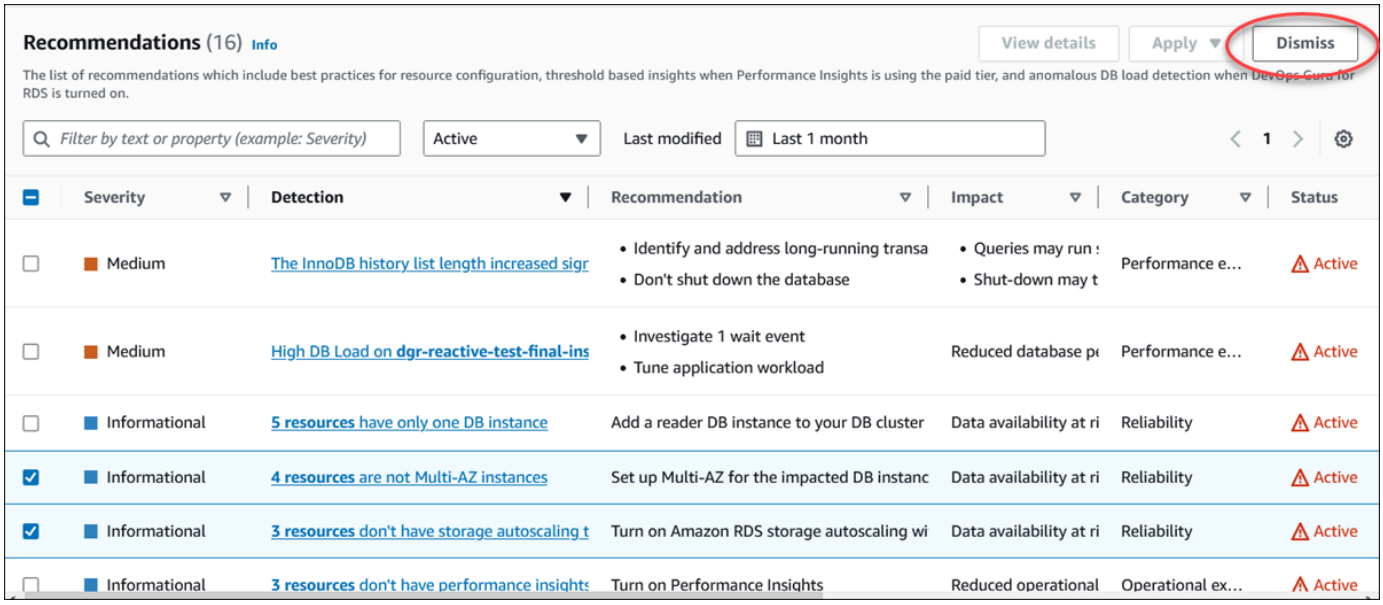
   - Wählen Sie Empfehlungen aus.

     Die Seite Empfehlungen wird mit der Liste aller Empfehlungen angezeigt.
   - Wählen Sie Datenbanken und dann Empfehlungen für eine Ressource auf der Datenbankseite aus.

     Die Details werden auf der Registerkarte Empfehlungen für die ausgewählte Empfehlung angezeigt.
   - Wählen Sie auf der Seite Empfehlungen die Option Erkennung für eine aktive Empfehlung oder auf der Seite Datenbanken die Registerkarte Empfehlungen aus.

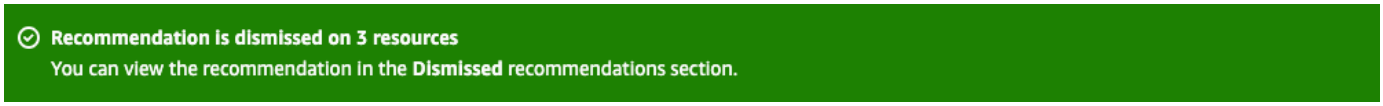
     Auf der Seite mit den Empfehlungsdetails wird die Liste der betroffenen Ressourcen angezeigt.
3. Wählen Sie eine oder mehrere Empfehlungen oder eine oder mehrere betroffene Ressourcen auf der Seite mit den Empfehlungsdetails und dann Verwerfen aus.

   Das folgende Beispiel zeigt die Seite Empfehlungen mit mehreren aktiven Empfehlungen, die zum Verwerfen ausgewählt wurden.



Ein Banner zeigt eine Meldung an, wenn die ausgewählten Empfehlungen verworfen werden.

Das folgende Beispiel zeigt das Banner mit der erfolgreichen Nachricht.



Das folgende Beispiel zeigt das Banner mit der Fehlermeldung.

CLI

So verwerfen Sie -Aurora-Empfehlung mithilfe der AWS CLI

1. Führen Sie den Befehl `aws rds describe-db-recommendations --filters "Name=status,Values=active"` aus.

   Die Ausgabe enthält eine Liste von Empfehlungen im `active` Status .
2. Suchen Sie die `recommendationId` für die Empfehlung, die Sie aus Schritt 1 verwerfen möchten.
3. Führen Sie den Befehl `>aws rds modify-db-recommendation --status dismissed --recommendationId <ID>` mit der `recommendationId` aus Schritt 2 aus, um die Empfehlung zu verwerfen.

RDS-API

Um -Aurora-Empfehlung mit der Amazon-RDS-API zu verwerfen, verwenden Sie die Operation ModifyDBRecommendation.

Ändern der verworfenen Amazon-Aurora-Empfehlungen in aktive Empfehlungen

Sie können eine oder mehrere verworfene Empfehlungen in aktive Empfehlungen verschieben.

Konsole

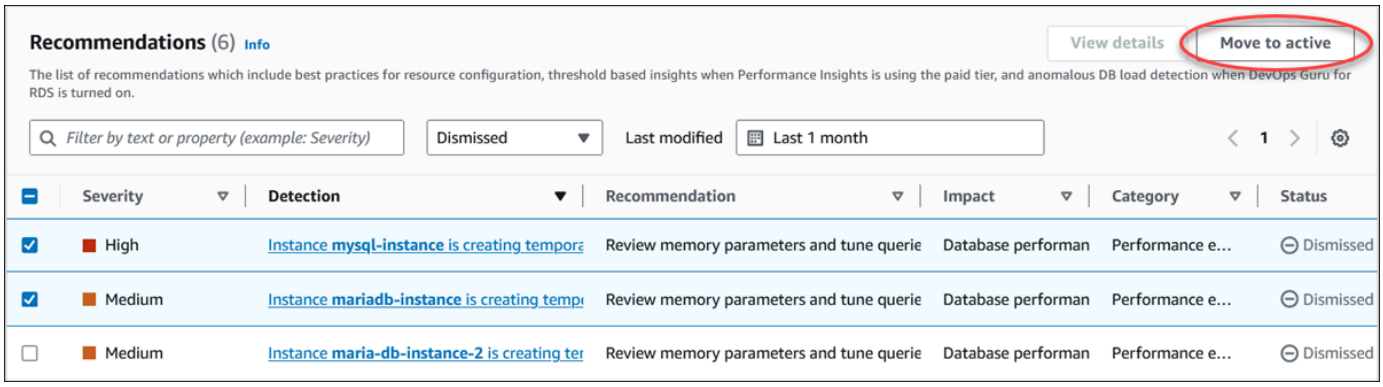
So verschieben Sie eine oder mehrere verworfene Empfehlungen in aktive Empfehlungen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus:

   - Wählen Sie Empfehlungen aus.

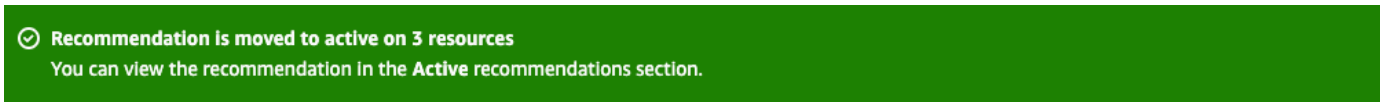
     Auf der Seite Empfehlungen wird eine Liste von Empfehlungen angezeigt, sortiert nach dem Schweregrad für alle Ressourcen in Ihrem Konto.
   - Wählen Sie Datenbanken und dann Empfehlungen für eine Ressource auf der Datenbankseite aus.

     Auf der Registerkarte Empfehlungen werden die Empfehlungen und ihre Details für die ausgewählte Ressource angezeigt.
3. Wählen Sie eine oder mehrere verworfene Empfehlungen aus der Liste aus und klicken Sie dann auf Zu aktivem verschieben.



Ein Banner zeigt eine Erfolgsmeldung oder eine Fehlermeldung an, wenn die die ausgewählten Empfehlungen von verworfen in den aktiven Status verschiebt.

Das folgende Beispiel zeigt das Banner mit der erfolgreichen Nachricht.



Das folgende Beispiel zeigt das Banner mit der Fehlermeldung.

CLI

So ändern Sie eine verworfene -Aurora-Empfehlung in eine aktive Empfehlung mithilfe der AWS CLI

1. Führen Sie den Befehl `aws rds describe-db-recommendations --filters "Name=status,Values=dismissed"` aus.

   Die Ausgabe enthält eine Liste von Empfehlungen im `dismissed` Status .
2. Suchen Sie die `recommendationId` für die Empfehlung, dass Sie den Status von Schritt 1 ändern möchten.
3. Führen Sie den Befehl `>aws rds modify-db-recommendation --status active --recommendationId <ID>` mit der `recommendationId` aus Schritt 2 aus, um zu einer aktiven Empfehlung zu wechseln.

RDS-API

Um eine verworfene -Aurora-Empfehlung mithilfe der Amazon-RDS-API in eine aktive Empfehlung zu ändern, verwenden Sie die Operation ModifyDBRecommendation.

Anzeigen von Metriken in der Amazon-RDS-Konsole

Amazon RDS lässt sich in Amazon CloudWatch integrieren, um eine Vielzahl von Aurora-DB-Cluster-Metriken in der RDS-Konsole anzuzeigen. Einige Metriken gelten auf Cluster-Ebene, während andere auf Instance-Ebene gelten.Für Beschreibungen (dieser Metriken)the instance-level and cluster-level metrics (der Instance-Ebene- und Cluster-Ebene-Metriken), finden Sie unter Amazon Aurora-Referenz für Metriken.

Für Ihren Aurora-DB-Cluster werden die folgenden Metrikkategorien überwacht:

- CloudWatch – zeigt die Amazon-CloudWatch-Metriken für Aurora , auf die Sie in der RDS-Konsole zugreifen können. Diese Metriken können Sie auch in der CloudWatch-Konsole aufrufen. Jede Metrik beinhaltet ein Diagramm, das die überwachte Metrik für ein bestimmtes Zeitintervall anzeigt. Eine Liste der CloudWatch-Metriken finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora.
- Enhanced Monitoring (Erweiterte Überwachung) – Zeigt eine Übersicht über Metriken des Betriebssystems an, wenn Ihre Aurora-DB-Cluster das Enhanced Monitoring aktiviert hat. RDS liefert die Metriken von „Enhanced Monitoring“·(Erweiterte·Überwachung) in Ihr Amazon-CloudWatch-Logs-Konto. Jede Betriebssystem-Metrik beinhaltet ein Diagramm, das die überwachte Metrik für ein bestimmtes Zeitintervall anzeigt. Eine Übersicht finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung). Eine Liste der Metriken für „Enhanced Monitoring“·(Erweiterte·Überwachung) finden Sie unter Betriebssystemmetriken im „Enhanced Monitoring“ (Erweiterte Überwachung).
- Betriebssystem-Prozessliste – Zeigt Detailinformationen über alle Prozesse, die innerhalb Ihres DB--Clusters ausgeführt werden.
- Performance Insights – Öffnet das Amazon-RDS-Performance-Insights-Dashboard für eine DB-Instance in Ihrem Aurora-DB-Cluster. Performance Insights wird auf Cluster-Ebene nicht unterstützt.Eine Übersicht über Performance Insights finden Sie unter Überwachung mit Performance Insights auf . Eine Liste der Peformance-Insights-Metriken finden Sie unter CloudWatch Amazon-Metriken für Performance Insights.

Amazon RDS bietet jetzt im Performance-Insights-Dashboard eine konsolidierte Ansicht der Performance-Insights- und CloudWatch-Metriken. Performance Insights muss aktiviert sein, damit Ihr DB-Cluster diese Ansicht verwenden kann. Sie können die neue Überwachungsansicht auf der Registerkarte Überwachung oder Performance Insights im Navigationsbereich auswählen.

Anweisungen zur Auswahl dieser Ansicht finden Sie unter Anzeigen von kombinierten Metriken in der Amazon-RDS-Konsole.

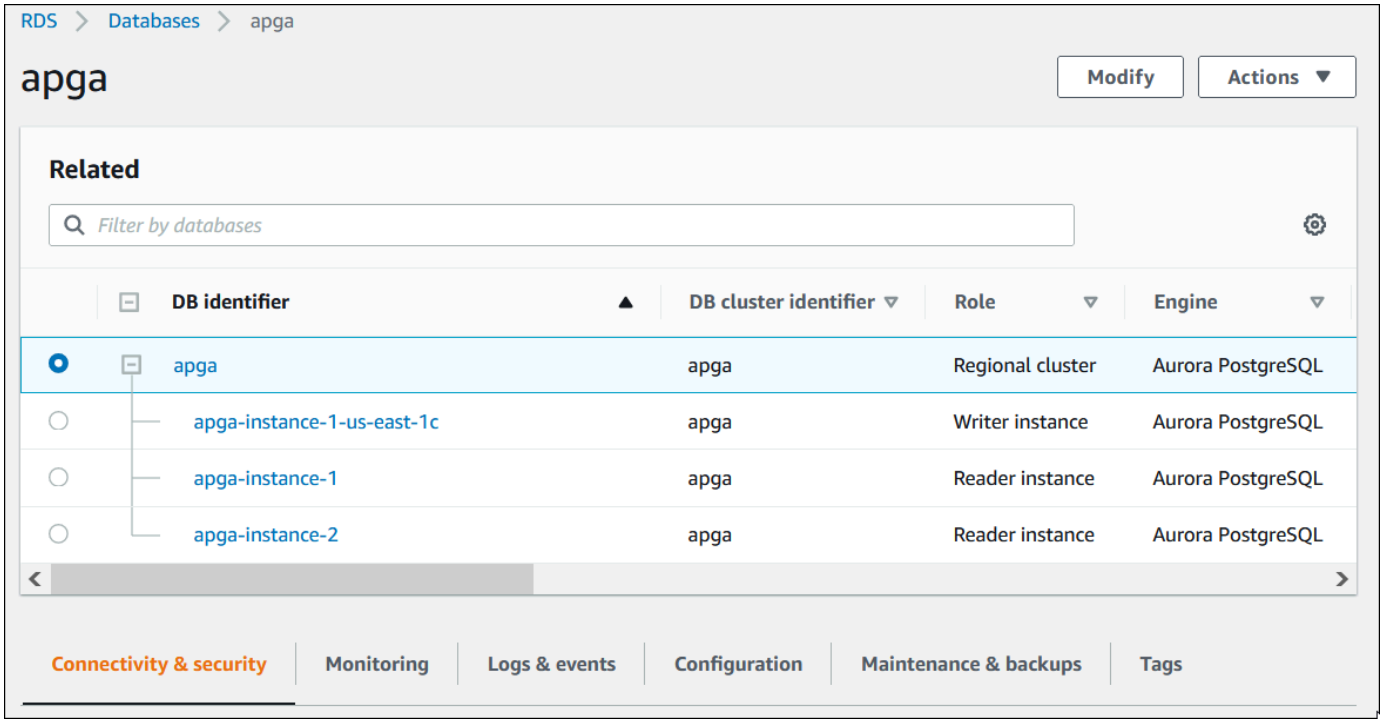
Wenn Sie die Legacy-Überwachungsansicht beibehalten möchten, setzen Sie dieses Verfahren fort.

> **Note**
>
> Die Legacy-Überwachungsansicht wird am 15. Dezember 2023 eingestellt.

So zeigen Sie Metriken für Ihren DB-Cluster in der Legacy-Überwachungsansicht an:

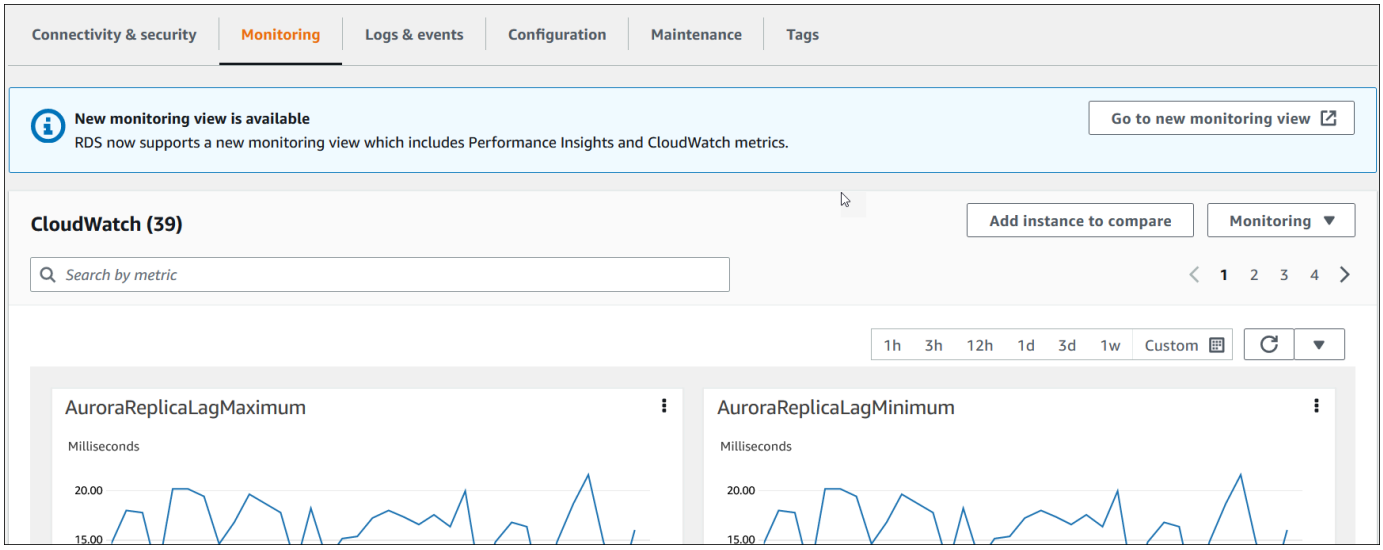
1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Namen des Aurora-DB--Cluster an, das Sie überwachen möchten.

   Der Bereich Datenbanken wird angezeigt. Das folgende Beispiel zeigt eine Amazon-Aurora-PostgreSQL-Datenbank namens apga an.

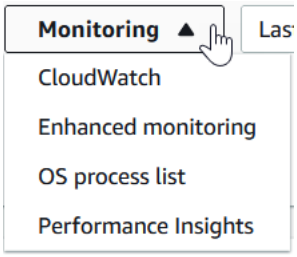


4. Scrollen Sie nach unten und wählen Sie Monitoring (Überwachung) aus.

Der Abschnitt „Überwachung“ wird angezeigt. Standardmäßig werden alle CloudWatch-Metriken angezeigt. Beschreibungen dieser Metriken finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora.

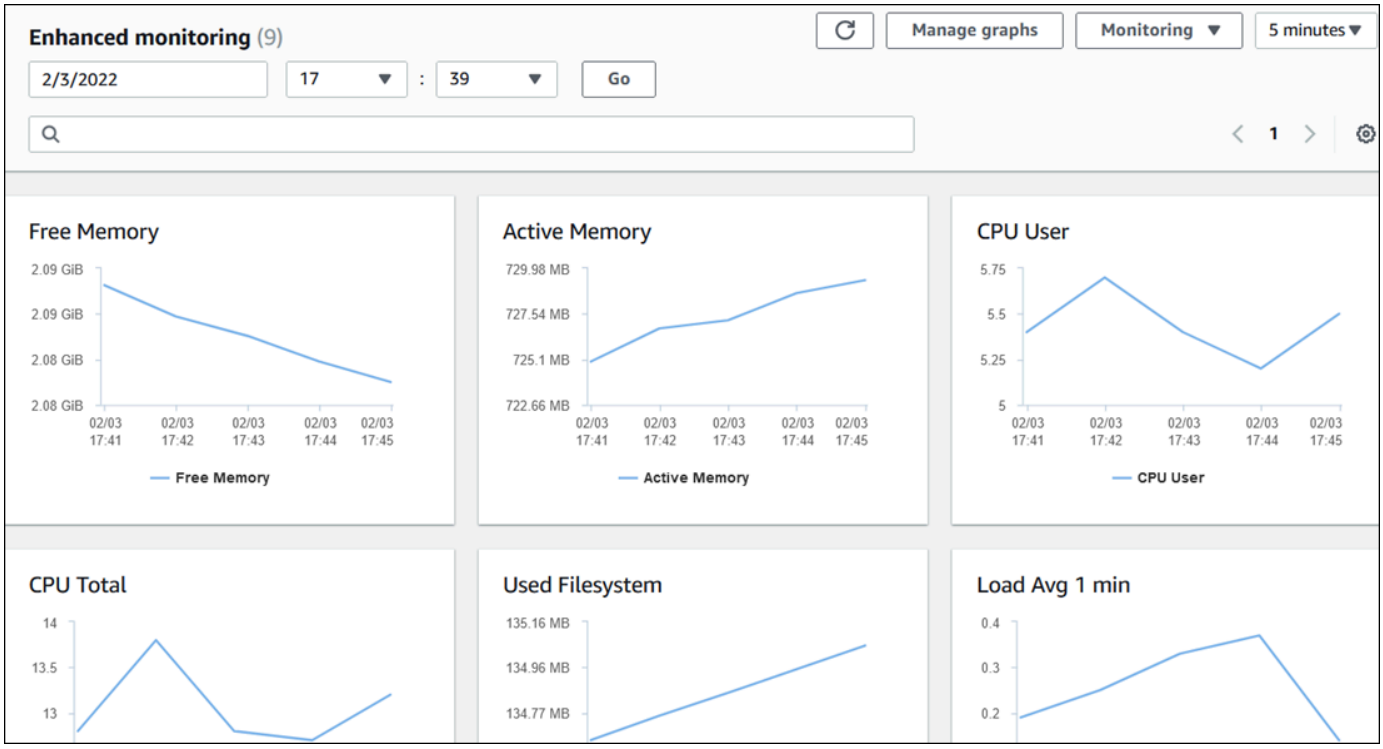


5. Wählen Sie Monitoring (Überwachung) aus, um die Metrik-Kategorien zu sehen.



6. Wählen Sie die Metrikkategorie aus, die Sie anzeigen möchten.

   Die folgende Abbildung zeigt Metriken für „Enhanced Monitoring“·(Erweiterte·Überwachung) an. Beschreibungen dieser Metriken finden Sie unter Betriebssystemmetriken im „Enhanced Monitoring“ (Erweiterte Überwachung).



Tip

Sie können den Zeitraum der durch die Diagramme dargestellten Metriken mit der Zeitraumliste auswählen.

Um eine Detailansicht anzuzeigen, können Sie ein beliebiges Diagramm auswählen. Sie können auch Metrik-spezifische Filter auf die Daten anwenden.

Anzeigen von kombinierten Metriken in der Amazon-RDS-Konsole

Amazon RDS bietet jetzt im Performance-Insights-Dashboard eine konsolidierte Ansicht der Performance-Insights- und CloudWatch-Metriken für Ihre DB-Instance. Sie können das vorkonfigurierte Dashboard verwenden oder ein benutzerdefiniertes Dashboard erstellen. Das vorkonfigurierte Dashboard enthält die am häufigsten verwendeten Metriken zur Diagnose von Leistungsproblemen für eine Datenbank-Engine. Alternativ können Sie ein benutzerdefiniertes Dashboard mit den Metriken für eine Datenbank-Engine erstellen, die Ihren Analyseanforderungen entsprechen. Verwenden Sie dann dieses Dashboard für alle DB-Instances dieses Datenbank-Engine-Typs in Ihrem AWS-Konto.

Sie können die neue Überwachungsansicht auf der Registerkarte Überwachung oder Performance Insights im Navigationsbereich auswählen. Wenn Sie zur Seite „Performance Insights“ navigieren, sehen Sie die Optionen, mit denen Sie zwischen der neuen und der Legacy-Überwachungsansicht wählen können. Die von Ihnen ausgewählte Option wird als Standardansicht gespeichert.

Performance Insights muss für Ihren DB-Cluster aktiviert sein, um die kombinierten Metriken im Performance-Insights-Dashboard anzeigen zu können. Weitere Informationen zum Aktivieren von Performance Insights finden Sie unter Performance Insights für Aurora ein- und ausschalten.

> **Note**
>
> Wir empfehlen, die neue Überwachungsansicht auszuwählen. Sie können die Legacy-Überwachungsansicht bis zum 15. Dezember 2023 verwenden. Dann wird sie eingestellt.

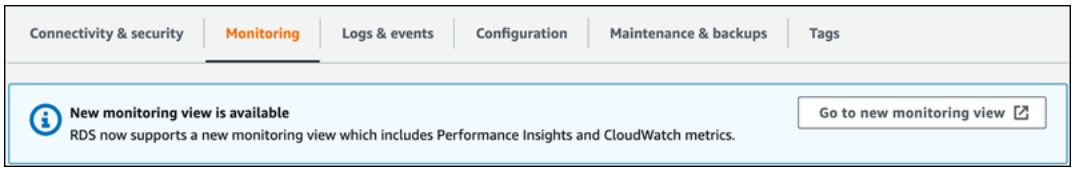
Auswählen der neuen Überwachungsansicht auf der Registerkarte Überwachung

So wählen Sie die neue Überwachungsansicht auf der Registerkarte Überwachung aus:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Datenbanken aus.
3. Wählen Sie den Aurora-DB-Cluster zur Überwachung aus.

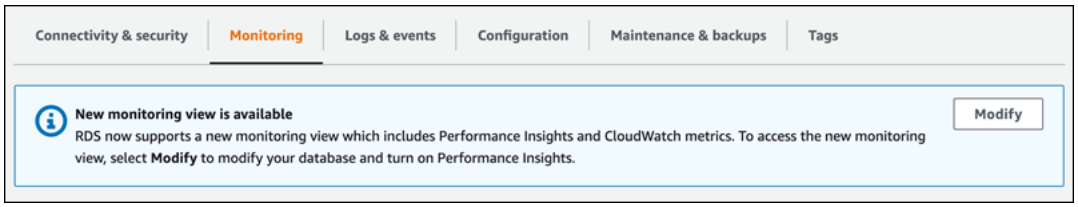
   Der Bereich Datenbanken wird angezeigt.
4. Scrollen Sie nach unten und wählen Sie die Registerkarte Überwachung aus.

Es erscheint ein Banner mit der Option, die neue Überwachungsansicht auszuwählen. Das folgende Beispiel veranschaulicht das Banner zur Auswahl der neuen Überwachungsansicht.



5. Wählen Sie Gehe zur neuen Überwachungsansicht aus, um das Performance-Insights-Dashboard mit Performance Insights- und CloudWatch-Metriken für Ihren DB-Cluster zu öffnen.
6. (Optional) Wenn Performance Insights für Ihre DB-Instance deaktiviert ist, wird ein Banner mit der Option angezeigt, Ihre DB-Instance zu ändern und Performance Insights zu aktivieren.

   Das folgende Beispiel veranschaulicht das Banner zum Ändern der DB-Instance auf der Registerkarte Überwachung.



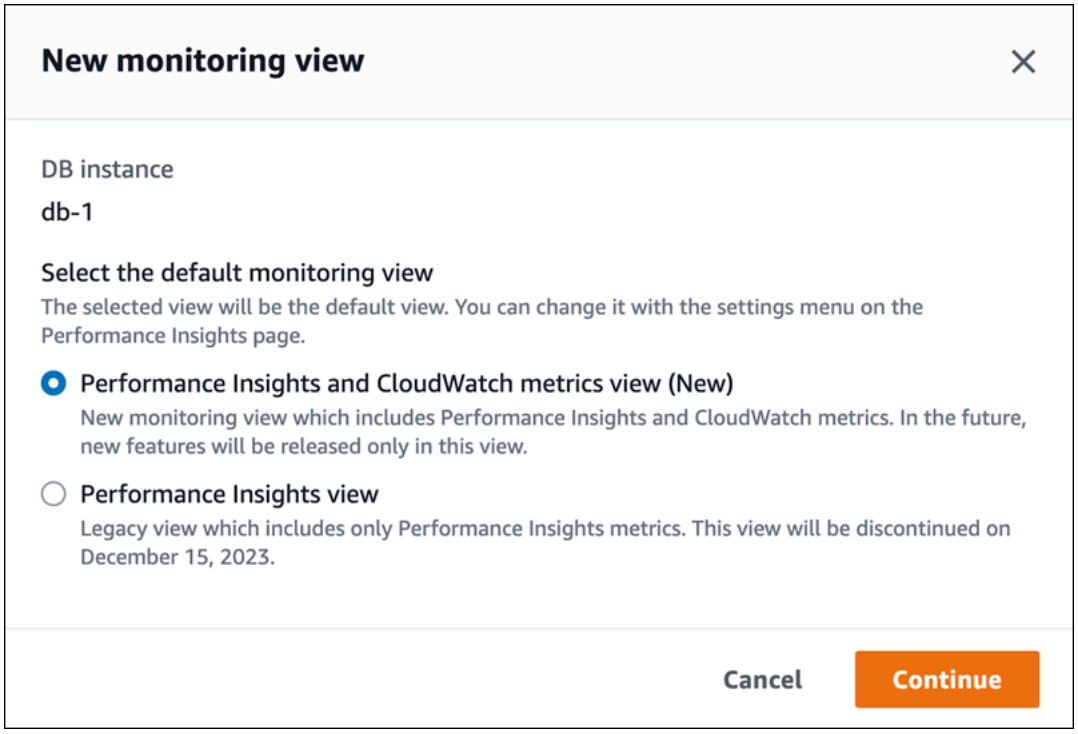
   Wählen Sie Ändern aus, um Ihre DB-Instance zu ändern und Performance Insights zu aktivieren. Weitere Informationen zum Aktivieren von Performance Insights finden Sie unter Performance Insights für Aurora ein- und ausschalten.

Auswählen der neuen Überwachungsansicht mit Performance Insights im Navigationsbereich

So wählen Sie die neue Überwachungsansicht mit Performance Insights im Navigationsbereich aus:

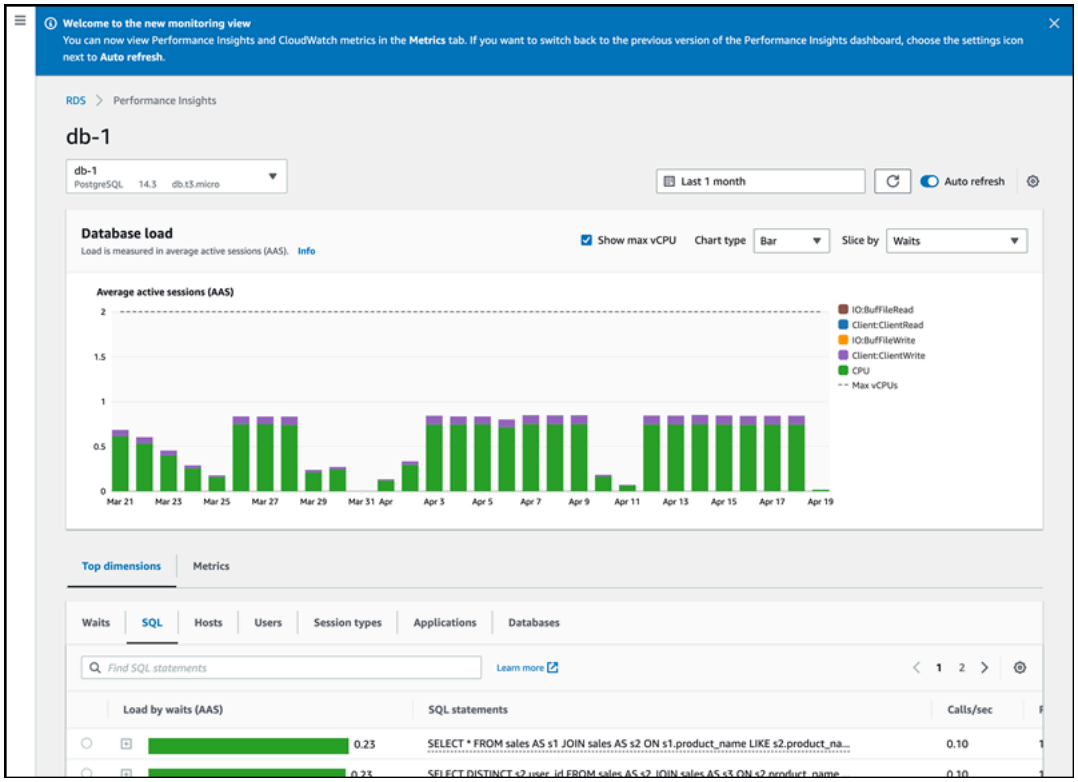
1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus, um ein Fenster mit den Optionen für die Überwachungsansicht zu öffnen.

   Das folgende Beispiel veranschaulicht das Fenster mit den Optionen für die Überwachungsansicht.



4. Wählen Sie die Option Performance-Insights- und CloudWatch-Metrikansicht (Neu) und dann Weiter aus.

   Sie können jetzt das Performance-Insights-Dashboard mit den Performance-Insights- und den CloudWatch-Metriken für Ihre DB-Instance anzeigen. Das folgende Beispiel veranschaulicht die Performance-Insights- und CloudWatch-Metriken im Dashboard.



Auswählen der Legacy-Ansicht mit Performance Insights im Navigationsbereich

Sie können die Legacy-Überwachungsansicht auswählen, um nur die Performance-Insights-Metriken für Ihre DB-Instance anzuzeigen.

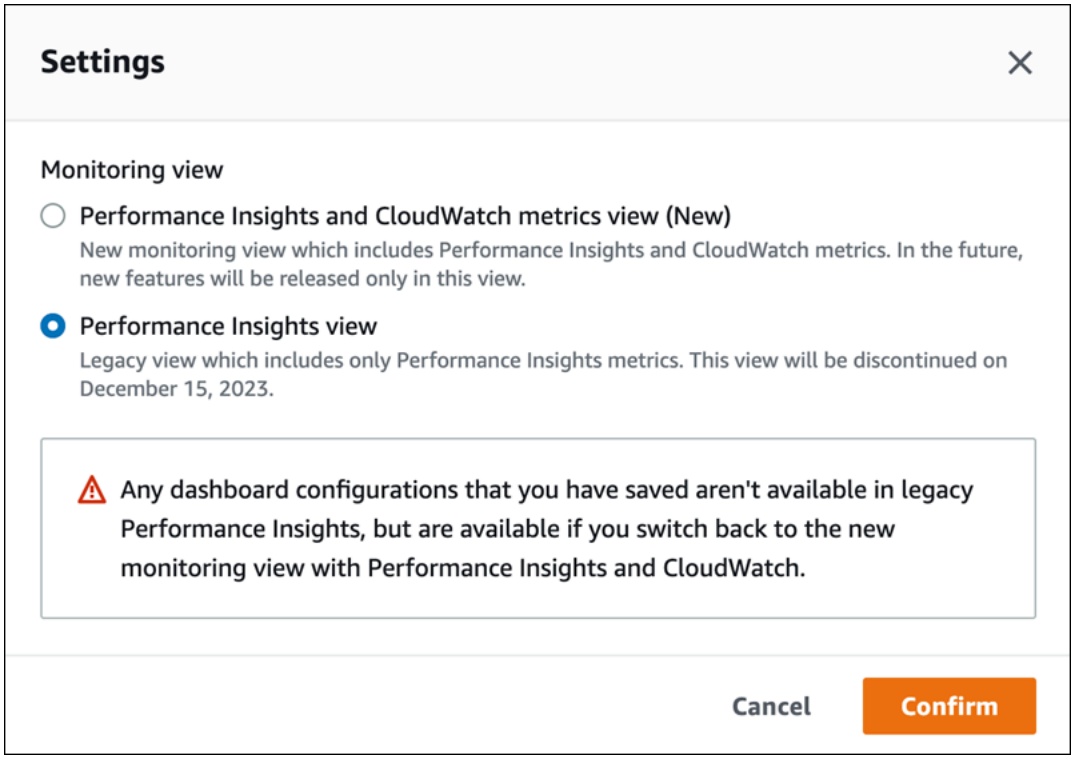
> **Note**
>
> Diese Ansicht wird am 15. Dezember 2023 eingestellt.

So wählen Sie die Legacy-Überwachsungsansicht mit Performance Insights im Navigationsbereich aus:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.
4. Wählen Sie das Einstellungensymbol im Performance-Insights-Dashboard aus.

Das Fenster Einstellungen wird mit der Option zur Auswahl der Legacy-Performance-Insights-Ansicht angezeigt.

Das folgende Beispiel veranschaulicht das Fenster mit der Option für die Legacy-Überwachungsansicht.



5. Wählen Sie die Option Performance-Insights-Ansicht und Weiter aus.

   Eine Warnmeldung wird angezeigt. Alle von Ihnen gespeicherten Dashboard-Konfigurationen sind in dieser Ansicht nicht verfügbar.

6. Wählen Sie Bestätigen aus, um mit der Legacy-Performance-Insights-Ansicht fortzufahren.

   Sie können jetzt das Performance-Insights-Dashboard nur mit den Performance-Insights-Metriken für Ihre DB-Instance anzeigen.

Erstellen eines benutzerdefinierten Dashboards mit Performance Insights im Navigationsbereich

In der neuen Überwachungsansicht können Sie ein benutzerdefiniertes Dashboard mit den Metriken erstellen, die Sie für Ihre Analyseanforderungen benötigen.

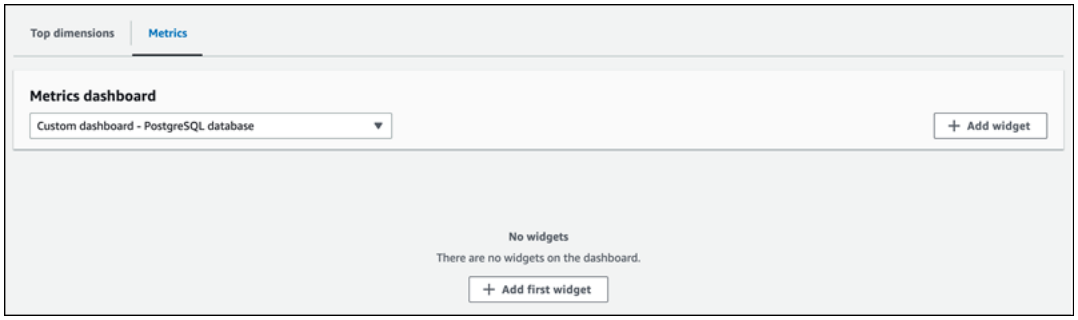
Sie können ein benutzerdefiniertes Dashboard erstellen, indem Sie Performance-Insights- und CloudWatch-Metriken für Ihre DB-Instance auswählen. Dieses benutzerdefinierte Dashboard können Sie für andere DB-Instances dieses Datenbank-Engine-Typs in Ihrem AWS-Konto verwenden.

> **Note**
>
> Das benutzerdefinierte Dashboard unterstützt bis zu 50 Metriken.

Verwenden Sie das Widget-Einstellungsmenü, um das Dashboard zu bearbeiten oder zu löschen und das Widget-Fenster zu verschieben oder in der Größe zu ändern.

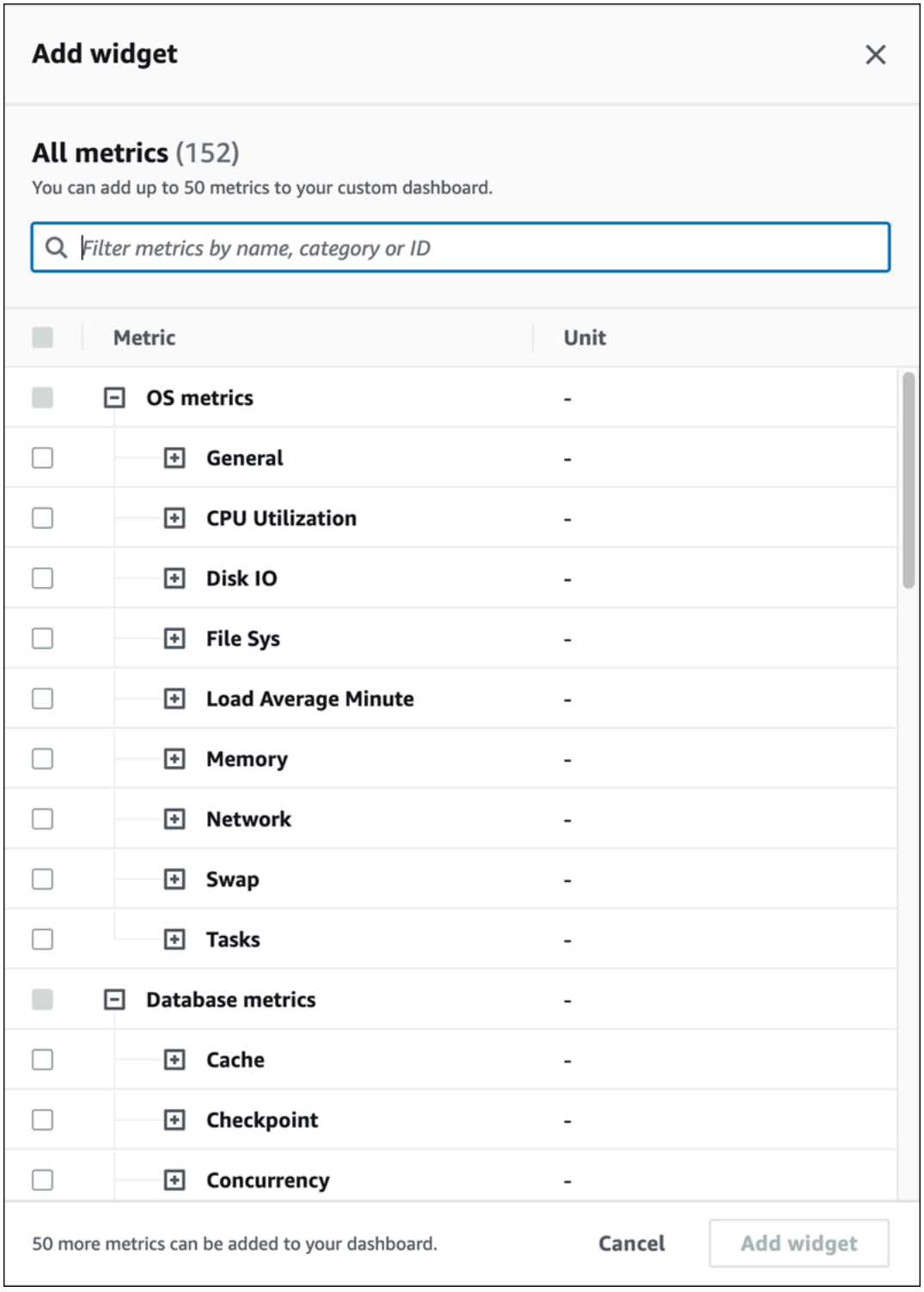
So erstellen Sie ein benutzerdefiniertes Dashboard mit Performance Insights im Navigationsbereich:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.
4. Scrollen Sie im Fenster nach unten zur Registerkarte Metriken.
5. Wählen Sie das benutzerdefinierte Dashboard aus der Dropdown-Liste aus. Das folgende Beispiel veranschaulicht die Erstellung eines benutzerdefinierten Dashboards.



6. Wählen Sie Widget hinzufügen aus, um das Fenster Widget hinzufügen zu öffnen. Sie können die verfügbaren Betriebssystem-Metriken, Datenbankmetriken und CloudWatch-Metriken in dem Fenster öffnen und anzeigen.

   Das folgende Beispiel veranschaulicht das Fenster Widget hinzufügen mit den Metriken.



7. Wählen Sie die Metriken aus, die Sie im Dashboard anzeigen möchten. Klicken Sie dann auf Widget hinzufügen. Sie können über das Suchfeld eine bestimmte Metrik suchen.

   Die ausgewählten Metriken werden in Ihrem Dashboard angezeigt.

8. (Optional) Wenn Sie Ihr Dashboard ändern oder löschen möchten, wählen Sie das Einstellungensymbol oben rechts im Widget und dann eine der folgenden Aktionen im Menü aus.
   - Bearbeiten – Ändern Sie die Metrikenliste im Fenster. Wählen Sie Widget aktualisieren aus, nachdem Sie die Metriken für Ihr Dashboard ausgewählt haben.
   - Löschen – Löscht das Widget. Wählen Sie im Bestätigungsfenster Löschen aus.

Auswählen des vorkonfigurierten Dashboards mit Performance Insights im Navigationsbereich

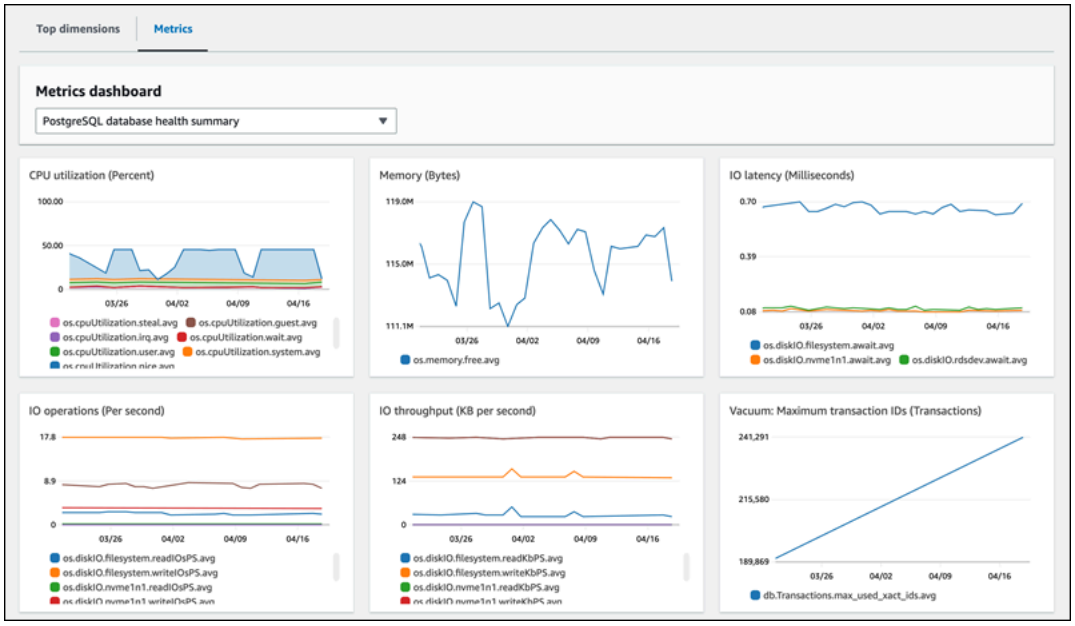
Sie können die am häufigsten verwendeten Metriken über das vorkonfigurierte Dashboard anzeigen. Dieses Dashboard hilft bei der Diagnose von Leistungsproblemen mit einer Datenbank-Engine und reduziert die durchschnittliche Wiederherstellungszeit von Stunden auf Minuten.

> **Note**
>
> Dieses Dashboard kann nicht bearbeitet werden.

So wählen Sie das vorkonfigurierte Dashboard mit Performance Insights im Navigationsbereich aus:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.
4. Scrollen Sie im Fenster nach unten zur Registerkarte Metriken.
5. Wählen Sie ein vorkonfiguriertes Dashboard aus der Dropdown-Liste aus.

   Sie können die Metriken für die DB-Instance im Dashboard anzeigen. Das folgende Beispiel veranschaulicht ein vorkonfiguriertes Metriken-Dashboard.


Top dimensions
Metrics
Metrics dashboard
PostgreSQL database health summary
CPU utilization (Percent)
100.00
50.00
0
03/26
04/02
04/09
04/16
os.cpuUtilization.steal.avg
os.cpuUtilization.guest.avg
os.cpuUtilization.irq.avg
os.cpuUtilization.wait.avg
os.cpuUtilization.user.avg
os.cpuUtilization.system.avg
Memory (Bytes)
119.0M
115.0M
111.1M
os.memory.free.avg
IO latency (Milliseconds)
0.70
0.39
0.08
os.diskIO.filesystem.await.avg
os.diskIO.nvme1n1.await.avg
os.diskIO.rdsdev.await.avg
IO operations (Per second)
17.8
8.9
os.diskIO.filesystem.readIOsPS.avg
os.diskIO.filesystem.writeIOsPS.avg
os.diskIO.nvme1n1.readIOsPS.avg
IO throughput (KB per second)
248
124
os.diskIO.filesystem.readKbPS.avg
os.diskIO.filesystem.writeKbPS.avg
os.diskIO.nvme1n1.readKbPS.avg
Vacuum: Maximum transaction IDs (Transactions)
241,291
215,580
189,869
db.Transactions.max_used_xact_ids.avg

Überwachen von Amazon Aurora-Metriken mit Amazon CloudWatch

Amazon CloudWatch ist ein Repository für Metriken. Das Repository erfasst und verarbeitet Rohdaten aus Amazon Aurora, um nahezu in Echtzeit lesbare Metriken bereitzustellen. Eine vollständige Liste von Amazon Aurora- Metriken, die an CloudWatch gesendet werden, finden Sie unter Metrikreferenz für Amazon Aurora.

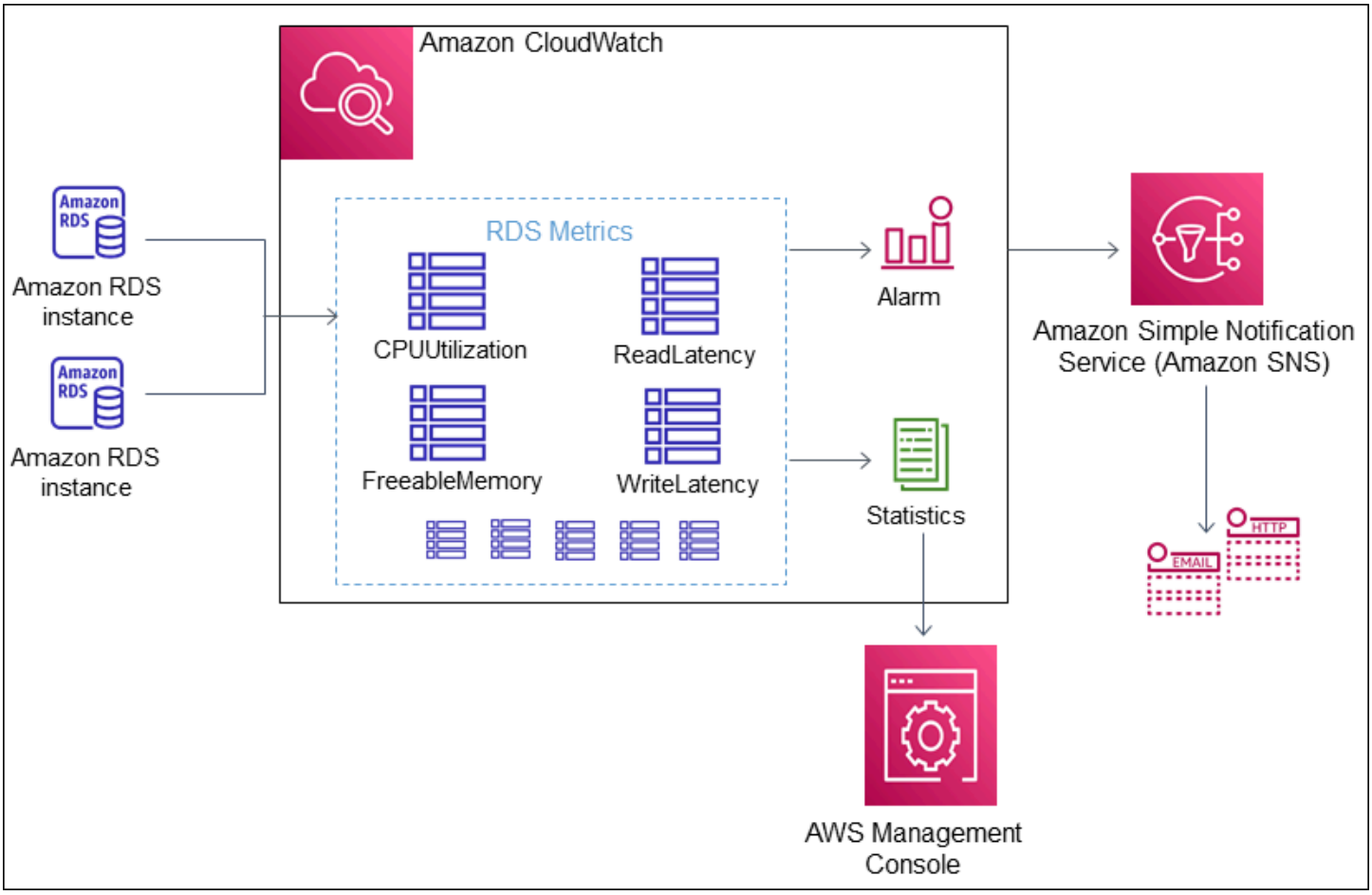
Themen

Übersicht über Amazon Aurora und Amazon CloudWatch

Standardmäßig werden Metrikdaten von Amazon Aurora in Abständen von 1 Minute automatisch an CloudWatch gesendet. Die Metrik `CPUUtilization` zeichnet z. B. den Prozentsatz der CPU-Auslastung für eine DB-Instance im Laufe der Zeit auf. Datenpunkte mit einem Zeitraum von 60 Sekunden (1 Minute) stehen 15 Tage lang zur Verfügung Dies bedeutet, dass Sie auf die Verlaufsdaten zugreifen und sehen können, wie die Leistung Ihrer Webanwendung oder Ihres Service ist.

Sie können jetzt Metrik-Dashboards von Performance Insights von Amazon RDS zu Amazon CloudWatch exportieren. Sie können die vorkonfigurierten oder benutzerdefinierten Metrik-Dashboards als neues Dashboard exportieren oder sie einem vorhandenen CloudWatch-Dashboard hinzufügen. Das exportierte Dashboard kann in der CloudWatch-Konsole angezeigt werden. Weitere Informationen zum Exportieren der Metrik-Dashboards von Performance Insights zu CloudWatch finden Sie unter Exportieren von Performance-Insights-Metriken nach CloudWatch.

Wie im folgenden Diagramm gezeigt, können Sie Alarme für Ihre CloudWatch-Metriken einrichten. Beispielsweise könnten Sie einen Alarm erstellen, der signalisiert, wenn die CPU-Auslastung für eine Instanz über 70 % beträgt. Sie können Amazon Simple Notification Service so konfigurieren, dass Sie eine E-Mail erhalten, wenn der Schwellenwert überschritten wird.



Amazon RDS veröffentlicht die folgenden Arten von Metriken auf Amazon CloudWatch:

- Aurora-Metriken sowohl auf Cluster- als auch auf Instance-Ebene

  Eine Tabelle dieser Metriken finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora.
- Performance-Insights-Metriken

  Eine Tabelle dieser Metriken finden Sie unter CloudWatch Amazon-Metriken für Performance Insights und Performance-Insights-Zählermetriken.
- Enhanced-Monitoring-Metriken (veröffentlicht in Amazon CloudWatch Logs)

  Eine Tabelle dieser Metriken finden Sie unter Betriebssystemmetriken im „Enhanced Monitoring“ (Erweiterte Überwachung).
- Nutzungsmetriken für die Amazon-RDS-Service-Quotas in Ihrem AWS-Konto

Eine Tabelle dieser Metriken finden Sie unter CloudWatch Amazon-Nutzungsmetriken für Amazon Aurora. Weitere Informationen über Amazon-RDS-Kontingente finden Sie unter Kontingente und Beschränkungen für Amazon Aurora.

Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im Amazon CloudWatch-Benutzerhandbuch. Weitere Informationen zur Aufbewahrung von CloudWatch-Metriken finden Sie unter Aufbewahrung von Metriken.

Anzeigen von DB-Cluster-Metriken in der - CloudWatch Konsole und AWS CLI

Im Folgenden finden Sie Details zum Anzeigen von Metriken für Ihre DB-Instance mit CloudWatch. Informationen zur Überwachung von Metriken für das Betriebssystem Ihrer DB-Instance in Echtzeit mithilfe von - CloudWatch Protokollen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).

Wenn Sie Amazon Aurora-Ressourcen verwenden, sendet Amazon Aurora CloudWatch jede Minute Metriken und Dimensionen an Amazon.

Sie können jetzt Metrik-Dashboards von Performance Insights von Amazon RDS nach Amazon exportieren CloudWatch und diese Metriken in der CloudWatch Konsole anzeigen. Weitere Informationen zum Exportieren der Metrik-Dashboards von Performance Insights nach CloudWatchfinden Sie unter Exportieren von Performance-Insights-Metriken nach CloudWatch.

Gehen Sie wie folgt vor, um die Metriken für Amazon Aurora in der CloudWatch Konsole und CLI anzuzeigen.

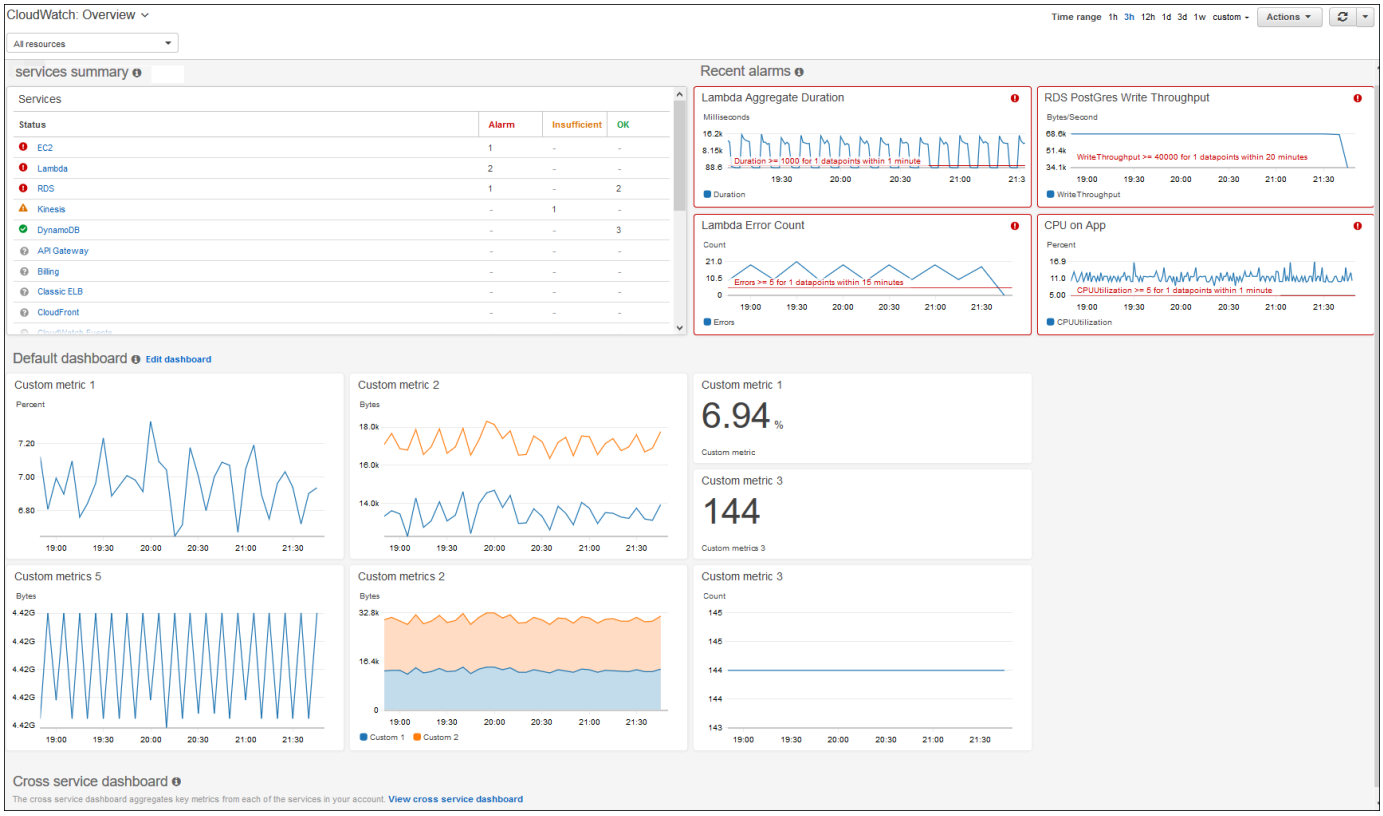
Konsole

So zeigen Sie Metriken mit der Amazon- CloudWatch Konsole an

Metriken werden zunächst nach dem Service-Namespace und anschließend nach den verschiedenen Dimensionskombinationen in den einzelnen Namespaces gruppiert.

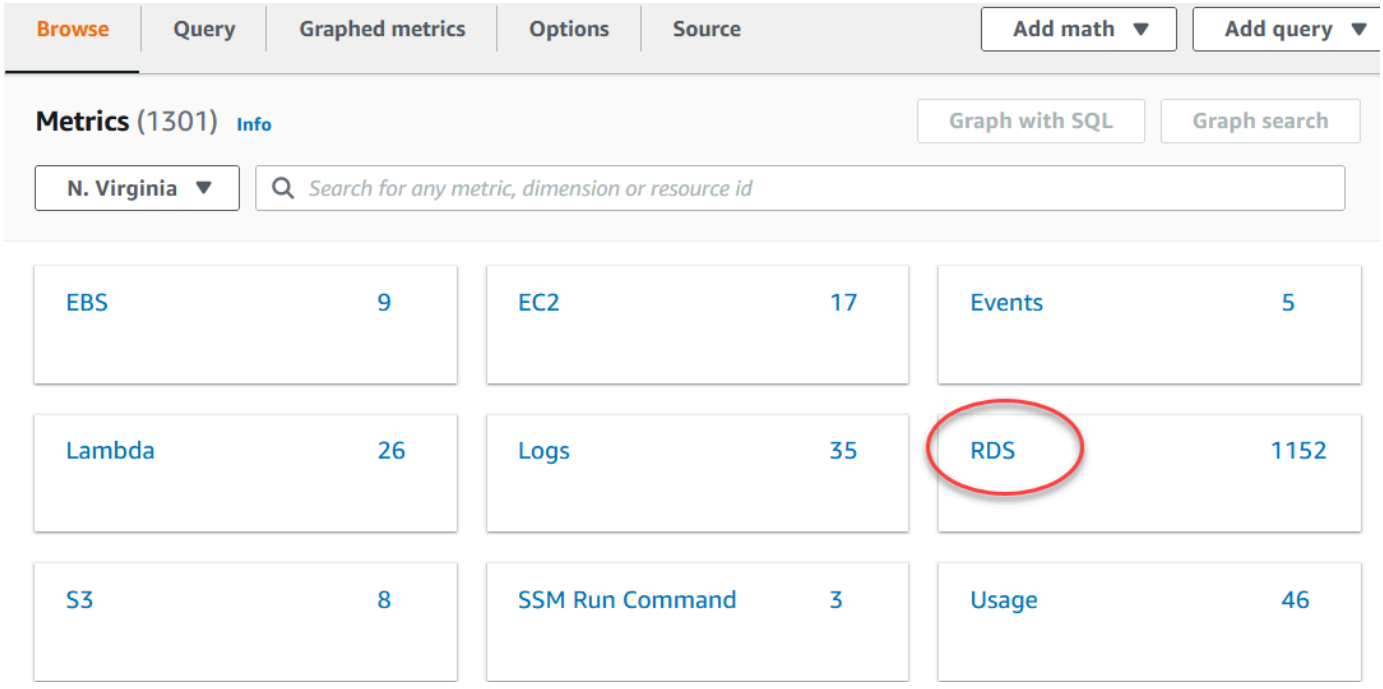
1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.

   Die CloudWatch Übersichtsstartseite wird angezeigt.



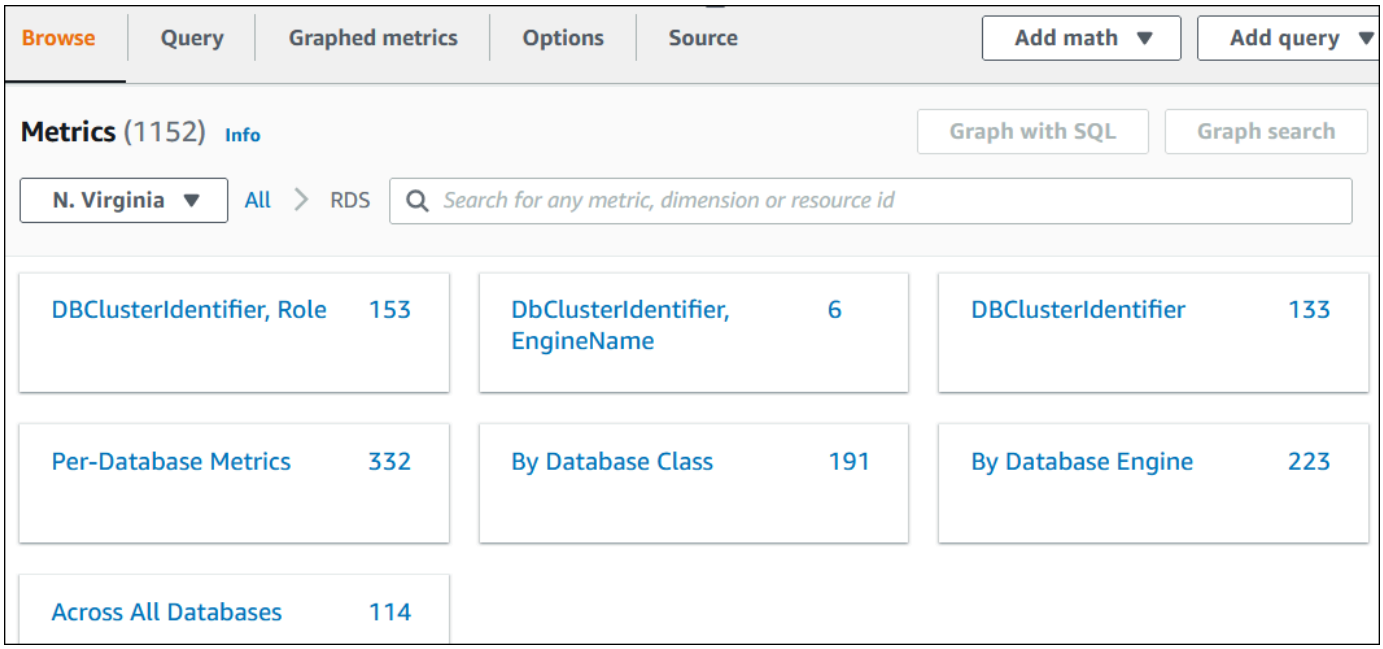
2. Ändern Sie, falls erforderlich, die AWS-Region. Wählen Sie in der Navigationsleiste die AWS-Region aus, in der sich Ihre AWS-Ressourcen befinden. Weitere Informationen finden Sie unter Regionen und Endpunkte.

3. Wählen Sie im Navigationsbereich Metrics (Metriken) und dann All metrics (Alle Metriken) aus.

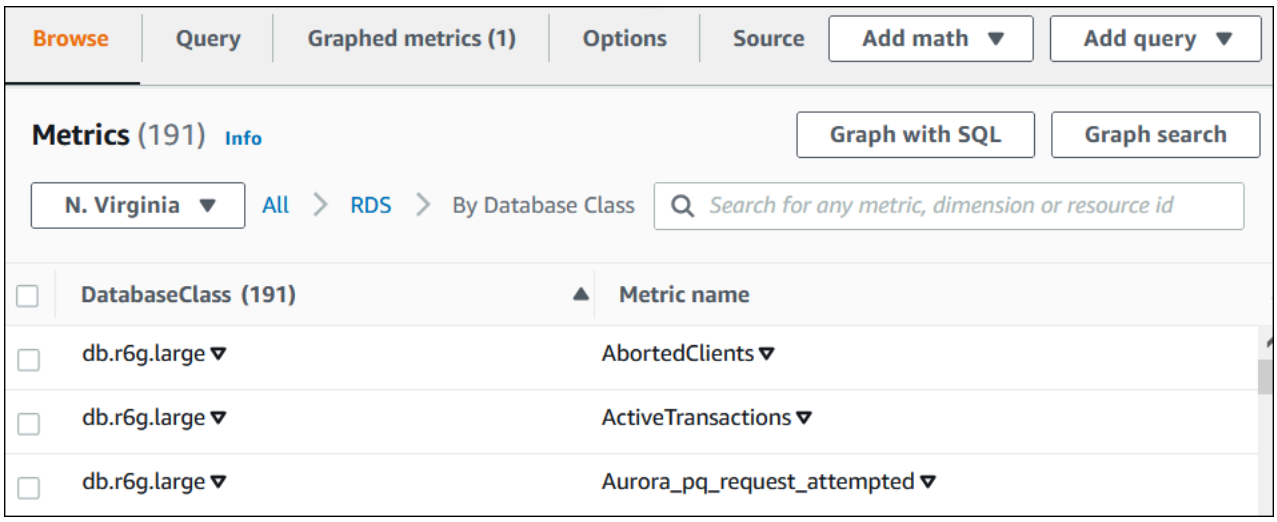


4. Scrollen Sie nach unten und wählen Sie den RDS-Namespace der Metrik aus.

   Auf der Seite werden die Amazon Aurora-Dimensionen angezeigt. Beschreibungen dieser Dimensionen finden Sie unter Amazon-CloudWatch-Dimensionen für Aurora.



5. Wählen Sie eine Metrikdimension, z. B. By Database Class (Nach Datenbanken-Klasse).

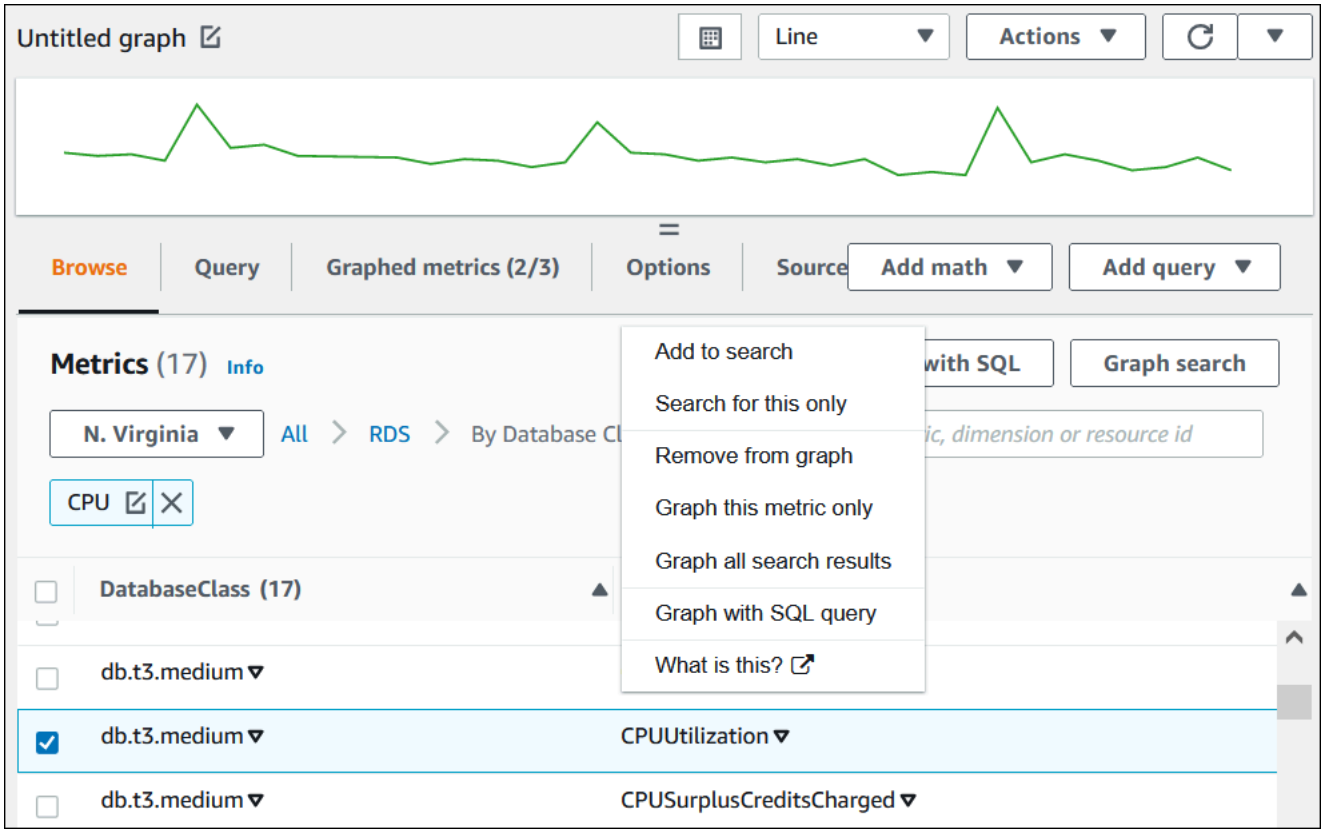


6. Führen Sie eine der folgenden Aktionen aus:

   - Verwenden Sie die Spaltenüberschrift, um die Metriken zu sortieren.
   - Um eine Metrik grafisch darzustellen, müssen Sie das Kontrollkästchen neben der Metrik aktivieren.

- Um nach Ressource zu filtern, müssen Sie zunächst die Ressourcen-ID und dann die Option Add to search (Zu Suche hinzufügen) wählen.
- Um nach Metrik zu filtern, müssen Sie den Metriknamen und anschließend Add to search (Zu Suche hinzufügen) wählen.

Das folgende Beispiel filtert die db.t3.medium-Klasse und stellt die CPUUtilization-Metrik grafisch dar.



Einzelheiten zur Analyse der Ressourcennutzung für Aurora PostgreSQL mithilfe von CloudWatch Metriken finden Sie. Weitere Informationen finden Sie unter Verwendung von CloudWatch Amazon-Metriken zur Analyse der Ressourcennutzung für Aurora PostgreSQL.

AWS CLI

Um Metrikinformationen mithilfe der abzurufenAWS CLI, verwenden Sie den CloudWatch Befehl `list-metrics`. Im folgenden Beispiel listen Sie alle Metriken im AWS/RDS-Namespace auf.

```
aws cloudwatch list-metrics --namespace AWS/RDS
```

Verwenden Sie den Befehl , um Metrikdaten abzurufen`get-metric-data`.

Im folgenden Beispiel werden `CPUUtilization` Statistiken für die Instance `my-instance` über den spezifischen Zeitraum von 24 Stunden mit einer 5-minütigen Granularität abgerufen.

Erstellen Sie eine JSON Datei mit dem Namen `CPU_metric.json` und dem folgenden Inhalt.

```
{
   "StartTime" : "2023-12-25T00:00:00Z",
   "EndTime" : "2023-12-26T00:00:00Z",
   "MetricDataQueries" : [{
     "Id" : "cpu",
     "MetricStat" : {
    "Metric" : {
        "Namespace" : "AWS/RDS",
        "MetricName" : "CPUUtilization",
        "Dimensions" : [{ "Name" : "DBInstanceIdentifier" , "Value" : my-instance}]
    },
       "Period" : 360,
       "Stat" : "Minimum"
     }
   }]
}
```

Example

Für Linux, macOSoder Unix:

```
aws cloudwatch get-metric-data \
    --cli-input-json file://CPU_metric.json
```

Windows:

```
aws cloudwatch get-metric-data ^
     --cli-input-json file://CPU_metric.json
```

Beispielausgabe:

```
{
    "MetricDataResults": [
        {
```

```
            "Id": "cpu",
            "Label": "CPUUtilization",
            "Timestamps": [
                "2023-12-15T23:48:00+00:00",
                "2023-12-15T23:42:00+00:00",
                "2023-12-15T23:30:00+00:00",
                "2023-12-15T23:24:00+00:00",
                ...
            ],
            "Values": [
                13.299778337027714,
                13.677507543049558,
                14.24976250395827,
                13.02521708695145,
                ...
            ],
            "StatusCode": "Complete"
        }
    ],
    "Messages": []
}
```


Weitere Informationen finden Sie unter Abrufen von Statistiken für eine Metrik im Amazon-CloudWatch Benutzerhandbuch.

Exportieren von Performance-Insights-Metriken nach CloudWatch

Mit Performance Insights können Sie das vorkonfigurierte oder benutzerdefinierte Metrik-Dashboard für Ihre DB-Instance nach Amazon exportieren CloudWatch. Sie können das Metrik-Dashboard als neues Dashboard exportieren oder es einem vorhandenen CloudWatch Dashboard hinzufügen. Wenn Sie das Dashboard zu einem vorhandenen CloudWatch Dashboard hinzufügen möchten, können Sie eine Kopfzeile erstellen, sodass die Metriken in einem separaten Abschnitt im CloudWatch Dashboard angezeigt werden.

Sie können das Dashboard für exportierte Metriken in der - CloudWatch Konsole anzeigen. Wenn Sie einem Performance-Insights-Metrik-Dashboard nach dem Export neue Metriken hinzufügen, müssen Sie dieses Dashboard erneut exportieren, um die neuen Metriken in der CloudWatch Konsole anzuzeigen.

Sie können auch ein Metrik-Widget im Performance-Insights-Dashboard auswählen und die Metrikdaten in der CloudWatch Konsole anzeigen.

Weitere Informationen zum Anzeigen der Metriken in der CloudWatch Konsole finden Sie unter Anzeigen von DB-Cluster-Metriken in der - CloudWatch Konsole und AWS CLI.

Exportieren von Performance-Insights-Metriken als neues Dashboard nach CloudWatch

Wählen Sie ein vorkonfiguriertes oder benutzerdefiniertes Metrik-Dashboard aus dem Performance-Insights-Dashboard aus und exportieren Sie es als neues Dashboard nach CloudWatch. Sie können das exportierte Dashboard in der CloudWatch -Konsole anzeigen.

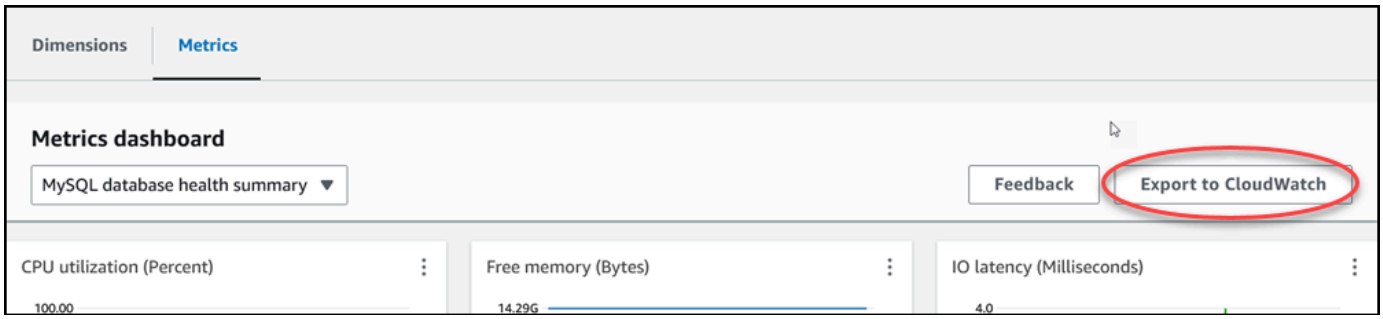
So exportieren Sie ein Performance-Insights-Metrik-Dashboard als neues Dashboard nach CloudWatch

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.

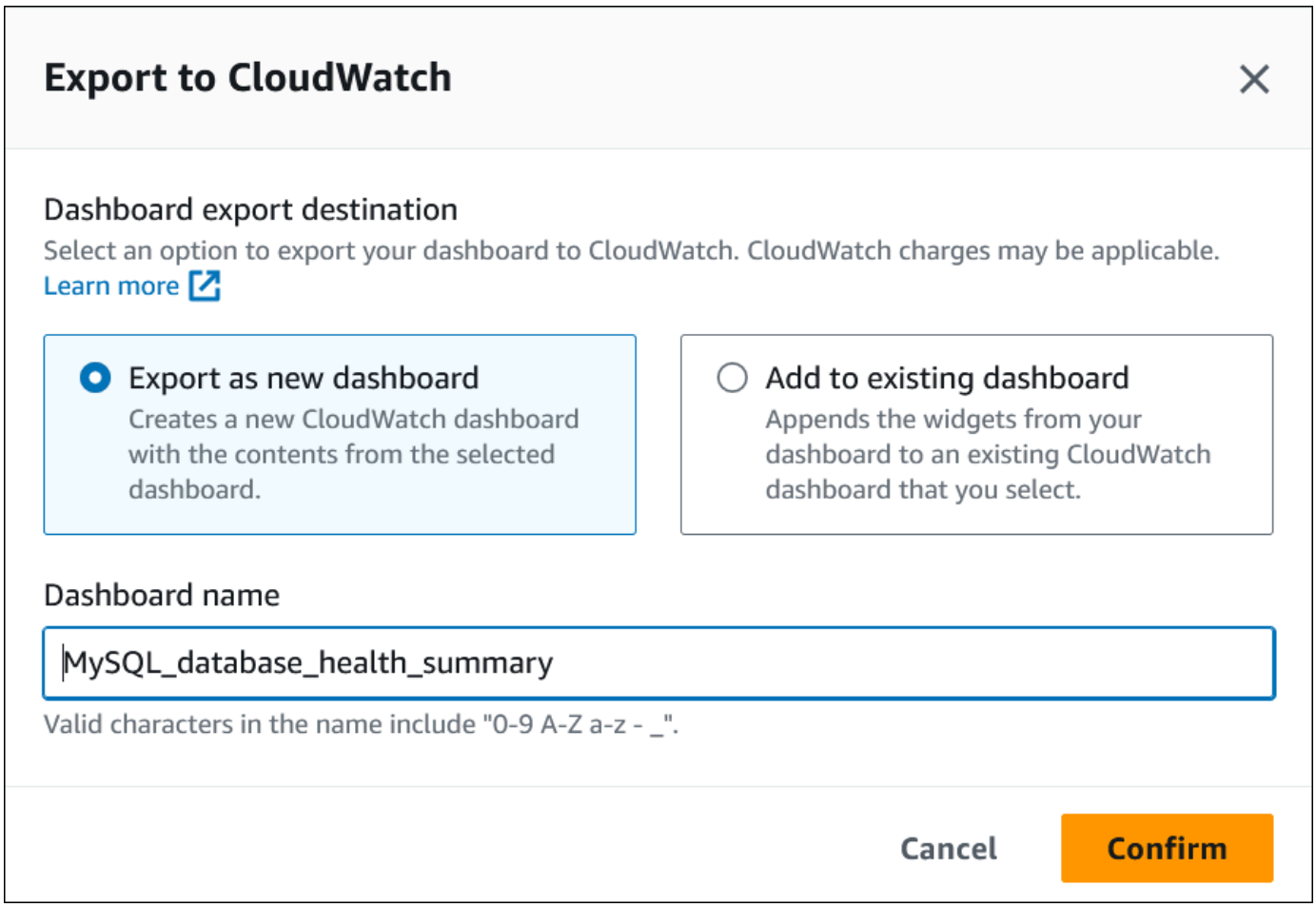
   Das Performance-Insights-Dashboard wird für die DB-Instance angezeigt.
4. Scrollen Sie nach unten und wählen Sie Metriken aus.

   Standardmäßig wird das vorkonfigurierte Dashboard mit Performance-Insights-Metriken angezeigt.
5. Wählen Sie ein vorkonfiguriertes oder benutzerdefiniertes Dashboard und dann Nach exportieren aus CloudWatch.

   Das Fenster Nach exportieren CloudWatch wird angezeigt.

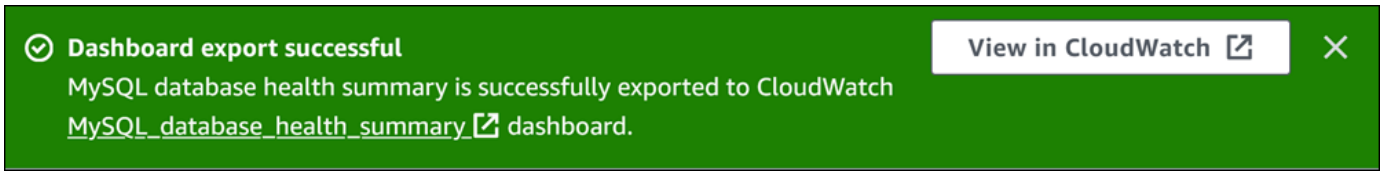


6. Wählen Sie Als neues Dashboard exportieren aus.



7. Geben Sie im Feld Dashboard-Name einen Namen für das neue Dashboard ein und wählen Sie Bestätigen aus.

   In einem Banner wird eine Meldung angezeigt, nachdem der Dashboard-Export erfolgreich war.



8. Wählen Sie im Banner den Link oder In anzeigen CloudWatch, um das Metrik-Dashboard in der CloudWatch Konsole anzuzeigen.

Hinzufügen von Performance-Insights-Metriken zu einem vorhandenen CloudWatch Dashboard

Fügen Sie einem vorhandenen CloudWatch Dashboard ein vorkonfiguriertes oder benutzerdefiniertes Metrik-Dashboard hinzu. Sie können dem Metrik-Dashboard eine Bezeichnung hinzufügen, die in einem separaten Abschnitt im CloudWatch Dashboard angezeigt wird.

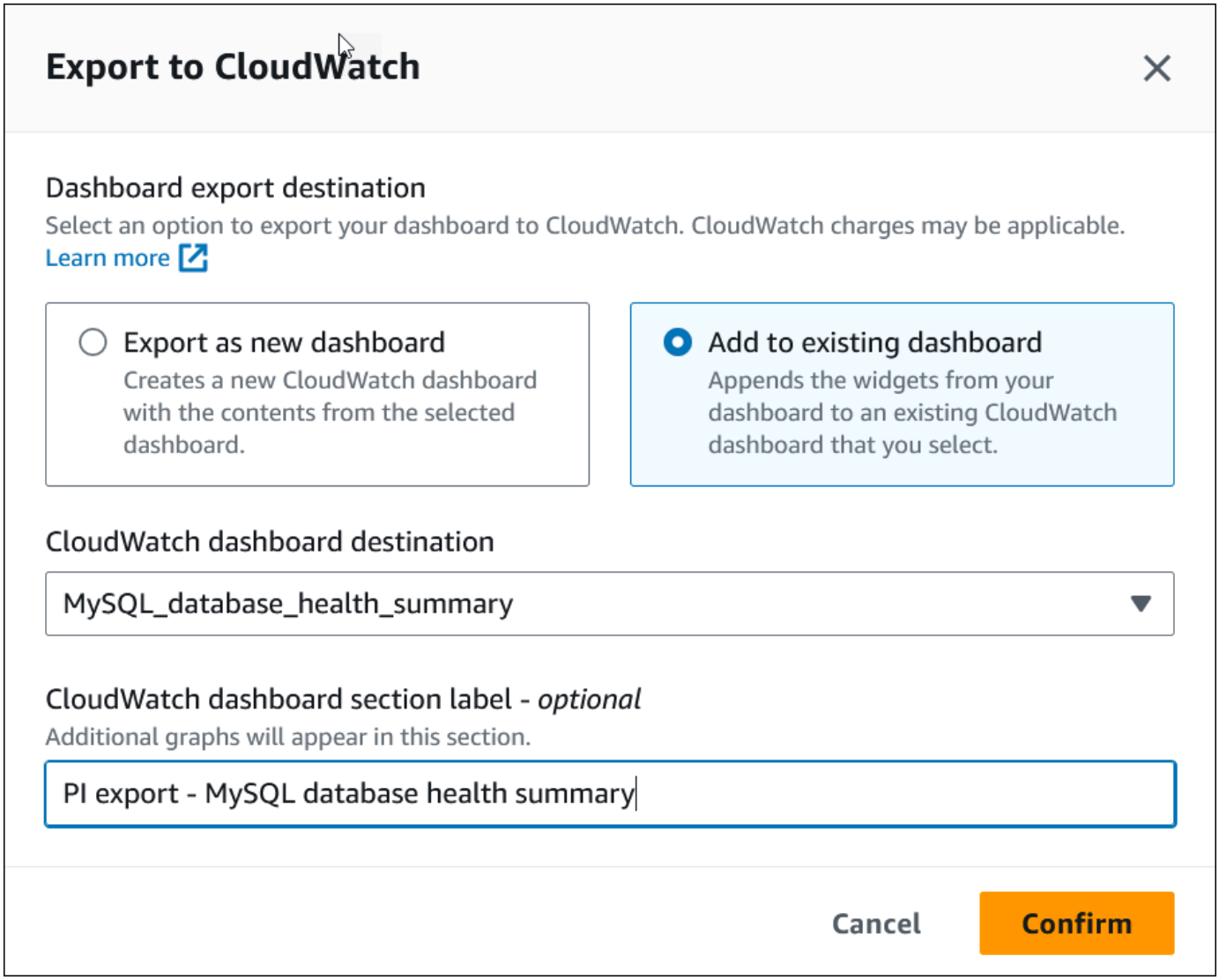
So exportieren Sie die Metriken in ein vorhandenes CloudWatch Dashboard

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.

   Das Performance-Insights-Dashboard wird für die DB-Instance angezeigt.
4. Scrollen Sie nach unten und wählen Sie Metriken aus.

   Standardmäßig wird das vorkonfigurierte Dashboard mit Performance-Insights-Metriken angezeigt.
5. Wählen Sie das vorkonfigurierte oder benutzerdefinierte Dashboard und dann Exportieren nach aus CloudWatch.

   Das Fenster Nach exportieren CloudWatch wird angezeigt.
6. Wählen Sie Zu vorhandenem Dashboard hinzufügen aus.



7. Geben Sie das Ziel und die Bezeichnung des Dashboards an und wählen Sie dann Bestätigen aus.

   - CloudWatch Dashboard-Ziel – Wählen Sie ein vorhandenes CloudWatch Dashboard aus.
   - DashboardCloudWatch -Abschnittsbezeichnung – optional – Geben Sie einen Namen für die Performance-Insights-Metriken ein, die in diesem Abschnitt im CloudWatch Dashboard angezeigt werden sollen.

   In einem Banner wird eine Meldung angezeigt, nachdem der Dashboard-Export erfolgreich war.

8. Wählen Sie im Banner den Link oder In anzeigen CloudWatch aus, um das Metrik-Dashboard in der CloudWatch Konsole anzuzeigen.

Anzeigen eines Performance-Insights-Metrik-Widgets in CloudWatch

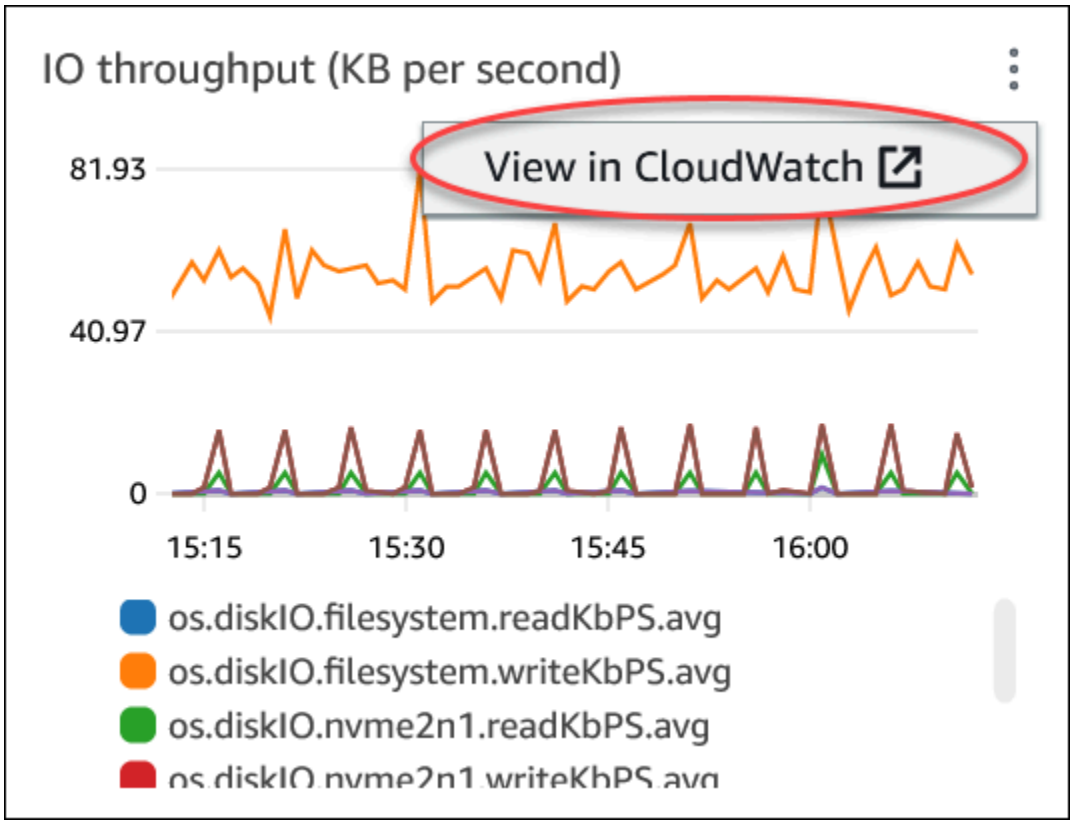
Wählen Sie im Dashboard von Amazon RDS Performance Insights ein Metrik-Widget aus und zeigen Sie die Metrikdaten in der CloudWatch Konsole an.

So exportieren Sie ein Metrik-Widget und zeigen die Metrikdaten in der CloudWatch Konsole an

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.

   Das Performance-Insights-Dashboard wird für die DB-Instance angezeigt.
4. Scrollen Sie nach unten zu Metriken.

   Standardmäßig wird das vorkonfigurierte Dashboard mit Performance-Insights-Metriken angezeigt.
5. Wählen Sie ein Metrik-Widget und dann im Menü Anzeigen in CloudWatch aus.



   Die Metrikdaten werden in der - CloudWatch Konsole angezeigt.

Erstellen von CloudWatch-Alarmen zur Überwachung von Amazon Aurora

Sie können einen CloudWatch-Alarm erstellen, der eine Amazon SNS-Nachricht sendet, sobald sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum. Der Alarm kann auch eine oder mehrere Aktionen durchführen, die vom Wert der Metrik im Vergleich zu einem gegebenen Schwellenwert in einer Reihe von Zeiträumen abhängt. Die Aktion ist eine Benachrichtigung, die an ein Amazon SNS-Thema oder eine Amazon EC2 Auto Scaling-Richtlinie gesendet wird.

Alarme rufen nur Aktionen für nachhaltige Statusänderungen auf. CloudWatch-Alarme rufen keine Aktionen auf, nur weil sie sich in einem bestimmten Status befinden. Der Status muss sich geändert haben und für eine festgelegte Anzahl an Zeiträumen aufrechterhalten worden sein.

> **Note**
>
> Sie sollten in Aurora `WRITER`- oder `READER`-Rollenmetriken zum Einrichten von Alarmen verwenden, statt sich auf Metriken für bestimmte DB-Instances zu verlassen. Aurora DB-Instance-Rollen können ihre Rolle mit der Zeit ändern. Sie finden diese rollenbasierten Metriken in der CloudWatch-Konsole.
> Aurora Auto Scaling legt Alarme automatisch auf der Basis von `READER`-Rollenmetriken fest. Weitere Informationen zu Aurora Auto Scaling finden Sie unter Verwenden von Amazon Aurora Auto Scaling mit Aurora Replicas.

Sie können die metrische mathematische Funktion DB_PERF_INSIGHTS in der CloudWatch-Konsole verwenden, um Amazon RDS nach Performance Insights-Zählermetriken abzufragen. Die Funktion DB_PERF_INSIGHTS umfasst auch die DBLoad-Metrik in Intervallen unter einer Minute. Sie können für diese Metriken CloudWatch-Alarme einstellen.

Weitere Informationen zum Erstellen eines Alarms finden Sie unter Erstellen eines Alarms zu Performance Insights-Zählermetriken aus einer AWS-Datenbank.

So richten Sie mit der einen Alarm ei AWS CLI

- Rufen Sie die folgende Seite auf `put-metric-alarm`. Weitere Informationen finden Sie in der AWS CLI-Befehlsreferenz.

So richten Sie mit der CloudWatch-API einen Alarm ein:

- Rufen Sie die folgende Seite auf `PutMetricAlarm`. Weitere Informationen finden Sie in der Amazon CloudWatch API-Referenz.

Weitere Informationen zum Festlegen von Amazon-SNS-Themen sowie zur Erstellung von Alarmen finden Sie unter Using Amazon CloudWatch alarms (Verwendung von Amazon-CloudWatch-Alarmen).

Überwachung mit Performance Insights auf

Performance Insights erweitert vorhandene Amazon-Aurora-Überwachungsfunktionen, um die Leistung Ihres Clusters zu veranschaulichen und ihre Analyse zu unterstützen. Mit dem Performance Insights-Dashboard können Sie die Datenbanklast Ihres Amazon-Aurora-Clusters visualisieren und die Last nach Wartezeiten, SQL-Anweisungen, Hosts oder Benutzern filtern. Weitere Informationen zur Verwendung von Performance Insights mit Amazon DocumentDB finden Sie im Amazon-DocumentDB-Entwicklerhandbuch.

Themen

Übersicht über Performance-Insights für Amazon Aurora

Standardmäßig aktiviert RDS Performance Insights im Assistenten zum Erstellen der Konsole für alle Amazon RDS-Engines. Wenn Sie Performance Insights auf DB-Cluster-Ebene aktivieren, aktiviert RDS Performance Insights für jede DB-Instance im Cluster.Wenn mehr als eine Datenbank auf einer DB-Instance vorhanden ist, aggregiert Performance Insights Leistungsdaten.

Das folgende Video gibt eine Übersicht über Performance Insights für Amazon Aurora.

Verwenden von Performance Insights, um die Leistung von Amazon Aurora-PostgreSQL zu analysieren

Themen

- DB-Engine-, Regions- und Instance-Klassenunterstützung von Amazon Aurora für Performance Insights
- Preisgestaltung und Datenaufbewahrung für Performance-Insights

Datenbanklast

Die Datenbanklast (DB Load) misst den Grad der Sitzungsaktivität in Ihrer Datenbank. `DBLoad`ist die wichtigste Metrik in Performance Insights, und Performance Insights erfasst jede Sekunde die Datenbanklast.

Themen

- Aktive Sitzungen
- Durchschnittliche aktive Sitzungen
- Durchschnittliche aktive Ausführungen
- Dimensionen

Aktive Sitzungen

Eine Datenbank-Sitzung repräsentiert den Dialog einer Anwendung mit einer relationalen Datenbank. Eine aktive Sitzung ist eine Verbindung, die Arbeit an die DB-Engine gesendet hat und auf eine Antwort wartet.

Eine Sitzung ist aktiv, wenn sie entweder auf der CPU läuft oder darauf wartet, dass eine Ressource verfügbar wird, damit sie fortfahren kann. Beispielsweise kann eine aktive Sitzung warten, bis eine Seite (oder ein Block) in den Speicher eingelesen wird, und verbraucht dann CPU, während sie Daten von der Seite liest.

Durchschnittliche aktive Sitzungen

Die durchschnittlich aktive Sitzungen (AAS) ist die Einheit für die `DBLoad`-Metrik in Performance Insights. Es wird gemessen, wie viele Sitzungen gleichzeitig in der Datenbank aktiv sind.

Jede Sekunde ruft Performance-Insights eine Stichprobe der Anzahl der Sitzungen ab, die gleichzeitig eine Abfrage ausführen. Für jede aktive Sitzung sammelt Performance Insights die folgenden Daten:

- SQL-Anweisung

- Sitzungsstatus (läuft auf der CPU oder wartet)
- Host
- Benutzer, der SQL ausführt

Performance Insights berechnet die AAS durch Dividieren der Gesamtzahl der Sitzungen durch die Gesamtzahl der Stichproben für einen bestimmten Zeitraum. Die folgende Tabelle zeigt beispielsweise 5 aufeinander folgende Stichproben einer laufenden Abfrage, die in Intervallen von 1 Sekunde abgefragt wurden.

Beispiel	Anzahl der Sitzungen, die eine Abfrage ausführen	AAS	Berechnung
1	2	2	2 Sitzungen insgesamt / 1 Stichprobe
2	0	1	2 Sitzungen insgesamt / 2 Stichproben
3	4	2	6 Sitzungen insgesamt / 3 Stichproben
4	0	1.5	6 Sitzungen insgesamt / 4 Stichproben
5	4	2	10 Sitzungen insgesamt / 5 Stichproben

Im vorherigen Beispiel beträgt die DB-Last für das Zeitintervall 2 AAS. Diese Messung bedeutet, dass im Durchschnitt 2 Sitzungen gleichzeitig während des Zeitraums aktiv waren, in dem die 5 Stichproben erfasst wurden.

Durchschnittliche aktive Ausführungen

Die durchschnittlichen aktiven Ausführungen (AAE) pro Sekunde stehen im Zusammenhang mit AAS. Um die AAE zu berechnen, teilt Performance Insights die Gesamtausführungszeit einer Abfrage durch das Zeitintervall. Die folgende Tabelle zeigt die AAE-Berechnung für dieselbe Abfrage in der vorherigen Tabelle.

Verstrichene Zeit	Gesamtausführungszeit	AAE	Berechnung
60	120	2	120 Durchführungssekunden/60 verstrichene Sekunden
120	120	1	120 Durchführungssekunden/120 verstrichene Sekunden
180	380	2.11	380 Ausführungssekunden/180 verstrichene Sekunden
240	380	1.58	380 Ausführungssekunden/240 verstrichene Sekunden
300	600	2	600 Durchführungssekunden/300 verstrichene Sekunden

In den meisten Fällen sind die AAS und die AAE für eine Abfrage ungefähr gleich. Da es sich bei den Eingaben zu den Berechnungen jedoch um unterschiedliche Datenquellen handelt, variieren die Berechnungen häufig geringfügig.

Dimensionen

Die`db.load` Metrik unterscheidet sich von den anderen Zeitreihenmetriken, da Sie sie in Unterkomponenten aufteilen können, die als Dimensionen bezeichnet werden. Sie können sich Dimensionen als „Aufteilungs“-Kategorien für die verschiedenen Merkmale der `DBLoad`-Metrik vorstellen.

Wenn Sie Leistungsprobleme diagnostizieren, sind die folgenden Dimensionen oft am nützlichsten:

Themen

- Warteereignisse

- Haupt-SQL

Eine vollständige Liste der Dimensionen für die Aurora-Engines finden Sie unter DB-Last aufgeteilt nach Dimensionen.

Warteereignisse

Ein Warteereignis bewirkt, dass eine SQL-Anweisung wartet, bis ein bestimmtes Ereignis eintritt, bevor sie mit der Ausführung fortfahren kann. Warteereignisse sind eine wichtige Dimension oder Kategorie für die DB-Last, da sie angeben, wo die Arbeit behindert wird.

Jede aktive Sitzung läuft entweder auf der CPU oder wartet. Sitzungen verbrauchen beispielsweise CPU, wenn sie Speicher nach einem Puffer suchen, eine Berechnung durchführen oder Prozeduralcode ausführen. Wenn Sitzungen keine CPU verbrauchen, warten sie möglicherweise darauf, dass ein Speicherpuffer frei wird, eine Datendatei gelesen oder ein Protokoll geschrieben wird. Je mehr Zeit eine Sitzung auf Ressourcen wartet, desto weniger Zeit läuft sie auf der CPU.

Wenn Sie eine Datenbank tunen, versuchen Sie oft, die Ressourcen herauszufinden, auf die Sitzungen warten. Beispielsweise könnten zwei oder drei Warteereignisse 90 Prozent der DB-Last ausmachen. Diese Maßnahme bedeutet, dass aktive Sitzungen im Durchschnitt die meiste Zeit damit verbringen, auf eine kleine Anzahl von Ressourcen zu warten. Wenn Sie die Ursache dieser Wartezeiten herausfinden können, können Sie eine Lösung versuchen.

Die Warteereignisse variieren je nach DB-Engine:

- Eine Liste der am häufigsten verwendeten Warteereignisse für Aurora MySQL finden Sie unter Aurora-MySQL-Warteereignisse. Um zu erfahren, wie man mit diesen Warteereignissen tunen kann, finden Sie unter Optimieren von Aurora MySQL.
- Informationen zu allen MySQL-Warteereignissen finden Sie unter Wait Event Summary Tables in der MySQL-Dokumentation.
- Eine Liste der am häufigsten verwendeten Warteereignisse für Aurora PostgreSQL finden Sie unter Amazon-Aurora-PostgreSQL-Warteereignisse. Um zu erfahren, wie man mit diesen Warteereignissen tunen kann, finden Sie unter Optimierung mit Warteereignissen für Aurora PostgreSQL.
- Informationen zu allen PostgreSQL-Warteereignissen finden Sie unter Der Statistikkollektor > Warteereignistabellen in der PostgreSQL-Dokumentation.

Haupt-SQL

Während Warteereignisse Engpässe zeigen, zeigt Top-SQL an, welche Abfragen am meisten zur DB-Last beitragen. Beispielsweise könnten derzeit viele Abfragen gleichzeitig in der Datenbank ausgeführt werden, aber eine einzelne Abfrage könnte 99 % der DB-Last verbrauchen. In diesem Fall könnte die hohe Belastung auf ein Problem mit der Abfrage hinweisen.

Standardmäßig zeigt die Performance Insights-Konsole die wichtigsten SQL-Abfragen an, die zur Datenbanklast beitragen. Die Konsole zeigt auch relevante Statistiken für jede Anweisung an. Um Leistungsprobleme für eine bestimmte Anweisung zu diagnostizieren, können Sie deren Ausführungsplan untersuchen.

Maximale CPU

Das Diagramm Datenbanklast im Dashboard dient zum Erfassen, Aggregieren und Anzeigen von Sitzungsinformationen. Um zu sehen, ob aktive Sitzungen die maximale CPU überschreiten, sehen Sie sich ihre Beziehung zur Max vCPU-Linie an. Performance Insights bestimmt den Max vCPU-Wert anhand der Anzahl der vCPU-Kerne (virtuelle CPU) für Ihre DB-Instance. Bei Aurora Serverless v2 stellt Max vCPU (vCPU-Max.) die geschätzte Anzahl von vCPUs dar.

Es kann jeweils ein Prozess auf einer vCPU ausgeführt werden. Wenn die Anzahl der Prozesse die Anzahl der vCPUs übersteigt, werden die Prozesse in die Warteschlange gestellt. Wenn die Warteschlangen länger werden, wird die Leistung beeinträchtigt. Wenn die DB-Last häufig über der Max vCPU-Linie liegt und der primäre Wartezustand „CPU“ lautet, ist die CPU überlastet. In diesem Fall sollten Sie Verbindungen zur Instance drosseln, SQL-Abfragen mit hoher CPU-Last anpassen oder eine größere Instance-Klasse in Betracht ziehen. Hohe und konsistente Instances von Wartezuständen deuten darauf hin, dass es möglicherweise Engpässe oder Probleme mit Ressourcenkonflikten gibt, die behoben werden müssen. Dies kann auch dann zutreffen, wenn die DB-Last die mit Max vCPU definierte Linie nicht überschreitet.

DB-Engine-, Regions- und Instance-Klassenunterstützung von Amazon Aurora für Performance Insights

Die folgende Tabelle enthält DB-Engines von Amazon Aurora, die Performance Insights unterstützen.

Amazon-Aurora-DB-Engine	Unterstützte Engine-Versionen und Regionen	Beschränkungen für Instance-Klasse
Amazon Aurora MySQL-Compatible Edition	Weitere Informationen über die Verfügbarkeit von Versionen und Regionen von Performance-Insights mit Aurora MySQL finden Sie unter Performance-Insights mit Aurora MySQL.	Bei Performance Insights gelten die folgenden Beschränkungen für die Engine-Klasse: • db.t2 – nicht unterstützt • db.t3 – nicht unterstützt • „db.t4g.micro“ und „db.t4g.small“ – nicht unterstützt
Amazon Aurora PostgreSQL-Compatible Edition	Weitere Informationen über die Verfügbarkeit von Versionen und Regionen von Performance-Insights mit Aurora PostgreSQL finden Sie unter Performance-Insights mit Aurora PostgreSQL.	N/A

DB-Engine-, Regions- und Instance-Klassenunterstützung von Amazon Aurora für Performance-Insights-Funktionen

Die folgende Tabelle enthält DB-Engines von Amazon Aurora, die Performance-Insights-Funktionen unterstützen.

Funktion	Preisstufe	Unterstützte Regionen	Unterstützte DB-Engines	Unterstützte Instance-Klassen
SQL-Statistiken für Performance Insights	Alle	Alle	Alle	Alle
Analysieren der Datenbank	Nur kostenpflichtige Stufe	• US East (Ohio)	Alle	

Funktion	Preisstufe	Unterstützte Regionen	Unterstützte DB-Engines	Unterstützte Instance-Klassen
leistung für einen bestimmten Zeitraum		• USA Ost (Nord-Virginia) • USA West (Nordkali fornien) • USA West (Oregon) • Asia Pacific (Mumbai) • Asia Pacific (Seoul) • Asien-Pazifik (Singapur) • Asien-Pazifik (Sydney) • Asien-Pazifik (Tokio) • Canada (Central) • Europe (Frankfurt) • Europa (Irland) • Europe (London) • Europe (Paris) • Europa (Stockholm)		Alle außer db.server less (Aurora Serverless v2)

Funktion	Preisstufe	Unterstützte Regionen	Unterstützte DB-Engines	Unterstützte Instance-Klassen
Anzeigen proaktiver Empfehlungen für Performance Insights	Nur kostenpflichtige Stufe	• US East (Ohio) • USA Ost (Nord-Virginia) • USA West (Nordkalifornien) • USA West (Oregon) • Asia Pacific (Mumbai) • Asia Pacific (Seoul) • Asien-Pazifik (Singapur) • Asien-Pazifik (Sydney) • Asien-Pazifik (Tokio) • Canada (Central) • Europe (Frankfurt) • Europa (Irland) • Europe (London) • Europe (Paris) • Europa (Stockholm)	Alle	Alle außer db.serverless (Aurora Serverless v2)

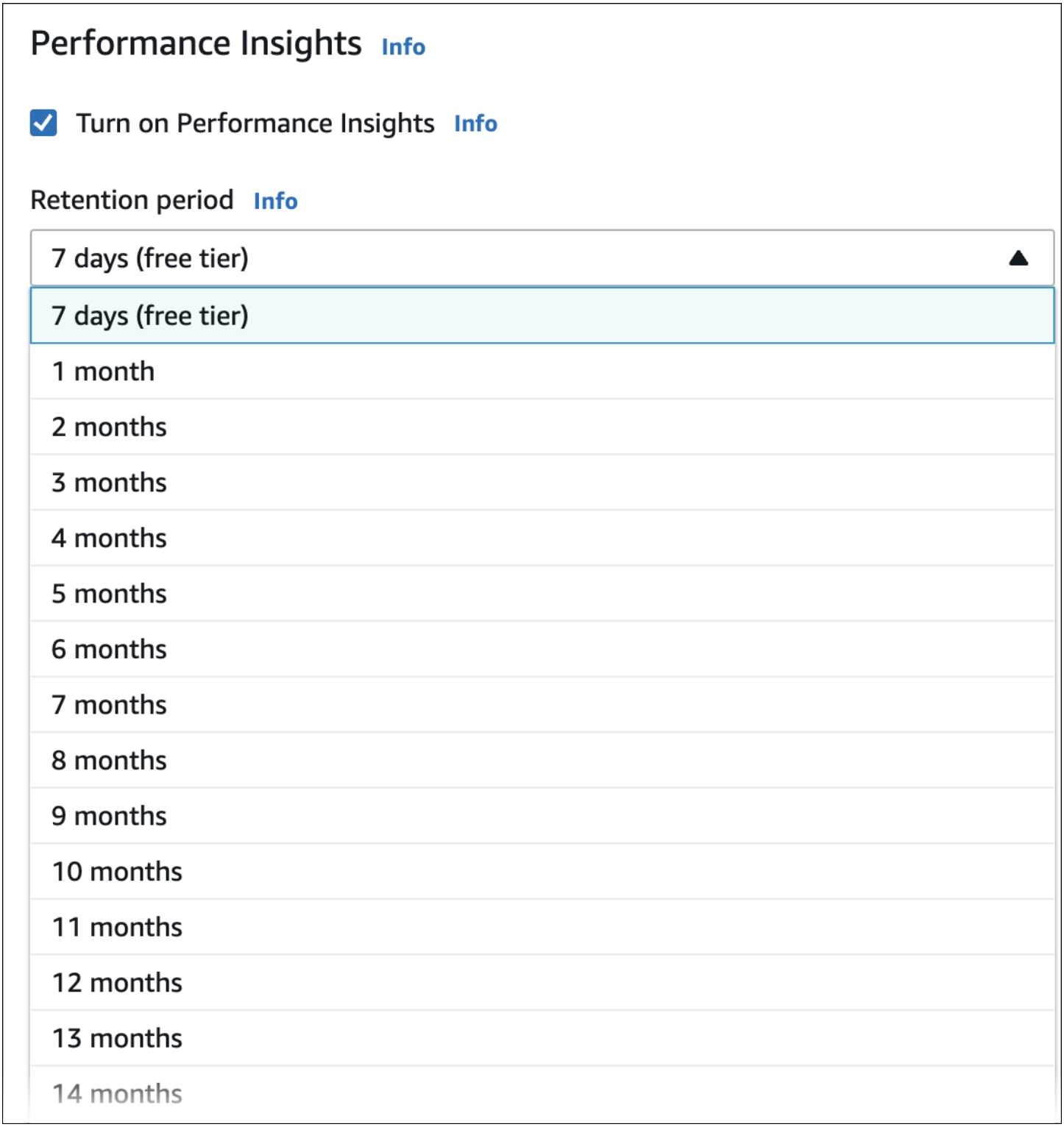
Funktion	Preisstufe	Unterstützte Regionen	Unterstützte DB-Engines	Unterstützte Instance-Klassen
		• Südamerika (São Paulo)		

Preisgestaltung und Datenaufbewahrung für Performance-Insights

Performance-Insights bietet standardmäßig ein kostenloses Kontingent, das 7 Tage Performance-Datenverlauf und 1 Million API-Anfragen pro Monat umfasst. Sie können auch längere Aufbewahrungsfristen erwerben. Weitere Informationen finden Sie unter Performance-Insights – Preise.

In der RDS-Konsole können Sie einen der folgenden Aufbewahrungszeiträume für Ihre Performance-Insights-Daten auswählen:

- Standard (7 Tage)
- ***n*** Monate, wobei ***n*** eine Zahl zwischen 1 und 24 ist



Informationen zum Festlegen einer Aufbewahrungsfrist mithilfe der AWS CLI finden Sie unter AWS CLI.

Performance Insights für Aurora ein- und ausschalten

Sie können Performance Insights für Ihren DB-Cluster beim Erstellen aktivieren. Bei Bedarf können Sie es später auf Instance-Ebene für jede Instance in Ihrem DB-Cluster deaktivieren. Das Aktivieren und Deaktivieren von Performance Insights führt nicht zu Ausfallzeiten, einem Neustart oder einem Failover.

> **Note**
>
> Das Leistungsschema ist ein optionales Leistungstool, das von Aurora MySQL verwendet wird. Nach dem Aktivieren oder Deaktivieren des Leistungsschemas müssen Sie neu starten. Wenn Sie jedoch Performance Insights aktivieren oder deaktivieren, müssen Sie keinen Neustart durchführen. Weitere Informationen finden Sie unter Aktivieren des Leistungsschemas für Performance Insights in Aurora MySQL.

Wenn Sie Performance Insights in Verbindung mit globalen Aurora-Datenbanken nutzen, aktivieren Sie Performance Insights individuell für die DB-Instances in jeder AWS-Region. Details hierzu finden Sie unter Überwachung einer Amazon Aurora globalen Datenbank mit Amazon RDS Performance Insights.

Der Performance Insights-Agent verbraucht eine begrenzte Menge an CPU und Arbeitsspeicher auf dem DB-Host. Wenn die DB-Last hoch ist, begrenzt der Agent die Auswirkungen auf die Leistung, indem Daten seltener erfasst werden.

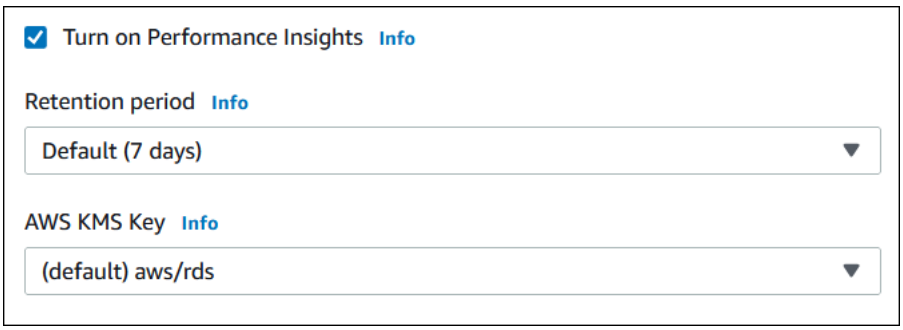
Konsole

In der Konsole können Sie Performance Insights aktivieren oder deaktivieren, wenn Sie einen DB-Cluster erstellen. Sie können eine DB-Instance im Cluster ändern, um Performance Insights für die Instance zu aktivieren oder zu deaktivieren.

Ein- oder Ausschalten von Performance Insights beim Erstellen eines DB-Clusters

Wenn Sie einen DB-Cluster erstellen, aktivieren Sie Performance Insights, indem Sie Enable Performance Insights (Performance Insights aktivieren) im Abschnitt Performance Insights auswählen. Oder wählen Sie Performance-Insights deaktivieren. Wenn Sie einen DB-Cluster erstellen möchten, befolgen Sie die Anweisungen für Ihre DB-Engine inErstellen eines Amazon Aurora-DB Clusters.

Der folgende Screenshot zeigt den Abschnitt Performance-Insights.



Wenn Sie Performance-Insights aktivieren wählen, haben Sie die folgenden Optionen:

- Retention (Aufbewahrung): die Zeit, wie lange Performance Insight-Daten aufbewahrt werden Die Aufbewahrungseinstellung im kostenlosen Kontingent ist Standard (7 Tage). Um Ihre Leistungsdaten länger aufzubewahren, geben Sie 1–24 Monate an. Weitere Informationen zum Aufbewahrungszeitraum finden Sie unter Preisgestaltung und Datenaufbewahrung für Performance-Insights.
- AWS KMS key— Spezifizieren Sie Ihre AWS KMS key. Performance Insights verschlüsselt alle potenziell sensiblen Daten mit Ihrem KMS-Schlüssel. Die Daten werden während der Übertragung und im Ruhezustand verschlüsselt. Weitere Informationen finden Sie unter Konfigurieren einer AWS KMS -Richtlinie für Performance Insights.

Ein- oder Ausschalten von Performance Insights beim Ändern einer DB-Instance in Ihrem DB-Cluster

In der Konsole können Sie eine DB-Instance in Ihrem DB-Cluster ändern, um Performance Insights zu aktivieren oder zu deaktivieren. Sie können Performance Insights auf Clusterebene nicht ein- oder ausschalten: Sie müssen diesen Vorgang für jede Instance im Cluster ausführen.

Ein- oder Ausschalten von Performance Insights für eine DB-Instance in Ihrem DB-Cluster über die Konsole

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Datenbanken aus.
3. Wählen Sie eine DB-Instance, und wählen Sie Modify (Ändern) aus.
4. Wählen Sie im Bereich Performance-Insights entweder Performance-Insights aktivieren oder Performance-Insights deaktivieren aus.

   Wenn Sie Performance-Insights aktivieren wählen, haben Sie die folgenden Optionen:

- Retention (Aufbewahrung): die Zeit, wie lange Performance Insight-Daten aufbewahrt werden Die Aufbewahrungseinstellung im kostenlosen Kontingent ist Standard (7 Tage). Um Ihre Leistungsdaten länger aufzubewahren, geben Sie 1–24 Monate an. Weitere Informationen zum Aufbewahrungszeitraum finden Sie unter Preisgestaltung und Datenaufbewahrung für Performance-Insights.
- AWS KMS key – Geben Sie Ihren KMS-Schlüssel an. Performance Insights verschlüsselt alle potenziell sensiblen Daten mit Ihrem KMS-Schlüssel. Die Daten werden während der Übertragung und im Ruhezustand verschlüsselt. Weitere Informationen finden Sie unter Verschlüsseln von Amazon Aurora-Ressourcen.

5. Klicken Sie auf Continue (Fortfahren).
6. Wählen Sie für Einplanung von Änderungen die Option Sofort anwenden aus. Wenn Sie im nächsten geplanten Wartungsfenster die Option Anwenden wählen, ignoriert Ihre Instance diese Einstellung und aktiviert Performance Insights sofort.
7. Wählen Sie Modify instance (Instance ändern).

AWS CLI

Wenn Sie den AWS CLI Befehl create-db-instance verwenden, aktivieren Sie Performance Insights, indem Sie Folgendes angeben. `--enable-performance-insights` Oder deaktivieren Sie Performance-Insights, indem Sie `--no-enable-performance-insights` angeben.

Sie können diese Werte auch mit den folgenden Befehlen angeben: AWS CLI

- create-db-instance-read-replica
- modify-db-instance
- restore-db-instance-from-s3

Im folgenden Verfahren wird beschrieben, wie Performance Insights für eine vorhandene DB-Instance in Ihrem DB-Cluster mit der AWS CLI aktiviert oder deaktiviert wird.

Um Performance Insights für eine DB-Instance in Ihrem DB-Cluster ein- oder auszuschalten, verwenden Sie AWS CLI

- Rufen Sie den AWS CLI Befehl modify-db-instance auf und geben Sie die folgenden Werte ein:
  - `--db-instance-identifier` – Der Name der DB-Instancein Ihrem DB-Cluster.

- `--enable-performance-insights` zum Aktivieren oder `--no-enable-performance-insights` zum Deaktivieren

Das folgende Beispiel aktiviert Performance Insights für `sample-db-instance`.

Für, oder: Linux macOS Unix

```
aws rds modify-db-instance \
    --db-instance-identifier sample-db-instance \
    --enable-performance-insights
```

Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier sample-db-instance ^
    --enable-performance-insights
```

Wenn Sie Performance Insights in der CLI aktivieren, können Sie mit der `--performance-insights-retention-period`-Option optional die Anzahl der Tage angeben, die Performance Insights-Daten aufbewahrt werden sollen. Sie können 7, *`Monat`** 31 (wo *`Monat`* eine Zahl zwischen 1 und 23 ist) oder `731` angeben. Wenn Sie beispielsweise Ihre Leistungsdaten 3 Monate lang aufbewahren möchten, geben Sie `93` an, was 3 * 31 ist. Der Standardwert ist 7 Tage. Weitere Informationen zum Aufbewahrungszeitraum finden Sie unter Preisgestaltung und Datenaufbewahrung für Performance-Insights.

Das folgende Beispiel aktiviert Performance Insights für `sample-db-instance` und legt fest, dass Performance-Insights-Daten für 93 Tage (3 Monate) aufbewahrt werden.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-instance \
    --db-instance-identifier sample-db-instance \
    --enable-performance-insights \
    --performance-insights-retention-period 93
```

Windows:

```
aws rds modify-db-instance ^
```

```
    --db-instance-identifier sample-db-instance ^
    --enable-performance-insights ^
    --performance-insights-retention-period 93
```

Wenn Sie eine Aufbewahrungsfrist wie 94 Tage angeben, was kein gültiger Wert ist, gibt RDS einen Fehler aus.

```
An error occurred (InvalidParameterValue) when calling the CreateDBInstance operation:
Invalid Performance Insights retention period. Valid values are: [7, 31, 62, 93, 124,
 155, 186, 217,
248, 279, 310, 341, 372, 403, 434, 465, 496, 527, 558, 589, 620, 651, 682, 713, 731]
```

RDS-API

Wenn Sie mittels der Amazon-RDS-API-Operation CreateDBInstance eine neue DB-Instance in Ihrem DB-Cluster erstellen, aktivieren Sie Performance Insights, indem Sie `EnablePerformanceInsights` auf `True` einstellen. Um Performance-Insights zu deaktivieren, setzen Sie `EnablePerformanceInsights` auf `False`.

Sie können den Wert für `EnablePerformanceInsights` auch mittels der folgenden API-Operationen angeben:

- ModifyDBInstance
- DB-Replikat erstellt InstanceRead
- DB S3 InstanceFrom wurde wiederhergestellt

Wenn Sie Performance Insights aktivieren, können Sie optional mit dem Parameter `PerformanceInsightsRetentionPeriod` den Zeitraum in Tagen angeben, wie lange Performance-Insights-Daten gespeichert werden sollen. Sie können 7, *`Monat`** 31 (wo *`Monat`* eine Zahl zwischen 1 und 23 ist) oder 731 angeben. Wenn Sie beispielsweise Ihre Leistungsdaten 3 Monate lang aufbewahren möchten, geben Sie 93 an, was 3 * 31 ist. Der Standardwert ist 7 Tage. Weitere Informationen zum Aufbewahrungszeitraum finden Sie unter Preisgestaltung und Datenaufbewahrung für Performance-Insights.

Aktivieren des Leistungsschemas für Performance Insights in Aurora MySQL

Das Leistungsschema ist eine optionale Funktion zur Überwachung der Laufzeitleistung von Aurora MySQL auf niedriger Detailebene. Das Leistungsschema ist so konzipiert, dass es minimale Auswirkungen auf die Datenbankleistung hat. Performance Insights ist eine separate Funktion, die Sie mit oder ohne Leistungsschema verwenden können.

Themen

Überblick über das Leistungsschema-Objekt

Das Leistungsschema überwacht Ereignisse in Aurora MySQL-Datenbanken. Ein Ereignis ist eine Datenbankserver-Aktion, die Zeit in Anspruch nimmt und instrumentiert wurde, damit Timing-Informationen erfasst werden können. Nachfolgend finden Sie Beispiele für Ereignisse:

- Funktionsaufrufe
- Wartet auf das Betriebssystem
- Phasen der SQL-Ausführung
- Gruppen von SQL-Anweisungen

Die `PERFORMANCE_SCHEMA`-Speicher-Engine ist ein Mechanismus zur Implementierung der Leistungsschema-Funktion. Diese Engine sammelt Ereignisdaten mithilfe der Instrumentierung im Quellcode der Datenbank. Die Engine speichert Ereignisse in Arbeitsspeichertabellen in der `performance_schema`-Datenbank. Sie können `performance_schema` genauso abfragen, wie Sie andere Tabellen abfragen können. Weitere Informationen finden Sie unter MySQL-Leistungsschema im MySQL-Referenzhandbuch.

Performance Insights und das Performance-Schema

Performance Insights und das Leistungsschema sind separate Funktionen, die jedoch verbunden sind. Das Verhalten von Performance Insights für Aurora MySQL hängt davon ab, ob das Performance-Schema aktiviert ist und wenn ja, ob Performance Insights das Performance-Schema automatisch verwaltet. Die folgende Tabelle beschreibt das Verhalten.

Performance-Schema ist aktiviert	Performance Insights-Verwaltungsmodus	Performance Insights-Verhalten
Ja	Automatisch	• Sammelt detaillierte Überwachungsinformationen auf niedriger Ebene • Sammelt jede Sekunde aktive Sitzungsmetriken • Zeigt die DB-Last kategorisiert nach detaillierten Warteereignissen an, mit denen Sie Engpässe identifizieren können
Ja	Manuell	• Erfasst Warteereignisse und Metriken pro SQL • Sammelt aktive Sitzungsmetriken alle fünf Sekunden statt jede Sekunde • Meldet Benutzerzustände wie Einfügen und Senden, mit denen Sie Engpässe nicht identifizieren können
Nein	N/A	• Erfasst keine Warteereignisse, Metriken pro SQL oder andere detaillierte Überwachungsinformationen auf niedriger Ebene • Sammelt aktive Sitzungsmetriken alle fünf Sekunden statt jede Sekunde •

Performance-Schema ist aktiviert	Performance Insights-Verwaltungsmodus	Performance Insights-Verhalten
		Meldet Benutzerzustände wie Einfügen und Senden, mit denen Sie Engpässe nicht identifizieren können

Automatische Verwaltung des Leistungsschemas durch Performance Insights

Wenn Sie eine Aurora-MySQL-DB-Instance erstellen und Performance Insights aktiviert ist, wird das Leistungsschema ebenfalls aktiviert. In diesem Fall verwaltet Performance Insights Ihre Parameter des Leistungsschemas automatisch. Dies ist die empfohlene Konfiguration.

Wenn Performance Insights das Leistungsschema automatisch verwaltet, `performance_schema` ist die Quelle von`system`.

> **Note**
>
> Die automatische Verwaltung des Leistungsschemas wird für die Instance-Klasse t4g.medium nicht unterstützt.

Sie können das Leistungsschema auch manuell verwalten. Wenn Sie diese Option auswählen, stellen Sie die Parameter entsprechend den Werten in der folgenden Tabelle ein.

Parametername	Parameterwert
`performance_schema`	1 (Die Spalte Source (Quelle) hat den Wert `system`)
`performance-schema-consumer-events-waits-current`	`ON`
`performance-schema-instrument`	`wait/%=ON`

Parametername	Parameterwert
`performance_schema_consumer_global_instrumentation`	1
`performance_schema_consumer_thread_instrumentation`	1

Wenn Sie den Parameterwert `performance_schema` manuell ändern und später zur automatischen Verwaltung zurückkehren möchten, finden Sie weitere Informationen unter Konfigurieren der Leistungsschema-Funktion für die automatische Verwaltung.

> **Important**
>
> Beim Aktivieren des Leistungsschemas durch Performance Insights werden die Parametergruppenwerte nicht geändert. Die Werte werden jedoch für die DB-Instances geändert, die ausgeführt werden. Die geänderten Werte können als einzige Möglichkeit über den Befehl `SHOW GLOBAL VARIABLES` eingesehen werden.

Auswirkung eines Neustarts auf das Leistungsschema

Performance Insights und das Leistungsschema unterscheiden sich in ihren Anforderungen für Neustarts der DB-Instance:

Leistungsschema

Sie müssen die DB-Instance neu starten, um diese Funktion ein- oder auszuschalten.

Performance Insights

Sie müssen die DB-Instance nicht neu starten, um diese Funktion ein- oder auszuschalten.

Wenn das Leistungsschema derzeit nicht aktiviert ist und Sie Performance Insights aktivieren, ohne die DB-Instance neu zu starten, wird das Leistungsschema nicht aktiviert.

Feststellen, ob Performance Insights das Leistungsschema verwaltet

Sehen Sie sich die folgende Tabelle an, um herauszufinden, ob Performance Insights derzeit das Leistungsschema für die Engine-Hauptversionen 5.6, 5.7 und 8.0 verwaltet.

Einstellung des performance_schema-Parameters	Einstellung der Spalte „Source“ (Quelle)	Performance Insights verwaltet das Leistungsschema?
`0`	`system`	Ja
`0` oder `1`	`user`	Nein

So stellen Sie fest, ob Performance Insights das Leistungsschema automatisch verwaltet

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Parameter groups (Parametergruppen).
3. Wählen Sie den Namen der Parametergruppe für Ihre DB-Instance.
4. Geben Sie im Suchfeld **`performance_schema`** ein.
5. Überprüfen Sie, ob für Source (Quelle) dem Systemstandardwert entspricht und für Values (Werte) 0 festgelegt ist. Ist das der Fall, verwaltet Performance Insights das Leistungsschema automatisch. Andernfalls verwaltet Performance Insights die Leistung nicht automatisch.

Konfigurieren der Leistungsschema-Funktion für die automatische Verwaltung

Angenommen, Performance Insights ist für Ihre DB-Instance aktiviert, verwaltet aber derzeit nicht das Leistungsschema. Wenn Sie zulassen möchten, dass Performance Insights das Leistungsschema automatisch verwaltet, führen Sie die folgenden Schritte aus.

So konfigurieren Sie das Leistungsschema für die automatische Verwaltung

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Parameter groups (Parametergruppen).
3. Wählen Sie den Namen der Parametergruppe für Ihre DB-Instance.
4. Geben Sie im Suchfeld **`performance_schema`** ein.
5. Wählen Sie den `performance_schema`-Parameter aus.
6. Wählen Sie Parameter bearbeiten aus.
7. Wählen Sie den `performance_schema`-Parameter aus.
8. Wählen Sie für Values (Werte) den Wert 0 aus.
9. Wählen Sie Änderungen speichern aus.
10. Starten Sie die DB-Instance neu.

> **Important**
>
> Wenn Sie das Leistungsschema aktivieren oder deaktivieren, müssen Sie die DB-Instance unbedingt neu starten.

Weitere Informationen zum Ändern von Instance-Parametern finden Sie unter Ändern von Parametern in einer DB-Parametergruppe. Weitere Informationen zu den Seiten im Dashboard finden Sie unter Analyse der Metriken mit dem Performance Insights-Dashboard. Weitere Informationen zum MySQL-Leistungsschema finden Sie im MySQL 8.0 Referenzhandbuch.

Konfigurieren von Zugriffsrichtlinien für Performance Insights

Um auf Performance Insights zugreifen zu können, muss ein Principal über die entsprechenden Berechtigungen von AWS Identity and Access Management (IAM) verfügen. Sie können den Zugriff wie folgt erteilen:

- Fügen Sie die `AmazonRDSPerformanceInsightsReadOnly`-verwaltete Richtlinie an einen Berechtigungssatz oder eine Rolle an, um auf alle schreibgeschützten Operationen der Performance-Insights-API zuzugreifen.

- Fügen Sie die `AmazonRDSPerformanceInsightsFullAccess`-verwaltete Richtlinie an einen Berechtigungssatz oder eine Rolle an, um auf alle Operationen der Performance-Insights-API zuzugreifen.
- Erstellen Sie eine benutzerdefinierte IAM-Richtlinie und fügen Sie diese an einen Berechtigungssatz oder eine Rolle an.

Wenn Sie bei der Aktivierung von Performance Insights einen vom Kunden verwalteten Schlüssel angegeben haben, stellen Sie sicher, dass die Benutzer in Ihrem Konto die `kms:GenerateDataKey` Berechtigungen `kms:Decrypt` und für AWS KMS key

Anhängen der AmazonRDSPerformanceInsightsReadOnly Richtlinie an einen IAM-Prinzipal

`AmazonRDSPerformanceInsightsReadOnly`ist eine AWS verwaltete Richtlinie, die Zugriff auf alle schreibgeschützten Operationen der Amazon RDS Performance Insights-API gewährt.

Wenn Sie `AmazonRDSPerformanceInsightsReadOnly` an einen Berechtigungssatz oder eine Rolle anfügen, kann der Empfänger Performance Insights mit anderen Konsolenfunktionen verwenden.

Weitere Informationen finden Sie unter AWS Von verwaltete Richtlinie: AmazonRDSPerformanceInsightsReadOnly.

Anhängen der AmazonRDSPerformanceInsightsFullAccess Richtlinie an einen IAM-Prinzipal

`AmazonRDSPerformanceInsightsFullAccess`ist eine AWS verwaltete Richtlinie, die Zugriff auf alle Operationen der Amazon RDS Performance Insights API gewährt.

Wenn Sie `AmazonRDSPerformanceInsightsFullAccess` an einen Berechtigungssatz oder eine Rolle anfügen, kann der Empfänger Performance Insights mit anderen Konsolenfunktionen verwenden.

Weitere Informationen finden Sie unter AWS Von verwaltete Richtlinie: AmazonRDSPerformanceInsightsFullAccess.

Erstellen einer benutzerdefinierten IAM-Richtlinie für Performance Insights

Benutzern, die nicht über die `AmazonRDSPerformanceInsightsFullAccess` Richtlinie `AmazonRDSPerformanceInsightsReadOnly` oder verfügen, können Sie Zugriff auf Performance Insights gewähren, indem Sie eine benutzerverwaltete IAM-Richtlinie erstellen oder ändern. Wenn Sie diese Richtlinie an einen IAM-Berechtigungssatz oder eine Rolle anfügen, kann der Empfänger Performance Insights verwenden.

Erstellen eine benutzerdefinierten Richtlinie

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Policies aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie auf der Seite „Richtlinie erstellen“ die Option JSON aus.
5. Kopieren Sie den Text, der im Abschnitt JSON-Richtliniendokument im Referenzhandbuch für AWS verwaltete Richtlinien für AmazonRDSPerformanceInsightsReadOnlyunsere Richtlinie bereitgestellt wird, und fügen Sie ihn ein. AmazonRDSPerformanceInsightsFullAccess
6. Wählen Sie Richtlinie prüfen.
7. Geben Sie einen Namen und optional eine Beschreibung für die Richtlinie an und wählen Sie dann Create policy (Richtlinie erstellen) aus.

Sie können die Richtlinie nun an einen Berechtigungssatz oder eine Rolle anfügen. Das folgende Verfahren setzt voraus, dass Sie für diesen Zweck bereits einen Benutzer zur Verfügung haben.

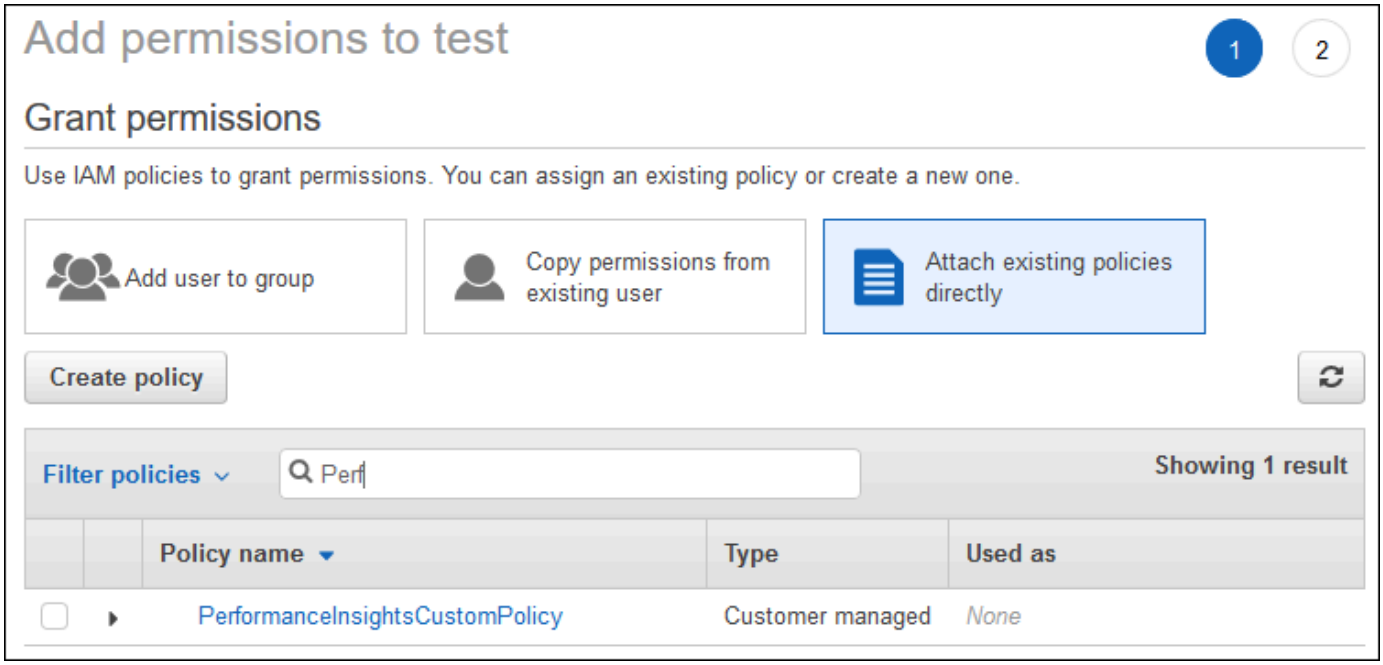
So fügen Sie die Richtlinie an einen Benutzer an

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich auf Users (Benutzer).
3. Wählen Sie einen vorhandenen Benutzer aus der Liste aus.

> **Important**
>
> Um Performance Insights verwenden zu können, benötigen Sie zusätzlich zur benutzerdefinierten Richtlinie Zugriff auf Amazon RDS. Beispielsweise bietet die vordefinierte Richtlinie `AmazonRDSPerformanceInsightsReadOnly`

schreibgeschützten Zugriff auf Amazon RDS. Weitere Informationen finden Sie unter Verwalten des Zugriffs mit Richtlinien.

4. Wählen Sie auf der Seite Übersicht die Option Add permissions (Berechtigungen hinzufügen) aus.
5. Wählen Sie Attach existing policies directly (Vorhandene Richtlinien direkt zuordnen). Geben Sie unter Suchen die ersten Zeichen Ihres Richtliniennamens ein, wie in der folgenden Abbildung gezeigt.



6. Wählen Sie Ihre Richtlinie und wählen Sie anschließend Nächster Schritt: Prüfen.
7. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.

Konfigurieren einer AWS KMS -Richtlinie für Performance Insights

Performance Insights verwendet an AWS KMS key , um sensible Daten zu verschlüsseln. Wenn Sie Performance Insights über die API oder die Konsole aktivieren, haben Sie folgende Möglichkeiten:

- Wählen Sie die Standardeinstellung Von AWS verwalteter Schlüssel.

  Amazon RDS verwendet die Von AWS verwalteter Schlüssel für Ihre neue DB-Instance. Amazon RDS erstellt einen Von AWS verwalteter Schlüssel für Ihr AWS-Konto. Ihr AWS-Konto hat für jeden ein anderes Von AWS verwalteter Schlüssel für Amazon RDS AWS-Region.
- Wählen Sie einen kundenverwalteten Schlüssel.

Wenn Sie einen vom Kunden verwalteten Schlüssel angeben, benötigen Benutzer in Ihrem Konto, die die Performance Insights API aufrufen, die Berechtigungen `kms:Decrypt` und `kms:GenerateDataKey` für den KMS-Schlüssel. Sie können diese Berechtigungen über IAM-Richtlinien konfigurieren. Wir empfehlen jedoch, dass Sie diese Berechtigungen über Ihre KMS-Schlüsselrichtlinie verwalten. Weitere Informationen finden Sie unter Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

Example

Das folgende Beispiel zeigt, wie Sie Ihrer KMS-Schlüsselrichtlinie Anweisungen hinzufügen können. Diese Anweisungen erlaubt den Zugriff auf Performance Insights. Je nachdem, wie Sie den KMS-Schlüssel verwenden, möchten Sie möglicherweise einige Einschränkungen ändern. Bevor Sie Ihrer Richtlinie Anweisungen hinzufügen, entfernen Sie alle Kommentare.

```
{
"Version" : "2012-10-17",
 "Id" : "your-policy",
 "Statement" : [ {
    //This represents a statement that currently exists in your policy.
 }
 ....,
 //Starting here, add new statement to your policy for Performance Insights.
 //We recommend that you add one new statement for every RDS instance
{
    "Sid" : "Allow viewing RDS Performance Insights",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            //One or more principals allowed to access Performance Insights
            "arn:aws:iam::444455556666:role/Role1"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition" : {
        "StringEquals" : {
            //Restrict access to only RDS APIs (including Performance Insights).
            //Replace region with your AWS Region.
```

```
            //For example, specify us-west-2.
            "kms:ViaService" : "rds.region.amazonaws.com"
        },
        "ForAnyValue:StringEquals": {
            //Restrict access to only data encrypted by Performance Insights.
            "kms:EncryptionContext:aws:pi:service": "rds",
            "kms:EncryptionContext:service": "pi",

            //Restrict access to a specific RDS instance.
            //The value is a DbiResourceId.
           "kms:EncryptionContext:aws:rds:db-id": "db-AAAAABBBBBCCCCDDDDDEEEEE"
        }
    }
}
```

So verwendet Performance Insights vom AWS KMS Kunden verwaltete Schlüssel

Performance Insights verwendet vom Kunden verwaltete Schlüssel, um vertrauliche Daten zu verschlüsseln. Wenn Sie Performance Insights aktivieren, können Sie einen AWS KMS -Schlüssel über die API bereitstellen. Performance Insights erstellt KMS-Berechtigungen für diesen Schlüssel. Das Feature verwendet den Schlüssel und führt die erforderlichen Operationen aus, um vertrauliche Daten zu verarbeiten. Zu den vertraulichen Daten gehören Felder wie Benutzer, Datenbank, Anwendung und SQL-Abfragetext. Performance Insights stellt sicher, dass die Daten sowohl im Ruhezustand als auch während der Übertragung verschlüsselt bleiben.

So arbeitet Performance Insights IAM mit AWS KMS

IAM erteilt Berechtigungen für spezifische APIs. Performance Insights verfügt über die folgenden öffentlichen APIs, die Sie mithilfe von IAM-Richtlinien einschränken können:

- `DescribeDimensionKeys`
- `GetDimensionKeyDetails`
- `GetResourceMetadata`
- `GetResourceMetrics`
- `ListAvailableResourceDimensions`
- `ListAvailableResourceMetrics`

Sie können die folgenden API-Abfragen verwenden, um vertrauliche Daten abzurufen.

- `DescribeDimensionKeys`
- `GetDimensionKeyDetails`
- `GetResourceMetrics`

Wenn Sie die API verwenden, um vertrauliche Daten abzurufen, nutzt Performance Insights die Anmeldeinformationen des Aufrufers. Diese Überprüfung stellt sicher, dass der Zugriff auf vertrauliche Daten auf Benutzer beschränkt ist, die Zugriff auf den KMS-Schlüssel haben.

Wenn Sie diese APIs aufrufen, benötigen Sie Berechtigungen zum Aufrufen der API über die IAM-Richtlinie und Berechtigungen zum Aufrufen der `kms:decrypt` Aktion über die AWS KMS Schlüsselrichtlinie.

Die API `GetResourceMetrics` kann sowohl vertrauliche als auch nicht vertrauliche Daten zurückgeben. Die Anforderungsparameter bestimmen, ob die Antwort vertrauliche Daten enthalten soll. Die API gibt vertrauliche Daten zurück, wenn die Anfrage eine vertrauliche Dimension im Filter- oder Group-by-Parameter enthält.

Weitere Informationen zu den Dimensionen, die Sie mit der `GetResourceMetrics` API verwenden können, finden Sie unter. DimensionGroup

Example Beispiele

Im folgenden Beispiel werden die vertraulichen Daten für die Gruppe `db.user` angefordert:

```
POST / HTTP/1.1
Host: <Hostname>
Accept-Encoding: identity
X-Amz-Target: PerformanceInsightsv20180227.GetResourceMetrics
Content-Type: application/x-amz-json-1.1
User-Agent: <UserAgentString>
X-Amz-Date: <Date>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
 Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ServiceType": "RDS",
  "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
  "MetricQueries": [
    {
```

```
      "Metric": "db.load.avg",
      "GroupBy": {
        "Group": "db.user",
        "Limit": 2
      }
    }
  ],
  "StartTime": 1693872000,
  "EndTime": 1694044800,
  "PeriodInSeconds": 86400
}
```

Example

Im folgenden Beispiel werden die nicht vertraulichen Daten für die Metrik `db.load.avg` angefordert:

```
POST / HTTP/1.1
Host: <Hostname>
Accept-Encoding: identity
X-Amz-Target: PerformanceInsightsv20180227.GetResourceMetrics
Content-Type: application/x-amz-json-1.1
User-Agent: <UserAgentString>
X-Amz-Date: <Date>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
 Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
    "ServiceType": "RDS",
    "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
    "MetricQueries": [
        {
            "Metric": "db.load.avg"
        }
    ],
    "StartTime": 1693872000,
    "EndTime": 1694044800,
    "PeriodInSeconds": 86400
}
```

Gewährung eines detaillierten Zugriffs für Performance Insights

Eine differenzierte Zugriffskontrolle bietet zusätzliche Möglichkeiten, den Zugriff auf Performance Insights zu kontrollieren. Diese Zugriffskontrolle kann den Zugriff auf einzelne Dimensionen für `GetResourceMetrics`, `DescribeDimensionKeys`, und `GetDimensionKeyDetails` Performance Insights Insights-Aktionen zulassen oder verweigern. Um einen differenzierten Zugriff zu verwenden, geben Sie Dimensionen in der IAM-Richtlinie mithilfe von Bedingungsschlüsseln an. Die Bewertung des Zugriffs folgt der Bewertungslogik der IAM-Richtlinie. Weitere Informationen finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch. Wenn in der IAM-Richtlinienanweisung keine Dimension angegeben ist, steuert die Anweisung den Zugriff auf alle Dimensionen für die angegebene Aktion. Eine Liste der verfügbaren Dimensionen finden Sie unter DimensionGroup.

Um herauszufinden, auf welche Dimensionen Ihre Anmeldeinformationen zugreifen dürfen, verwenden Sie den `AuthorizedActions` Parameter in `ListAvailableResourceDimensions` und geben Sie die Aktion an. Die zulässigen Werte für `AuthorizedActions` lauten wie folgt:

- `GetResourceMetrics`
- `DescribeDimensionKeys`
- `GetDimensionKeyDetails`

Wenn Sie den `AuthorizedActions` Parameter beispielsweise angeben`GetResourceMetrics`, wird die Liste der Dimensionen `ListAvailableResourceDimensions` zurückgegeben, auf die die `GetResourceMetrics` Aktion zugreifen darf. Wenn Sie im `AuthorizedActions` Parameter mehrere Aktionen angeben, wird ein Schnittpunkt von Dimensionen `ListAvailableResourceDimensions` zurückgegeben, auf die diese Aktionen zugreifen dürfen.

Example

Das folgende Beispiel bietet Zugriff auf die angegebenen Dimensionen `GetResourceMetrics` und `DescribeDimensionKeys` Aktionen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowToDiscoverDimensions",
            "Effect": "Allow",
            "Action": [
```

```
                "pi:ListAvailableResourceDimensions"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ]
        },
        {
            "Sid": "SingleAllow",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ],
            "Condition": {
                "ForAllValues:StringEquals": {
                    // only these dimensions are allowed. Dimensions not included in
                    // a policy with "Allow" effect will be denied
                    "pi:Dimensions": [
                        "db.sql_tokenized.id",
                        "db.sql_tokenized.statement"
                    ]
                }
            }
        }


    ]
}
```

Im Folgenden finden Sie die Antwort für die angeforderte Dimension:

```
 // ListAvailableResourceDimensions API
// Request
{
    "ServiceType": "RDS",
    "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
```

```
    "Metrics": [ "db.load" ],
    "AuthorizedActions": ["DescribeDimensionKeys"]
}

// Response
{
    "MetricDimensions": [ {
        "Metric": "db.load",
        "Groups": [
            {
                "Group": "db.sql_tokenized",
                "Dimensions": [
                    { "Identifier": "db.sql_tokenized.id" },
                  //  { "Identifier": "db.sql_tokenized.db_id" }, // not included
 because not allows in the IAM Policy
                    { "Identifier": "db.sql_tokenized.statement" }
                ]
            }

        ] }
    ]
}
```

Im folgenden Beispiel wird für die Dimensionen eine Option „Zulassen“ und zwei „Zugriff verweigern“ angegeben.

```
{
    "Version": "2012-10-17",
    "Statement": [
          {
            "Sid": "AllowToDiscoverDimensions",
            "Effect": "Allow",
            "Action": [
                "pi:ListAvailableResourceDimensions"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ]
          },

          {
            "Sid": "O01AllowAllWithoutSpecifyingDimensions",
```

```
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ]
        },

        {
            "Sid": "O01DenyAppDimensionForAll",
            "Effect": "Deny",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "pi:Dimensions": [
                        "db.application.name"
                    ]
                }
            }
        },

        {
            "Sid": "O01DenySQLForGetResourceMetrics",
            "Effect": "Deny",
            "Action": [
                "pi:GetResourceMetrics"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "pi:Dimensions": [
```

```
                        "db.sql_tokenized.statement"
                    ]
                }
            }
        }
    ]
}
```

Im Folgenden finden Sie die Antworten für die angeforderten Dimensionen:

```
   // ListAvailableResourceDimensions API
// Request
{
    "ServiceType": "RDS",
    "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
    "Metrics": [ "db.load" ],
    "AuthorizedActions": ["GetResourceMetrics"]
}

// Response
{
    "MetricDimensions": [ {
        "Metric": "db.load",
        "Groups": [
            {
                "Group": "db.application",
                "Dimensions": [

                  // removed from response because denied by the IAM Policy
                  //  { "Identifier": "db.application.name" }
                ]
            },
            {
                "Group": "db.sql_tokenized",
                "Dimensions": [
                    { "Identifier": "db.sql_tokenized.id" },
                    { "Identifier": "db.sql_tokenized.db_id" },

                  // removed from response because denied by the IAM Policy
                  //  { "Identifier": "db.sql_tokenized.statement" }
                ]
```

```
            },
            ...
        ] }
    ]
}
```

```
// ListAvailableResourceDimensions API
// Request
{
    "ServiceType": "RDS",
    "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
    "Metrics": [ "db.load" ],
    "AuthorizedActions": ["DescribeDimensionKeys"]
}

// Response
{
    "MetricDimensions": [ {
        "Metric": "db.load",
        "Groups": [
            {
                "Group": "db.application",
                "Dimensions": [
                  // removed from response because denied by the IAM Policy
                  //  { "Identifier": "db.application.name" }
                ]
            },
            {
                "Group": "db.sql_tokenized",
                "Dimensions": [
                    { "Identifier": "db.sql_tokenized.id" },
                    { "Identifier": "db.sql_tokenized.db_id" },

                  // allowed for DescribeDimensionKeys because our IAM Policy
                  // denies it only for GetResourceMetrics
                    { "Identifier": "db.sql_tokenized.statement" }
                ]
            },
            ...
        ] }
    ]
}
```

Analyse der Metriken mit dem Performance Insights-Dashboard

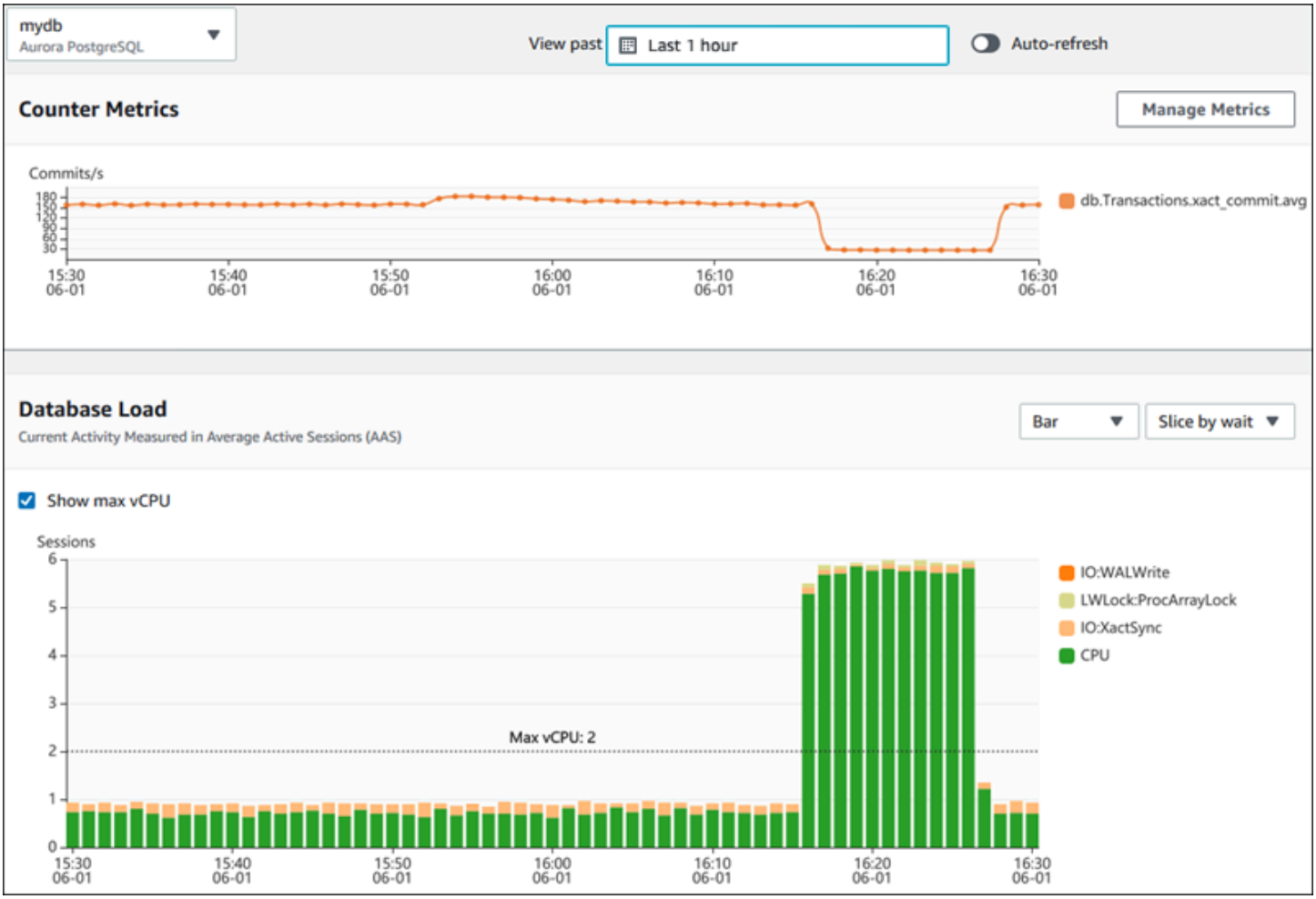
Das Dashboard von Performance Insights enthält Informationen zur Datenbank-Performance, die Sie bei der Analyse und Behebung von Performance-Problemen unterstützen. Auf der Dashboard-Hauptseite finden Sie Informationen zur Datenbanklast. Sie können DB-Lasten nach Dimensionen wie Warteereignissen oder SQL „aufteilen“.

Verwenden der Performance Insights-Dashboard-Komponenten

- Überblick über Performance Insights
- Zugriff auf das Performance-Insights-Dashboard
- Analysieren der DB-Last nach Warteereignissen
- Analysieren der Datenbankleistung für einen bestimmten Zeitraum
- Analyse von Abfragen mit dem Performance-Insights-Dashboard

Überblick über Performance Insights

Das Dashboard ist die einfachste Möglichkeit, mit Performance Insights zu interagieren. Das folgende Beispiel zeigt das Dashboard für eine MySQL-DB-Instance.



Themen

- Zeitraum-Filter
- Zählermetriken-Diagramm
- Datenbank-Ladediagramm
- Dimensionen pro Tabelle

Zeitraum-Filter

Standardmäßig zeigt das Dashboard von Performance Insights die DB-Last der letzten Stunde an. Sie können diesen Bereich so einstellen, dass er 5 Minuten oder bis zu 2 Jahre lang ist. Sie können auch einen benutzerdefinierten relativen Bereich auswählen.

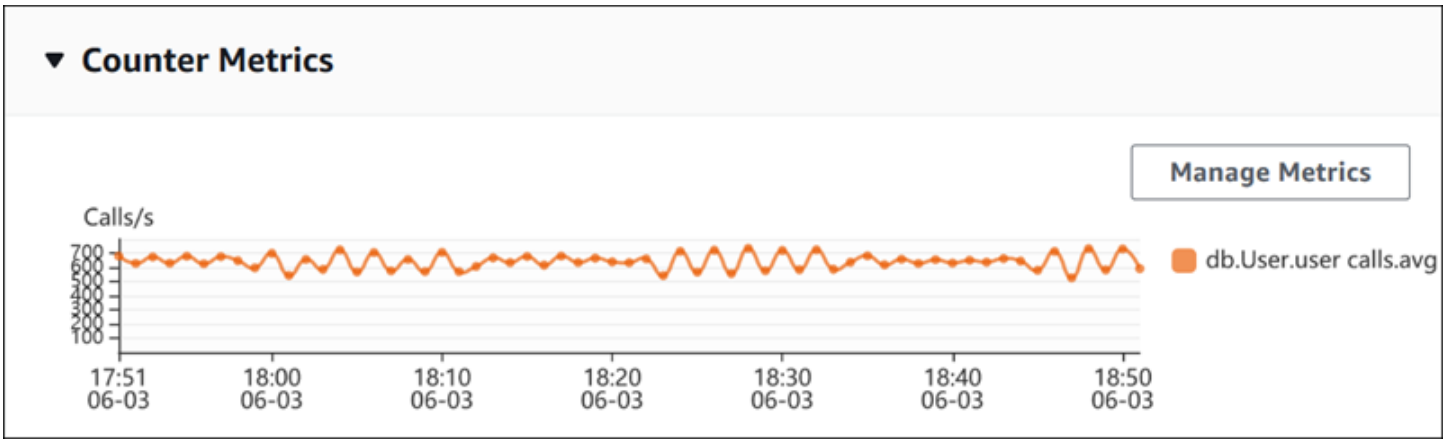
Sie können einen absoluten Bereich mit einem Anfangs- und Enddatum und einer Uhrzeit auswählen. Das folgende Beispiel zeigt den Zeitraum, der am 11.04.22 um Mitternacht beginnt und am 14.4.22 um 23:59 Uhr endet.

Zählermetriken-Diagramm

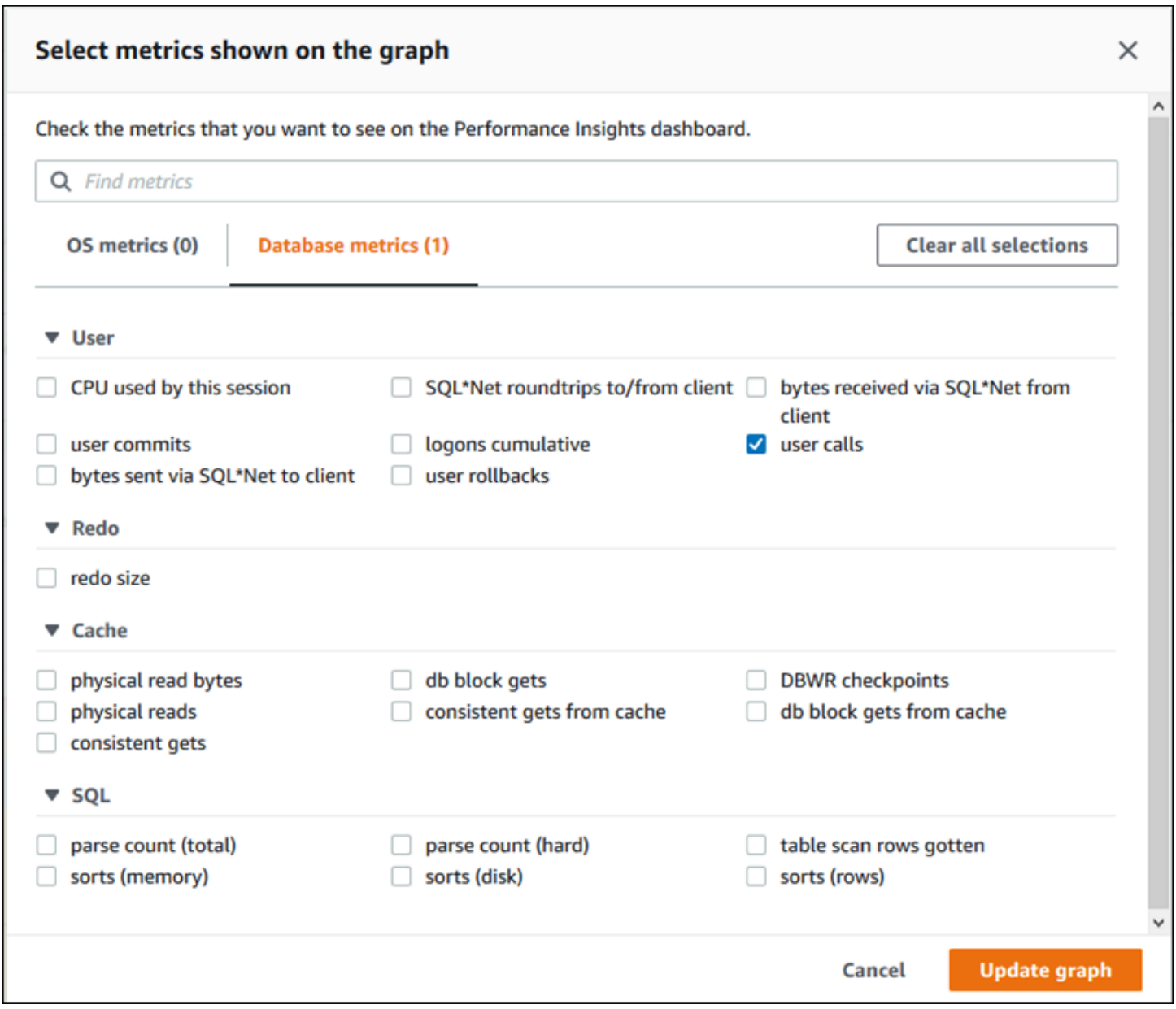
Mithilfe von Zählermetriken können Sie das Performance Insights-Dashboard anpassen und bis zu 10 weitere Diagramme aufnehmen. Diese Diagramme enthalten eine Auswahl von Dutzenden von Betriebssystem- und Datenbank-Performance-Metriken. Diese Informationen können mit der Datenbanklast korreliert werden, um Performance-Probleme zu identifizieren und zu analysieren.

Das Counter Metrics (Zählermetriken)-Diagramm enthält Daten zu Leistungsindikatoren. Die Standardmetriken hängen von der DB-Engine ab.

- Aurora MySQL– `db.SQL.Innodb_rows_read.avg`
- Aurora PostgreSQL – `db.Transactions.xact_commit.avg`



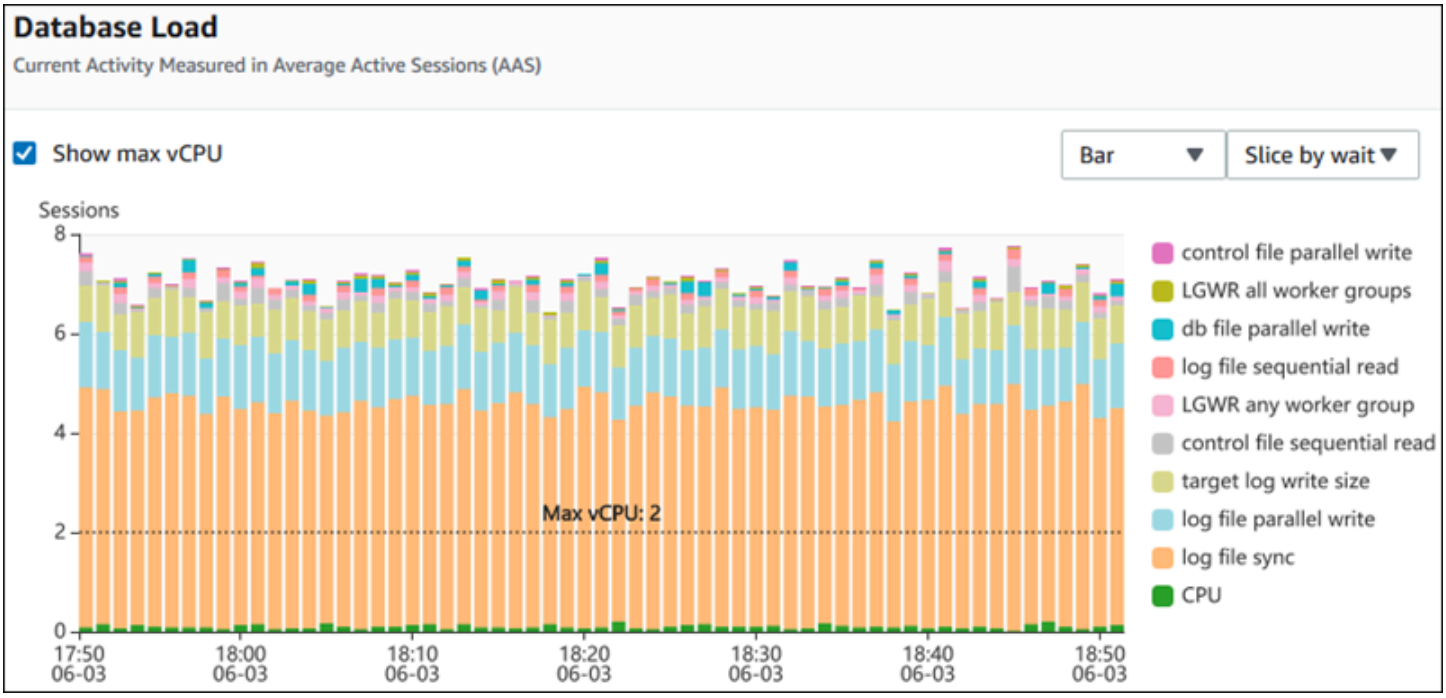
Ändern Sie die Leistungsindikatoren, indem Sie Metriken verwalten wählen. Sie können mehrere Betriebssystem-Metriken oder Datenbank-Metriken, auswählen, wie im folgenden Screenshot veranschaulicht. Um Details für jede Metrik anzuzeigen, bewegen Sie den Mauszeiger über den Metriknamen.



Beschreibungen der Zählermetriken, die Sie für jede DB-Engine hinzufügen können, finden Sie unter Performance-Insights-Zählermetriken.

Datenbank-Ladediagramm

Das Diagramm Database Load (Datenbank-Last) zeigt die Datenbanklast im Vergleich zur Kapazität der DB-Instance, die durch die Max vCPU-Linie dargestellt wird. Standardmäßig stellt das gestapelte Liniendiagramm die DB-Last als durchschnittliche aktive Sitzungen pro Zeiteinheit dar. Die DB-Last wird nach Wartestatus aufgeteilt (gruppiert).

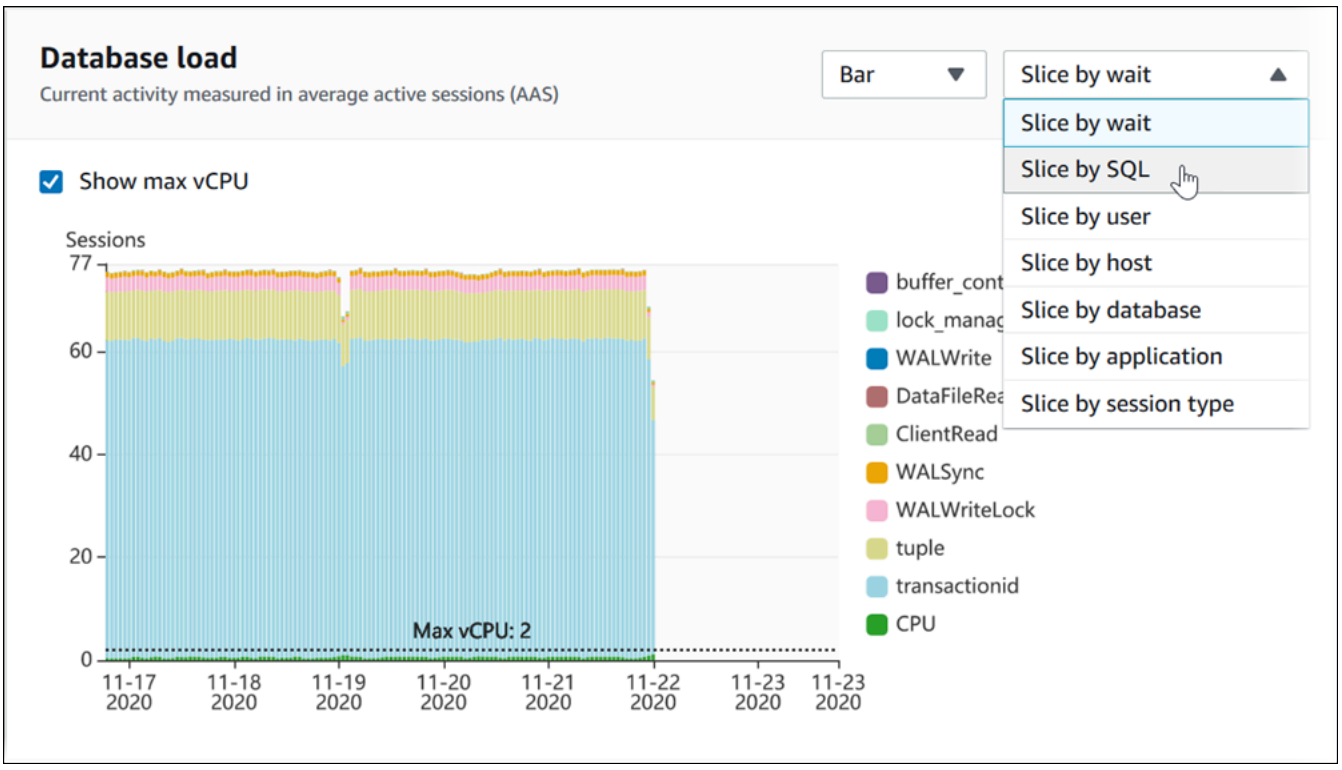


DB-Last aufgeteilt nach Dimensionen

Sie können die Last als aktive Sitzungen anzeigen, die nach unterstützten Dimensionen gruppiert sind. Die folgende Tabelle zeigt, welche Dimensionen für die verschiedenen Engines unterstützt werden.

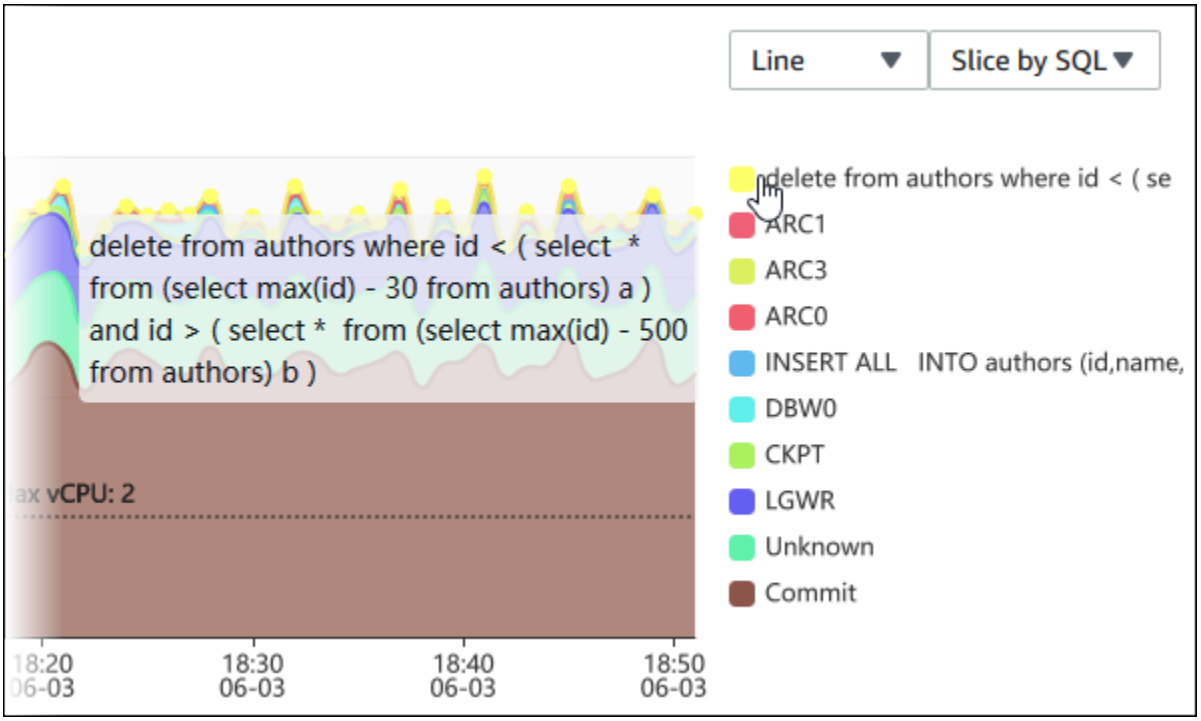
Dimension	Aurora PostgreSQL	Aurora MySQL
Host	Ja	Ja
SQL	Ja	Ja
Benutzer	Ja	Ja
Waits (Warteereignis)	Ja	Ja
Anwendung	Ja	Nein
Datenbank	Ja	Ja
Session type (Sitzungstyp)	Ja	Nein

Der folgende Screenshot zeigt die Dimensionen für eine PostgreSQL-DB-Instance.

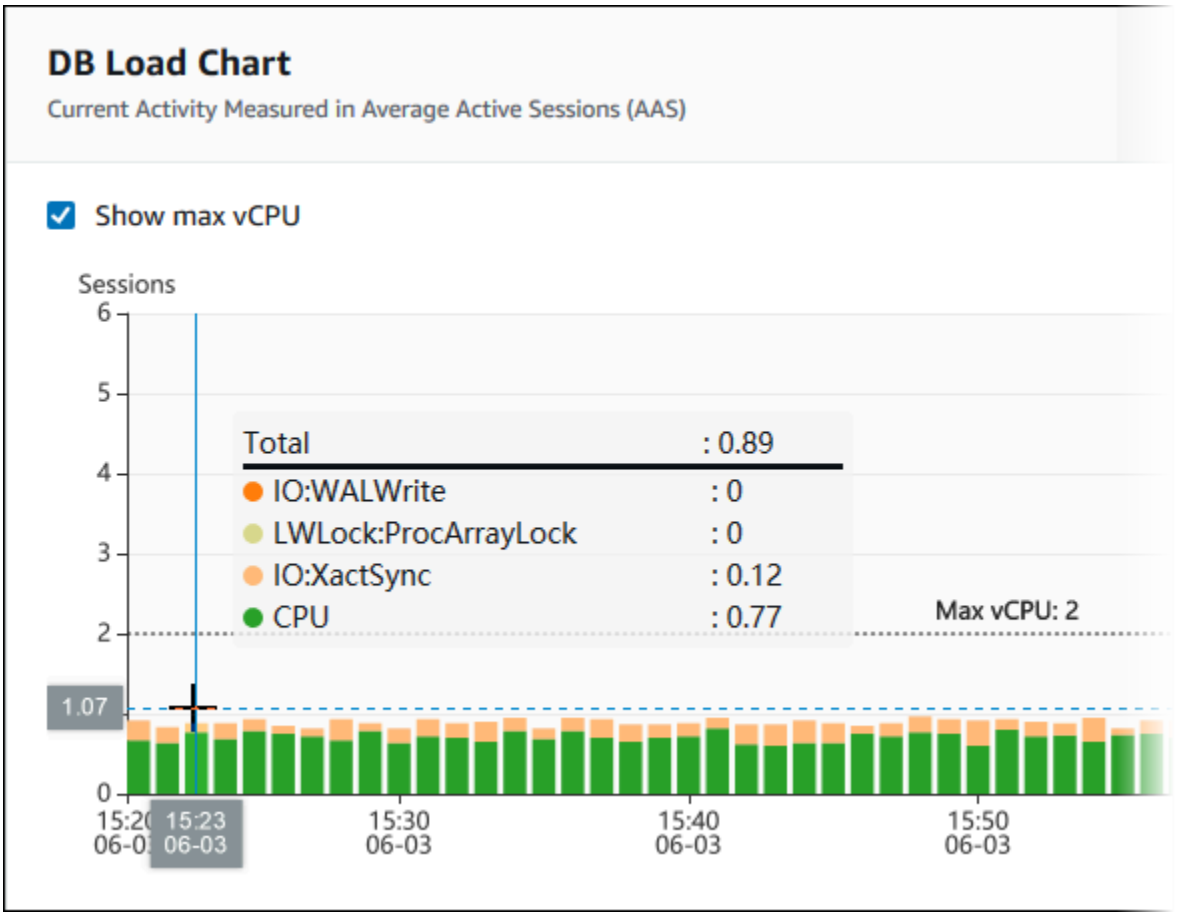


DB-Ladedetails für ein Dimensionselement

Um Details zu einem DB-Lastelement innerhalb einer Dimension anzuzeigen, bewegen Sie den Mauszeiger über den Elementnamen. Die folgende Abbildung zeigt Details zu einer SQL-Anweisung.

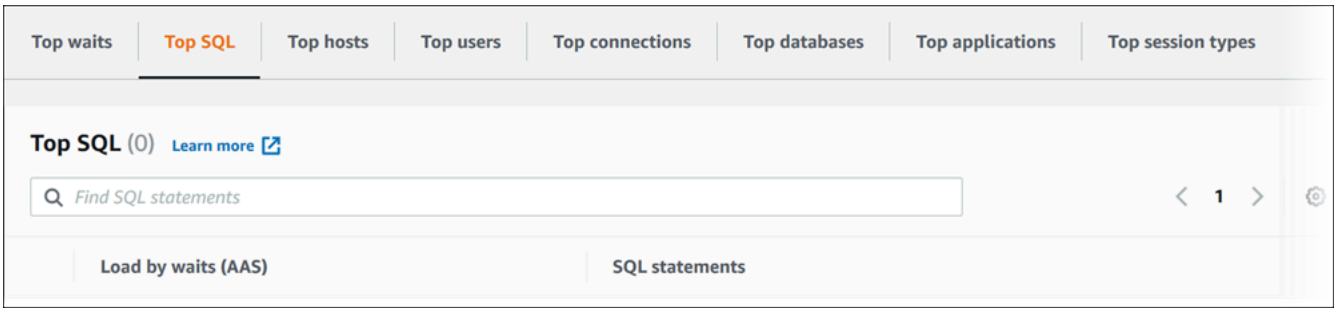


Um Details zu einem Element für den ausgewählten Zeitraum in der Legende anzuzeigen, bewegen Sie den Mauszeiger über dieses Element.



Dimensionen pro Tabelle

Die Tabelle mit den oberen Abmessungen schneidet die DB-Ladung um verschiedene Dimensionen auf. Eine Dimension ist eine Kategorie oder „Aufteilung“ für verschiedene Merkmale der DB-Last. Wenn die Dimension SQL ist, zeigt Haupt-SQL die SQL-Anweisungen an, die am meisten zur DB-Last beitragen.



Wählen Sie eine der folgenden Dimensionsregisterkarten.

Tab	Beschreibung	Unterstützte Engines
Haupt-SQL	Die SQL-Anweisungen, die derzeit ausgeführt werden	Alle
Top waits (Top-Warteereignis)	Das Ereignis, auf das das Datenbank-Backend wartet	Alle
Top hosts (Top-Hosts)	Der Hostname des verbunden en Clients	Alle
Top users (Top-Benutzer)	Der bei der Datenbank angemeldete Benutzer	Alle
Top applications (Top-Anwe ndungen)	Der Name der Anwendung , die mit der Datenbank verbunden ist	Nur Aurora PostgreSQL
Top session types (Top-Sitz ungstypen)	Der Typ der aktuellen Sitzung	Nur Aurora PostgreSQL

So lernen Sie, wie Sie Abfragen analysieren können, indem Sie die Registerkarte Haupt-SQL nutzen, siehe Überblick über die Registerkarte „Top SQL“.

Zugriff auf das Performance-Insights-Dashboard

Amazon RDS bietet im Performance-Insights-Dashboard eine konsolidierte Ansicht der Performance-Insights- und CloudWatch-Metriken.

Gehen Sie wie folgt vor, um auf das Performance-Insights-Dashboard zuzugreifen.

So zeigen Sie das Dashboard von Performance Insights in der AWS-Managementkonsole an

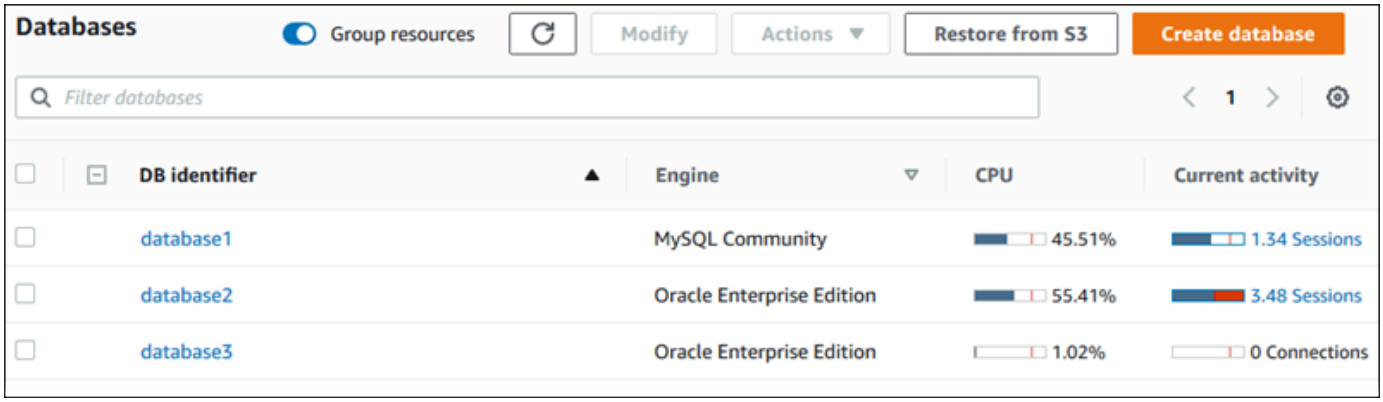
1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.
4. Wählen Sie im angezeigten Fenster die Standard-Überwachungsansicht aus.

- Wählen Sie die Option Performance-Insights- und CloudWatch-Metriken anzeigen (Neu) und Weiter aus, um Performance-Insights- und CloudWatch-Metriken anzuzeigen.
- Wählen Sie die Option Performance-Insights-Ansicht und Weiter für die Legacy-Überwachungsansicht aus. Fahren Sie anschließend mit diesem Verfahren fort.

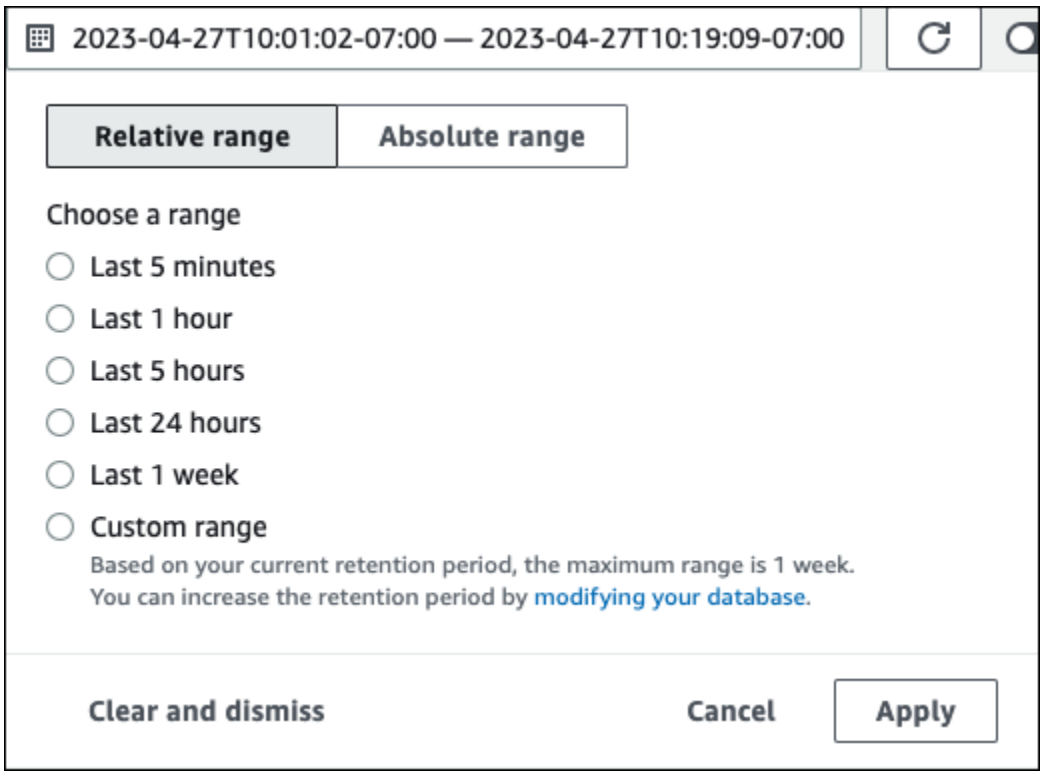
> **Note**
>
> Diese Ansicht wird am 15. Dezember 2023 eingestellt.

Das Performance-Insights-Dashboard wird für die DB-Instance angezeigt.

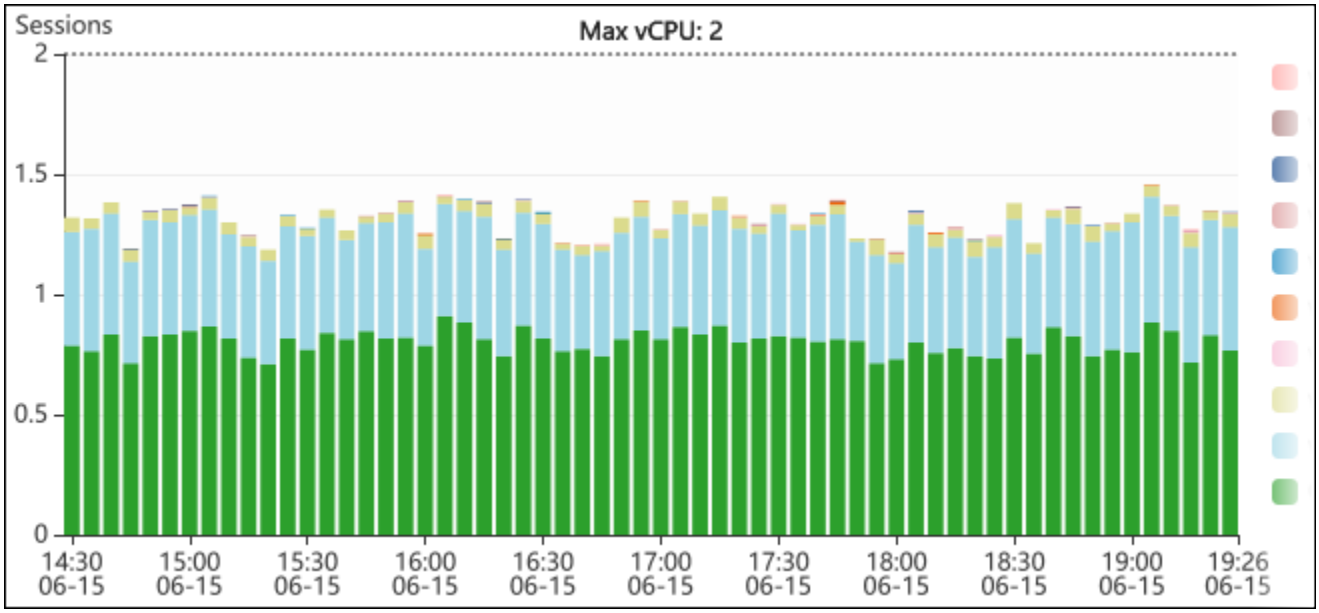
Für DB-Instances, bei denen Performance Insights aktiviert sind, können Sie auf das Dashboard auch über das Element Sitzungen in der DB-Instance-Liste zugreifen. Unter Aktuelle Aktivität zeigt das Element Sitzungen die Datenbanklast von durchschnittlichen, aktiven Sitzungen der letzten fünf Minuten an. Der Balken zeigt die Last grafisch an. Ist der Balken leer, wird die DB-Instance nicht verwendet. Wenn die Last ansteigt, wird der Balken blau ausgefüllt. Wenn die Last die Anzahl von virtuellen CPUs (vCPUs) auf der DB-Instance-Klasse überschreitet, wird der Balken rot und zeigt so einen potenziellen Engpass an.



5. (Optional) Wählen Sie das Datum oder den Zeitraum oben rechts aus und geben Sie ein anderes relatives oder absolutes Zeitintervall an. Sie können jetzt einen Zeitraum angeben und einen Bericht zur Datenbankleistungsanalyse erstellen. Der Bericht enthält die identifizierten Einblicke und Empfehlungen. Weitere Informationen finden Sie unter Erstellen eines Leistungsanalyseberichts.

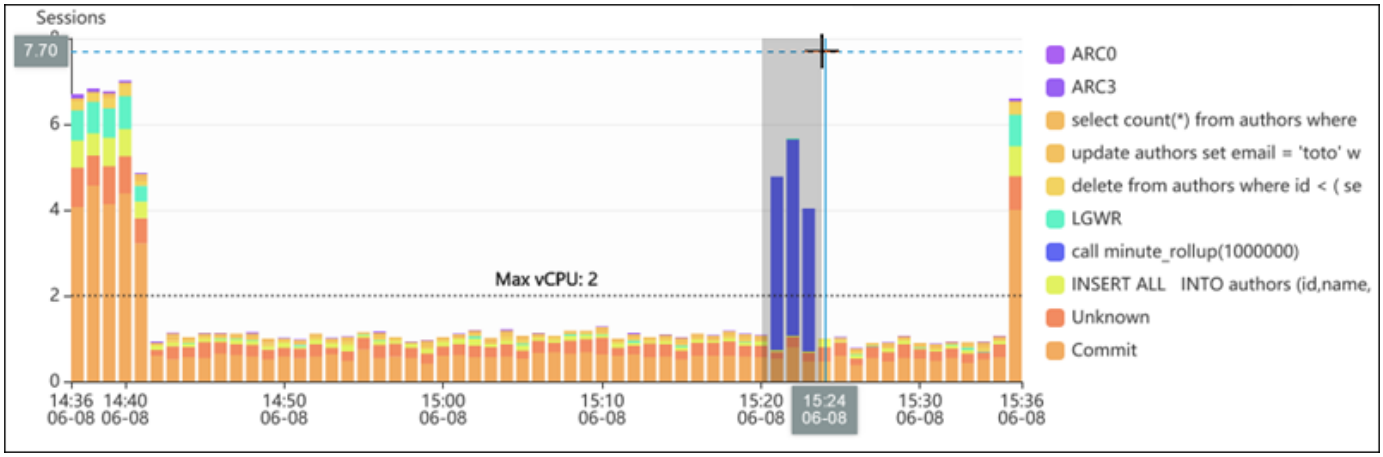


Im folgenden Screenshot beträgt das DB-Last-Intervall 5 Stunden.

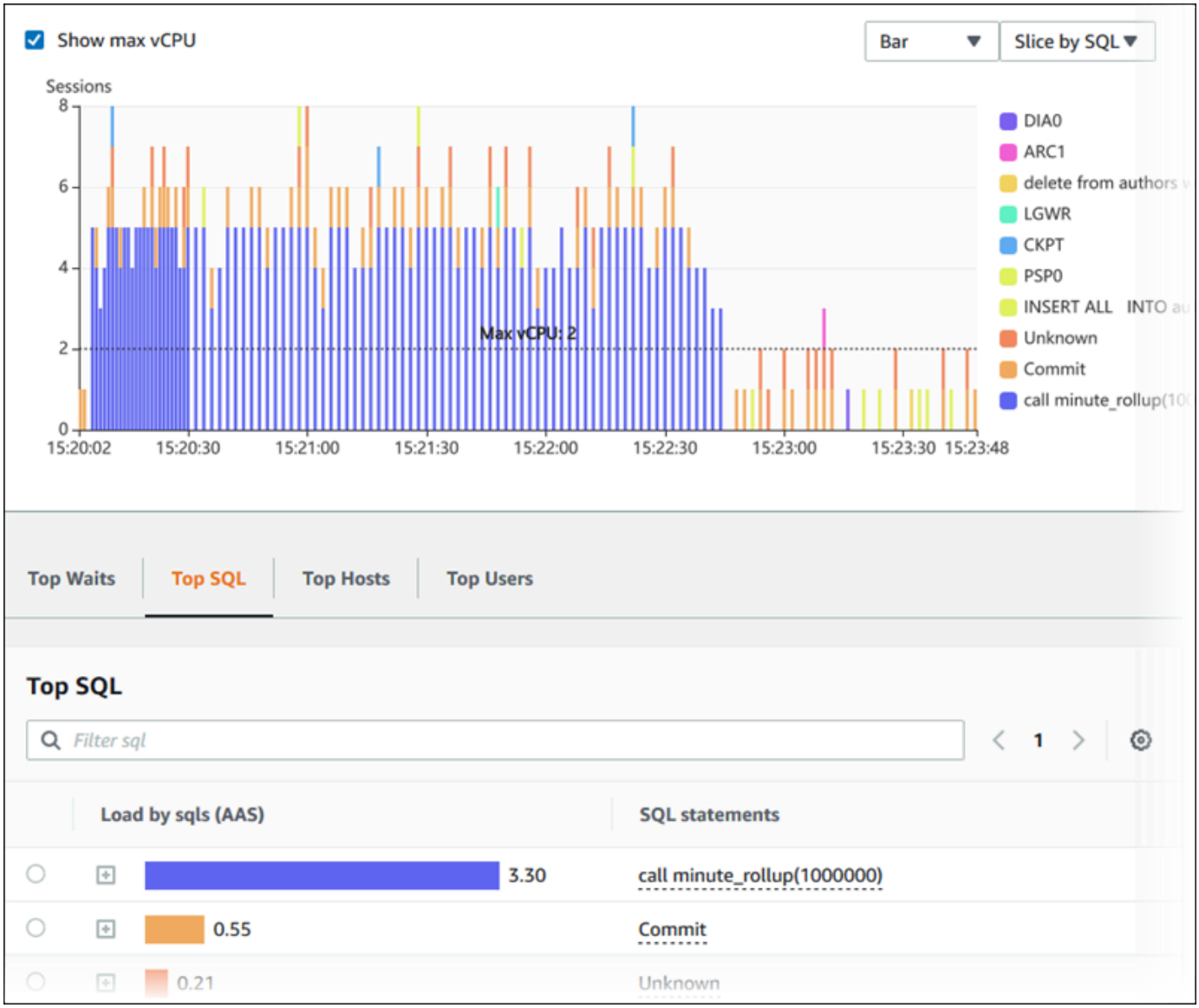


6. (Optional) Um einen Teil des DB-Lastdiagramms zu vergrößern, wählen Sie die Startzeit und ziehen sie mit der Maus an das Ende des gewünschten Zeitraums.

   Der ausgewählte Bereich wird im DB-Lastdiagramm hervorgehoben.



Wenn Sie die Maustaste loslassen, vergrößert sich das DB-Lastdiagramm auf die ausgewählte AWS-Region und die Tabelle Top dimensions (Hauptdimensionen) wird neu berechnet.



7. (Optional) Um Ihre Daten automatisch zu aktualisieren, aktivieren Sie Automatische Aktualisierung.

Das Performance-Insights-Dashboard wird automatisch mit neuen Daten aktualisiert. Die Aktualisierungsrate hängt von der Menge der angezeigten Daten ab:

- 5 Minuten wird alle 10 Sekunden aktualisiert.
- 1 Stunde wird alle 5 Minuten aktualisiert.
- 5 Stunden wird alle 5 Minuten aktualisiert.
- 24 Stunden wird alle 30 Minuten aktualisiert.

- 1 Woche wird jeden Tag aktualisiert.
- 1 Monat wird jeden Tag aktualisiert.

Analysieren der DB-Last nach Warteereignissen

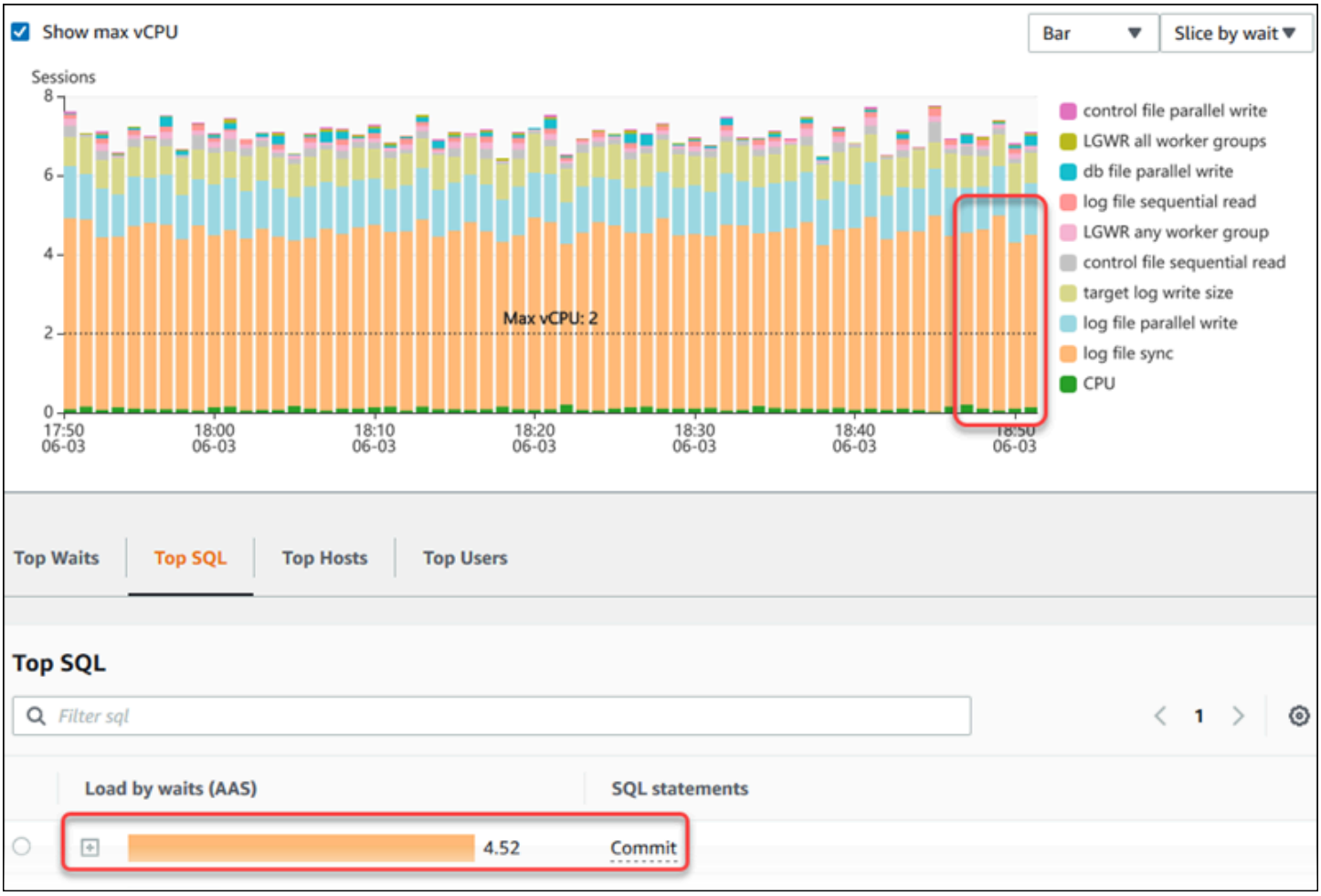
Wenn das Diagramm der durchschnittlich aktiven Sitzungen einen Engpass anzeigt, können Sie herausfinden, woher die Last kommt. Betrachten Sie dazu die Tabelle mit den Hauptlastelementen unterhalb des Datenbanklast-Diagramms Wählen Sie ein bestimmtes Element, wie z. B. eine SQL-Abfrage oder einen Benutzer, um es aufzuschlüsseln und Details zu diesem Element anzuzeigen.

Die DB-Last, gruppiert nach Wartezeiten und Top-SQL-Abfragen, ist die standardmäßige Ansicht im Performance Insights-Dashboard. Diese Kombination bietet typischerweise den besten Einblick in Performance-Probleme. DB-Last gruppiert nach Wartezeiten zeigt an, ob Ressourcen- oder Parallelitätsengpässe in der Datenbank vorhanden sind. In diesem Fall zeigt die SQL-Registerkarte der Tabelle der Hauptlastelemente, welche Abfragen diese Last verursachen.

Ihr typischer Workflow für die Diagnose von Performance-Problemen ist folgendermaßen:

1. Überprüfen Sie das Diagramm der durchschnittlich aktiven Sitzungen auf irgendwelche Ereignisse, in denen die Datenbanklast die Max CPU-Linie übersteigt.
2. Wenn ja, schauen Sie sich das Diagramm der durchschnittlich aktiven Sitzungen an und identifizieren Sie, welcher Wartezustand oder welche Zustände primär dafür verantwortlich sind.
3. Identifizieren Sie die zusammengefassten Abfragen, welche die Last verursachen, indem Sie nachsehen, welche Abfragen in der SQL-Registerkarte der Tabelle der Hauptlastelemente hauptsächlich zu diesen Wartezuständen beitragen. Sie finden sie in der Spalte DB Load by Wait (DB-Last nach Wartezuständen).
4. Wählen Sie eine dieser zusammengefassten Abfragen in der Registerkarte SQL aus, um sie zu expandieren und untergeordnete Abfragen anzuzeigen, aus denen sie besteht.

Beispielsweise wird im folgenden Dashboard die Protokolldateisynchronisierung für den größten Teil der DB-Last berücksichtigt. Die Wartezeit für Alle Worker-Gruppen in LGWR ist ebenfalls hoch. Das Diagramm Haupt-SQL zeigt auf, wodurch die Wartezustände der Protokolldatei-Synchronisierung verursacht werden: häufige `COMMIT`-Anweisungen. In diesem Fall wird durch eine weniger häufige Übergabe mit Commit die DB-Last reduziert.



Analysieren der Datenbankleistung für einen bestimmten Zeitraum

Analysieren Sie die Datenbankleistung mit On-Demand-Analysen, indem Sie einen Leistungsanalysebericht für einen bestimmten Zeitraum erstellen. Sehen Sie sich Leistungsanalyseberichte an, um Leistungsprobleme wie Ressourcenengpässe oder Änderungen an einer Abfrage in Ihrer DB-Instance zu finden. Im Performance-Insights-Dashboard können Sie einen Zeitraum auswählen und einen Leistungsanalysebericht erstellen. Sie können dem Bericht auch ein oder mehrere Tags hinzufügen.

Um diese Funktion nutzen zu können, müssen Sie die Aufbewahrungsfrist für die kostenpflichtige Stufe verwenden. Weitere Informationen finden Sie unter Preisgestaltung und Datenaufbewahrung für Performance-Insights.

Der Bericht kann auf der Registerkarte Leistungsanalyseberichte – neu ausgewählt und angezeigt werden. Der Bericht enthält die Erkenntnisse, zugehörigen Metriken und Empfehlungen zur

Lösung des Leistungsproblems. Der Bericht kann für die Dauer des Aufbewahrungszeitraums von Performance Insights eingesehen werden.

Der Bericht wird gelöscht, wenn die Startzeit des Berichtsanalysezeitraums außerhalb des Aufbewahrungszeitraums liegt. Sie können den Bericht auch vor Ablauf der Aufbewahrungsfrist löschen.

Sie müssen Performance Insights aktivieren, um die Leistungsprobleme zu erkennen und den Analysebericht für Ihre DB-Instance zu erstellen. Weitere Informationen zum Aktivieren von Performance Insights finden Sie unter Performance Insights für Aurora ein- und ausschalten.

Informationen zur Unterstützung dieser Funktion nach Region, DB-Engine und Instance-Klasse finden Sie unter DB-Engine-, Regions- und Instance-Klassenunterstützung von Amazon Aurora für Performance-Insights-Funktionen.

Erstellen eines Leistungsanalyseberichts

Im Performance-Insights-Dashboard können Sie einen Leistungsanalysebericht für einen bestimmten Zeitraum erstellen. Sie können einen Zeitraum auswählen und dem Analysebericht ein oder mehrere Tags hinzufügen.

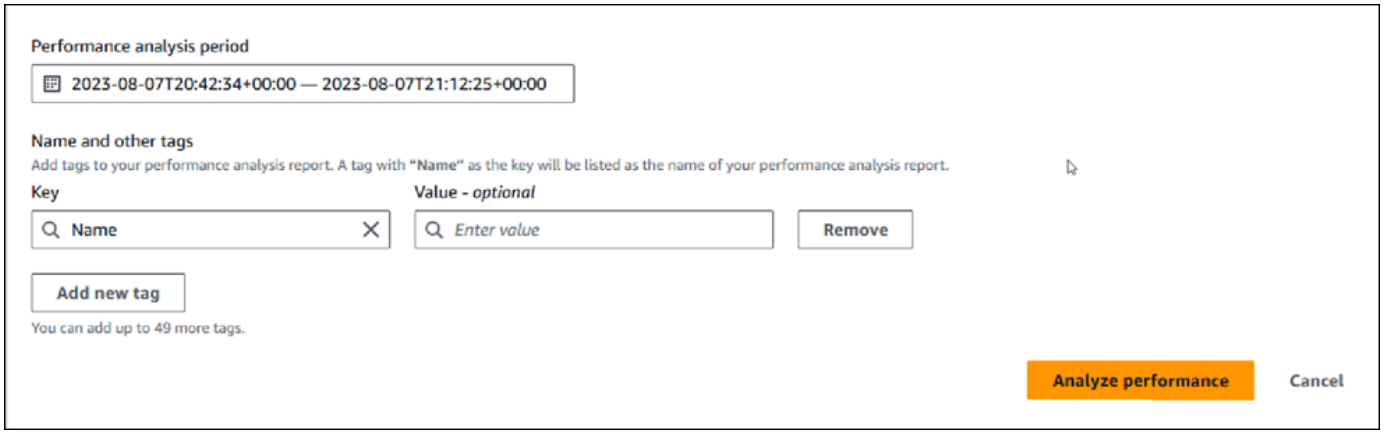
Der Analysezeitraum kann zwischen 5 Minuten und 6 Tagen liegen. Vor dem Start der Analyse müssen mindestens 24 Stunden an Leistungsdaten vorliegen.

So erstellen Sie einen Leistungsanalysebericht für einen bestimmten Zeitraum

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.

   Das Performance-Insights-Dashboard wird für die DB-Instance angezeigt.
4. Wählen Sie Leistung analysieren im Abschnitt Datenbanklast im Dashboard aus.

   Die Felder zum Festlegen des Zeitraums und zum Hinzufügen eines oder mehrerer Tags zum Leistungsanalysebericht werden angezeigt.

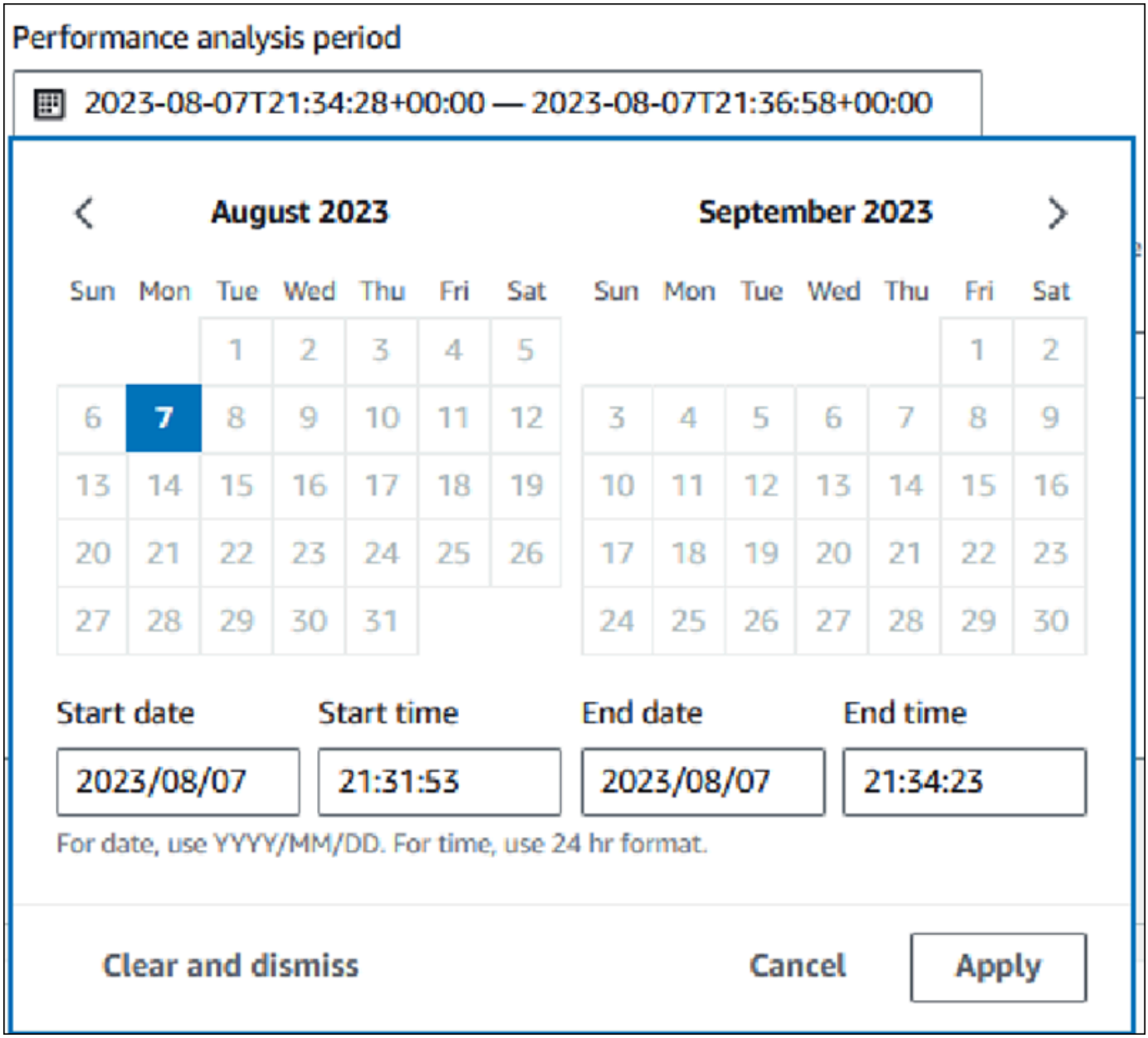


5. Wählen Sie den Zeitraum aus. Wenn Sie oben rechts einen Zeitraum im Abschnitt Relativer Bereich oder Absoluter Bereich festlegen, können Sie nur Datum und Uhrzeit des Analyseberichts innerhalb dieses Zeitraums eingeben oder auswählen. Wenn Sie den Analysezeitraum außerhalb dieses Zeitraums auswählen, wird eine Fehlermeldung angezeigt.

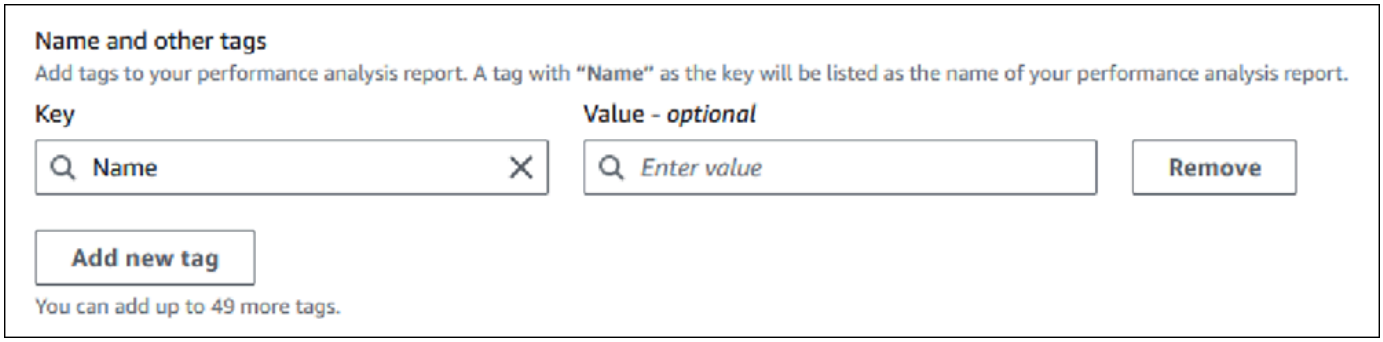
   Führen Sie einen der folgenden Schritte aus, um den Zeitraum festzulegen:

   - Drücken und ziehen Sie einen der Schieberegler im DB-Lastdiagramm.

     Das Feld Zeitraum der Leistungsanalyse zeigt den ausgewählten Zeitraum an und das DB-Lastdiagramm hebt den ausgewählten Zeitraum hervor.
   - Wählen Sie Startdatum, Startzeit, Enddatum und Endzeit im Feld Zeitraum der Leistungsanalyse aus.



6. (Optional) Geben Sie Schlüssel und Wertoptional ein, um ein Tag für den Bericht hinzuzufügen.



7. Wählen Sie Leistung analysieren aus.

   In einem Banner wird eine Meldung angezeigt, die angibt, ob die Berichtserstellung erfolgreich war oder fehlgeschlagen ist. Die Nachricht enthält auch den Link zum Anzeigen des Berichts.

   Das folgende Beispiel zeigt das Banner mit der Meldung, dass der Bericht erfolgreich erstellt wurde.

   Der Bericht kann auf der Registerkarte Leistungsanalyseberichte – neu angezeigt werden.

Mit der AWS CLI können Sie einen Leistungsanalysebericht erstellen. Ein Beispiel zur Erstellung eines Berichts mithilfe von finden Sie AWS CLI unter. Erstellen eines Leistungsanalyseberichts für einen bestimmten Zeitraum

Anzeigen eines Leistungsanalyseberichts

Die Registerkarte Leistungsanalysebericht – neu listet alle Berichte auf, die für die DB-Instance erstellt wurden. Für jeden Bericht wird Folgendes angezeigt:

- ID: eindeutige Kennung des Berichts.
- Name: der Tag-Schlüssel, der dem Bericht hinzugefügt wurde.
- Erstellungszeit des Berichts: Uhrzeit, zu der Sie den Bericht erstellt haben.
- Startzeit der Analyse: Startzeit der Analyse im Bericht.
- Endzeit der Analyse: Endzeit der Analyse im Bericht.

So zeigen Sie einen Leistungsanalysebericht an

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus, für die Sie den Analysebericht anzeigen möchten.

   Das Performance-Insights-Dashboard wird für die DB-Instance angezeigt.
4. Scrollen Sie nach unten und wählen Sie die Registerkarte Leistungsanalyseberichte – neu aus.

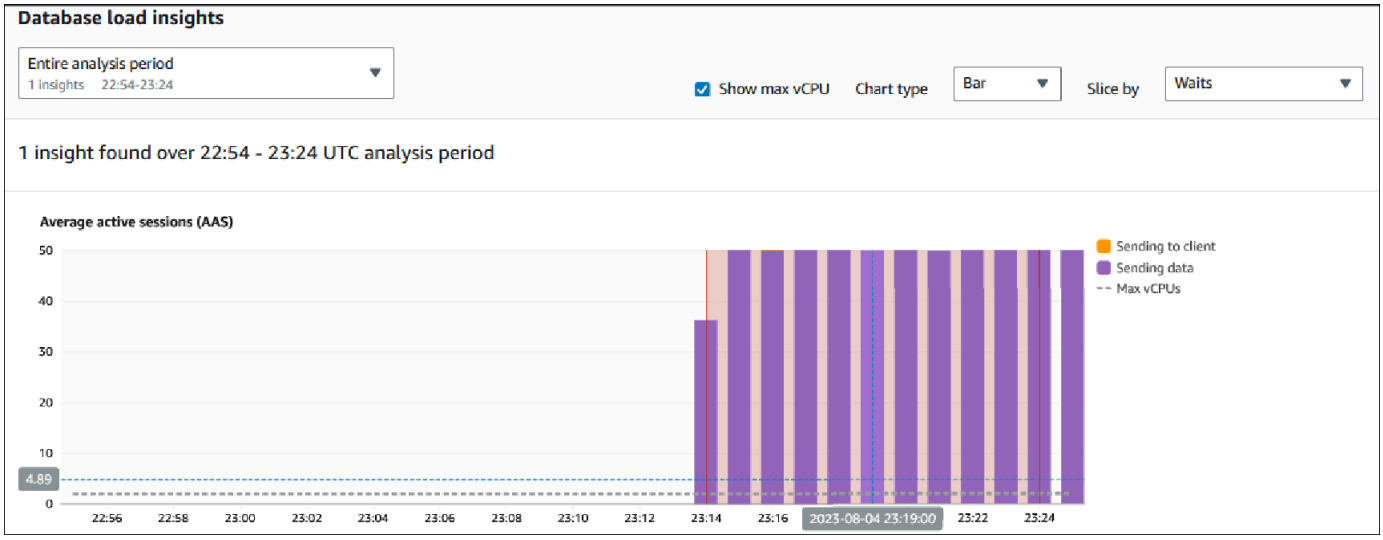
   Es werden alle Analyseberichte für die verschiedenen Zeiträume angezeigt.

5. Wählen Sie die ID des Berichts aus, den Sie ansehen möchten.

   Das DB-Lastdiagramm zeigt standardmäßig den gesamten Analysezeitraum an, wenn mehr als ein Einblick identifiziert wurde. Wenn der Bericht einen Einblick identifiziert hat, zeigt das DB-Lastdiagramm den Einblick standardmäßig an.

   Das Dashboard listet außerdem die Tags für den Bericht im Abschnitt Tags auf.

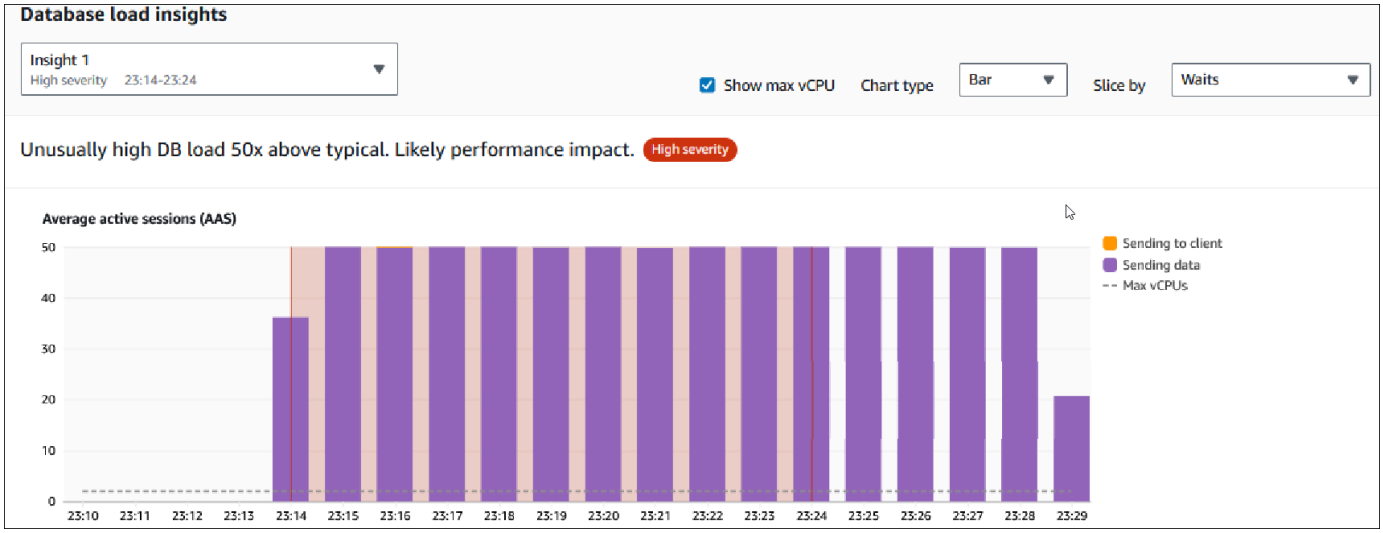
   Das folgende Beispiel zeigt den gesamten Analysezeitraum für den Bericht.

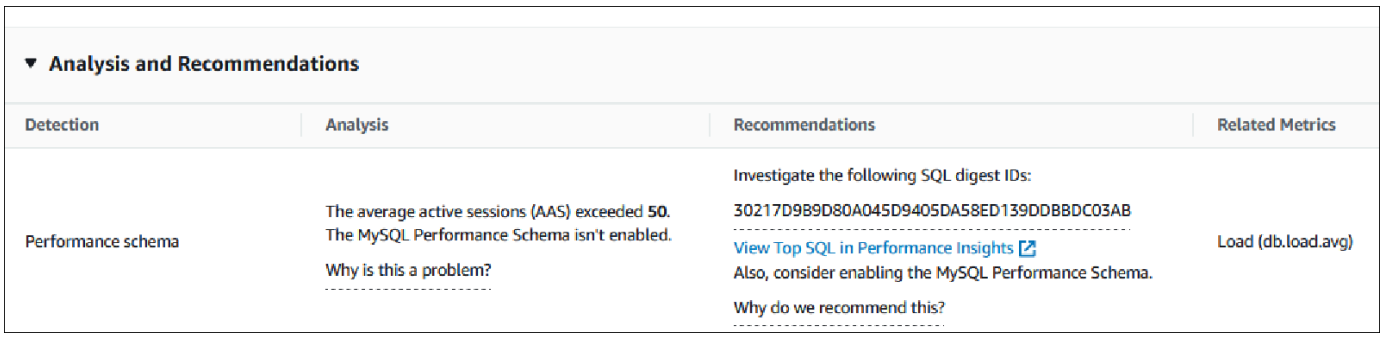


6. Wählen Sie die Einsicht in der Liste Einblicke in die Datenbanklast aus, die Sie anzeigen möchten, wenn im Bericht mehr als ein Einblick identifiziert wird.

   Das Dashboard zeigt die Einblickmeldung, wobei im DB-Lastdiagramm der Zeitraum des Einblicks, die Analyse und Empfehlungen hervorgehoben werden sowie die Liste der Berichts-Tags enthalten ist.

   Das folgende Beispiel zeigt den DB-Lasteinblick im Bericht.





Hinzufügen von Tags zu einem Leistungsanalysebericht

Sie können ein Tag hinzufügen, wenn Sie einen Bericht erstellen oder ansehen. Sie können bis zu 50 Tags für einen Bericht hinzufügen.

Sie benötigen Berechtigungen, um Tags hinzuzufügen. Weitere Informationen zu Zugriffsrichtlinien für Performance Insights finden Sie unter Konfigurieren von Zugriffsrichtlinien für Performance Insights.

Informationen zum Hinzufügen eines oder mehrerer Tags bei der Erstellung eines Berichts finden Sie in Schritt 6 des Verfahrens Erstellen eines Leistungsanalyseberichts.

So fügen Sie beim Anzeigen eines Berichts ein oder mehrere Tags hinzu

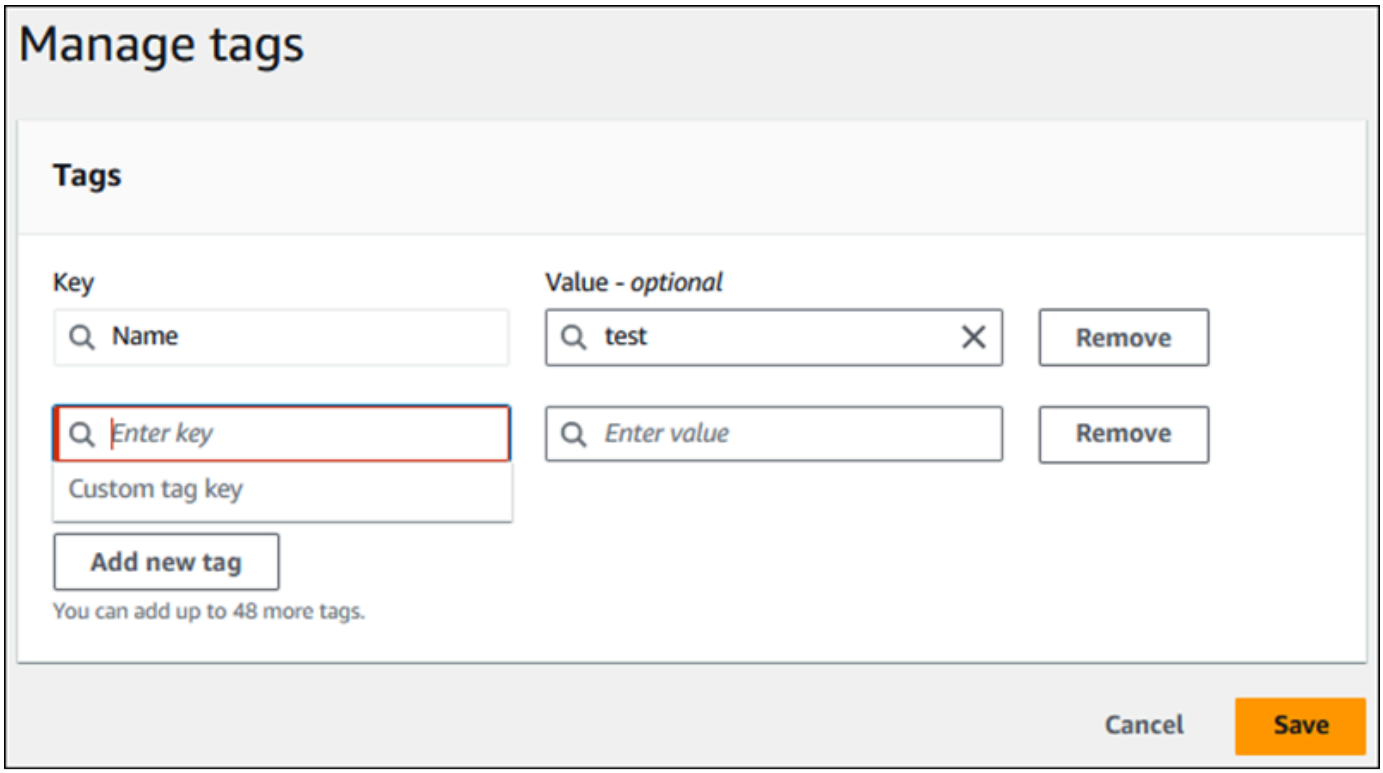
1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.

Das Performance-Insights-Dashboard wird für die DB-Instance angezeigt.

4. Scrollen Sie nach unten und wählen Sie die Registerkarte Leistungsanalyseberichte – neu aus.
5. Wählen Sie den Bericht aus, für den Sie die Tags hinzufügen möchten.

   Das Dashboard zeigt den Bericht an.
6. Scrollen Sie nach unten zu Tags und wählen Sie Tags verwalten aus.
7. Wählen Sie Neues Tag hinzufügen aus.
8. Geben Sie Schlüssel und Wert – optional ein und wählen Sie Neues Tag hinzufügen aus.

   Das folgende Beispiel bietet die Option, ein neues Tag für den ausgewählten Bericht hinzuzufügen.



   Ein neues Tag wird für den Bericht erstellt.

   Im Dashboard wird die Liste der Tags für den Bericht im Abschnitt Tags aufgelistet. Wenn Sie ein Tag aus dem Bericht entfernen möchten, wählen Sie Entfernen neben dem Tag aus.

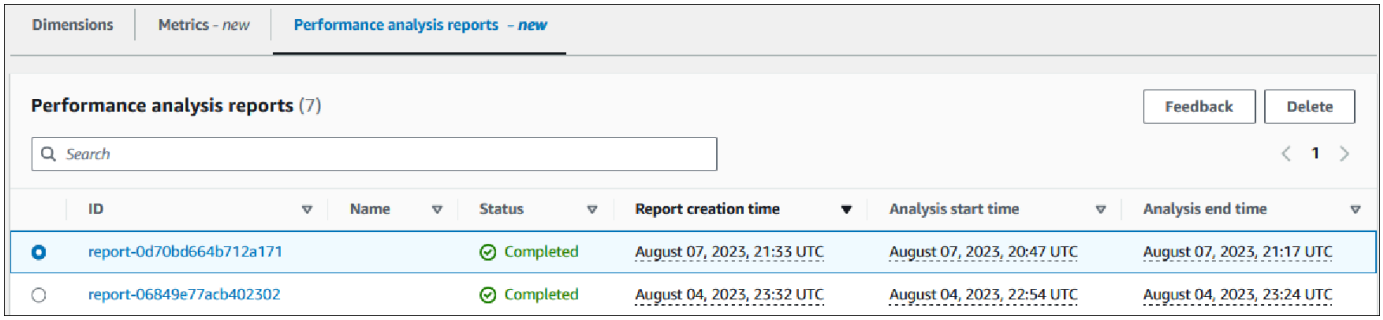
Löschen eines Leistungsanalyseberichts

Sie können einen Bericht aus der Liste der Berichte, die auf der Registerkarte Leistungsanalyseberichte angezeigt werden, oder beim Anzeigen eines Berichts löschen.

So löschen Sie einen Bericht

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.
3. Wählen Sie eine DB-Instance aus.

   Das Performance-Insights-Dashboard wird für die DB-Instance angezeigt.
4. Scrollen Sie nach unten und wählen Sie die Registerkarte Leistungsanalyseberichte – neu aus.
5. Wählen Sie den Bericht aus, den Sie löschen möchten, und klicken Sie oben rechts auf Löschen.



   Ein Bestätigungsfenster wird angezeigt. Der Bericht wird gelöscht, nachdem Sie „Bestätigen“ ausgewählt haben.
6. (Optional) Wählen Sie die ID des Berichts, den Sie löschen möchten.

   Wählen Sie oben rechts auf der Seite Löschen aus.

   Ein Bestätigungsfenster wird angezeigt. Der Bericht wird gelöscht, nachdem Sie „Bestätigen“ ausgewählt haben.

Analyse von Abfragen mit dem Performance-Insights-Dashboard

Im Amazon-RDS-Performance-Insights-Dashboard finden Sie Informationen zu laufenden Abfragen auf dem Tab Top SQL (Haupt-SQL) der Tabelle Top dimensions (Hauptdimensionen). Sie können diese Informationen verwenden, um Ihre Abfragen zu optimieren.

Themen

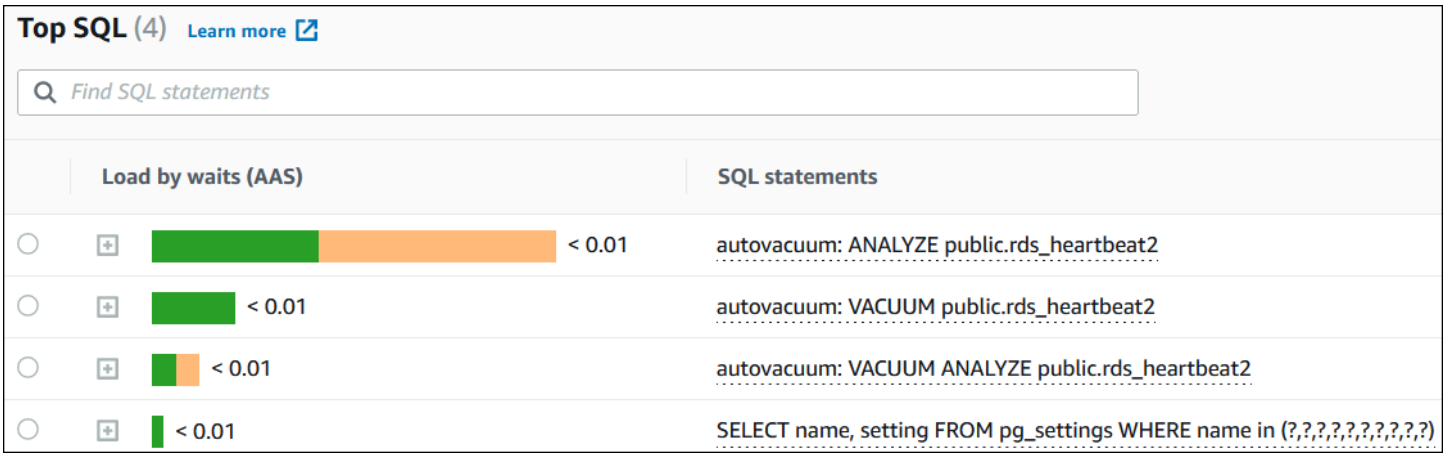
Überblick über die Registerkarte „Top SQL“

Standardmäßig werden auf der Registerkarte Top SQL (Top-SQL) die 25 Abfragen angezeigt, die hauptsächlich zur Datenbanklast beitragen. Wenn Sie Ihre Abfragen optimieren möchten, können Sie Informationen wie den Abfragetext und SQL-Statistiken analysieren. Sie können auch die Statistiken auswählen, die in der Haupt-SQL Tabulatortaste angezeigt werden.

Themen

SQL-Text

Standardmäßig zeigt jede Zeile in der Tabelle Top SQL (Top-SQL) für jede Anweisung 500 Byte Text an.

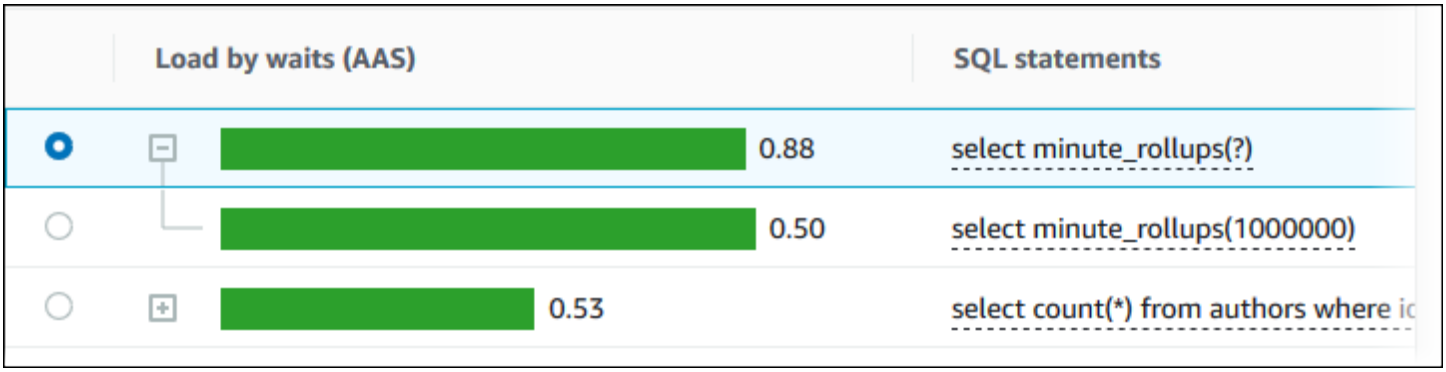


Wie Sie mehr als die standardmäßigen 500 Byte SQL-Text sehen können, erfahren Sie unter Zugriff auf mehr SQL-Text im Performance-Insights-Dashboard.

Ein SQL-Digest ist eine Zusammenstellung mehrerer tatsächlicher Abfragen, die strukturell ähnlich sind, aber möglicherweise unterschiedliche Literalwerte aufweisen. Der Digest ersetzt fest codierte Werte durch ein Fragezeichen. Zum Beispiel könnte `SELECT * FROM emp WHERE lname= ?` ein Digest sein. Dieser Digest kann die folgenden untergeordneten Abfragen enthalten:

```
SELECT * FROM emp WHERE lname = 'Sanchez'
SELECT * FROM emp WHERE lname = 'Olagappan'
SELECT * FROM emp WHERE lname = 'Wu'
```

Um die literalen SQL-Anweisungen in einem Digest anzuzeigen, wählen Sie die Abfrage aus und dann das Plussymbol (+) aus und dann das Plussymbol (+). Im folgenden Beispiel ist die ausgewählte Abfrage ein Digest.

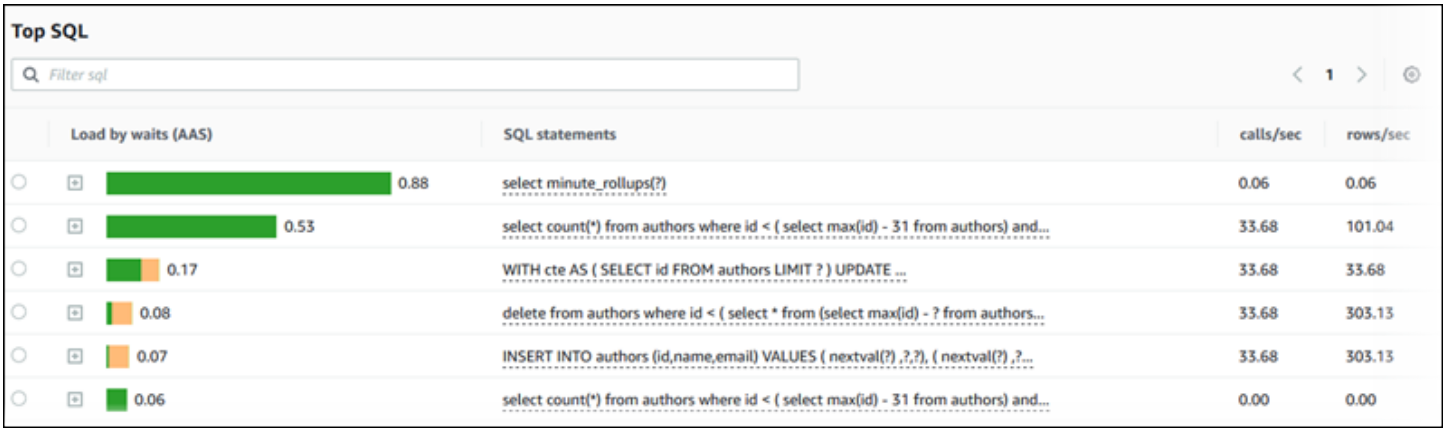


> **Note**
>
> Ein SQL-Digest gruppiert ähnliche SQL-Anweisungen, redigiert jedoch keine sensiblen Daten.

SQL-Statistiken

SQL-Statistiken sind leistungsbezogene Metriken zu SQL-Abfragen. Performance Insights könnte beispielsweise Ausführungen pro Sekunde oder pro Sekunde verarbeitete Zeilen anzeigen. Performance Insights erfasst Statistiken nur für die häufigsten Abfragen. In der Regel entsprechen diese den Top-Abfragen nach Last, die im Performance Insights-Dashboard angezeigt werden.

Jede Zeile in der Haupt-SQL-Tabelle zeigt relevante Statistiken für die SQL-Anweisung oder -Digest, wie im folgenden Beispiel beschrieben.



Performance Insights kann `0.00` und `-` (unbekannt) für SQL-Statistiken melden. Diese Situation tritt unter den folgenden Bedingungen auf:

- Es ist nur eine Stichprobe vorhanden. Performance Insights berechnet beispielsweise Veränderungsraten für Aurora-PostgreSQL-Abfragen basierend auf mehreren Stichproben der Ansicht `pg_stat_statements`. Wenn eine Workload für kurze Zeit ausgeführt wird, erfasst Performance Insights möglicherweise nur eine Stichprobe, was bedeutet, dass keine Änderungsrate berechnet werden kann. Der unbekannte Wert wird durch einen Bindestrich (`-`) dargestellt.
- Zwei Stichproben haben die gleichen Werte. Performance Insights kann keine Änderungsrate berechnen, da keine Änderung stattgefunden hat, weshalb die Rate als `0.00` gemeldet wird.
- Einer Aurora-PostgreSQL-Anweisung fehlt ein gültiger Bezeichner. PostgreSQL erstellt erst nach dem Parsen und Analysieren einen Bezeichner für eine Anweisung. Somit kann eine Anweisung in den internen In-Memory-Strukturen von PostgreSQL ohne Bezeichner vorhanden sein. Da Performance Insights einmal pro Sekunde interne In-Memory-Strukturen erfasst, werden Abfragen mit niedriger Latenz möglicherweise nur für eine einzige Stichprobe angezeigt. Wenn die Abfrage-ID für dieses Beispiel nicht verfügbar ist, kann Performance Insights diese Anweisung nicht mit den entsprechenden Statistiken verknüpfen. Der unbekannte Wert wird durch einen Bindestrich (`-`) dargestellt.

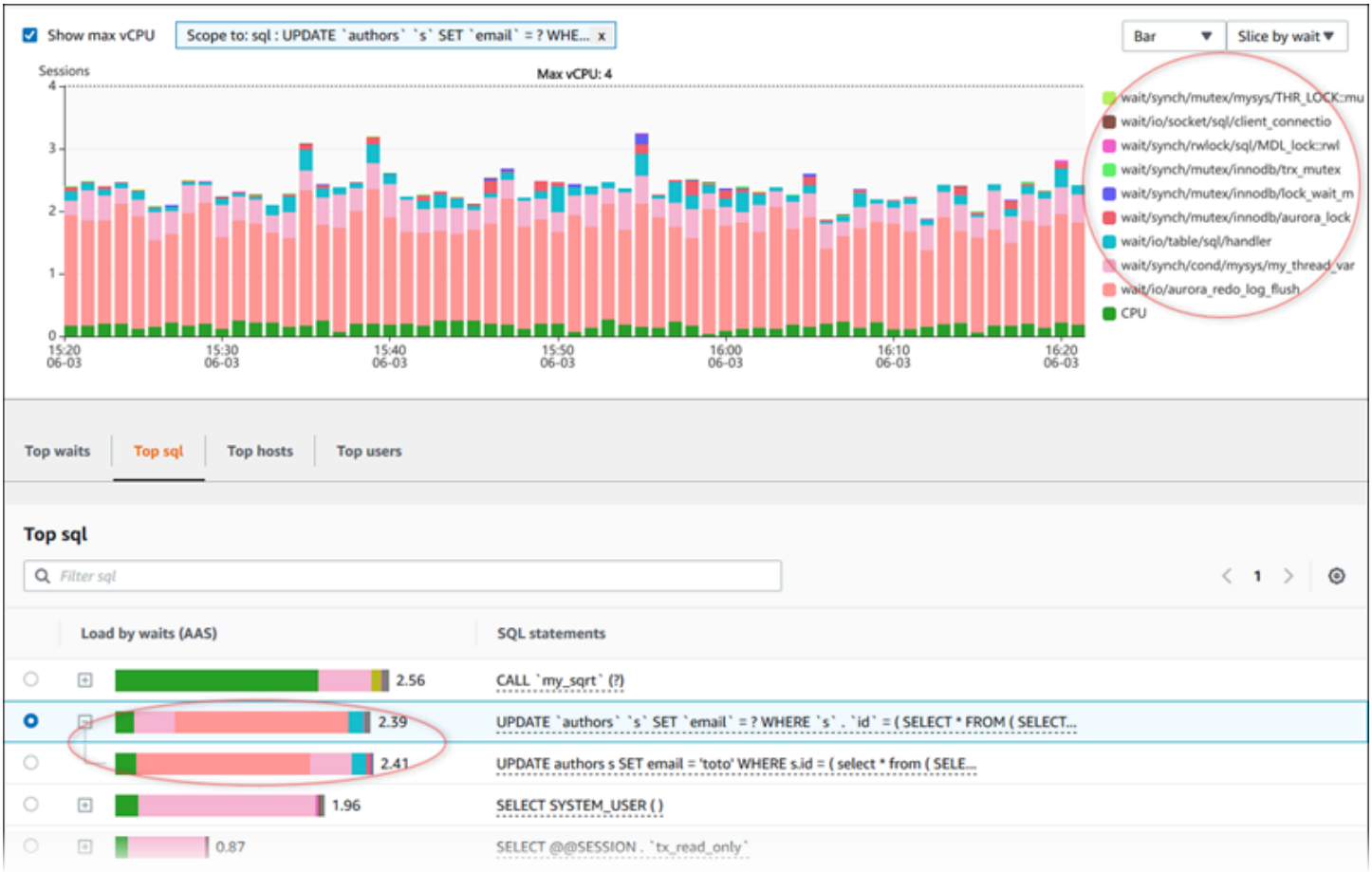
Eine Beschreibung der SQL-Statistiken für die Aurora-Engines finden Sie unter SQL-Statistiken für Performance Insights.

Nach Waits laden (AAS)

In Haupt-SQL veranschaulicht die Spalte Last nachWartezuständen (AAS) den Prozentsatz der Datenbanklast, die jedem Hauptlastelement zugeordnet ist. In dieser Spalte wird die Last für dieses

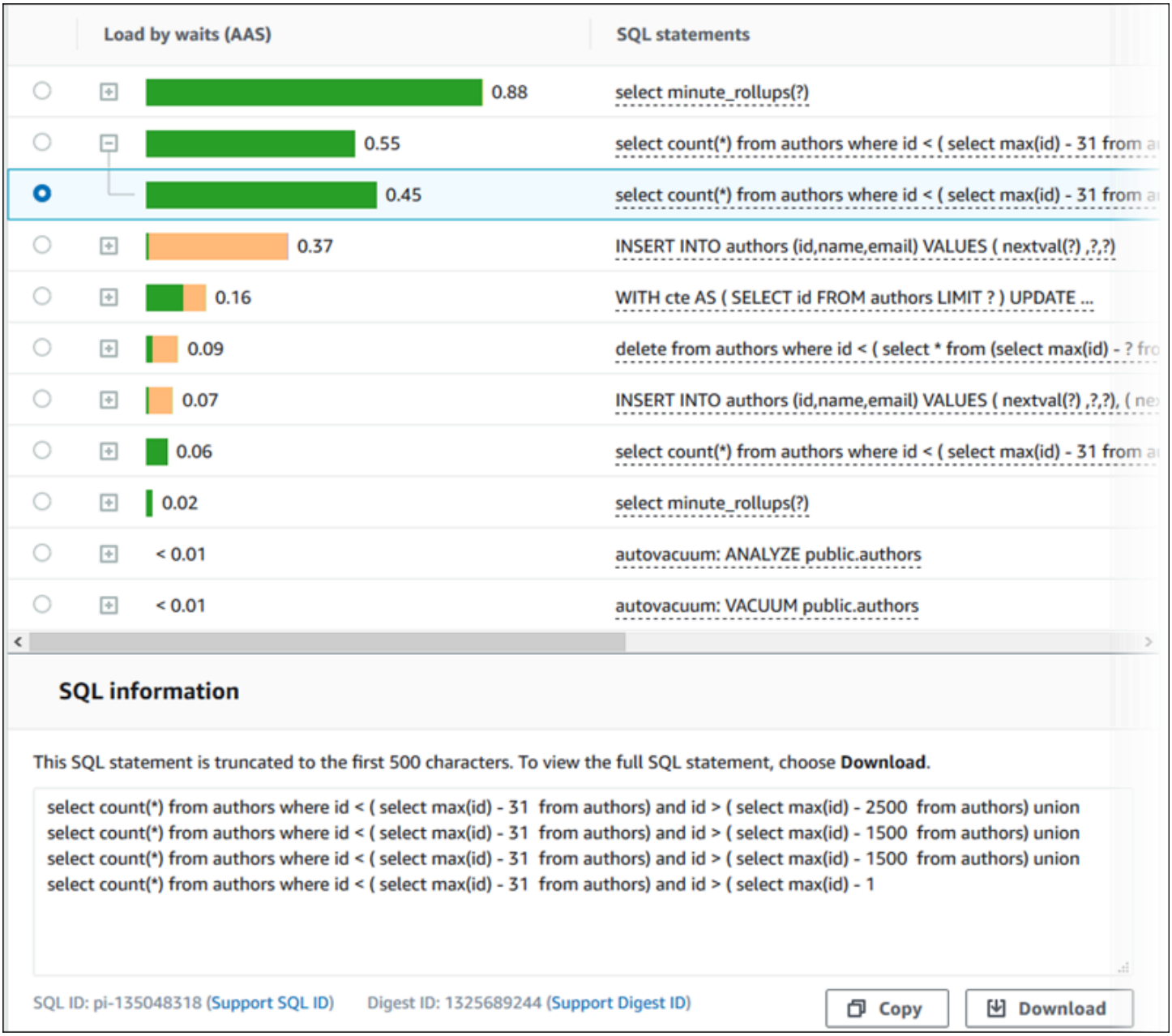
Element nach der aktuell im DB-Last-Diagramm ausgewählten Gruppierung wiedergegeben. Weitere Informationen zu durchschnittlichen aktiven Sitzungen (AAS) finden Sie unter Durchschnittliche aktive Sitzungen.

Beispielsweise können Sie das DB-Last-Diagramm nach Wartezuständen gruppieren. Sie untersuchen SQL-Abfragen in der Tabelle der Hauptlastelemente. In diesem Fall ist der Balken DB Load by Waits (DB-Last nach Wartezuständen) so groß, segmentiert und farbcodiert, dass angezeigt wird, zu wieviel Prozent diese Abfrage zum betreffenden Wartezustand beiträgt. Es zeigt zudem auf, welche Wartezustände sich auf die ausgewählte Abfrage auswirken.



SQL-Informationen

In der Tabelle Haupt-SQL können Sie eine Anweisung öffnen, um ihre Informationen anzuzeigen. Die Informationen werden im unteren Bereich angezeigt.

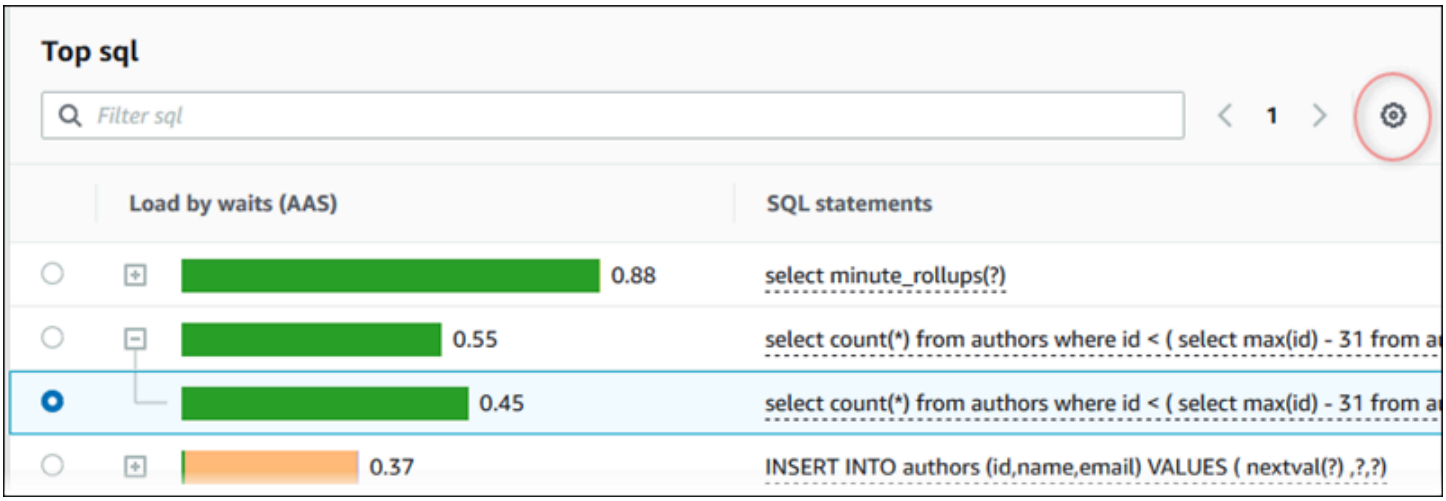


Auf der Registerkarte Haupt-SQL sehen Sie die folgenden ID-Typen, die SQL-Anweisungen zugeordnet sind:

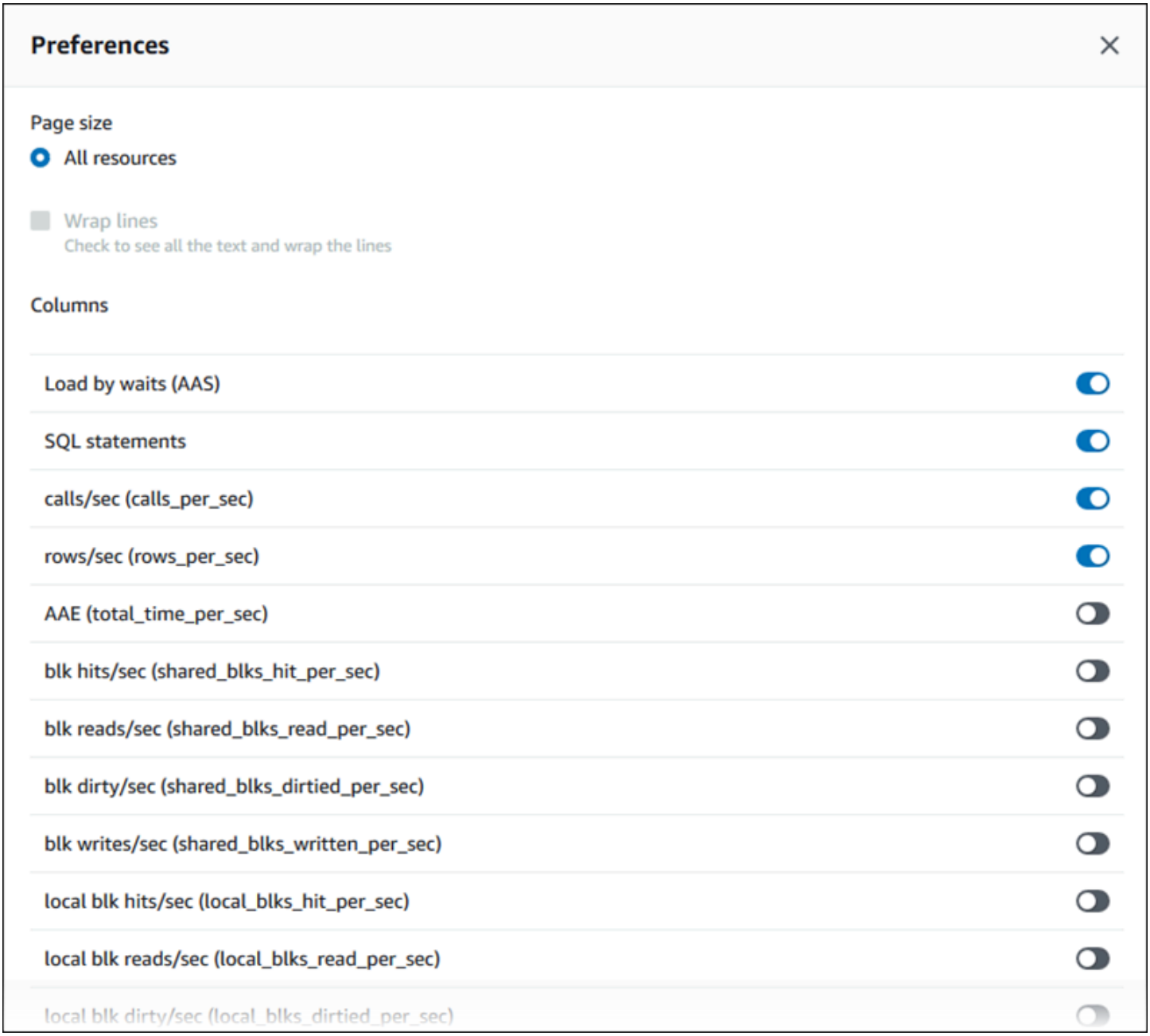
- Support-SQL-ID: ein Hash-Wert der SQL-ID Dieser Wert dient nur zum Verweisen auf eine SQL-ID, wenn Sie mit AWS Support arbeiten. AWS Der Support hat keinen Zugriff auf Ihre tatsächlichen SQL-IDs und SQL-Text.
- Support-Digest-ID: ein Hash-Wert der Digest-ID Dieser Wert dient nur zum Verweisen auf eine Digest-ID, wenn Sie mit AWS Support zusammenarbeiten. AWS Der Support hat keinen Zugriff auf Ihre tatsächlichen Digest-IDs und SQL-Text.

Präferenzen

Sie können die Statistiken steuern, die auf der Registerkarte Haupt-SQL angezeigt werden, indem Sie das Symbol Voreinstellungen auswählen.



Durch das Auswählen des Symbols Präferenzen wird das Fenster Präferenzen geöffnet. Der folgende Screenshot ist ein Beispiel für das Fenster Preferences (Präferenzen).



Aktivieren Sie die Statistiken, die auf der Registerkarte Haupt-SQL angezeigt werden sollen, führen Sie einen Bildlauf mit der Maus zum unteren Rand des Fensters durch und wählen Sie dann Weiter.

Weitere Informationen zu Statistiken pro Sekunde oder pro Aufruf für die Aurora-Engines finden Sie im Abschnitt der Engine-spezifischen SQL-Statistiken unter SQL-Statistiken für Performance Insights.

Zugriff auf mehr SQL-Text im Performance-Insights-Dashboard

Standardmäßig zeigt jede Zeile in der Tabelle Haupt-SQL für jede SQL-Anwendung 500 Byte SQL-Text an.

Wenn eine SQL-Anweisung 500 Byte überschreitet, können Sie mehr Text im SQL-Text-Abschnitt unterhalb der Haupt-SQL-Tabelle sehen. In diesem Fall beträgt die maximale Länge für den in SQL-Text angezeigten Text 4 KB. Dieses Limit wird von der Konsole eingeführt und unterliegt den von der Datenbank-Engine festgelegten Grenzwerten. Zum Speichern des in SQL-Text gezeigten Texts wählen Sie Herunterladen.

Themen

- Beschränkungen der Textgröße für Aurora MySQL
- Festlegen des SQL-Textlimits für Aurora PostgreSQL-DB-Instances
- Anzeigen und Herunterladen von SQL-Text im Performance-Insights-Dashboard

Beschränkungen der Textgröße für Aurora MySQL

Beim Herunterladen von SQL-Text bestimmt die Datenbank-Engine dessen maximale Länge. Sie können SQL-Text bis zu den folgenden Grenzwerten pro Engine herunterladen.

DB-Engine	Maximale Länge des heruntergeladenen Textes
Aurora MySQL	4,096 Bytes

Der SQL-Text-Abschnitt der Performance Insights-Konsole zeigt den maximalen Wert an, den die Engine zurückgibt. Wenn Aurora MySQL beispielsweise höchstens 1 KB an Performance Insights zurückgibt, kann es nur 1 KB sammeln und anzeigen, auch wenn die ursprüngliche Abfrage größer ist. Wenn Sie also die Abfrage in SQL-Text anzeigen oder herunterladen, gibt Performance Insights die gleiche Anzahl von Bytes zurück.

Wenn Sie die API AWS CLI oder verwenden, hat Performance Insights nicht das von der Konsole erzwungene Limit von 4 KB. `DescribeDimensionKeys`und `GetResourceMetrics` gibt höchstens 500 Byte zurück.

> **Note**
>
> `GetDimensionKeyDetails`gibt die vollständige Abfrage zurück, aber die Größe unterliegt dem Engine-Limit.

Festlegen des SQL-Textlimits für Aurora PostgreSQL-DB-Instances

Aurora PostgreSQL behandelt Text anders. Sie können die Textgrößenbeschränkung mit dem DB-Instance-Parameter `track_activity_query_size` festlegen. Dieser Parameter hat folgende Merkmale:

Standardtextgröße

In Aurora PostgreSQL Version 9.6 ist die Standardeinstellung für den `track_activity_query_size`-Parameter 1.024 Byte. In Aurora PostgreSQL Version 10 oder höher ist die Standardeinstellung 4.096 Byte.

Maximale Textgröße

Das Limit für `track_activity_query_size` ist 102.400 Bytes für Aurora PostgreSQL Version 12 und niedriger. Das Maximum beträgt 1 MB für Version 13 und höher.

Wenn die Engine 1 MB an Performance Insights zurückgibt, zeigt die Konsole nur die ersten 4 KB an. Wenn Sie die Abfrage herunterladen, erhalten Sie die gesamten 1 MB. In diesem Fall geben das Anzeigen und Herunterladen eine unterschiedliche Anzahl von Bytes zurück. Weitere Informationen über den DB-Instance Parameter `track_activity_query_size` finden Sie unter Laufzeitstatistik in der PostgreSQL-Dokumentation.

Um die SQL-Textgröße zu erhöhen, erhöhen Sie das `track_activity_query_size`-Limit. Um den Parameter zu ändern, ändern Sie die Parametereinstellung in der Parametergruppe, die der Aurora PostgreSQL-DB-Instance zugeordnet ist.

Ändern Sie die Einstellung wie folgt, wenn die Instance die Standardparametergruppe verwendet:

1. Erstellen Sie eine neue DB-Instance-Parametergruppe für die entsprechende DB-Engine und DB-Engine-Version.
2. Stellen Sie den Parameter in der neuen Parametergruppe ein.
3. Ordnen Sie die neue Parametergruppe der DB-Instance zu.

Informationen über das Einstellen eines DB-Instance-Parameters finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.

Anzeigen und Herunterladen von SQL-Text im Performance-Insights-Dashboard

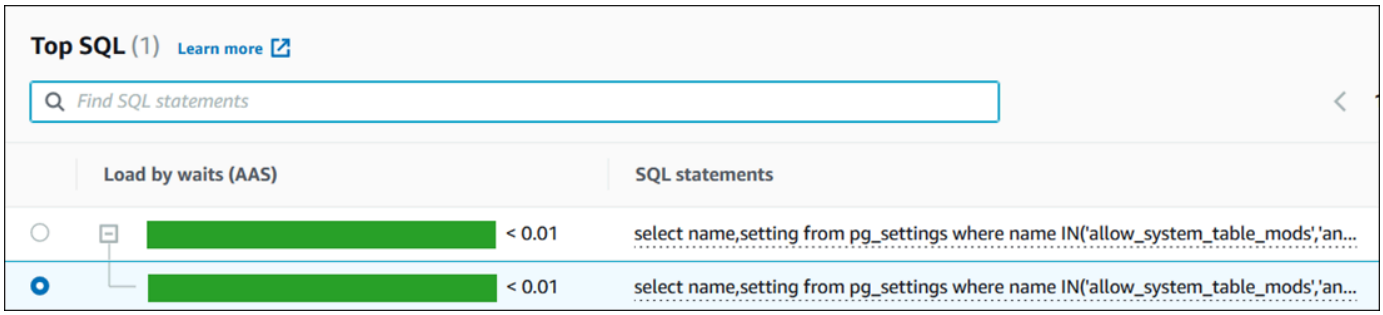
Im Performance-Insights-Dashboard können Sie SQL-Text anzeigen oder herunterladen.

So zeigen Sie mehr SQL-Text im Performance Insights-Dashboard an

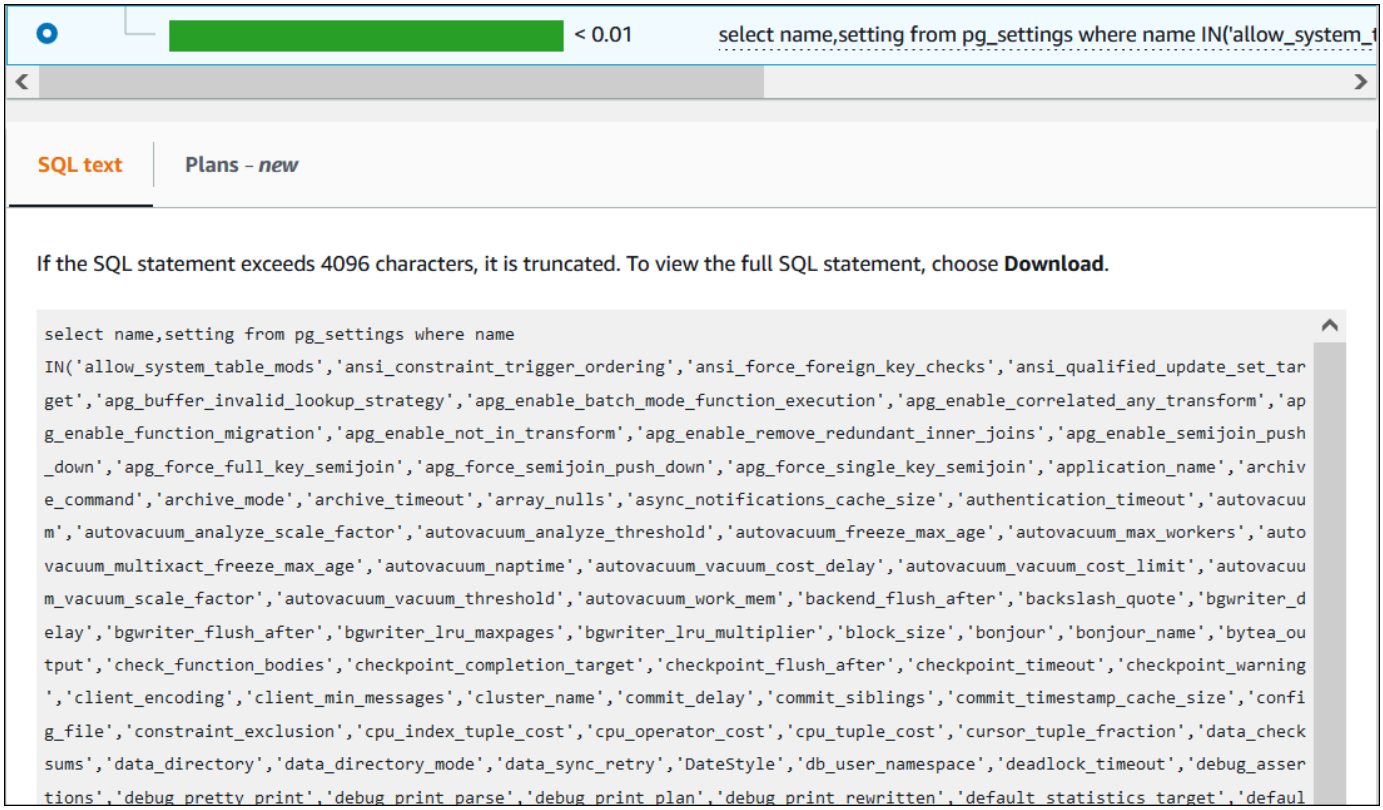
1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus.

   Das Performance-Insights-Dashboard wird für diese DB-Instance angezeigt.
4. Scrollen Sie nach unten zur Registerkarte Top SQL (Top-SQL).
5. Wählen Sie das Pluszeichen, um einen SQL-Digest zu erweitern, und wählen Sie eine der untergeordneten Abfragen des Digests aus.

   SQL-Anweisungen mit Text größer als 500 Byte sehen in etwa wie folgt aus.



6. Scrollen Sie nach unten zur Registerkarte SQL text (SQL-Text).



Das Performance Insights-Dashboard kann bis zu 4.096 Byte für jede SQL-Anweisung anzeigen.

7. (Optional) Wählen Sie Kopieren, um die angezeigte SQL-Anweisung zu kopieren, oder wählen Sie Herunterladen, um die SQL-Anweisung herunterzuladen, um den SQL-Text bis zum Limit der DB-Engine anzuzeigen.

> **Note**
>
> Um die SQL-Anweisung zu kopieren oder herunterzuladen, deaktivieren Sie Popup-Blocker.

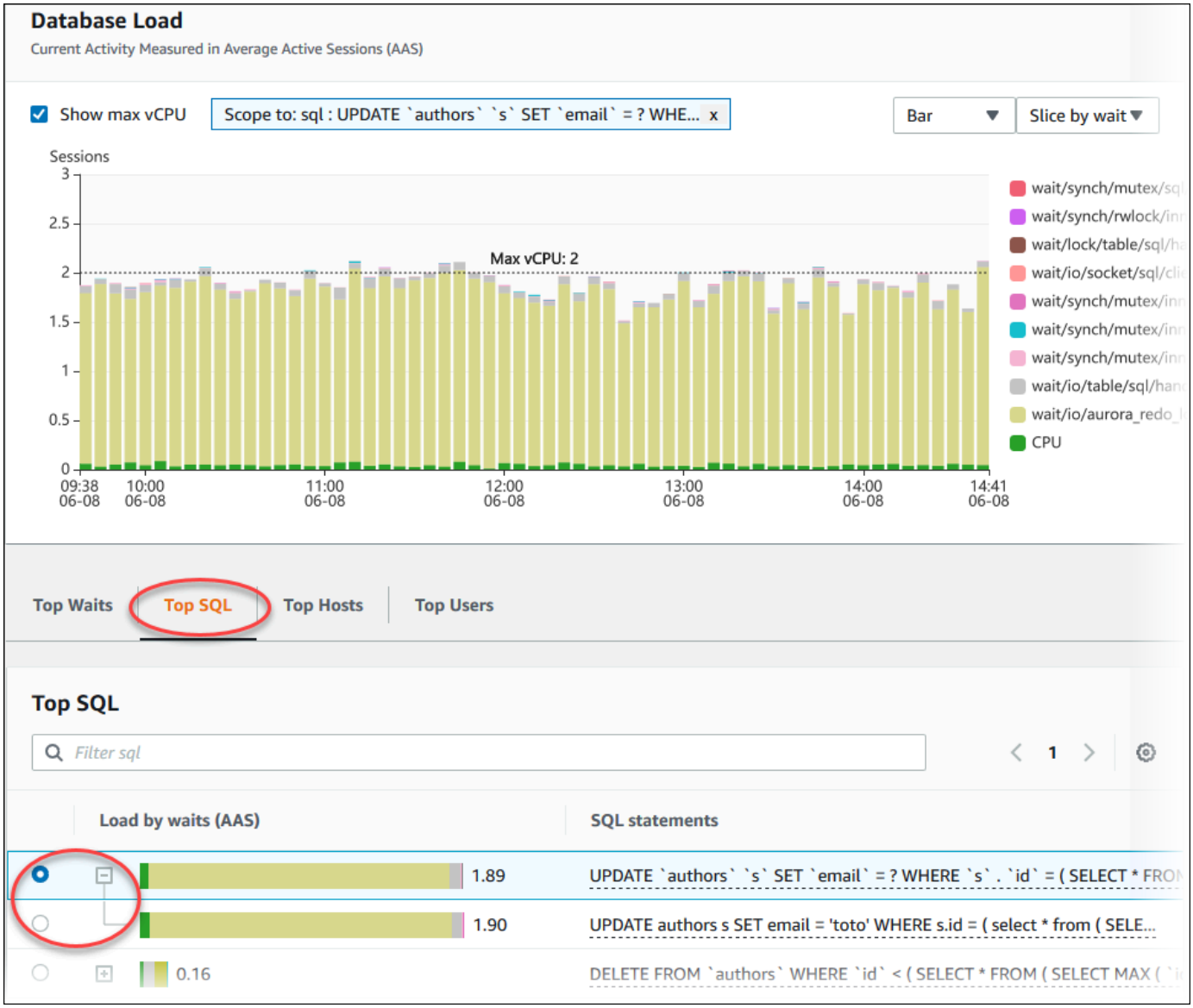
Anzeigen von SQL-Statistiken im Performance-Insights-Dashboard

Im Performance-Insights-Dashboard stehen SQL-Statistiken auf dem Tab Top SQL (Haupt-SQL) des Diagramms Database load (Datenbanklast) zur Verfügung.

Sehen Sie sich SQL-Statistiken wie folgt an

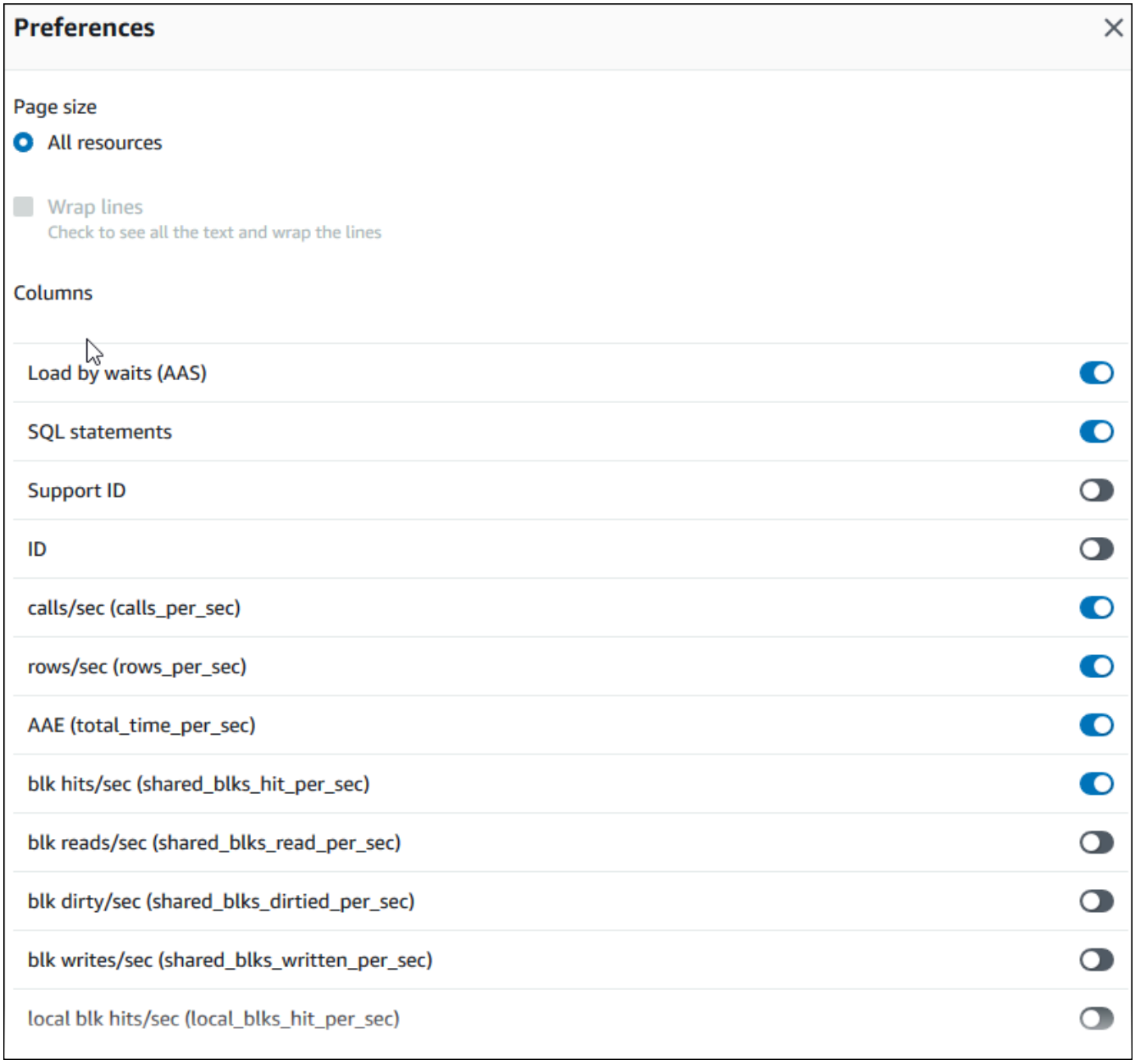
1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im linken Navigationsbereich Performance Insights aus.

3. Wählen Sie oben auf der Seite die Datenbank aus, deren SQL-Statistiken Sie anzeigen lassen möchten.
4. Scrollen Sie an das Seitenende und klicken Sie auf den Tab Top SQL (Haupt-SQL).
5. Wählen Sie eine individuelle Anweisung (nur Aurora MySQL) oder Digest-Abfrage aus.

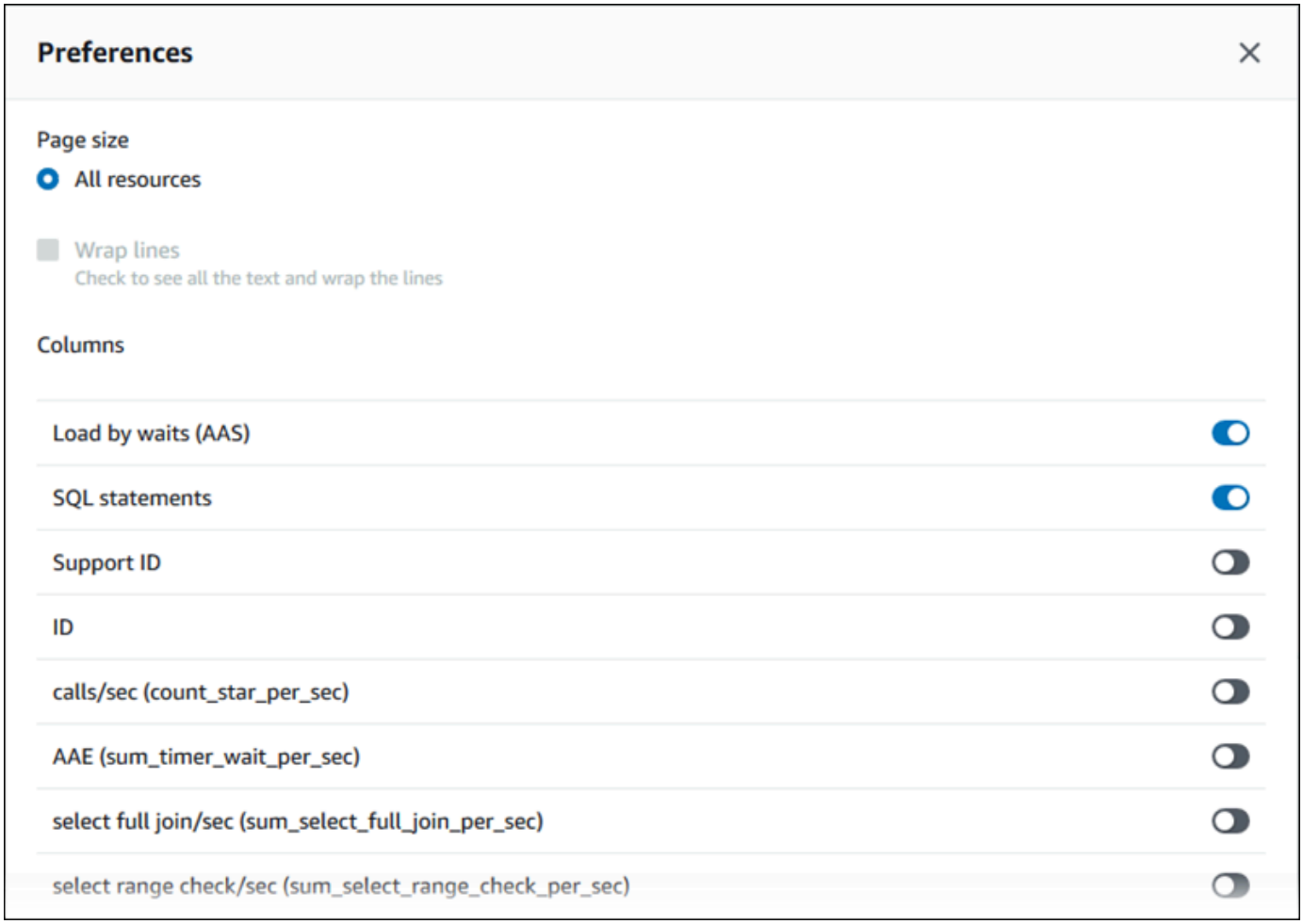


6. Sie können die Statistiken auswählen, die angezeigt werden sollen, indem Sie oben rechts im Diagramm das Zahnradsymbol auswählen. Beschreibungen der SQL-Statistiken für die Amazon RDSAurora-Engines finden Sie unter SQL-Statistiken für Performance Insights.

   Das folgende Beispiel zeigt die Einstellungen für Aurora PostgreSQL.



Das folgende Beispiel zeigt die Einstellungen für Aurora MySQL-DB-Instances.



7. Wählen Sie „Save“ (Speichern) aus, um Ihre Einstellungen zu speichern.

   Die Tabelle Top SQL (Haupt-SQL) wird aktualisiert.

Anzeigen proaktiver Empfehlungen für Performance Insights

Amazon RDS Performance Insights überwacht bestimmte Metriken und erstellt automatisch Schwellenwerte, indem analysiert wird, welche Stufen für eine bestimmte Ressource potenziell problematisch sein könnten. Wenn die neuen Metrikwerte über einen bestimmten Zeitraum einen vordefinierten Schwellenwert überschreiten, generiert Performance Insights eine proaktive Empfehlung. Diese Empfehlung trägt dazu bei, zukünftige Auswirkungen auf die Datenbankleistung zu vermeiden. Um diese proaktiven Empfehlungen zu erhalten, müssen Sie Performance Insights mit einem Aufbewahrungszeitraum für kostenpflichtige Stufen aktivieren.

Weitere Informationen zum Aktivieren von Performance Insights finden Sie unter Performance Insights für Aurora ein- und ausschalten. Informationen zu Preisen und zur Datenaufbewahrung für

Performance Insights finden Sie unter Preisgestaltung und Datenaufbewahrung für Performance-Insights.

Informationen zu den Regionen, DB-Engines und Instance-Klassen, die für die proaktiven Empfehlungen unterstützt werden, finden Sie unter DB-Engine-, Regions- und Instance-Klassenunterstützung von Amazon Aurora für Performance-Insights-Funktionen.

Sie können die detaillierte Analyse und die empfohlenen Untersuchungen proaktiver Empfehlungen auf der Seite mit den Empfehlungsdetails einsehen.

Weitere Informationen zu Empfehlungen finden Sie unter Anzeigen und Beantworten von Amazon-Aurora-Empfehlungen.

So zeigen Sie die detaillierte Analyse einer proaktiven Empfehlung an

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Führen Sie im Navigationsbereich einen der folgenden Schritte aus:

   - Wählen Sie Empfehlungen aus.

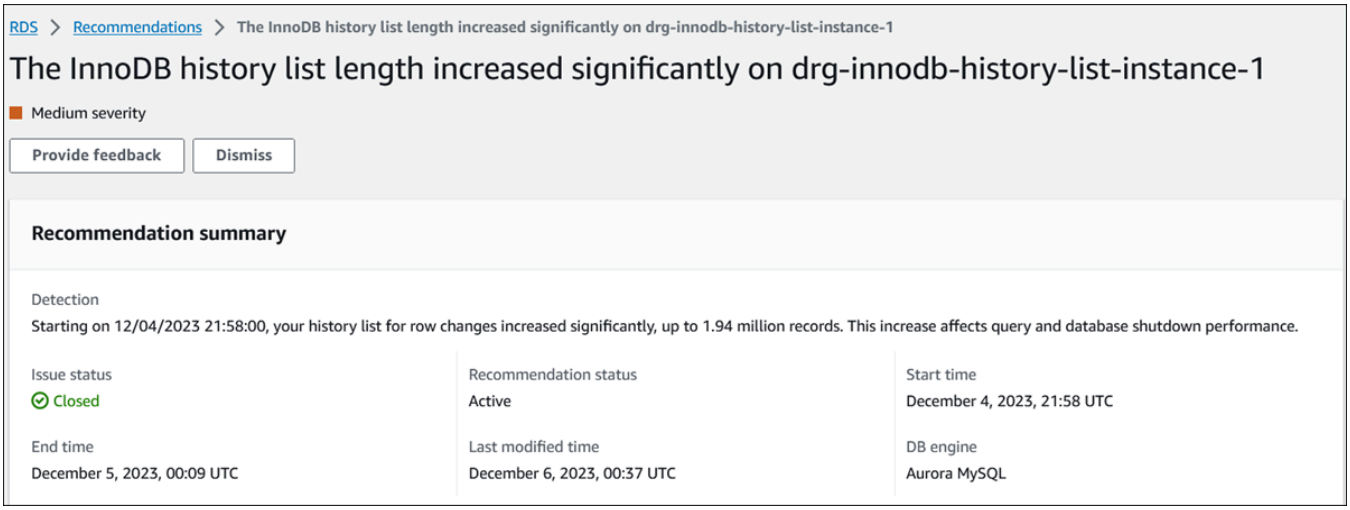
     Auf der Seite Empfehlungen wird eine Liste von Empfehlungen angezeigt, sortiert nach dem Schweregrad für alle Ressourcen in Ihrem Konto.
   - Wählen Sie Datenbanken und dann Empfehlungen für eine Ressource auf der Datenbankseite aus.

     Auf der Registerkarte Empfehlungen werden die Empfehlungen und ihre Details für die ausgewählte Ressource angezeigt.
3. Suchen Sie eine proaktive Empfehlung und wählen Sie Details anzeigen aus.

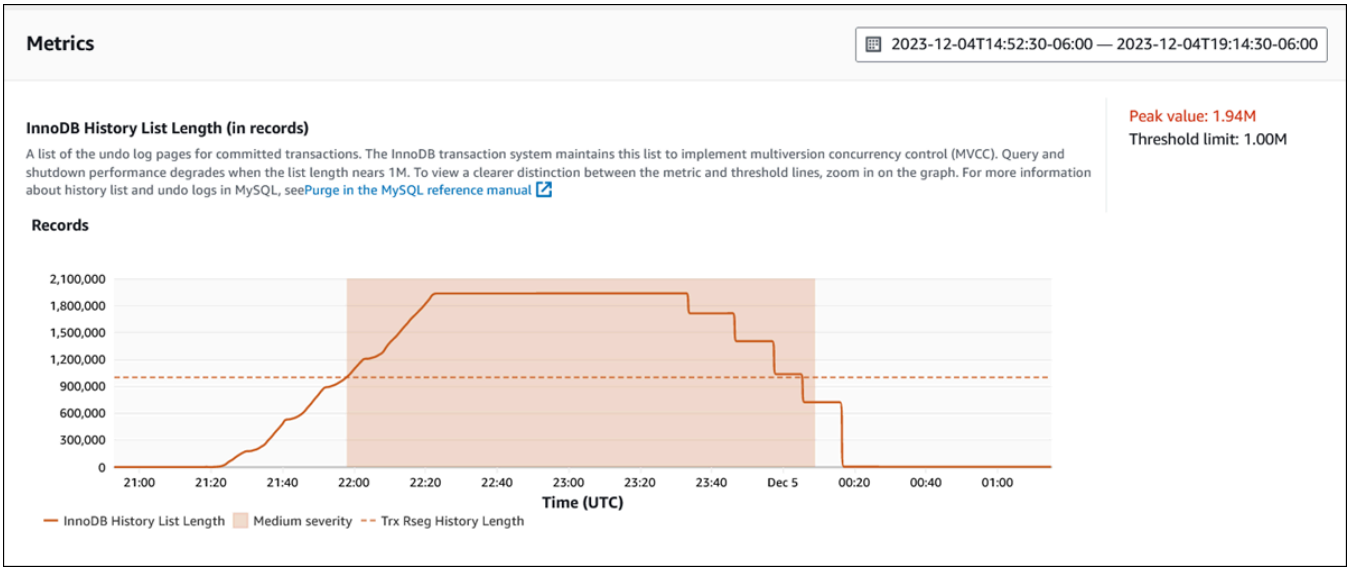
   Die Seite mit den Empfehlungsdetails wird angezeigt. Der Titel enthält den Namen der betroffenen Ressource mit dem erkannten Problem und dem Schweregrad.

   Im Folgenden sind die Komponenten auf der Seite mit den Empfehlungsdetails aufgeführt:

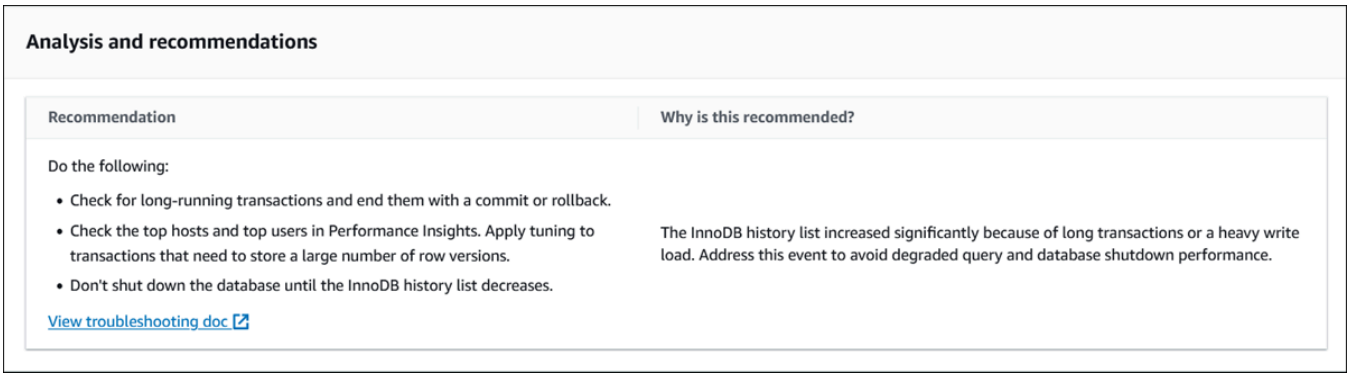
   - Zusammenfassung der Empfehlung – Das erkannte Problem, der Empfehlungs- und Problemstatus, die Start- und Endzeit des Problems, die geänderte Zeit der Empfehlung und der Engine-Typ.



- Metriken – Die Diagramme des erkannten Problems. Jedes Diagramm zeigt einen Schwellenwert an, der durch das Basisverhalten der Ressource und die Daten der Metrik bestimmt wird, die von der Startzeit des Problems gemeldet wurde.



- Analyse und Empfehlungen – Die Empfehlung und der Grund für die vorgeschlagene Empfehlung.



Sie können die Ursache des Problems überprüfen und dann die vorgeschlagenen empfohlenen Maßnahmen ergreifen, um das Problem zu beheben, oder oben rechts Verwerfen wählen, um die Empfehlung zu verwerfen.

Metriken mit der Performance Insights API für Aurora abrufen

Wenn Performance Insights aktiviert ist, bietet die API Einblicke in die Instance-Leistung. Amazon CloudWatch Logs bietet die maßgebliche Quelle für verkaufte Monitoring-Metriken für AWS Services.

Performance Insights bietet eine domänenspezifische Ansicht der Datenbanklast, gemessen als durchschnittliche aktive Sitzungen (AAS). Diese Metrik erscheint API-Verbrauchern als zweidimensionaler Zeitreihendatensatz. Die Zeitdimension der Daten stellt die Datenbanklastdaten für jeden Zeitpunkt im abgefragten Zeitraum bereit. Für jeden Zeitpunkt wird die Gesamtlast bezogen auf die angeforderten Dimensionen zerlegt, z. B. `SQL`, `Wait-event`, `User` oder `Host`, gemessen zum betreffenden Zeitpunkt.

Amazon RDS Performance Insights überwacht Ihren , damit Sie die Datenbankleistung analysieren und beheben können. Eine Möglichkeit zum Anzeigen von Performance Insights-Daten bietet die AWS Management Console. Performance Insights stellt außerdem eine öffentliche API bereit, sodass Sie Ihre eigenen Daten abfragen können. Sie können die API für Folgendes verwenden:

- Auslagern von Daten in eine Datenbank
- Hinzufügen von Performance Insights-Daten zu bestehenden Überwachungs-Dashboards
- Entwickeln von Überwachungstools

Zum Verwenden der Performance Insights-API aktivieren Sie Performance Insights auf einer Ihrer Amazon RDS-DB-Instances. Weitere Informationen zum Aktivieren von Performance Insights finden Sie unter Performance Insights für Aurora ein- und ausschalten. Weitere Informationen zur Performance Insights-API finden Sie in der Referenz zur Amazon RDS Performance Insights-API.

Die Performance Insights-API bietet die folgenden Operationen.

Performance-Insights-Aktion	AWS CLI Befehl	Beschreibung
CreatePerformanceAnalysisReport	aws pi create-performance-analysis-report	Erstellt einen Leistungsanalysebericht für die DB-Instance für einen bestimmten Zeitraum. Das Ergebnis lautet `AnalysisReportId`. Dies ist der eindeutige Bezeichner des Berichts.
DeletePerformanceAnalysisReport	aws pi delete-performance-analysis-report	Löscht einen Leistungsanalysebericht.
DescribeDimensionKeys	aws pi describe-dimension-keys	Ruft die Schlüssel der Top N-Dimension für eine Metrik für einen bestimmten Zeitraum ab.
GetDimensionKeyDetails	aws pi get-dimension-key-details	Ruft die Attribute der angegebenen Dimensionsgruppe für eine DB-Instance oder Datenquelle ab. Wenn Sie beispielsweise eine SQL-ID angeben und die Dimensionsdetails sind verfügbar, ruft `GetDimensionKeyDetails` den Volltext der Dimension `db.sql.statement` ab, die mit dieser ID verknüpft ist. Dieser Vorgang ist nützlich, da `GetResourceMetrics` und `DescribeDimensionKeys` das Abrufen von umfangreichen SQL-Anweisungen nicht unterstützt.

Performance-Insights-Aktion	AWS CLI Befehl	Beschreibung
GetPerformanceAnalysisReport	aws pi get-performance-analysis-report	Ruft den Bericht einschließlich der Erkenntnisse für den Bericht ab. Das Ergebnis umfasst den Berichtsstatus, die Berichts-ID, Details zum Berichtszeitpunkt, Erkenntnisse und Empfehlungen.
GetResourceMetadata	aws pi get-resource-metadata	Rufen Sie die Metadaten für verschiedene Funktionen ab. Die Metadaten könnten beispielsweise darauf hindeuten, dass eine Funktion für eine bestimmte DB-Instance ein- oder ausgeschaltet ist.
GetResourceMetrics	aws pi get-resource-metrics	Ruft Performance Insights-Metriken für eine Reihe von Datenquellen über einen Zeitraum ab. Sie können spezifische Dimensionsgruppen und Dimensionen bereitstellen und Aggregation und Filterkriterien für jede Gruppe bereitstellen.
ListAvailableResourceDimensions	aws pi list-available-resource-dimensions	Rufen Sie die Dimensionen ab, die für jeden angegebenen Metriktyp für eine bestimmte Instance abgefragt werden können.

Performance-Insights-Aktion	AWS CLI Befehl	Beschreibung
ListAvailableResourceMetrics	aws pi list-available-resource-metrics	Rufen Sie alle verfügbaren Metriken der angegebenen Metriktypen ab, die für eine bestimmte DB-Instance abgefragt werden können.
ListPerformanceAnalysisReports	aws pi list-performance-analysis-reports	Ruft alle Analyseberichte ab, die für die DB-Instance verfügbar sind. Die Berichte werden auf der Grundlage der Startzeit jedes Berichts aufgelistet.
ListTagsForResource	aws pi list-tags-for-resource	Listet alle Metadaten-Tags auf, die der Ressource hinzugefügt wurden. Die Liste enthält den Namen und den Wert des Tags.
TagResource	aws pi tag-resource	Fügt einer Amazon-RDS-Ressource Metadaten-Tags hinzu. Das Tag enthält einen Namen und einen Wert.
UntagResource	aws pi untag-resource	Entfernt die Metadaten-Tags von der Ressource.

Themen

- AWS CLI für Performance Insights
- Abrufen von Zeitreihenmetriken
- AWS CLI Beispiele für Performance Insights

AWS CLI für Performance Insights

Sie können Performance Insights-Daten über die anzeige AWS CLI. Sie können die Hilfe zu den AWS CLI Befehlen für Performance Insights anzeigen, indem Sie in der Befehlszeile Folgendes eingeben.

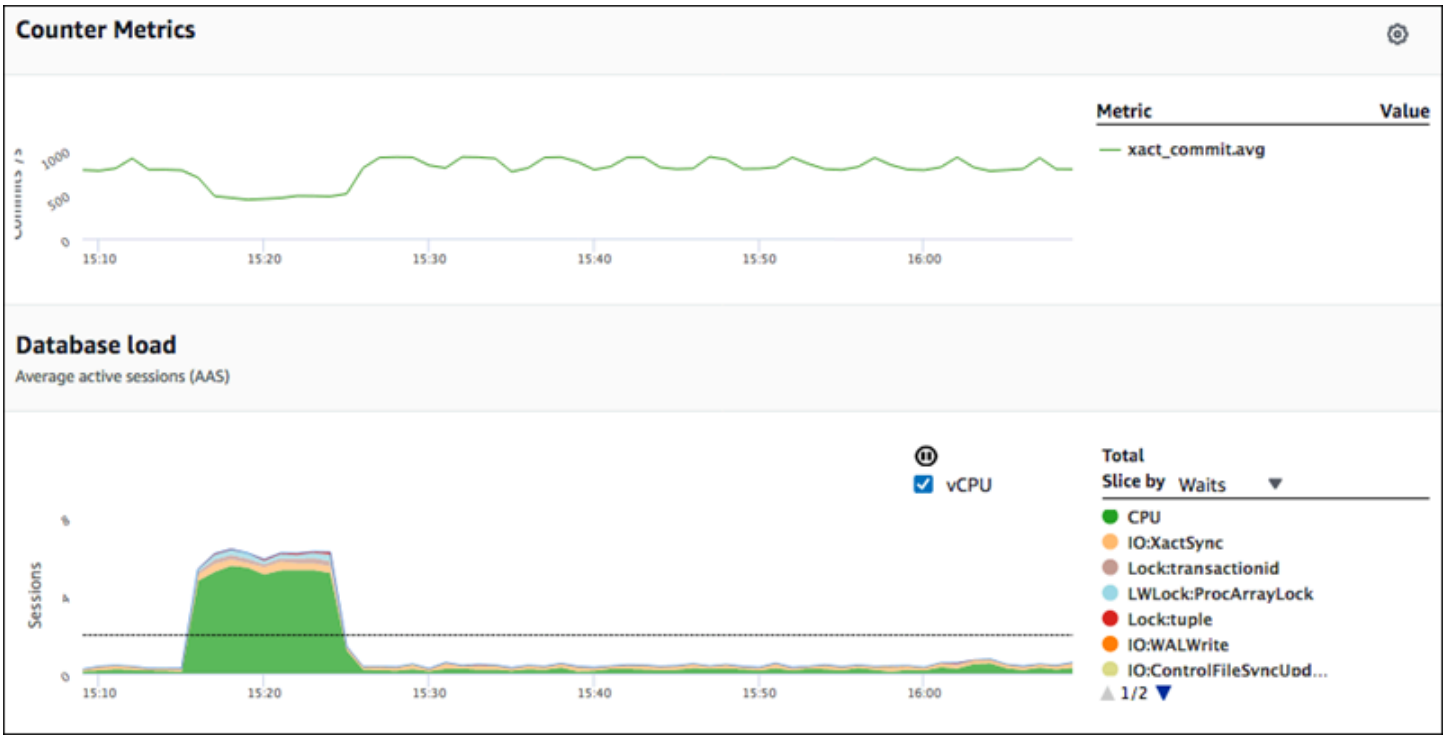
```
aws pi help
```

Falls Sie das nicht AWS CLI installiert haben, finden Sie unter Installation von AWS CLI im AWS CLI Benutzerhandbuch weitere Informationen zur Installation.

Abrufen von Zeitreihenmetriken

Mit der `GetResourceMetrics`-Operation werden ein oder mehrere Zeitreihenmetriken aus den Performance Insights-Daten abgerufen. Für `GetResourceMetrics` ist eine Metrik und ein Zeitraum erforderlich, damit eine Antwort mit einer Liste von Datenpunkten zurückgegeben wird.

Zum Beispiel die Benutzer, AWS Management Console `GetResourceMetrics` um die Diagramme „Counter Metrics“ und „Database Load“ auszufüllen, wie in der folgenden Abbildung dargestellt.



Alle von zurückgegebenen Metriken`GetResourceMetrics` sind Standard-Zeitreihenmetriken, mit Ausnahme von`db.load`. Diese Metrik wird im Diagramm Database Load (Datenbanklast)

angezeigt. Die`db.load` Metrik unterscheidet sich von den anderen Zeitreihenmetriken, da Sie sie in Unterkomponenten aufteilen können, die als Dimensionen bezeichnet werden. In der vorherigen Abbildung wird `db.load` unterteilt und nach Wartezuständen gruppiert, aus denen `db.load` besteht.

> **Note**
>
> `GetResourceMetrics` kann auch die `db.sampleload`-Metrik zurückgeben, aber die `db.load`-Metrik ist in den meisten Fällen angemessen.

Informationen zu den Zählermetriken, die von `GetResourceMetrics` zurückgegeben werden, finden Sie unter Performance-Insights-Zählermetriken.

Die folgenden Berechnungen werden für die Metriken unterstützt:

- Durchschnitt – Der durchschnittliche Wert für die Metrik über einen bestimmten Zeitraum. Fügen Sie dem Metriknamen `.avg` an.
- Minimum – Der minimale Wert für die Metrik über einen bestimmten Zeitraum. Fügen Sie dem Metriknamen `.min` an.
- Maximum – Der maximale Wert für die Metrik über einen bestimmten Zeitraum. Fügen Sie dem Metriknamen `.max` an.
- Summe – Die Summe der Metrikwerte über einen bestimmten Zeitraum. Fügen Sie dem Metriknamen `.sum` an.
- Beispielanzahl – Die Anzahl, wie oft die Metrik über einen bestimmten Zeitraum erfasst wurde. Fügen Sie dem Metriknamen `.sample_count` an.

Nehmen wir an, dass eine Metrik beispielsweise 300 Sekunden (5 Minuten) lang erfasst wird und dass die Metrik einmal pro Minute erfasst wird. Die Werte für jede Minute sind 1, 2, 3, 4 und 5. In diesem Fall werden die folgenden Berechnungen zurückgegeben:

- Durchschnitt – 3
- Minimum – 1
- Maximum – 5
- Summe – 15
- Beispielanzahl – 5

Hinweise zur Verwendung des `get-resource-metrics` AWS CLI Befehls finden Sie unter `get-resource-metrics`.

Geben Sie für die `--metric-queries`-Option eine oder mehrere Abfragen an, um die entsprechenden Ergebnisse zu erhalten. Jede Abfrage besteht aus einem obligatorischen `Metric`- sowie optionalen `GroupBy`- und `Filter`-Parametern. Es folgt ein Beispiel für eine Spezifikation der `--metric-queries`-Option.

```
{
   "Metric": "string",
   "GroupBy": {
     "Group": "string",
     "Dimensions": ["string", ...],
     "Limit": integer
   },
   "Filter": {"string": "string"
     ...}
```

AWS CLI Beispiele für Performance Insights

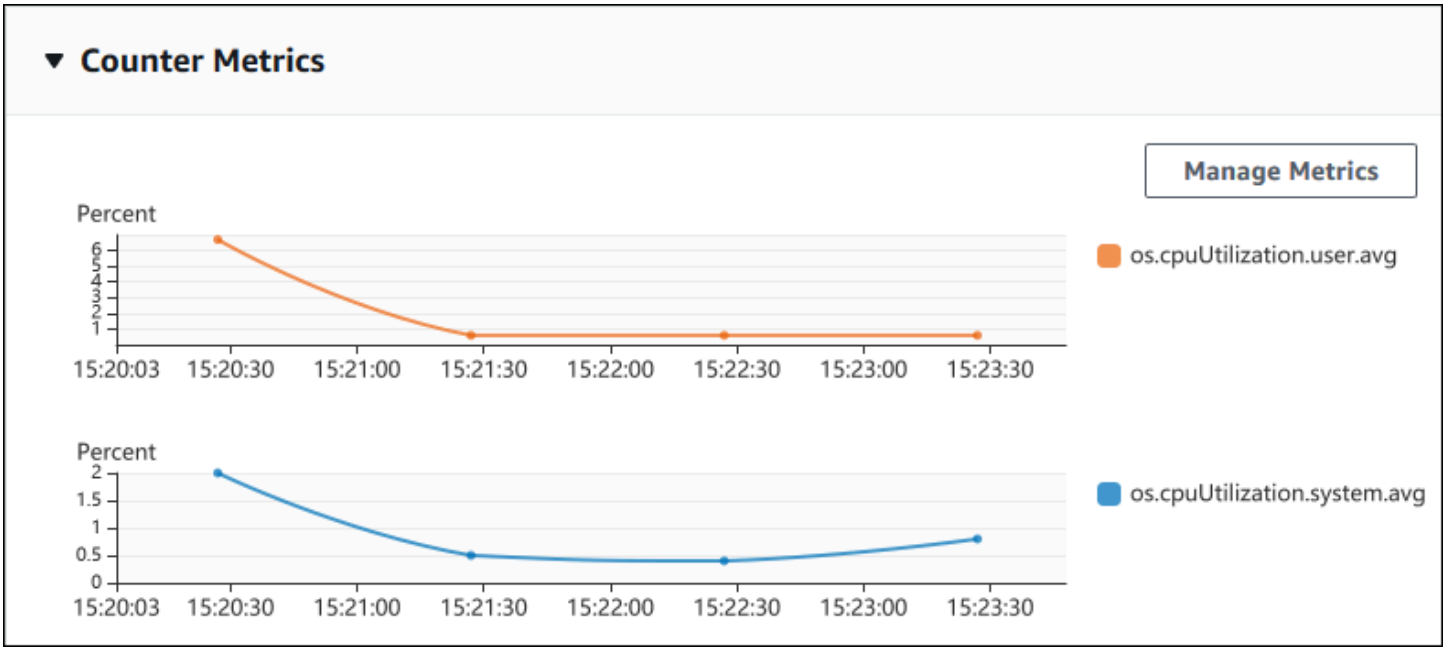
Die folgenden Beispiele zeigen, wie Sie AWS CLI for Performance Insights verwenden können.

Themen

- Abrufen von Zählermetriken
- Abrufen des DB-Lastdurchschnitts für Top-Warteereignisse
- Abrufen des DB-Lastdurchschnitts für Top-SQL-Anweisungen
- Abrufen des nach SQL gefilterten DB-Lastdurchschnitts
- Abrufen des Volltextes einer SQL-Anweisung
- Erstellen eines Leistungsanalyseberichts für einen bestimmten Zeitraum
- Abrufen eines Leistungsanalyseberichts
- Auflisten aller Leistungsanalyseberichte für die DB-Instance
- Löschen eines Leistungsanalyseberichts
- Hinzufügen eines Tags zu einem Leistungsanalysebericht
- Auflisten aller Tags für einen Leistungsanalysebericht
- Löschen der Tags eines Leistungsanalyseberichts

Abrufen von Zählermetriken

Der folgende Screenshot zeigt zwei Zählermetriken-Diagramme in der AWS Management Console.



Das folgende Beispiel zeigt, wie dieselben Daten erfasst werden, die zur Generierung der beiden Zählermetrikdiagramme AWS Management Console verwendet werden.

Für LinuxmacOS, oderUnix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-30T00:00:00Z \
   --end-time   2018-10-30T01:00:00Z \
   --period-in-seconds 60 \
   --metric-queries '[{"Metric": "os.cpuUtilization.user.avg"  },
                      {"Metric": "os.cpuUtilization.idle.avg"}]'
```

Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-30T00:00:00Z ^
   --end-time   2018-10-30T01:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries '[{"Metric": "os.cpuUtilization.user.avg"  },
```

```
                    {"Metric": "os.cpuUtilization.idle.avg"}]'
```

Sie können einen Befehl besser lesbar gestalten, indem Sie eine Datei für die Option `--metrics-query` angeben. Im folgenden Beispiel wird eine Datei namens query.json für die Option verwendet. Die Datei enthält Folgendes.

```
[
    {
        "Metric": "os.cpuUtilization.user.avg"
    },
    {
        "Metric": "os.cpuUtilization.idle.avg"
    }
]
```

Führen Sie den folgenden Befehl aus, um die Datei zu verwenden.

Für LinuxmacOS, oderUnix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-30T00:00:00Z \
   --end-time   2018-10-30T01:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-30T00:00:00Z ^
   --end-time   2018-10-30T01:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

Das vorige Beispiel gibt die folgenden Werte für die Optionen an:

- `--service-type` – RDS für Amazon RDS
- `--identifier` – Die Ressource-ID für die DB-Instance

- `--start-time` und `--end-time` – Die ISO 8601-Werte `DateTime` für den abzufragenden Zeitraum mit mehreren unterstützten Formaten

Der Abfragezeitraum beträgt eine Stunde:

- `--period-in-seconds` – `60` für eine Abfrage pro Minute
- `--metric-queries` – Ein Array mit zwei Abfragen, jeweils für nur eine Metrik.

  Der Metrikname verwendet Punkte, um die Metrik in eine sinnvolle Kategorie einzustufen, wobei das letzte Element eine Funktion ist. Im Beispiel lautet die Funktion `avg` für jede Abfrage. Wie bei Amazon CloudWatch sind die unterstützten Funktionen `min`, `max`, `total`, und `avg`.

Die Antwort sieht in etwa so aus:

```
{
    "Identifier": "db-XXX",
    "AlignedStartTime": 1540857600.0,
    "AlignedEndTime": 1540861200.0,
    "MetricList": [
        { //A list of key/datapoints
            "Key": {
                "Metric": "os.cpuUtilization.user.avg" //Metric1
            },
            "DataPoints": [
                //Each list of datapoints has the same timestamps and same number of
 items
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 4.0
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 4.0
                },
                {
                    "Timestamp": 1540857780.0, //Minute 3
                    "Value": 10.0
                }
                //... 60 datapoints for the os.cpuUtilization.user.avg metric
            ]
        },
```

```
        {
            "Key": {
                "Metric": "os.cpuUtilization.idle.avg" //Metric2
            },
            "DataPoints": [
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 12.0
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 13.5
                },
                //... 60 datapoints for the os.cpuUtilization.idle.avg metric
            ]
        }
    ] //end of MetricList
} //end of response
```

Die Antwort enthält Werte für `Identifier`, `AlignedStartTime` und `AlignedEndTime`. Bei einem `--period-in-seconds`-Wert von `60` wurden Start- und Endzeiten auf die Minute ausgerichtet. Wenn der `--period-in-seconds`-Wert `3600` lautet, werden Start- und Endzeiten auf die Stunde ausgerichtet.

Die `MetricList` in der Antwort enthält eine Reihe von Einträgen, und zwar jeweils mit einem `Key`- und einem `DataPoints`-Eintrag. Jeder `DataPoint` verfügt über einen `Timestamp` und einen `Value`. Jede `Datapoints`-Liste enthält 60 Datenpunkte, da die Abfragen eine Stunde lang jede Minute Daten abfragen, und zwar mit den Werten `Timestamp1/Minute1`, `Timestamp2/Minute2` usw. bis `Timestamp60/Minute60`.

Da sich die Abfrage auf zwei verschiedene Zählermetriken bezieht, enthält die -Antwort zwei Element `MetricList`.

Abrufen des DB-Lastdurchschnitts für Top-Warteereignisse

Das folgende Beispiel ist dieselbe Abfrage, die AWS Management Console verwendet wird, um ein gestapeltes Flächenliniendiagramm zu generieren. Mit diesem Beispiel wird der `db.load.avg`-Wert für die letzte Stunde abgerufen, wobei die Last auf die sieben Top-Warteereignisse aufgeteilt ist. Der Befehl ist mit dem Befehl unter identisc Abrufen von Zählermetriken. Die Datei query.json enthält hingegen Folgendes.

```
[
```

```
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_event", "Limit": 7 }
    }
]
```

Führen Sie den folgenden Befehl aus.

Für LinuxmacOS, oderUnix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-30T00:00:00Z \
   --end-time   2018-10-30T01:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-30T00:00:00Z ^
   --end-time   2018-10-30T01:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

Das Beispiel gibt die Metrik `db.load.avg` und eine `GroupBy`-Sortierung der sieben Top-Warteereignisse an. Einzelheiten zu gültigen Werten für dieses Beispiel finden Sie DimensionGroupin der Performance Insights API-Referenz.

Die Antwort sieht in etwa so aus:

```
{
    "Identifier": "db-XXX",
    "AlignedStartTime": 1540857600.0,
    "AlignedEndTime": 1540861200.0,
    "MetricList": [
        { //A list of key/datapoints
            "Key": {
                //A Metric with no dimensions. This is the total db.load.avg
```

```
                "Metric": "db.load.avg"
            },
            "DataPoints": [
                //Each list of datapoints has the same timestamps and same number of
items
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 0.5166666666666667
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 0.38333333333333336
                },
                {
                    "Timestamp": 1540857780.0, //Minute 3
                    "Value": 0.26666666666666666
                }
                //... 60 datapoints for the total db.load.avg key
            ]
        },
        {
            "Key": {
                //Another key. This is db.load.avg broken down by CPU
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.name": "CPU",
                    "db.wait_event.type": "CPU"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 0.35
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 0.15
                },
                //... 60 datapoints for the CPU key
            ]
        },
        //... In total we have 8 key/datapoints entries, 1) total, 2-8) Top Wait Events
    ] //end of MetricList
```

```
} //end of response
```

In dieser Antwort gibt es acht Einträge in der `MetricList`. Davon bezieht sich ein Eintrag auf den `db.load.avg`-Gesamtwert und sieben Einträge jeweils auf den `db.load.avg`-Wert, der auf eines der sieben Top-Warteereignisse aufgeteilt ist. Im Gegensatz zum ersten Beispiel, bei dem eine Gruppierungsdimension vorlag, muss für jede Gruppierung der Metrik ein Schlüssel vorliegen. Für jede Metrik kann nicht nur ein Schlüssel vorhanden sein, wie im Anwendungsfall der Basiszählermetrik.

Abrufen des DB-Lastdurchschnitts für Top-SQL-Anweisungen

Im folgenden Beispiel werden `db.wait_events` entsprechend der 10 Top-SQL-Anweisungen gruppiert. Es gibt zwei verschiedene Gruppen für SQL-Anweisungen.

- `db.sql` – Die vollständige SQL-Anweisung, wie `select * from customers where customer_id = 123`
- `db.sql_tokenized` – Die SQL-Anweisung mit Token, wie `select * from customers where customer_id = ?`

Beim Analysieren der Datenbank-Performance kann es nützlich sein, SQL-Anweisungen, die sich nur durch ihre Parameter unterscheiden, als ein logisches Element zu betrachten. In diesem Fall können Sie `db.sql_tokenized` beim Abfragen verwenden. In manchen Fällen, insbesondere wenn Sie an Explain-Plänen interessiert sind, ist es jedoch sinnvoller, die vollständigen SQL-Anweisungen mit Parametern zu untersuchen und die Abfrage nach `db.sql` zu gruppieren. Zwischen SQL-Anweisungen mit Token und vollständigen SQL-Anweisungen besteht eine Beziehung der Über-/Unterordnung. Mehrere vollständige (untergeordnete) SQL-Anweisungen befinden sich unter derselben (übergeordneten) SQL-Anweisung mit Token.

Der Befehl in diesem Beispiel ähnelt dem Befehl unter Abrufen des DB-Lastdurchschnitts für Top-Warteereignisse. Die Datei query.json enthält hingegen Folgendes.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.sql_tokenized", "Limit": 10 }
    }
]
```

Im folgenden Beispiel wird verwende `db.sql_tokenized`.

Für LinuxmacOS, oderUnix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-29T00:00:00Z \
   --end-time   2018-10-30T00:00:00Z \
   --period-in-seconds 3600 \
   --metric-queries file://query.json
```

Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-29T00:00:00Z ^
   --end-time   2018-10-30T00:00:00Z  ^
   --period-in-seconds 3600 ^
   --metric-queries file://query.json
```

In diesem Beispiel werden Abfragen über 24 Stunden mit einer Stunde abgefragt period-in-seconds.

Das Beispiel gibt die Metrik `db.load.avg` und eine `GroupBy`-Sortierung der sieben Top-Warteereignisse an. Einzelheiten zu gültigen Werten für dieses Beispiel finden Sie DimensionGroupin der Performance Insights API-Referenz.

Die Antwort sieht in etwa so aus:

```
{
    "AlignedStartTime": 1540771200.0,
    "AlignedEndTime": 1540857600.0,
    "Identifier": "db-XXX",

    "MetricList": [ //11 entries in the MetricList
        {
            "Key": { //First key is total
                "Metric": "db.load.avg"
            }
            "DataPoints": [ //Each DataPoints list has 24 per-hour Timestamps and a
 value
                {
```

```
                    "Value": 1.6964980544747081,
                    "Timestamp": 1540774800.0
                },
                //... 24 datapoints
            ]
        },
        {
            "Key": { //Next key is the top tokenized SQL
                "Dimensions": {
                    "db.sql_tokenized.statement": "INSERT INTO authors (id,name,email)
 VALUES\n( nextval(?)  ,?,?)",
                    "db.sql_tokenized.db_id": "pi-2372568224",
                    "db.sql_tokenized.id": "AKIAIOSFODNN7EXAMPLE"
                },
                "Metric": "db.load.avg"
            },
            "DataPoints": [ //... 24 datapoints
            ]
        },
        // In total 11 entries, 10 Keys of top tokenized SQL, 1 total key
    ] //End of MetricList
} //End of response
```

Diese Antwort umfasst 11 Einträge in der `MetricList` (1 gesamt, 10 Top-SQL mit Token), wobei jeder Eintrage 24 `DataPoints` pro Stunde aufweist.

Für SQL-Anweisungen mit Token gibt es in jeder Dimensionsliste drei Einträge:

- `db.sql_tokenized.statement` – Die SQL-Anweisung mit Token.
- `db.sql_tokenized.db_id` – Entweder die native Datenbank-ID zum Verweisen auf die SQL-Anweisung oder eine synthetische ID, die von Performance Insights generiert wird, wenn keine native Datenbank-ID verfügbar ist. In diesem Beispiel wird die synthetische ID `pi-2372568224` zurückgegeben.
- `db.sql_tokenized.id` – Die ID der Abfrage innerhalb von Performance-Insights.

  In der AWS Management Console wird diese ID als Support-ID bezeichnet. Es trägt diesen Namen, weil es sich bei der ID um Daten handelt, die der AWS Support untersuchen kann, um Ihnen bei der Behebung eines Problems mit Ihrer Datenbank zu helfen. AWS nimmt die Sicherheit und den Datenschutz Ihrer Daten sehr ernst und fast alle Daten werden mit Ihrem AWS KMS Schlüssel verschlüsselt gespeichert. Daher AWS kann niemand im Inneren diese Daten einsehen. Im vorherigen Beispiel wird sowohl `tokenized.statement` als auch `tokenized.db_id`

verschlüsselt gespeichert. Wenn Sie ein Problem mit Ihrer Datenbank haben, kann Ihnen der AWS Support unter Angabe der Support-ID weiterhelfen.

Beim Abfragen empfiehlt es sich ggf., eine `Group` in `GroupBy` anzugeben. Für eine präzisere Kontrolle der Daten, die zurückgegeben werden, sollten Sie allerdings die Dimensionsliste angeben. Wenn z. B. lediglich eine `db.sql_tokenized.statement` erforderlich ist, kann der query.json-Datei ein `Dimensions`-Attribut hinzugefügt werden.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": {
            "Group": "db.sql_tokenized",
            "Dimensions":["db.sql_tokenized.statement"],
            "Limit": 10
        }
    }
]
```

Abrufen des nach SQL gefilterten DB-Lastdurchschnitts

Die vorherige Abbildung zeigt, dass eine bestimmte Abfrage ausgewählt ist, und das Stapelflächendiagramm der durchschnittlichen aktiven Top-Sitzungen ist auf diese Abfrage beschränkt. Obwohl sich die Abfrage nach wie vor auf die sieben Top-Gesamtwarteereignisse bezieht, wird der Wert der Antwort gefiltert. Durch das Filtern werden nur die Sitzungen berücksichtigt, die mit dem entsprechenden Filter übereinstimmen.

Die entsprechende API-Abfrage in diesem Beispiel ähnelt dem Befehl unter Abrufen des DB-Lastdurchschnitts für Top-SQL-Anweisungen. Die Datei query.json enthält hingegen Folgendes.

```
[
 {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_event", "Limit": 5  },
        "Filter": { "db.sql_tokenized.id": "AKIAIOSFODNN7EXAMPLE" }
    }
]
```

Für LinuxmacOS, oderUnix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-30T00:00:00Z \
   --end-time   2018-10-30T01:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-30T00:00:00Z ^
   --end-time   2018-10-30T01:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

Die Antwort sieht in etwa so aus:

```
{
    "Identifier": "db-XXX",
```

```
    "AlignedStartTime": 1556215200.0,
    "MetricList": [
        {
            "Key": {
                "Metric": "db.load.avg"
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 1.4878117913832196
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 1.192823803967328
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "io",
                    "db.wait_event.name": "wait/io/aurora_redo_log_flush"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 1.1360544217687074
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 1.058051341890315
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "io",
                    "db.wait_event.name": "wait/io/table/sql/handler"
                }
            },
```

```
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 0.16241496598639457
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 0.05163360560093349
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "synch",
                    "db.wait_event.name": "wait/synch/mutex/innodb/
aurora_lock_thread_slot_futex"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 0.11479591836734694
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 0.013127187864644107
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "CPU",
                    "db.wait_event.name": "CPU"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 0.05215419501133787
                },
```

```
                {
                    "Timestamp": 1556222400.0,
                    "Value": 0.05805134189031505
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "synch",
                    "db.wait_event.name": "wait/synch/mutex/innodb/lock_wait_mutex"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 0.017573696145124718
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 0.002333722287047841
                }
            ]
        }
    ],
    "AlignedEndTime": 1556222400.0
} //end of response
```

In dieser Antwort werden alle Werte gemäß des Beitrags der SQL-Anweisung mit Token AKIAIOSFODNN7EXAMPLE gefiltert, die in der query.json-Datei angegeben ist. Die Schlüssel sind möglicherweise in einer anderen Reihenfolge angeordnet als bei einer Abfrage ohne Filter, da die gefilterte SQL-Anweisung von den fünf Top-Warteereignisse beeinflusst wurde.

Abrufen des Volltextes einer SQL-Anweisung

Im folgenden Beispiel wird der Volltext einer SQL-Anweisung für die DB-Instance abgerufe `db-10BCD2EFGHIJ3KL4M5NO6PQRS5`. `--group` ist `db.sql` und `--group-identifier` ist `db.sql.id`. In diesem Beispiel stellt *`my-sql-id`* eine SQL-ID dar, die durch Aufrufen von`pi get-resource-metrics` oder `pi describe-dimension-keys` abgerufen wurde.

Führen Sie den folgenden Befehl aus.

Für LinuxmacOS, oderUnix:

```
aws pi get-dimension-key-details \
   --service-type RDS \
   --identifier db-10BCD2EFGHIJ3KL4M5NO6PQRS5 \
   --group db.sql \
   --group-identifier my-sql-id \
   --requested-dimensions statement
```

Windows:

```
aws pi get-dimension-key-details ^
   --service-type RDS ^
   --identifier db-10BCD2EFGHIJ3KL4M5NO6PQRS5 ^
   --group db.sql ^
   --group-identifier my-sql-id ^
   --requested-dimensions statement
```

In diesem Beispiel sind die Dimensionsdetails verfügbar. Performance Insights ruft also den vollständigen Text der SQL-Anweisung ab, ohne ihn abzuschneiden.

```
{
    "Dimensions":[
    {
        "Value": "SELECT e.last_name, d.department_name FROM employees e, departments d
 WHERE e.department_id=d.department_id",
        "Dimension": "db.sql.statement",
        "Status": "AVAILABLE"
    },
    ...
    ]
}
```

Erstellen eines Leistungsanalyseberichts für einen bestimmten Zeitraum

Im folgenden Beispiel wird ein Leistungsanalysebericht mit der Startzeit `1682969503` und der Endzeit `1682979503` für die`db-loadtest-0`-Datenbank erstellt.

```
aws pi create-performance-analysis-report \
        --service-type RDS \
        --identifier db-loadtest-0 \
        --start-time 1682969503 \
```

```
        --end-time 1682979503 \
        --region us-west-2
```

Die Antwort ist der eindeutige Bezeichner `report-0234d3ed98e28fb17` für den Bericht.

```
{
   "AnalysisReportId": "report-0234d3ed98e28fb17"
}
```

Abrufen eines Leistungsanalyseberichts

Im folgenden Beispiel werden die Details des Analyseberichts für den Bericht `report-0d99cc91c4422ee61` abgerufen.

```
aws pi get-performance-analysis-report \
--service-type RDS \
--identifier db-loadtest-0 \
--analysis-report-id report-0d99cc91c4422ee61 \
--region us-west-2
```

Die Antwort enthält den Berichtsstatus, die ID, Zeitdetails und Einblicke.

```
        {
    "AnalysisReport": {
        "Status": "Succeeded",
        "ServiceType": "RDS",
        "Identifier": "db-loadtest-0",
        "StartTime": 1680583486.584,
        "AnalysisReportId": "report-0d99cc91c4422ee61",
        "EndTime": 1680587086.584,
        "CreateTime": 1680587087.139,
        "Insights": [
           ... (Condensed for space)
        ]
    }
}
```

Auflisten aller Leistungsanalyseberichte für die DB-Instance

Das folgende Beispiel listet alle verfügbaren Leistungsanalyseberichte für die `db-loadtest-0`-Datenbank auf.

```
aws pi list-performance-analysis-reports \
--service-type RDS \
--identifier db-loadtest-0 \
--region us-west-2
```

In der Antwort werden alle Berichte mit der Berichts-ID, dem Status und den Details zum Zeitraum aufgeführt.


```
{
    "AnalysisReports": [
        {
            "Status": "Succeeded",
            "EndTime": 1680587086.584,
            "CreationTime": 1680587087.139,
            "StartTime": 1680583486.584,
            "AnalysisReportId": "report-0d99cc91c4422ee61"
        },
        {
            "Status": "Succeeded",
            "EndTime": 1681491137.914,
            "CreationTime": 1681491145.973,
            "StartTime": 1681487537.914,
            "AnalysisReportId": "report-002633115cc002233"
        },
        {
            "Status": "Succeeded",
            "EndTime": 1681493499.849,
            "CreationTime": 1681493507.762,
            "StartTime": 1681489899.849,
            "AnalysisReportId": "report-043b1e006b47246f9"
        },
        {
            "Status": "InProgress",
            "EndTime": 1682979503.0,
            "CreationTime": 1682979618.994,
            "StartTime": 1682969503.0,
            "AnalysisReportId": "report-01ad15f9b88bcbd56"
        }
    ]
}
```

Löschen eines Leistungsanalyseberichts

Im folgenden Beispiel wird der Analysebericht für die `db-loadtest-0`-Datenbank gelöscht.

```
aws pi delete-performance-analysis-report \
--service-type RDS \
--identifier db-loadtest-0 \
--analysis-report-id report-0d99cc91c4422ee61 \
--region us-west-2
```

Hinzufügen eines Tags zu einem Leistungsanalysebericht

Im folgenden Beispiel wird ein Tag mit dem Schlüssel `name` und dem Wert `test-tag` zum Bericht `report-01ad15f9b88bcbd56` hinzugefügt.

```
aws pi tag-resource \
--service-type RDS \
--resource-arn arn:aws:pi:us-west-2:356798100956:perf-reports/RDS/db-loadtest-0/
report-01ad15f9b88bcbd56 \
--tags Key=name,Value=test-tag \
--region us-west-2
```

Auflisten aller Tags für einen Leistungsanalysebericht

Das folgende Beispiel listet alle Tags für den Bericht `report-01ad15f9b88bcbd56` auf.

```
aws pi list-tags-for-resource \
--service-type RDS \
--resource-arn arn:aws:pi:us-west-2:356798100956:perf-reports/RDS/db-loadtest-0/
report-01ad15f9b88bcbd56 \
--region us-west-2
```

In der Antwort werden der Wert und der Schlüssel für alle dem Bericht hinzugefügten Tags aufgeführt:

```
{
    "Tags": [
        {
            "Value": "test-tag",
            "Key": "name"
        }
    ]
```

```
}
```

Löschen der Tags eines Leistungsanalyseberichts

Im folgenden Beispiel wird das Tag `name` aus dem Bericht `report-01ad15f9b88bcbd56` gelöscht.

```
aws pi untag-resource \
--service-type RDS \
--resource-arn arn:aws:pi:us-west-2:356798100956:perf-reports/RDS/db-loadtest-0/
report-01ad15f9b88bcbd56 \
--tag-keys name \
--region us-west-2
```

Nachdem das Tag gelöscht wurde, wird beim Abrufen der API `list-tags-for-resource` dieses Tag nicht mehr aufgelistet.

Protokollieren von Performance Insights-An AWS CloudTrail

Performance Insights wird mit AWS CloudTrail ausgeführt, einem Service, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS-Service in Performance Insights ausgeführt werden. CloudTrail erfasst alle API-Aufrufe für Performance Insights als Ereignisse. Diese Erfassung umfasst Aufrufe von der Amazon-RDS-Konsole und von Code-Aufrufen an die Performance Insights-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3-Bucket, einschließlich Ereignissen für Performance Insights, aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen. Anhand der von CloudTrail erfassten Informationen können Sie bestimmte Details festlegen. Diese Informationen umfassen die Anforderung an Performance Insights, die IP-Adresse, von der die Anforderung gesendet wurde, den Initiator sowie den Zeitpunkt der Anforderung. Sie enthalten auch weitere Angaben.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Arbeiten mit Performance Insights-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Wenn Aktivität in Performance-Insights auftritt, wird diese zusammen mit anderen AWS-Service-Ereignissen in der CloudTrail-Konsole in einem CloudTrail-Ereignisprotokoll im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere

Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf im AWS CloudTrail-Benutzerhandbuch.

Erstellen Sie einen Trail für einen fortlaufenden Datensatz zu Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für Performance Insights. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen AWS-Regionen in der AWS-Partition und stellt die Protokolldateien in dem Amazon-S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail-Benutzerhandbuch:

- Übersicht zum Erstellen eines Trails
- Von CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon-SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle Performance Insights-Vorgänge werden von CloudTrail protokolliert und in der Performance Insights-API-Referenz dokumentiert. Zum Beispiel werden durch Aufrufe der `DescribeDimensionKeys`- und `GetResourceMetrics`-Operationen Einträge in den CloudTrail-Protokolldateien generiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter dem CloudTrail userIdentity-Element.

Performance Insights-Protokolldateieinträge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder

mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Jedes Ereignis enthält unter anderem Informationen über die angeforderte Operation, etwaige Anforderungsparameter und das Datum und die Uhrzeit der Operation. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die `GetResourceMetrics`-Operation demonstriert:


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
         "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/johndoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "johndoe"
    },
    "eventTime": "2019-12-18T19:28:46Z",
    "eventSource": "pi.amazonaws.com",
    "eventName": "GetResourceMetrics",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "aws-cli/1.16.240 Python/3.7.4 Darwin/18.7.0 botocore/1.12.230",
    "requestParameters": {
        "identifier": "db-YTDU5J5V66X7CXSCVDFD2V3SZM",
        "metricQueries": [
            {
                "metric": "os.cpuUtilization.user.avg"
            },
            {
                "metric": "os.cpuUtilization.idle.avg"
            }
        ],
        "startTime": "Dec 18, 2019 5:28:46 PM",
        "periodInSeconds": 60,
        "endTime": "Dec 18, 2019 7:28:46 PM",
        "serviceType": "RDS"
    },
    "responseElements": null,
    "requestID": "9ffbe15c-96b5-4fe6-bed9-9fccff1a0525",
    "eventID": "08908de0-2431-4e2e-ba7b-f5424f908433",
```

```
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Analysieren von Aurora-Leistungsanomalien mit Amazon DevOps Guru für Amazon RDS

Amazon DevOps Guru ist ein vollständig verwalteter Betriebsservice, der Entwicklern und Betreibern hilft, die Leistung und Verfügbarkeit ihrer Anwendungen zu verbessern. DevOpsGuru überträgt Ihnen die Aufgaben im Zusammenhang mit der Identifizierung betrieblicher Probleme, sodass Sie schnell Empfehlungen zur Verbesserung Ihrer Anwendung umsetzen können. Weitere Informationen finden Sie unter Was ist Amazon DevOps Guru? im Amazon DevOps Guru-Benutzerhandbuch.

DevOpsGuru erkennt, analysiert und gibt Empfehlungen für bestehende Betriebsprobleme für alle Amazon RDS-DB-Engines. DevOpsGuru for RDS erweitert diese Funktion, indem es maschinelles Lernen auf Performance Insights Insights-Metriken für Amazon Aurora anwendet. Diese Überwachungsfunktionen ermöglichen es DevOps Guru for RDS, Leistungsengpässe zu erkennen und zu diagnostizieren und spezifische Korrekturmaßnahmen zu empfehlen. DevOpsGuru for RDS kann auch problematische Bedingungen in Ihren Aurora-Datenbanken () erkennen, bevor sie auftreten.

Sie können sich diese Empfehlungen jetzt in der RDS-Konsole ansehen. Weitere Informationen finden Sie unter Anzeigen und Beantworten von Amazon-Aurora-Empfehlungen.

Das folgende Video gibt einen Überblick über DevOps Guru for RDS.

Weitere Informationen zu diesem Thema finden Sie unter Amazon DevOps Guru for RDS unter der Haube.

Themen

- Vorteile von DevOps Guru für RDS
- Wie funktioniert DevOps Guru for RDS
- DevOpsGuru für RDS einrichten

Vorteile von DevOps Guru für RDS

Wenn Sie für eine Datenbank von Amazon Aurora verantwortlich sind, wissen Sie möglicherweise nicht, dass ein Ereignis oder eine Regression auftritt, die sich auf diese Datenbank auswirkt. Wenn Sie von dem Problem erfahren, wissen Sie möglicherweise nicht, warum es auftritt und was Sie dagegen tun können. Anstatt sich an einen Datenbankadministrator (DBA) zu wenden, um Hilfe zu

erhalten oder sich auf Tools von Drittanbietern zu verlassen, können Sie den Empfehlungen von DevOps Guru for RDS folgen.

Die detaillierte Analyse von DevOps Guru for RDS bietet Ihnen die folgenden Vorteile:

Schnelle Diagnose

DevOpsGuru for RDS überwacht und analysiert kontinuierlich die Datenbanktelemetrie. Performance Insights, Enhanced Monitoring und Amazon CloudWatch sammeln Telemetriedaten für Ihre . DevOpsGuru for RDS verwendet statistische Techniken und Techniken des maschinellen Lernens, um diese Daten zu analysieren und Anomalien zu erkennen. Weitere Informationen zu Telemetriedaten finden Sie unter Überwachung mit Performance Insights auf Amazon Aurora und Überwachen von Betriebssystem-Metriken mit „Enhanced Monitoring“ (Erweiterte Überwachung) im Amazon-Aurora-Benutzerhandbuch .

Schnelle Auflösung

Jede Anomalie identifiziert das Leistungsproblem und schlägt Möglichkeiten für Untersuchungen oder Korrekturmaßnahmen vor. DevOpsGuru for RDS könnte Ihnen beispielsweise empfehlen, bestimmte Warteereignisse zu untersuchen. Oder es empfiehlt sich, Ihre Anwendungspooleinstellungen zu optimieren, um die Anzahl der Datenbankverbindungen zu begrenzen. Basierend auf diesen Empfehlungen können Sie Leistungsprobleme schneller beheben als durch eine manuelle Fehlerbehebung.

Proaktive Einblicke

DevOpsGuru for RDS verwendet Metriken aus Ihren Ressourcen, um potenziell problematisches Verhalten zu erkennen, bevor es zu einem größeren Problem wird. Es kann beispielsweise erkennen, wann Ihre Datenbank eine zunehmende Anzahl von temporären Tabellen auf der Festplatte verwendet, was negative Auswirkungen auf die Leistung zur Folge haben kann. DevOpsGuru gibt Ihnen dann Empfehlungen, die Ihnen helfen, Probleme zu lösen, bevor sie zu größeren Problemen werden.

Fundierte Kenntnisse der Amazon-Ingenieure und Machine Learning

DevOpsGuru for RDS setzt auf maschinelles Lernen (ML) und fortschrittliche mathematische Formeln, um Leistungsprobleme zu erkennen und Engpässe zu beheben. Die Datenbankingenieure von Amazon haben zur Entwicklung der Ergebnisse von DevOps Guru for RDS beigetragen, die auf viele Jahre der Verwaltung von Hunderttausenden von Datenbanken zurückzuführen sind. Durch die Nutzung dieses kollektiven Wissens kann DevOps Guru for RDS Ihnen bewährte Verfahren vermitteln.

Wie funktioniert DevOps Guru for RDS

DevOpsGuru for RDS sammelt Daten über Ihre Aurora von Amazon RDS Performance Insights. Die wichtigste Metrik ist. `DBLoad` DevOpsGuru for RDS nutzt die Performance Insights Insights-Metriken, analysiert sie mit maschinellem Lernen und veröffentlicht die Erkenntnisse im Dashboard.

Ein Insight ist eine Sammlung verwandter Anomalien, die von Guru entdeckt wurden. DevOps

In DevOps Guru for RDS ist eine Anomalie ein Muster, das von dem abweicht, was als normale Leistung für Ihre Amazon Aurora angesehen wird.

Proaktive Einblicke

Ein proaktiver Einblick informiert Sie über problematisches Verhalten, bevor es auftritt. Er enthält Anomalien mit Empfehlungen und zugehörigen Metriken, die Ihnen helfen, Auffälligkeiten in Ihren Datenbanken von Amazon Aurora anzugehen, bevor sie zu größeren Problemen werden. Diese Erkenntnisse werden im Guru-Dashboard veröffentlicht. DevOps

DevOpsGuru könnte beispielsweise feststellen, dass Ihre Aurora PostgreSQL-Datenbank viele temporäre Tabellen auf der Festplatte erstellt. Wenn dieser Trend nicht angegangen wird, kann er zu Leistungsproblemen führen. Jeder proaktive Einblick beinhaltet Empfehlungen für korrektives Verhalten und Links zu relevanten Themen in Optimierung von Aurora MySQL mit proaktiven Einblicken von Amazon DevOps Guru oder Optimierung von Aurora PostgreSQL mit proaktiven Einblicken von Amazon DevOps Guru. Weitere Informationen finden Sie unter Working with Insights in DevOps Guru im Amazon DevOps Guru-Benutzerhandbuch.

Reaktive Einblicke

Ein reaktiver Einblick identifiziert anomales Verhalten, sobald es auftritt. Wenn DevOps Guru for RDS Leistungsprobleme in Ihren Amazon Aurora feststellt, veröffentlicht es einen reaktiven Einblick im DevOps Guru-Dashboard. Weitere Informationen finden Sie unter Working with Insights in DevOps Guru im Amazon DevOps Guru-Benutzerhandbuch.

Kausale Anomalien

Eine kausale Anomalie ist eine Anomalie der obersten Ebene innerhalb eines Einblicks. Die Datenbanklast (DB-Last) ist die ursächliche Anomalie für DevOps Guru for RDS.

Eine Anomalie misst die Leistungseinbußen durch Zuweisen eines Schweregrads von Hoch, Mittel oder Niedrig. Weitere Informationen finden Sie unter Wichtige Konzepte für DevOps Guru for RDS im Amazon DevOps Guru-Benutzerhandbuch.

Wenn DevOps Guru eine aktuelle Anomalie in Ihrer DB-Instance feststellt, werden Sie auf der Datenbankseite der RDS-Konsole benachrichtigt. Die Konsole warnt Sie auch bei Anomalien, die in den letzten 24 Stunden aufgetreten sind. Um von der RDS-Konsole zur Anomalieseite zu gelangen, wählen Sie den Link in der Warnmeldung. Die RDS-Konsole warnt Sie auch auf der Seite für Ihren DB-Cluster von Amazon Aurora .

Kontextbezogene Anomalien

Eine kontextbezogene Anomalie ist ein Befund innerhalb der Datenbanklast (DB-Last), der zu einem reaktiven Einblick gehört. Jede kontextbezogene Anomalie beschreibt ein bestimmtes Leistungsproblem von Amazon Aurora , das untersucht werden muss. DevOpsGuru for RDS könnte Ihnen beispielsweise empfehlen, eine Erhöhung der CPU-Kapazität in Betracht zu ziehen oder Warteereignisse zu untersuchen, die zur DB-Auslastung beitragen.

> **Important**
>
> Wir empfehlen Ihnen alle Änderungen in einer Test-Instance zu prüfen, bevor Sie eine produktive Instance ändern. Auf diese Weise verstehen Sie die Auswirkungen der Änderung.

Weitere Informationen finden Sie unter Analysieren von Anomalien in Amazon RDS im Amazon DevOps Guru-Benutzerhandbuch.

DevOpsGuru für RDS einrichten

Führen Sie die folgenden Aufgaben aus, um DevOps Guru for Amazon RDS die Veröffentlichung von Erkenntnissen zu ermöglichen.

Themen

- Konfiguration von IAM-Zugriffsrichtlinien für Guru for RDS DevOps
- Aktivieren von Performance Insights für Ihre DB-Instances von Aurora
- DevOpsGuru einschalten und die Ressourcenabdeckung angeben

Konfiguration von IAM-Zugriffsrichtlinien für Guru for RDS DevOps

Um Benachrichtigungen von DevOps Guru in der RDS-Konsole anzuzeigen, muss Ihr AWS Identity and Access Management (IAM-) Benutzer oder Ihre Rolle über eine der folgenden Richtlinien verfügen:

- Die AWS verwaltete Richtlinie `AmazonDevOpsGuruConsoleFullAccess`
- Die AWS verwaltete Richtlinie `AmazonDevOpsGuruConsoleReadOnlyAccess` und eine der folgenden Richtlinien:
  - Die AWS verwaltete Richtlinie `AmazonRDSFullAccess`
  - Eine vom Kunden verwaltete Richtlinie, die `pi:GetResourceMetrics` und `pi:DescribeDimensionKeys` einschließt

Weitere Informationen finden Sie unter Konfigurieren von Zugriffsrichtlinien für Performance Insights.

Aktivieren von Performance Insights für Ihre DB-Instances von Aurora

DevOpsGuru for RDS verlässt sich bei seinen Daten auf Performance Insights. Ohne Performance Insights veröffentlicht DevOps Guru Anomalien, beinhaltet aber keine detaillierten Analysen und Empfehlungen.

Wenn Sie einen Aurora-DB-Cluster erstellen oder eine Cluster-Instance ändern, können Sie Performance Insights aktivieren. Weitere Informationen finden Sie unter Performance Insights für Aurora ein- und ausschalten.

DevOpsGuru einschalten und die Ressourcenabdeckung angeben

Sie können DevOps Guru aktivieren, damit es Ihre Amazon Aurora auf eine der folgenden Arten überwacht.

Themen

- DevOpsGuru in der RDS-Konsole einschalten
- Hinzufügen von Ressourcen für Aurora in der Guru-Konsole DevOps
- Hinzufügen von Aurora mit AWS CloudFormation

DevOpsGuru in der RDS-Konsole einschalten

Sie können in der Amazon RDS-Konsole mehrere Wege wählen, um DevOps Guru zu aktivieren.

Themen

- DevOpsGuru einschalten, wenn Sie eine Aurora erstellen
- DevOpsGuru über das Benachrichtigungsbanner einschalten

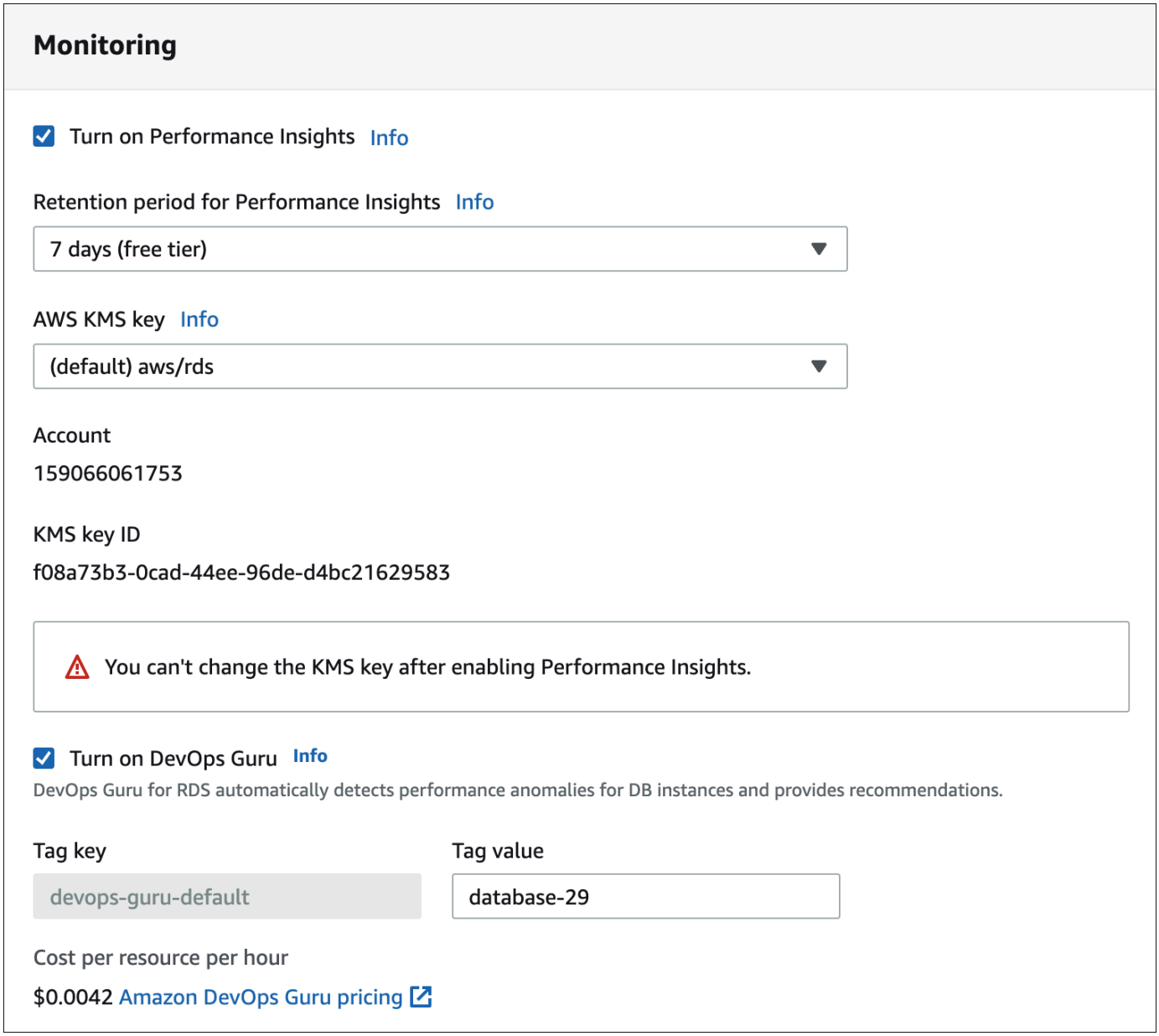
- Du reagierst auf einen Berechtigungsfehler, wenn du DevOps Guru einschaltest

DevOpsGuru einschalten, wenn Sie eine Aurora erstellen

Der Erstellungs-Workflow umfasst eine Einstellung, mit der die DevOps Guru-Abdeckung für Ihre Datenbank aktiviert wird. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Vorlage Production (Produktion) auswählen.

Um DevOps Guru zu aktivieren, wenn Sie eine Aurora erstellen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Führen Sie die Schritte unter Erstellen eines DB-Clusters bis auf den Schritt aus, in dem Sie Überwachungseinstellungen wählen.
3. Wählen Sie unter Monitoring (Überwachung) die Option Turn on Performance Insights (Performance Insights aktivieren) aus. Damit DevOps Guru for RDS eine detaillierte Analyse von Leistungsanomalien bereitstellen kann, muss Performance Insights aktiviert sein.
4. Wählen Sie Turn on Guru. DevOps



5. Erstellen Sie ein Tag für Ihre Datenbank, damit DevOps Guru es überwachen kann. Gehen Sie wie folgt vor:

   - Geben Sie im Textfeld für Tag key (Tag-Schlüssel) einen Namen ein, der mit **`Devops-Guru-`** beginnt.
   - Geben Sie im Textfeld für Tag value (Tag-Wert) einen beliebigen Wert ein. Wenn Sie z. B. **`rds-database-1`** als Name Ihrer Datenbank von Aurora eingeben, können Sie auch **`rds-database-1`** als Tag-Wert eingeben.

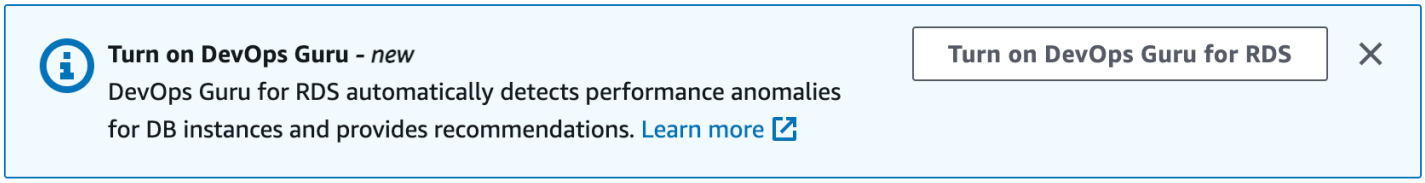
Weitere Informationen zu Tags finden Sie unter „Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren“ im Amazon DevOps Guru-Benutzerhandbuch.

6. Führen Sie die verbleibenden Schritte unter Erstellen eines DB-Clusters aus.

DevOpsGuru über das Benachrichtigungsbanner einschalten

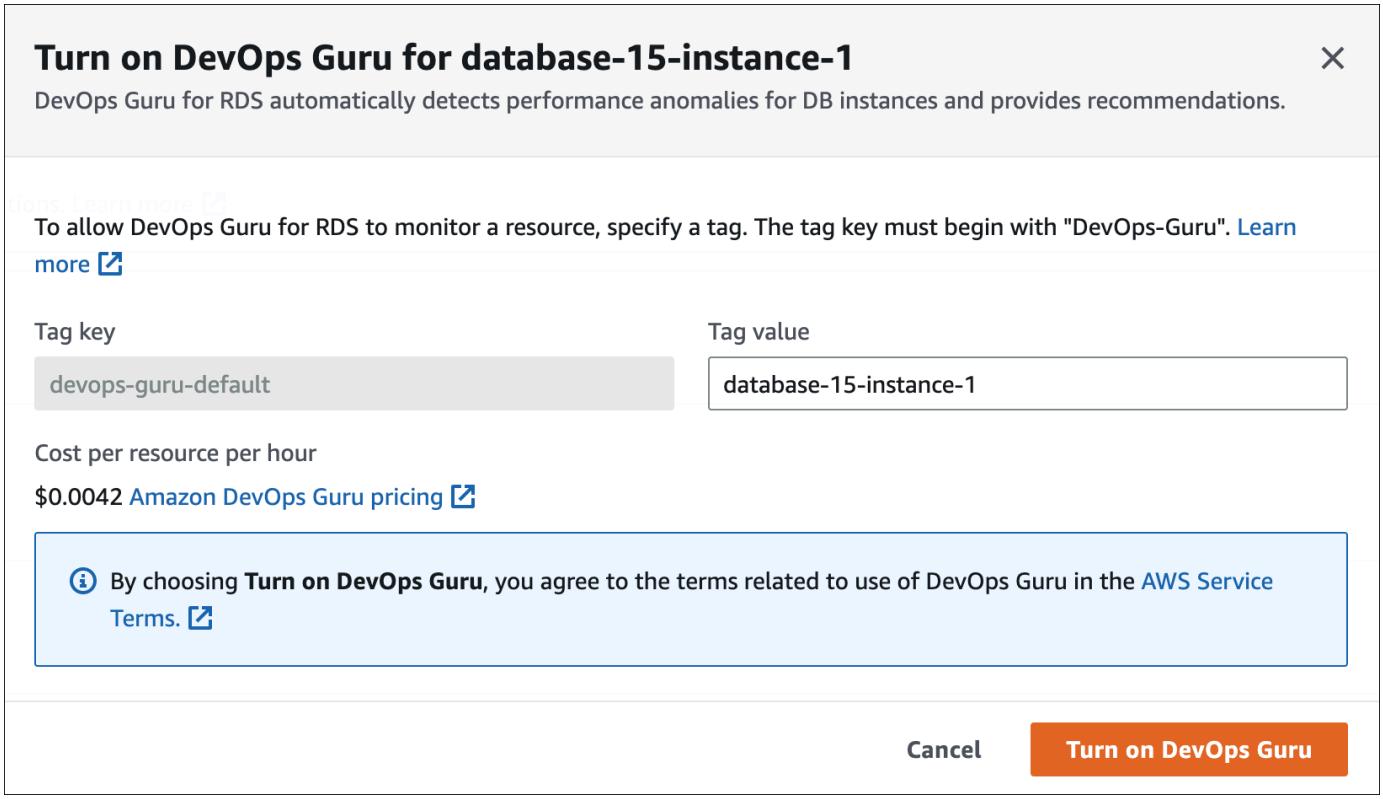
Wenn Ihre Ressourcen nicht von DevOps Guru abgedeckt werden, benachrichtigt Sie Amazon RDS mit einem Banner an den folgenden Stellen:

- Auf der Registerkarte Monitoring (Überwachung) einer DB-Cluster-Instance
- Im Performance-Insights-Dashboard



So aktivieren Sie DevOps Guru für Ihre Aurora

1. Wählen Sie im Banner Turn on DevOps Guru for RDS aus.
2. Geben Sie einen Schlüsselnamen und einen Wert für das Tag ein. Weitere Informationen zu Tags finden Sie unter „Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren“ im Amazon DevOps Guru-Benutzerhandbuch.



3. Wähle DevOpsGuru einschalten.

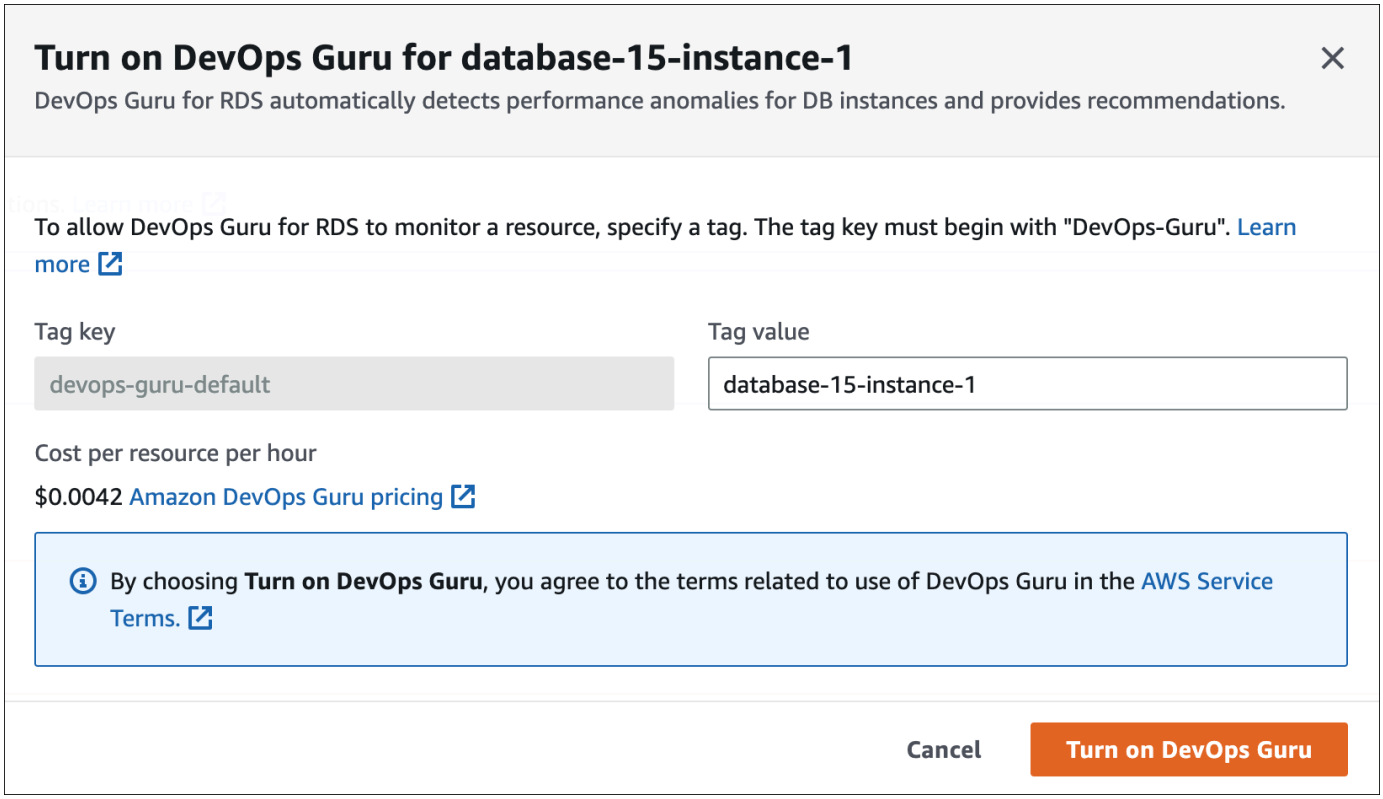
Du reagierst auf einen Berechtigungsfehler, wenn du DevOps Guru einschaltest

Wenn Sie DevOps Guru bei der Erstellung einer Datenbank von der RDS-Konsole aus aktivieren, zeigt RDS möglicherweise das folgende Banner mit fehlenden Berechtigungen an.

So reagieren Sie auf einen Berechtigungsfehler

1. Gewähren Sie Ihrem IAM-Benutzer oder Ihrer Rolle die vom Benutzer verwaltete Rolle `AmazonDevOpsGuruConsoleFullAccess`. Weitere Informationen finden Sie unter Konfiguration von IAM-Zugriffsrichtlinien für Guru for RDS DevOps.
2. Öffnen Sie die RDS-Konsole.
3. Wählen Sie im Navigationsbereich Performance-Insights aus.
4. Wählen Sie eine DB-Instance in dem Cluster aus, den Sie soeben erstellt haben.
5. Wählen Sie den Schalter, um DevOpsGuru für RDS einzuschalten.

6. Wählen Sie einen Tag-Wert aus. Weitere Informationen finden Sie unter „Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren“ im Amazon DevOps Guru-Benutzerhandbuch.



7. Wählen Sie DevOpsGuru einschalten.

Hinzufügen von Ressourcen für Aurora in der Guru-Konsole DevOps

Sie können die Abdeckung Ihrer DevOps Guru-Ressourcen auf der DevOps Guru-Konsole angeben. Folgen Sie dem unter Spezifizieren Sie den Umfang Ihrer DevOps Guru-Ressourcen im Amazon DevOps Guru-Benutzerhandbuch beschriebenen Schritt. Wählen Sie eine der folgenden Optionen aus, wenn Sie Ihre analysierten Ressourcen bearbeiten:

- Wählen Sie Alle Kontoressourcen, um alle unterstützten Ressourcen, einschließlich der Aurora , in Ihrer Region AWS-Konto und Ihrer Region zu analysieren.
- Wählen Sie CloudFormation Stacks aus, um die Aurora zu analysieren, die sich in Stacks Ihrer Wahl befinden. Weitere Informationen finden Sie unter Verwenden von AWS CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen im Amazon DevOps Guru-Benutzerhandbuch.

- Klicken Sie auf Tags, um die Datenbanken von Aurora zu analysieren, die Sie mit einem Tag versehen haben. Weitere Informationen finden Sie unter Verwenden von Tags zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen im Amazon DevOps Guru-Benutzerhandbuch.

Weitere Informationen finden Sie unter Enable DevOps Guru im Amazon DevOps Guru-Benutzerhandbuch.

Hinzufügen von Aurora mit AWS CloudFormation

Sie können Tags verwenden, um Ihren Vorlagen die Abdeckung Ihrer Aurora hinzuzufügen. CloudFormation Das folgende Verfahren setzt voraus, dass Sie eine CloudFormation Vorlage sowohl für Ihre Aurora Ihren DevOps Guru-Stack haben.

So geben Sie eine Aurora mithilfe eines Tags an CloudFormation

1. Definieren Sie in der CloudFormation Vorlage für Ihre DB-Instance ein Tag mit einem Schlüssel/Wert-Paar.

   Das folgende Beispiel weist `Devops-guru-cfn-default` einer Aurora-DB-Instance den Wert `my-aurora-db-instance1`.

   ```
   MyAuroraDBInstance1:
     Type: "AWS::RDS::DBInstance"
     Properties:
       DBClusterIdentifier: my-aurora-db-cluster
       DBInstanceIdentifier: my-aurora-db-instance1
       Tags:
         - Key: Devops-guru-cfn-default
           Value: devopsguru-my-aurora-db-instance1
   ```

2. Geben Sie in der CloudFormation Vorlage für Ihren DevOps Guru-Stack dasselbe Tag in Ihrem Ressourcensammlungsfilter an.

   Im folgenden Beispiel wird DevOps Guru so konfiguriert, dass die Ressource mit dem Tag-Wert `my-aurora-db-instance1` abgedeckt wird.

   ```
   DevOpsGuruResourceCollection:
     Type: AWS::DevOpsGuru::ResourceCollection
     Properties:
       ResourceCollectionFilter:
   ```

```
      Tags:
        - AppBoundaryKey: "Devops-guru-cfn-default"
          TagValues:
          - "devopsguru-my-aurora-db-instance1"
```

Das folgende Beispiel deckt alle Ressourcen innerhalb der Anwendungsgrenze `Devops-guru-cfn-default` ab.

```
DevOpsGuruResourceCollection:
  Type: AWS::DevOpsGuru::ResourceCollection
  Properties:
    ResourceCollectionFilter:
      Tags:
        - AppBoundaryKey: "Devops-guru-cfn-default"
          TagValues:
          - "*"
```

Weitere Informationen finden Sie unter AWS::DevOpsGuru::ResourceCollectionund AWS: :RDS: :DBInstance im AWS CloudFormation Benutzerhandbuch.

Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung)

Mit „Enhanced Monitoring“ (Erweiterte Überwachung) können Sie das Betriebssystem Ihrer DB-Instance in Echtzeit überwachen. Wenn Sie sehen möchten, wie verschiedene Prozesse oder Threads die CPU verwenden, sind Enhanced Monitoring-Metriken nützlich.

Themen

Überblick über „Enhanced Monitoring“ (Erweiterte Überwachung)

Amazon RDS stellt in Echtzeit Metriken für das Betriebssystem bereit, auf dem Ihre DB-Instance ausgeführt wird. Sie können alle Systemmetriken und Prozessinformationen für Ihre RDS-DB-Instances in der Konsole anzeigen. Sie können verwalten, welche Metriken Sie für jede Instance überwachen möchten, und das Dashboard entsprechend Ihren Anforderungen anpassen. Beschreibungen der Metriken für Enhanced Monitoring finden Sie unter Betriebssystemmetriken im „Enhanced Monitoring“ (Erweiterte Überwachung).

RDS übermittelt die Metriken von Enhanced Monitoring an Ihr Amazon- CloudWatch Logs-Konto. Sie können Metrikfilter in CloudWatch aus CloudWatch Protokollen erstellen und die Diagramme im CloudWatch Dashboard anzeigen. Sie können die Enhanced Monitoring JSON-Ausgabe von CloudWatch Logs in einem Überwachungssystem Ihrer Wahl verwenden. Weitere Informationen finden Sie unterEnhanced Monitoring (Erweiterte Überwachung) in den Amazon RDS-FAQs.

Themen

Unterschiede zwischen Metriken für CloudWatch und Enhanced Monitoring

Ein Hypervisor erstellt und führt virtuelle Maschinen (VMs) aus. Mithilfe eines Hypervisors kann eine Instance mehrere Gast-VMs unterstützen, indem sie Speicher- und CPU. CloudWatch gathers-Metriken über die CPU-Auslastung vom Hypervisor für eine DB-Instance virtuell gemeinsam verwendet. Im Gegensatz dazu sammelt „Enhanced Monitoring“ (Erweiterte Überwachung) seine Metriken von einem Agenten auf der DB-Instance.

Möglicherweise finden Sie Unterschiede zwischen den Messungen CloudWatch und Enhanced Monitoring, da die Hypervisor-Ebene einen geringen Arbeitsaufwand ausführt. Die Unterschiede können größer sein, wenn Ihre DB-Instances kleinere Instance-Klassen verwenden. In diesem Szenario werden wahrscheinlich mehr virtuelle Maschinen (VMs) von der Hypervisorschicht auf einer einzelnen physischen Instance verwaltet.

Beschreibungen der Metriken für Enhanced Monitoring finden Sie unter Betriebssystemmetriken im „Enhanced Monitoring“ (Erweiterte Überwachung). Weitere Informationen zu CloudWatch Metriken finden Sie im Amazon- CloudWatch Benutzerhandbuch.

Aufbewahrung von Enhanced Monitoring-Metriken

Standardmäßig werden Enhanced Monitoring-Metriken 30 Tage lang in den CloudWatch Protokollen gespeichert. Dieser Aufbewahrungszeitraum unterscheidet sich von typischen CloudWatch Metriken.

Um zu ändern, wie lange die Metriken in den CloudWatch Protokollen gespeichert werden, ändern Sie die Aufbewahrung für die `RDSOSMetrics` Protokollgruppe in der CloudWatch Konsole. Weitere Informationen finden Sie unter Ändern der Aufbewahrung von Protokolldaten in CloudWatch - Protokollen im Amazon- CloudWatch Logs-Benutzerhandbuch.

Kosten für „Enhanced Monitoring“ (Erweiterte Überwachung)

Enhanced Monitoring-Metriken werden in den CloudWatch Protokollen gespeichert und nicht in CloudWatch Metriken. Die Kosten für „Enhanced Monitoring“ (Erweiterte Überwachung) hängen von folgenden Faktoren ab:

- Enhanced Monitoring wird Ihnen nur in Rechnung gestellt, wenn Sie das kostenlose Kontingent von Amazon CloudWatch Logs überschreiten. Die Gebühren basieren auf den Datenübertragungs- und Speichergebühren für CloudWatch Protokolle.
- Die Menge der für eine RDS-Instance übertragenen Informationen ist direkt proportional zur definierten Granularität für „Enhanced Monitoring“ (Erweiterte Überwachung). Ein kürzeres

Überwachungsintervall führt zu häufigeren Berichten über Betriebssystem-Metriken und erhöht Ihre Überwachungskosten. Um Kosten zu verwalten, legen Sie unterschiedliche Granularitäten für verschiedene Instances in Ihren Konten fest.

- Nutzungskosten für „Enhanced Monitoring“ (Erweiterte Überwachung) werden auf jede DB-Instance angewendet, für die Enhanced Monitoring (Erweiterte Überwachung) aktiviert ist. Die Überwachung einer großen Zahl von DB-Instances ist kostspieliger als die Überwachung von nur wenigen Instances.
- DB-Instances, die eine rechenintensivere Workload unterstützen, müssen mehr Aktivitäten von Betriebssystemprozessen melden und bedeuten höhere Kosten für „Enhanced Monitoring“ (Erweiterte Überwachung).

Weitere Informationen zu Preisen finden Sie unter Amazon- CloudWatch Preise.

Einrichten und Aktivieren von „Enhanced Monitoring“ (Erweiterte Überwachung)

Um „Enhanced Monitoring“ (Erweiterte Überwachung) zu verwenden, müssen Sie eine IAM-Rolle erstellen und dann „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren.

Themen

- So erstellen Sie eine IAM-Rolle für „Enhanced Monitoring“ (Erweiterte Überwachung)
- Aktivieren und Deaktivieren von „Enhanced Monitoring“ (Erweiterte Überwachung)
- Schutz vor dem Confused-Deputy-Problem

So erstellen Sie eine IAM-Rolle für „Enhanced Monitoring“ (Erweiterte Überwachung)

Enhanced Monitoring erfordert die Erlaubnis, in Ihrem Namen zu handeln, um Betriebssystem-Metrikinformationen an CloudWatch Logs zu senden. Sie gewähren Enhanced Monitoring-Berechtigungen mithilfe einer AWS Identity and Access Management (IAM-) Rolle. Sie können diese Rolle entweder erstellen, wenn Sie „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren oder vorher erstellen.

Themen

- Erstellen der IAM-Rolle, wenn Sie „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren
- Erstellen der IAM-Rolle, bevor Sie „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren

Erstellen der IAM-Rolle, wenn Sie „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren

Wenn Sie „Enhanced Monitoring“ (Erweiterte Überwachung) in der RDS-Konsole aktivieren, kann Amazon RDS die erforderliche IAM-Rolle für Sie erstellen. Der Name der Rolle lautet `rds-monitoring-role`. RDS verwendet diese Rolle für die angegebene DB-Instance, das Lesereplikat oder den Multi-AZ-DB-Cluster.

So erstellen Sie die IAM-Rolle beim Aktivieren von „Enhanced Monitoring“ (Erweiterte Überwachung)

1. Führen Sie die Schritte unter au Aktivieren und Deaktivieren von „Enhanced Monitoring“ (Erweiterte Überwachung).
2. Setzen Sie die Überwachungsrolle in dem Schritt, in dem Sie eine Rolle auswählen auf Standard.

Erstellen der IAM-Rolle, bevor Sie „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren

Sie können die erforderliche Rolle erstellen, bevor Sie „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren. Wenn Sie „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren, geben Sie den Namen Ihrer neuen Rolle an. Sie müssen diese erforderliche Rolle erstellen, wenn Sie „Enhanced Monitoring“ (Erweiterte Überwachung) mithilfe der AWS CLI oder RDS API aktivieren.

Der Benutzer, der „Enhanced Monitoring“ (Erweiterte Überwachung) aktiviert, muss über die `PassRole`-Berechtigung verfügen. Weitere Informationen finden Sie unter Beispiel 2 unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle an einen AWS Dienst im IAM-Benutzerhandbuch.

So erstellen Sie eine IAM-Rolle für „Enhanced Monitoring“ (Erweiterte Überwachung) in Amazon RDS

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie Rolle erstellen aus.
4. Wählen Sie die Registerkarte AWS -Service und RDS in der Liste der Services aus.
5. Wählen Sie RDS – Enhanced Monitoring (RDS – erweiterte Überwachung) und Next (Weiter) aus.
6. Vergewissern Sie sich, dass in den Berechtigungsrichtlinien AmazonRDS angezeigt wirdEnhancedMonitoringRole, und klicken Sie dann auf Weiter.
7. Geben Sie unter Role name (Rollenname) einen Namen für Ihre Rolle ein. Geben Sie z. B. ei **`emaccess`**.

Die vertrauenswürdige Entität für Ihre Rolle ist der AWS Service monitoring.rds.amazonaws.com.

8. Wählen Sie Rolle erstellen aus.

Aktivieren und Deaktivieren von „Enhanced Monitoring“ (Erweiterte Überwachung)

Sie können Enhanced Monitoring mithilfe der, oder RDS-API ein- und ausschalten. AWS Management Console AWS CLI Sie wählen die RDS-DB-Instances aus, auf denen Sie die „Enhanced Monitoring“ (Erweiterte Überwachung) aktivieren möchten. Sie können für jede DB-Instance unterschiedliche Granularitäten für die Metriksammlung festlegen.

Konsole

Sie können die erweiterte·Überwachung) aktivieren, wenn Sie einen DB-Cluster oder ein Lesereplikat erstellen oder wenn Sie eine DB-Instance ändern. Wenn Sie eine DB-Instance ändern, um „Enhanced Monitoring“·(Erweiterte·Überwachung) zu aktivieren, müssen Sie Ihre DB-Instance nicht neu starten, damit die Änderung wirksam wird.

Sie können „Enhanced Monitoring“·(Erweiterte·Überwachung) in der RDS-Konsole aktivieren, wenn Sie eine der folgenden Aktionen auf der Seite Databases (Datenbanken) ausführen:

- Erstellen einer DB-eines Clusters – Wählen Sie Create database (Datenbank erstellen) aus.
- Erstellen eines Lesereplikats – Wählen Sie Actions (Aktionen) und dann Create Read Replica (Lesereplikat erstellen) aus.
- Modify a DB instance (Eine DB-Instance ändern) – wählen Sie Modify (Ändern) aus.

„Enhanced Monitoring“ (Erweiterte Überwachung) in der RDS-Konsole aktivieren/deaktivieren

1. Scrollen Sie zu Additional Configuration (Zusätzliche Konfiguration).
2. Wählen Sie unter Monitoring Enable enhanced monitoring (Erweiterte Überwachung aktivieren) für Ihre DB-Instance oder Ihr Lesereplikat aus. Klicken Sie zum Deaktivieren von „Enhanced Monitoring“ (Erweiterte Überwachung) auf Disable Enhanced Monitoring (Erweiterte Überwachung deaktivieren).
3. Setzen Sie die Eigenschaft Monitoring Role auf die IAM-Rolle, die Sie erstellt haben, damit Amazon RDS für Sie mit Amazon CloudWatch Logs kommunizieren kann, oder wählen Sie Standard, damit RDS eine Rolle für Sie erstellt. `rds-monitoring-role`

4. Stellen Sie die Eigenschaft Granularity (Granularität) auf das Intervall (in Sekunden) zwischen Punkten ein, an denen Metriken für Ihre DB-Instance oder Ihr Lesereplikat erfasst werden. Die Eigenschaft Granularität kann auf einen der folgenden Werte eingestellt werden: `1`, `5`, `10`, `15`, `30` oder `60`.

   Die schnellste Aktualisierung der RDS-Konsole erfolgt alle 5 Sekunden. Wenn Sie die Granularität in der RDS-Konsole auf 1 Sekunde einstellen, sehen Sie die aktualisierten Metriken dennoch nur alle 5 Sekunden. Mithilfe von Logs können Sie Metrik-Updates innerhalb von einer CloudWatch Sekunde abrufen.

AWS CLI

Um Enhanced Monitoring mit den AWS CLI folgenden Befehlen zu aktivieren, setzen Sie die `--monitoring-interval` Option auf einen anderen Wert als `0` und setzen Sie die `--monitoring-role-arn` Option auf die Rolle, in So erstellen Sie eine IAM-Rolle für „Enhanced Monitoring“ (Erweiterte Überwachung) der Sie sie erstellt haben.

- create-db-instance
- create-db-instance-read-replikat
- modify-db-instance

Die Option `--monitoring-interval` gibt das Intervall in Sekunden zwischen den Punkten an, an denen Enhanced Monitoring-Metriken erfasst werden. Gültige Werte für die Option sind `0`, `1`, `5`, `10`, `15`, `30` und `60`.

Um Enhanced Monitoring mit dem zu deaktivieren AWS CLI, setzen Sie die `--monitoring-interval` Option `0` in diesen Befehlen auf.

Example

Im folgenden Beispiel wird „Enhanced Monitoring“·(Erweiterte·Überwachung) für eine DB-Instance aktiviert:

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --monitoring-interval 30 \
```

```
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --monitoring-interval 30 ^
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

Example

Im folgenden Beispiel wird „Enhanced Monitoring“·(Erweiterte·Überwachung) für ein Multi-AZ-DB-Cluster aktiviert:

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --monitoring-interval 30 \
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --monitoring-interval 30 ^
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

RDS-API

Um „Enhanced Monitoring“ (Erweiterte Überwachung) mithilfe der RDS API zu aktivieren, setzen Sie den Parameter `MonitoringInterval` auf einen anderen Wert als `0` und legen Sie den Parameter `MonitoringRoleArn` auf die Rolle fest, die Sie in So erstellen Sie eine IAM-Rolle für „Enhanced Monitoring“ (Erweiterte Überwachung) erstellt haben. Legen Sie diese Parameter in den folgenden Aktionen fest:

- CreateDBInstance
- B wurde erstellt InstanceReadReplica
- ModifyDBInstance

Der Parameter `MonitoringInterval` gibt das Intervall in Sekunden zwischen den Punkten an, an denen Enhanced Monitoring-Metriken erfasst werden. Gültige Werte sind: `0`, `1`, `5`, `10`, `15`, `30` und `60`.

Um „Enhanced Monitoring“ (Erweiterte Überwachung) mit Hilfe der RDS API zu deaktivieren, setzen Sie `MonitoringInterval` auf `0`.

Schutz vor dem Confused-Deputy-Problem

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zum Problem des verwirrten Stellvertreters führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben. Weitere Informationen finden Sie unter Confused-Deputy-Problem.

Um die Berechtigungen einzuschränken, die Amazon RDS einem anderen Service für eine Ressource gewährt, empfehlen wir die globalen Bedingungskontextschlüssel `aws:SourceArn` und `aws:SourceAccount` in einer Vertrauensrichtlinie für Ihre Enhanced-Monitoring-Rolle. Wenn Sie beide globalen Bedingungskontextschlüssel verwenden, müssen diese dieselbe Konto-ID verwenden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontextschlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Setzen Sie für Amazon RDS `aws:SourceArn` auf `arn:aws:rds:`*`Region`*`:`*`my-account-id`*`:db:`*`dbname`*.

Im folgenden Beispiel werden die globalen Bedingungskontextschlüssel `aws:SourceArn` und `aws:SourceAccount` in einer Vertrauensrichtlinie verwendet, um das Confused-Deputy-Problem zu verhindern.

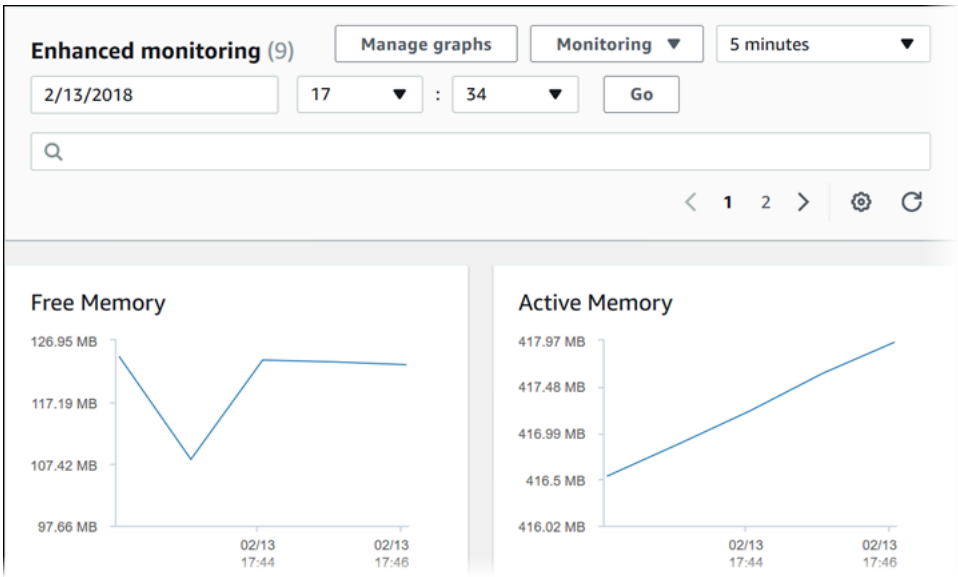
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "monitoring.rds.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:rds:Region:my-account-id:db:dbname"
        },
        "StringEquals": {
          "aws:SourceAccount": "my-account-id"
        }
      }
    }
  ]
}
```

Anzeigen von Betriebssystem-Metriken in der RDS-Konsole

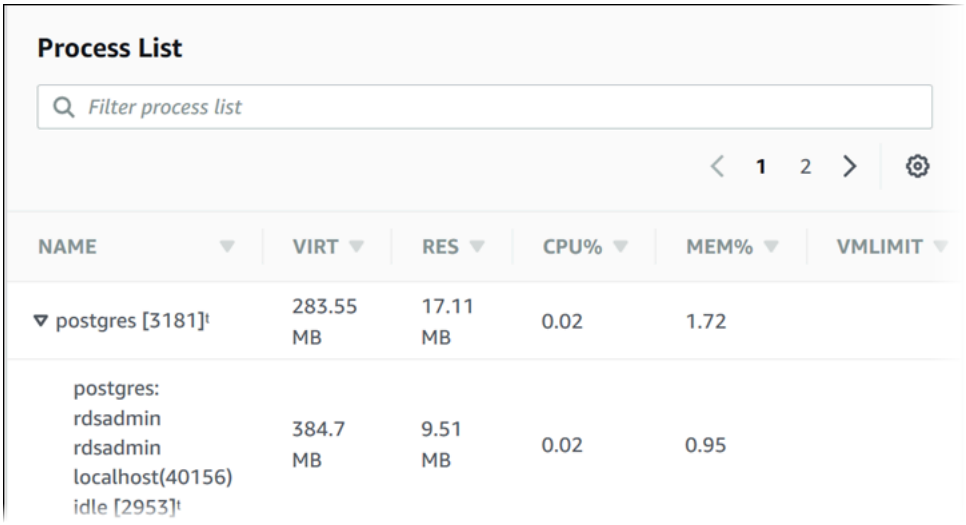
Sie können Betriebssystemmetriken anzeigen, die von Enhanced Monitoring in der RDS-Konsole gemeldet werden, indem Sie Enhanced monitoring (Erweiterte Überwachung) unter Monitoring (Überwachung) auswählen.

Das folgende Beispiel zeigt die Seite „Enhanced Monitoring“ an. Beschreibungen der Metriken für Enhanced Monitoring finden Sie unter Betriebssystemmetriken im „Enhanced Monitoring“ (Erweiterte Überwachung).



Wenn Sie Details für die auf Ihrer DB-Instance ausgeführten Prozesse ansehen möchten, wählen Sie die Betriebssystem-Prozessliste für Überwachung aus.

Die Ansicht Process List (Prozessliste) wird nachstehend angezeigt.



Die Enhanced Monitoring-Metriken, die in der Ansicht Process list (Prozessliste) gezeigt werden, sind wie folgt organisiert:

- RDS child processes (Untergeordnete RDS-Prozesse) – Zeigt eine Übersicht über die RDS-Prozesse, die die DB-Instance unterstützen, z. B. `aurora` für Amazon Aurora-DB-Cluster und . Prozess-Threads erscheinen unter dem übergeordneten Prozess. Prozess-Threads zeigen nur die CPU-Nutzung, da andere Metriken für alle Threads des Prozesses gleich sind. Die Konsole zeigt maximal 100 Prozesse und Threads. Das Ergebnis ist eine Kombination der CPU-intensivsten und Memory-intensivsten Prozesse und Threads. Wenn über 50 Prozesse und über 50 Threads vorhanden sind, zeigt die Konsole für jede Kategorie die 50 mit dem höchsten Verbrauch. Anhand dieser Anzeige können Sie feststellen, welche Prozesse die größte Auswirkung auf die Performance haben.
- RDS-Prozesse – Zeigt eine Übersicht über die vom RDS-Management-Agent verwendeten Ressourcen, Diagnoseüberwachungsprozesse und andere AWS-Prozesse, die zur Unterstützung von RDS-DB-Instances erforderlich sind.
- OS processes (Betriebssystemprozesse): Zeigt eine Übersicht über Kernel- und Systemprozesse, die im Allgemeinen einen geringen Einfluss auf die Performance haben.

Die aufgelisteten Elemente für jeden Prozess sind:

- VIRT: Zeigt die virtuelle Größe des Prozesses an.
- RES: Zeigt den tatsächlichen physischen Speicher an, der vom Prozess verwendet wird.
- CPU%: Zeigt den Prozentsatz der gesamten CPU-Bandbreite an, die vom Prozess verwendet wird.
- MEM%: Zeigt den Prozentsatz des Gesamtspeichers an, der vom Prozess verwendet wird.

Die in der RDS-Konsole gezeigten Überwachungsdaten werden aus Amazon CloudWatch Logs abgerufen. Sie können die Metriken für eine DB-Instance auch als Protokoll-Stream aus CloudWatch Logs abrufen. Weitere Informationen finden Sie unter Anzeigen von Betriebssystemmetriken mit CloudWatch Logs.

Metriken für „Enhanced Monitoring“ (Erweiterte Überwachung) werden in folgenden Situationen nicht geliefert:

- Failover der DB-Instance.
- Ändern der Instance-Klasse für die DB-Instance (Skalierung der Datenverarbeitung).

Metriken für „Enhanced Monitoring“ (Erweiterte Überwachung) werden während eines Neustarts einer DB-Instance zurückgegeben, da nur die Datenbank-Engine neu gestartet wird. Metriken für das Betriebssystem werden weiterhin mitgeteilt.

Anzeigen von Betriebssystemmetriken mit CloudWatch Logs

Nach dem Aktivieren von „Enhanced Monitoring“·(Erweiterte·Überwachung) für Ihre DB- den Cluster können Sie die Metriken dafür mithilfe von CloudWatch Logs ansehen, wobei jeder Protokoll-Stream eine einzelne überwachte DB-Instance oder ein DB-Cluster darstellt. Die Protokoll-Stream-Kennung ist die Ressourcenkennung (`DbiResourceId`) für die DB-Instance oder das DB-Cluster.

So zeigen Sie Enhanced Monitoring-Protokolldaten an

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie bei Bedarf die AWS-Region, in der sich Ihre DB-Cluster befindet. Weitere Informationen finden Sie unter Regionen und Endpunkte in der Allgemeinen Amazon Web Services-Referenz.
3. Wählen Sie im Navigationsbereich Protokolle.
4. Wählen Sie RDSOSMetrics in der Liste der Protokollgruppen.
5. Wählen Sie aus der Liste den Protokoll-Stream, den Sie anzeigen möchten.

Amazon Aurora-Referenz für Metriken

In dieser Referenz finden Sie Beschreibungen von Amazon Aurora-Metriken für Amazon CloudWatch, Performance Insights und „Enhanced Monitoring“ (Erweiterte Überwachung).

Themen

CloudWatch Amazon-Metriken für Amazon Aurora

Der `AWS/RDS`-Namespace umfasst die folgenden Metriken, die für Datenbankentitäten gelten, die in Amazon Aurora ausgeführt werden. Einige Metriken gelten entweder für Aurora MySQL, Aurora PostgreSQL oder beide. Darüber hinaus sind einige Metriken spezifisch für einen DB-Cluster, eine primäre DB-Instance, eine Replica-DB-Instance oder alle DB-Instances.

Informationen zu globalen Aurora-Datenbankmetriken finden Sie unter Amazon-CloudWatch-Metriken für die Schreibweiterleitung in Aurora MySQL und CloudWatch Amazon-Metriken für die Schreibweiterleitung in Aurora PostgreSQL. Informationen zu parallelen Aurora-Abfragemetriken finden Sie unter Überwachen von Parallel Query.

Themen

Metriken auf Clusterebene für Amazon Aurora

In der folgenden Tabelle werden Metriken beschrieben, die für Aurora-Cluster spezifisch sind.

Metriken auf Clusterebene für Amazon Aurora

Metrik	Beschreibung	Gilt für	Einheiten
`AuroraGlobalDBDataTransferBytes`	In einer Aurora Global Database die Menge der Redo-Log-Daten, die von der AWS Master-Region in eine sekundäre AWS Region übertragen wurden. **Note** Diese Metrik ist nur in der AWS-Regio n Sekundärregion verfügbar.	Aurora MySQL und Aurora PostgreSQL	Bytes
`AuroraGlobalDBProgressLag`	In einer Aurora Global Database das Maß dafür, wie weit der sekundäre Cluster sowohl bei Benutzert ransaktionen als auch bei Systemtransaktionen hinter dem primären Cluster zurückliegt. **Note** Diese Metrik ist nur im Sekundärbereich verfügbar AWS-Region.	Aurora MySQL und Aurora PostgreSQL	Milliseku nden
`AuroraGlobalDBReplicatedWriteIO`	In einer Aurora Global Database die Anzahl der I/O-Schreibvorgänge, die	Aurora MySQL	Anzahl

Metrik	Beschreibung	Gilt für	Einheiten
	von der primären AWS Region auf das Cluster-Volume in einer sekundären AWS Region repliziert wurden. Bei den Abrechnungsberechnungen für die sekundären AWS Regionen in einer globalen Datenbank werden Schreibvorgänge berücksichtigt`VolumeWriteIOPs`, die innerhalb des Clusters ausgeführt wurden. Bei den Abrechnungsberechnungen für die primäre AWS Region in einer globalen `VolumeWriteIOPs` Datenbank werden die Schreibaktivitäten innerhalb dieses Clusters und `AuroraGlobalDBReplicatedWriteIO` die regionsübergreifende Replikation innerhalb der globalen Datenbank berücksichtigt. **Note** Diese Metrik ist nur im sekundären AWS-Region Bereich verfügbar.	und Aurora PostgreSQL	

Metrik	Beschreibung	Gilt für	Einheiten
`AuroraGlobalDBReplicationLag`	In einer globalen Aurora-Datenbank, der Umfang der Verzögerung bei der Replikation von Updates aus der primären AWS -Region. **Note** Diese Metrik ist nur im Sekundärbereich verfügbar AWS-Region.	Aurora MySQL und Aurora PostgreSQL	Millisekunden
`AuroraGlobalDBRPOLag`	In einer Aurora Global Database ist die Recovery Point Objective (RPO) Verzögerungszeit. Diese Metrik misst, wie weit der sekundäre Cluster bei Benutzertransaktionen hinter dem primären Cluster zurückliegt. **Note** Diese Metrik ist nur im Sekundärbereich verfügbar AWS-Region.	Aurora MySQL und Aurora PostgreSQL	Millisekunden

Metrik	Beschreibung	Gilt für	Einheiten
`AuroraVolumeBytesLeftTotal`	Der verbleibende verfügbare Speicherplatz für das Cluster-Volume. Während das Cluster-Volume wächst, verringert sich dieser Wert. Wenn sie Null erreicht, meldet der Cluster einen out-of-space Fehler. Wenn Sie feststellen möchten, ob sich Ihr Aurora-MySQL-Cluster dem Größenlimit von 128 Tebibyte (TiB) nähert, kann dieser Wert einfacher und zuverlässiger überwacht werden als `VolumeBytesUsed` . `AuroraVolumeBytesLeftTotal` berücksichtigt Speicherplatz, der für die interne Verwaltung und andere Zuordnungen verwendet wird, die sich nicht auf Ihre Speicherabrechnung auswirken.	Aurora MySQL	Byte
`BacktrackChangeRecordsCreationRate`	Die Anzahl der Datensätze zur Rückverfolgungsänderung, die über 5 Minuten für den DB-Cluster erstellt wurden.	Aurora MySQL	Anzahl pro 5 Minuten

Metrik	Beschreibung	Gilt für	Einheiten
`BacktrackChangeRecordsStored`	Die Anzahl der Datensätze zur Rückverfolgungsänderung, die von Ihrem DB-Cluster verwendet werden.	Aurora MySQL	Anzahl
`BackupRetentionPeriodStorageUsed`	Die Gesamtmenge des Backup-Speichers, der zur Unterstützung der point-in-time Wiederherstellungsfunktion innerhalb des Backup-Aufbewahrungsfensters des Aurora-DB-Clusters verwendet wird. Dieser Wert ist in dem von der `TotalBackupStorageBilled` - Metrik gemeldeten Gesamtwert enthalten. Er wird für jeden Aurora-Cluster separat berechnet. Detaillierte Anweisungen finden Sie unter Grundlegendes zur Backup-Speicher-Nutzung in Amazon Aurora.	Aurora MySQL und Aurora PostgreSQL	Byte
`ServerlessDatabaseCapacity`	Die aktuelle Kapazität eines Aurora Serverless-DB-Clusters.	Aurora MySQL und Aurora PostgreSQL	Anzahl

Metrik	Beschreibung	Gilt für	Einheiten
`SnapshotStorageUsed`	Die gesamte Sicherungsspeicher, der von allen Aurora-Snapshots für einen Aurora-DB-Cluster außerhalb des Zeitfensters für die Aufbewahrung von Backups genutzt wird. Dieser Wert ist in dem von der `TotalBackupStorageBilled` -Metrik gemeldeten Gesamtwert enthalten. Er wird für jeden Aurora-Cluster separat berechnet. Detaillierte Anweisungen finden Sie unter Grundlegendes zur Backup-Speicher-Nutzung in Amazon Aurora.	Aurora MySQL und Aurora PostgreSQL	Byte

Metrik	Beschreibung	Gilt für	Einheiten
`TotalBackupStorageBilled`	Die gesamte Sicherungsspeicher in Bytes, der Ihnen für einen bestimmten Aurora-DB-Cluster in Rechnung gestellt wird. Die Metrik umfasst den Sicherungsspeicher gemessen von den Metriken `BackupRetentionPeriodStorageUsed` und `SnapshotStorageUsed`. Diese Metrik wird für jeden Aurora-Cluster separat berechnet. Detaillierte Anweisungen finden Sie unter Grundlegendes zur Backup-Speicher-Nutzung in Amazon Aurora.	Aurora MySQL und Aurora PostgreSQL	Bytes

Metrik	Beschreibung	Gilt für	Einheiten
`VolumeBytesUsed`	Die Menge an Speicherplatz, die von Ihrem Aurora-DB-Cluster verwendet wird. Dieser Wert wirkt sich auf die Kosten für den Aurora-DB-Cluster aus (Informationen zu Preisen erhalten Sie auf der Preisgestaltungsseite zu Amazon RDS). Dieser Wert berücksichtigt einige interne Speicherzuweisungen nicht, die keine Auswirkungen auf die Speicherabrechnung haben. Bei Aurora MySQL können Sie out-of-space Probleme genauer antizipieren, indem Sie testen, ob es `AuroraVolumeBytesLeftTotal` sich Null nähert, anstatt es mit dem Speicherlimit von 128 TiB zu `VolumeBytesUsed` vergleichen. Bei Clustern, bei denen es sich um Klone handelt, hängt der Wert dieser Metrik von der Menge der zum Klon hinzugefügten oder geänderten Daten ab. Die Metrik kann sich auch	Aurora MySQL und Aurora PostgreSQL	Byte

Metrik	Beschreibung	Gilt für	Einheiten
	erhöhen oder verringern, wenn der ursprüngliche Cluster gelöscht wird oder wenn neue Klone hinzugefügt oder gelöscht werden. Details hierzu finden Sie unter Löschen eines Quell-Cluster-Volumes		

Metrik	Beschreibung	Gilt für	Einheiten
`VolumeReadIOPs`	Die Anzahl von in Rechnung gestellten I/O-Operationen aus einem Cluster-Volume innerhalb eines fünfminütigen Intervalls. In Rechnung gestellte Leseoperationen werden auf Cluster-Volume-Ebene berechnet, aus allen Instances im Aurora-DB-Cluster zusammengestellt und dann in 5-minütigen Intervallen gemeldet. Der Wert wird anhand des Werts der Metrik für Read operations (Leseoperationen) über einen fünfminütigen Zeitraum berechnet. Sie können die Menge an in Rechnung gestellten Leseoperationen pro Sekunde bestimmen, indem Sie den Wert der Metrik Billed read operations (In Rechnung gestellte Operationen) durch 300 Sekunden teilen. Wenn beispielsweise die Metrik Billed read operations (In Rechnung gestellte Leseoperationen) den Wert 13 686 zurückgibt, wurden pro Sekunde 45 Leseopera	Aurora MySQL und Aurora PostgreSQL	Anzahl pro 5 Minuten

Metrik	Beschreibung	Gilt für	Einheiten
	tionen in Rechnung gestellt (13 686 / 300 = 45,62). In Rechnung gestellte Leseoperationen fallen für Abfragen für nicht im Buffer-Cache enthaltene Datenbankseiten an, die erst aus dem Speicher geladen werden müssen. Sie sehen evtl. Spitzenwerte in den in Rechnung gestellten Operationen, da Abfrageergebnisse aus dem Speicher gelesen und anschließend in den Buffer-Cache geladen werden. **Tip** Wenn Ihr Aurora-MySQL-Cluster eine parallele Abfrage verwendet, wird möglicherweise eine Zunahme der `VolumeReadIOPS` -Werte. Parallel Query verwendet den Bufferpool nicht. Obwohl die Abfragen schnell sind, kann diese optimierte Verarbeit		

Metrik	Beschreibung	Gilt für	Einheiten
	ung zu einem Anstieg der Lesevorgänge und damit verbundenen Gebühren führen.		
`VolumeWriteIOPs`	Die Anzahl an Write-Disk-I/O-Operationen im Cluster-Volume (Meldung in fünfminütigen Intervallen). Eine ausführliche Beschreibung, wie in Rechnung gestellte Schreibvorgänge berechnet werden, finden Sie unter `VolumeReadIOPs` .	Aurora MySQL und Aurora PostgreSQL	Anzahl pro 5 Minuten

Metriken auf Instance-Ebene für Amazon Aurora

Die folgenden instanzspezifischen CloudWatch Metriken gelten für alle Aurora MySQL- und Aurora PostgreSQL-Instances, sofern nicht anders angegeben.

Metriken auf Instance-Ebene für Amazon Aurora

Metrik	Beschreibung	Gilt für	Einheiten
`AbortedClients`	Die Anzahl der Clientverbindungen, die nicht ordnungsgemäß geschlossen wurden.	Aurora MySQL	Anzahl
`ActiveTransactions`	Die durchschnittliche Anzahl von aktuellen Transaktionen, die in einer Aurora-Datenbank-Instance pro Sekunde ausgeführt werden.	Aurora MySQL	Anzahl pro Sekunde

Metrik	Beschreibung	Gilt für	Einheiten
	Diese Metrik wird von Aurora standardmäßig nicht aktiviert. Um mit der Messung dieses Wertes zu beginnen, setzen Sie `innodb_monitor_enable='all'` in der DB-Parametergruppe für eine bestimmte DB-Instance.		
`ACUUtilization`	Der Wert der `ServerlessDatabaseCapacity` -Metrik geteilt durch den maximalen ACU-Wert des DB-Clusters. Diese Metrik gilt nur für Aurora Serverless v2.	Aurora MySQL und Aurora PostgreSQL	Prozentsatz

Metrik	Beschreibung	Gilt für	Einheiten
`AuroraBinlogReplicaLag`	Der Zeitmenge, die ein binärer Protokoll-Replikat -DB-Cluster, der in einer Aurora MySQL-kompatiblen Edition ausgeführt wird, hinter der binären Protokollreplikati onsquelle zurückbleibt. Eine Verzögerung bedeutet, dass die Quelle Datensätze schneller generiert, als das Replikat sie anwenden kann. Diese Metrik gibt je nach Engine-Version unterschi edliche Werte an: Aurora-MySQL-Version 2 Das `Seconds_B ehind_Master` - Feld des `SHOW SLAVE STATUS` von MySQL Aurora-MySQL-Version 3 `SHOW REPLICA STATUS` Sie können diese Metrik verwenden, um Fehler und Replikatverzögerung in einem Cluster zu überwachen, der als binäres Protokollreplikat fungiert. Der Metrikwert gibt Folgendes an:	Primär für Aurora MySQL	Sekunden

Metrik	Beschreibung	Gilt für	Einheiten

	Einen hohen Wert
	Das Replikat verzögert die Replikationsquelle.
	`0` oder einen Wert nahe `0`
	Der Replikatprozess ist aktiv und aktuell.
	`-1`
	Aurora kann die Verzögerung nicht ermitteln, die während der Replikateinrichtung auftreten kann oder wenn sich das Replikat in einem Fehlerzustand befindet.
	
	Da die Binärprotokollrepl ikation nur auf der Writer-In stance des Clusters stattfind et, empfehlen wir, die Version dieser Metrik zu verwenden , die mit der WRITER-Rolle verknüpft ist.
	
	Weitere Hinweise zum Verwalten der Replikation finden Sie unter Replizier en von Amazon-Aurora-MySQL-DB-Clustern über AWS-Regionen hinweg. Weitere Informationen zur Fehlerbehebung finden Sie		

Metrik	Beschreibung	Gilt für	Einheiten
	unter Replikationsprobleme mit Amazon Aurora MySQL.		
`AuroraEstimatedSharedMemoryBytes`	Die geschätzte Menge an freigegebenem Puffer oder Pufferpoolspeicher, die während des letzten konfigurierten Abfrageintervalls aktiv genutzt wurde.		Bytes
`AuroraOptimizedReadsCacheHitRatio`	Der Prozentsatz der Anfragen, die vom Cache für optimierte Lesevorgänge bedient werden. Der Wert wird anhand der folgenden Formel berechnet: `orcache_blks_hit/ (orcache_blks_hit + storage_blks_read)` Wenn der Wert 100% `AuroraOptimizedReadsCacheHitRatio` ist, bedeutet das, dass keine Seiten aus dem Cache für optimierte Lesevorgänge gelesen wurden. Der Wert ist also gleich`0`.	Primärer Knoten für Aurora PostgreSQL	Prozentsatz
`AuroraReplicaLag`	Der Verzögerungszeitraum für eine Aurora-Replica, wenn Updates aus der primären Instance repliziert werden.	Replica für Aurora MySQL und Aurora PostgreSQL	Millisekunden

Metrik	Beschreibung	Gilt für	Einheiten
`AuroraReplicaLagMaximum`	Der maximale Verzögerungszeitraum zwischen der primären Instance und einer der Aurora-DB-Instances im DB-Cluster. Wenn Read Replicas gelöscht oder umbenannt werden, kann es zu einem vorübergehenden Anstieg der Replikationsverzögerung kommen, da die alte Ressource einem Wiederverwendungsprozess unterzogen wird. Um eine genaue Darstellung der Replikationsverzögerung während dieses Zeitraums zu erhalten, empfehlen wir, die `AuroraReplicaLag` Metrik für jede Read Replica-Instanz zu überwachen.	Primärer Knoten für Aurora MySQL und Aurora PostgreSQL	Millisekunden
`AuroraReplicaLagMinimum`	Der minimale Verzögerungszeitraum zwischen der primären Instance und einer der Aurora-DB-Instances im DB-Cluster.	Primärer Knoten für Aurora MySQL und Aurora PostgreSQL	Millisekunden

Metrik	Beschreibung	Gilt für	Einheiten
AuroraSlowConnectionHandleCount	Die Anzahl der Verbindungen, die mindestens zwei Sekunden gewartet haben, um den Handshake zu starten. Diese Metrik gilt nur für Aurora MySQL Version 3.	Aurora MySQL	Anzahl
AuroraSlowHandshakeCount	Die Anzahl der Verbindungen, die mindestens 50 Millisekunden gewartet haben, um den Handshake zu beenden. Diese Metrik gilt nur für Aurora MySQL Version 3.	Aurora MySQL	Anzahl
BacktrackWindowActual	Der Unterschied zwischen dem Ziel-Backtrack-Fenster und dem tatsächlichen Backtrack-Fenster.	Primärer Knoten für Aurora MySQL	Minuten
BacktrackWindowAlert	Der Multiplikator, zu dem das tatsächliche Rückverfolgungsfenster für einen bestimmten Zeitraum kleiner als das Ziel-Rückverfolgungsfenster ist.	Primärer Knoten für Aurora MySQL	Anzahl
BlockedTransactions	Die durchschnittliche Anzahl an gesperrten Transaktionen in der Datenbank pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde

Metrik	Beschreibung	Gilt für	Einheiten
`BufferCacheHitRatio`	Der Prozentsatz der vom Buffer-Cache bedienten Anfragen.	Aurora MySQL und Aurora PostgreSQL	Prozentsatz
`CommitLatency`	Die durchschnittliche Dauer, die Engine und Speicher benötigen, um die Commit-Operationen abzuschließen.	Aurora MySQL und Aurora PostgreSQL	Milliseku nden
`CommitThroughput`	Durchschnittliche Anzahl der Commit-Operationen pro Sekunde.	Aurora MySQL und Aurora PostgreSQL	Anzahl pro Sekunde
`ConnectionAttempts`	Die Anzahl der Versuche, eine Verbindung mit einer Instance herzustellen, unabhängig davon, ob erfolgreich oder nicht.	Aurora MySQL	Anzahl

Metrik	Beschreibung	Gilt für	Einheiten
`CPUCreditBalance`	Die Anzahl der in 5-Minuten-Intervallen gemeldeten CPU-Guthaben, die eine Instance angesammelt hat. Sie können diese Metrik verwenden, um zu bestimmen, wie lange eine DB-Instance das normale Leistungslevel bei gegebener Leistungsrate übersteigen kann. Diese Metrik gilt nur für diese Instance-Klassen: • Aurora MySQL: `db.t2.small` , `db.t2.medium` , `db.t3` und `db.t4g` • Aurora PostgreSQL: `db.t3` und `db.t4g` **Note** Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter DB-	Aurora MySQL und Aurora PostgreSQL	Anzahl

Metrik	Beschreibung	Gilt für	Einheiten
	Instance-Klasse narten. Startguthaben funktioni eren in Amazon RDS genauso wie in Amazon EC2. Weitere Informationen finden Sie unter Launch credits (Startguthaben) im Amazon Elastic Compute Cloud-Ben utzerhandbuch für Linux-Ins tances.		

Metrik	Beschreibung	Gilt für	Einheiten
`CPUCreditUsage`	Die Anzahl der während des angegebenen Zeitraums verwendeten CPU-Guthaben (Meldung in 5-Minuten-Intervallen). Diese Metrik misst den Zeitraum, für den physikalische CPUs für die Verarbeitung von Instruktionen von den der DB-Instance zugeteilten virtuellen CPUs verwendet wurden. Diese Metrik gilt nur für diese Instance-Klassen: • Aurora MySQL: `db.t2.small` , `db.t2.medium` , `db.t3` und `db.t4g` • Aurora PostgreSQL: `db.t3` und `db.t4g` **Note** Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter DB-	Aurora MySQL und Aurora PostgreSQL	Anzahl

Metrik	Beschreibung	Gilt für	Einheiten
	Instance-Klassenarten.		
`CPUSurplusCreditBalance`	Die Anzahl überzähliger Guthaben, die von einer Unlimited-Instance verbraucht wurden, wenn ihr `CPUCreditBalance` -Wert null ist. Der `CPUSurplusCreditBalance` -Wert wird durch erworbene CPU-Guthaben abgezahlt. Wenn die Anzahl überzähliger Guthaben die Höchstzahl der Guthaben überschreitet, die die Instance in einem 24-Stunden-Zeitraum verdienen kann, fallen für die verbrauchten überzähligen Guthaben zusätzliche Gebühren an. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar.	Aurora MySQL und Aurora PostgreSQL	Guthaben (vCPU-Minuten)

Metrik	Beschreibung	Gilt für	Einheiten
`CPUSurplusCreditsCharged`	Die Anzahl verbrauchter überzähliger Guthaben, die nicht durch verdiente CPU-Guthaben zurückgezahlt wurden, und für die deshalb eine zusätzliche Gebühr anfällt. Verbrauchte überzähliger Guthaben werden in Rechnung gestellt, wenn einer der folgenden Fälle auftritt: • Die ausgegebenen überzähligen Guthaben überschreiten die maximale Anzahl an Guthaben, die die Instance in einem 24-Stunden-Zeitraum verdienen kann. Über das Maximum hinaus ausgegebene überzählige Guthaben werden am Ende der Stunde abgerechnet. • Die Instance wird angehalten oder beendet. • Die Instance wird von `unlimited` in `standard` geändert. Die Metriken für CPU-Guthaben sind nur mit einer	Aurora MySQL und Aurora PostgreSQL	Guthaben (vCPU-Minuten)

Metrik	Beschreibung	Gilt für	Einheiten
	fünfminütigen Frequenz verfügbar.		
`CPUUtilization`	Prozentsatz des gegenwärtig von einer Aurora-DB-Instance benutzten CPU-Speichers.	Aurora MySQL und Aurora PostgreSQL	Prozentsatz
`DatabaseConnections`	Die Anzahl der Clientnet zwerkverbindungen zur Datenbank-Instance. Die Anzahl der Datenbank sitzungen kann höher als der Metrikwert sein, da der Metrikwert Folgendes nicht enthält: • Sitzungen, die keine Netzwerkverbindung mehr haben, die die Datenbank jedoch nicht bereinigt hat • Sitzungen, die von der Datenbank-Engine für eigene Zwecke erstellt wurden • Sitzungen, die durch die Funktionen zur parallelen Ausführung der Datenbank -Engine erstellt wurden • Vom Auftrags-Scheduler der Datenbank-Engine erstellte Sitzungen • Amazon-Aurora-Verb indungen	Aurora MySQL und Aurora PostgreSQL	Anzahl

Metrik	Beschreibung	Gilt für	Einheiten
DDLLatency	Die durchschnittliche Dauer von Anfragen wie beispielsweise „Erstellen“, „Ändern“ und „Verwerfen von Anfragen“.	Aurora MySQL	Millisekunden
DDLThroughput	Die durchschnittliche Anzahl an DDL-Anfragen pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde
Deadlocks	Die durchschnittliche Anzahl an Deadlocks in der Datenbank pro Sekunde.	Aurora MySQL und Aurora PostgreSQL	Anzahl pro Sekunde
DeleteLatency	Die durchschnittliche Dauer von Löschvorgängen.	Aurora MySQL	Millisekunden
DeleteThroughput	Durchschnittliche Anzahl Delete-Abfragen pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde
DiskQueueDepth	Anzahl der offenstehenden I/O (Lese-/Schreibanforderungen), die auf die Festplatte zugreifen möchten.	Aurora MySQL und Aurora PostgreSQL	Anzahl
DMLLatency	Die durchschnittliche Dauer von Einfügungen, Aktualisierungen und Löschungen.	Aurora MySQL	Millisekunden
DMLThroughput	Durchschnittliche Anzahl von Einfügungen, Updates und Löschungen pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde

Metrik	Beschreibung	Gilt für	Einheiten
`EngineUptime`	Der Zeitraum, für den die Instance ausgeführt wurde.	Aurora MySQL und Aurora PostgreSQL	Sekunden
`FreeableMemory`	Verfügbarer Arbeitsspeicher.	Aurora MySQL und Aurora PostgreSQL	Bytes
`FreeEphemeralStorage`	Die Menge des verfügbaren flüchtigen NVMe-Speicherplatzes	Aurora PostgreSQL	Bytes

Metrik	Beschreibung	Gilt für	Einheiten
`FreeLocalStorage`	Die Menge des verfügbaren lokalen Speichers. Im Gegensatz zu anderen DB-Engines gibt diese Metrik für Aurora DB-Instances die Menge des für jede DB-Instance verfügbaren Speichers an. Dieser Wert hängt von der DB-Instance-Klasse ab (Informationen zu den Preisen erhalten Sie auf der Preisgestaltungsseite zu Amazon RDS). Sie können die Menge an freiem Speicherplatz für eine Instance erhöhen, indem Sie eine größere DB-Instance-Klasse für Ihre Instance auswählen. (Dies gilt nicht für Aurora Serverless v2.)	Aurora MySQL und Aurora PostgreSQL	Bytes
`InsertLatency`	Die durchschnittliche Dauer von Einfügeoperationen.	Aurora MySQL	Millisekunden
`InsertThroughput`	Durchschnittliche Anzahl der Einfügeoperationen pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde
`LoginFailures`	Die durchschnittliche Anzahl fehlgeschlagener Anmeldeversuche pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde

Metrik	Beschreibung	Gilt für	Einheiten
`MaximumUsedTransactionIDs`	Das Alter der ältesten nicht vakuumierten Transaktions-ID in Transaktionen. Erreicht dieser Wert 2.146.483.648 (2^31 - 1.000.000), wird die Datenbank in den Nur-Lese-Modus gezwungen, um den Wraparound der Transaktions-ID zu vermeiden. Weitere Informationen finden Sie unter Transaktions-ID-Wraparound-Fehler vermeiden in der PostgreSQL-Dokumentation.	Aurora PostgreSQL	Anzahl
`NetworkReceiveThroughput`	Die Menge des Netzwerkdurchsatzes, den jede Instance im Aurora-DB-Cluster von Clients erhält. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im Aurora-DB-Cluster und dem Cluster-Volume.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde (Konsole zeigt Megabyte pro Sekunde an)

Metrik	Beschreibung	Gilt für	Einheiten
`NetworkThroughput`	Die Menge des Netzwerkd urchsatzes, der von jeder Instance im Aurora-DB-Cluster sowohl von Clients empfangen als auch an diese übertragen wird. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im Aurora-DB-Cluster und dem Cluster-Volume.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde
`NetworkTransmitThroughput`	Die Menge des von Clients gesendeten Netzwerkd urchsatzes für jede Instance im Aurora-DB-Cluster. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im -DB-Cluster und dem Cluster-Volumen.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde (Konsole zeigt Megabyte pro Sekunde an)
`NumBinaryLogFiles`	Die Anzahl der generierten Binärprotokolldateien.	Aurora MySQL	Anzahl
`OldestReplicationSlotLag`	Der Verzögerungsgrößen wert des Replikats, das in Bezug auf die empfangen en Write-Ahead-Log-Daten (WAL) die höchste Verzögeru ng aufweist.	Aurora PostgreSQL	Bytes

Metrik	Beschreibung	Gilt für	Einheiten
`PurgeBoundary`	Transaktionsnummer, bis zu der InnoDB-Bereinigung zulässig ist. Wenn sich diese Metrik über einen längeren Zeitraum nicht weiterent wickelt, ist dies ein gutes Anzeichen dafür, dass das Löschen von InnoDB durch Transaktionen mit langer Laufzeit blockiert wird. Überprüfen Sie zur Untersuchung die aktiven Transaktionen auf Ihrem Aurora MySQL-DB-Cluster.	Aurora MySQL Version 2, Versionen 2.11 und höher	Anzahl
`PurgeFinishedPoint`	Transaktionsnummer, bis zu der die InnoDB-Bereinigung durchgeführt wird. Mithilfe dieser Metrik können Sie untersuchen, wie schnell die InnoDB-Bereinigung voranschreitet.	Aurora MySQL Version 2, Versionen 2.11 und höher	Anzahl
`Queries`	Durchschnittliche Anzahl der ausgeführten Abfragen pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde
`RDSToAuroraPostgreSQLReplicaLag`	Die Verzögerung bei der Replikation von Updates aus einer primären RDS PostgreSQL-Instance in andere Knoten im Cluster.	Replica für Aurora PostgreSQL	Sekunden

Metrik	Beschreibung	Gilt für	Einheiten
`ReadIOPS`	Die durchschnittliche Anzahl der Datenträger-E/A-Operationen pro Sekunde, gibt Lese- und Schreib-IOPS jedoch separat und in 1-Minuten-Intervallen an.	Aurora MySQL und Aurora PostgreSQL	Anzahl pro Sekunde
`ReadIOPSEphemeralStorage`	Die durchschnittliche Anzahl von Festplatten-I/O-Lesevorgängen im flüchtigen NVMe-Speicher	Aurora PostgreSQL	Anzahl pro Sekunde
`ReadLatency`	Die durchschnittliche Dauer für einen Festplatten-I/O-Vorgang.	Aurora MySQL und Aurora PostgreSQL	Sekunden
`ReadLatencyEphemeralStorage`	Die durchschnittliche Zeit, die pro Festplatten-I/O-Lesevorgang für den flüchtigen NVMe-Speicher benötigt wird	Aurora PostgreSQL	Millisekunden
`ReadThroughput`	Die durchschnittliche Anzahl Byte, die pro Sekunde vom Datenträger gelesen werden.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde
`ReadThroughputEphemeralStorage`	Die durchschnittliche Anzahl von Bytes, die pro Sekunde von der Festplatte für den flüchtigen NVMe-Speicher gelesen werden.	Aurora PostgreSQL	Bytes pro Sekunde
`ReplicationSlotDiskUsage`	Die Menge an Speicherplatz, die von Replikationsslotdateien belegt wird.	Aurora PostgreSQL	Bytes

Metrik	Beschreibung	Gilt für	Einheiten
ResultSetCacheHitRatio	Der Prozentsatz der vom Ergebnismengen-Cache bedienten Anfragen.	Aurora MySQL	Percentage
RollbackSegmentHistoryListLength	Die Protokolle für das Rückgängigmachen, die festgeschriebene Transaktionen mit zum Löschen markierten Datensätzen aufzeichnen. Diese Datensätze sind für die Verarbeitung durch den InnoDB-Löschvorgang geplant.	Aurora MySQL	Anzahl
RowLockTime	Die Gesamtzeit für das Erfassen von Zeilensperren für InnoDB-Tabellen.	Aurora MySQL	Millisekunden
SelectLatency	Die durchschnittliche Zeit für ausgewählte Vorgänge.	Aurora MySQL	Millisekunden
SelectThroughput	Durchschnittliche Anzahl Select-Abfragen pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde
ServerlessDatabaseCapacity	Die aktuelle Kapazität eines Aurora Serverless-DB-Clusters.	Aurora MySQL und Aurora PostgreSQL	Anzahl
StorageNetworkReceiveThroughput	Der Umfang des vom Aurora-Speicheruntersystem erhaltenen Netzwerkdurchsatzes für jede Instance im DB-Cluster.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde

Metrik	Beschreibung	Gilt für	Einheiten
StorageNetworkThroughput	Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Aurora-DB-Cluster vom Aurora-Speichersubsystem empfangen und an dieses gesendet wird.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde
StorageNetworkTransmitThroughput	Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Aurora-DB-Cluster an das Aurora-Speichersubsystem gesendet wird.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde
SumBinaryLogSize	Die Gesamtgröße der Binärprotokolldateien.	Aurora MySQL	Byte
SwapUsage	Die Größe des verwendeten Auslagerungsbereichs. Diese Metrik ist für die folgenden DB-Instance-Klassen nicht verfügbar: • db.r3.*, db.r4.* und db.r7g.* (Aurora MySQL) • db.r7g.* (Aurora PostgreSQL)	Aurora MySQL und Aurora PostgreSQL	Bytes

Metrik	Beschreibung	Gilt für	Einheiten
`TempStorageIOPS`	Die Anzahl der IOPS sowohl für Lese- als auch Schreibvorgänge, die im lokalen Speicher durchgeführt werden, der der DB-Instance angefügt ist. Diese Metrik stellt eine Zählung dar und wird einmal pro Sekunde gemessen. Diese Metrik gilt nur für Aurora Serverless v2.	Aurora MySQL und Aurora PostgreSQL	Anzahl pro Sekunde
`TempStorageThroughput`	Die Menge der mit der DB-Instance verknüpften Daten, die in und aus dem lokalen Speicher übertragen wurden. Diese Metrik wird in Byte angegeben und einmal pro Sekunde gemessen. Diese Metrik gilt nur für Aurora Serverless v2.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde

Metrik	Beschreibung	Gilt für	Einheiten
`TransactionLogsDiskUsage`	Der von Transaktionsprotokollen genutzte Festplattenplatz auf der DB-Instance von Aurora-PostgreSQL. Diese Metrik wird nur generiert, wenn Aurora PostgreSQL logische Replikation oder verwendet. AWS Database Migration Service Standardmäßig verwendet Aurora PostgreSQL Protokolldatensätze, nicht Transaktionsprotokolle. Wenn Transaktionsprotokolle nicht verwendet werden, lautet der Wert für diese Metrik `-1`.	Primärer Knoten für Aurora PostgreSQL	Bytes
`TruncateFinishedPoint`	Transaktions-ID, bis zu der die Kürzung rückgängig gemacht wird.	Aurora MySQL Version 2, Versionen 2.11 und höher	Anzahl
`UpdateLatency`	Die durchschnittliche Zeit für Aktualisierungsvorgänge.	Aurora MySQL	Millisekunden
`UpdateThroughput`	Durchschnittliche Anzahl Updates pro Sekunde.	Aurora MySQL	Anzahl pro Sekunde

Metrik	Beschreibung	Gilt für	Einheiten
`WriteIOPS`	Die Anzahl der pro Sekunde generierten Aurora-Sp eicherdatensätze. Dies entspricht etwa der Anzahl der Protokolldatensätze, die von der Datenbank generiert werden. Diese entsprech en weder den 8K-Seiten -Schreibvorgängen noch den gesendeten Netzwerkp aketen.	Aurora MySQL und Aurora PostgreSQL	Anzahl pro Sekunde
`WriteIOPSEphemeral Storage`	Die durchschnittliche Anzahl von Festplatten-I/O-Sc hreibvorgängen im flüchtigen NVMe-Speicher	Aurora PostgreSQL	Anzahl pro Sekunde
`WriteLatency`	Die durchschnittliche Dauer für einen Festplatten-I/O-Vo rgang.	Aurora MySQL und Aurora PostgreSQL	Sekunden
`WriteLatencyEpheme ralStorage`	Die durchschnittliche Zeit, die pro Festplatten-I/O-Sc hreibvorgang für den flüchtige n NVMe-Speicher benötigt wird	Aurora PostgreSQL	Milliseku nden
`WriteThroughput`	Die durchschnittliche Anzahl von Bytes, die jede Sekunde in persistenten Speicher geschrieben werden.	Aurora MySQL und Aurora PostgreSQL	Bytes pro Sekunde

Metrik	Beschreibung	Gilt für	Einheiten
`WriteThroughputEphemeralStorage`	Die durchschnittliche Anzahl von Bytes, die pro Sekunde für den flüchtigen NVMe-Speicher auf die Festplatte geschrieben werden	Aurora PostgreSQL	Bytes pro Sekunde

CloudWatch Amazon-Nutzungsmetriken für Amazon Aurora

Der `AWS/Usage` Namespace in Amazon CloudWatch enthält Nutzungsmetriken auf Kontoebene für Ihre Amazon RDS-Servicekontingenten. CloudWatch sammelt automatisch Nutzungsmetriken für alle. AWS-Regionen

Weitere Informationen finden Sie unter CloudWatch Nutzungsmetriken im CloudWatch Amazon-Benutzerhandbuch. Weitere Informationen zu Kontingenten finden Sie unter Kontingente und Beschränkungen für Amazon Aurora und Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Metrik	Beschreibung	Einheiten *
`DBClusterParameterGroups`	Die Anzahl der DB-Cluster-Parametergruppen in Ihrem AWS-Konto. In der Anzahl sind keine Standardparameterg ruppen enthalten.	Anzahl
`DBClusters`	Die Anzahl der Amazon-Aurora-DB-Cluster in Ihrem AWS-Konto.	Anzahl
`DBInstances`	Die Anzahl der DB-Instances in Ihrem AWS-Konto.	Anzahl
`DBParameterGroups`	Die Anzahl der DB-Parametergruppen in Ihrem AWS-Konto . In der Anzahl sind keine Standard-DB-Parametergruppen enthalten.	Anzahl
`DBSubnetGroups`	Die Anzahl der DB-Subnetzgruppen in Ihrem AWS-Konto . In der Anzahl ist die Standardsubnetzgruppe nicht enthalten.	Anzahl

Metrik	Beschreibung	Einheiten *
`ManualClusterSnapshots`	Die Anzahl der manuell erstellten DB-Cluster-Snapshots in Ihrem AWS-Konto. In der Anzahl sind ungültige Snapshots nicht enthalten.	Anzahl
`OptionGroups`	Die Anzahl der Optionsgruppen in Ihrem AWS-Konto . In der Anzahl sind die Standardoptionsgruppen nicht enthalten.	Anzahl
`ReservedDBInstances`	Die Anzahl der reservierten DB-Instances in Ihrem AWS-Konto. In der Anzahl sind außer Betrieb genommene oder abgelehnte Instances nicht enthalten.	Anzahl

> **Note**
>
> Amazon RDS veröffentlicht keine Einheiten für Nutzungsmetriken CloudWatch. Die Einheiten werden nur in der Dokumentation angezeigt.

Amazon-CloudWatch-Dimensionen für Aurora

Sie können Aurora-Metrikdaten filtern, indem Sie eine beliebige Dimension in der folgenden Tabelle verwenden.

Dimension	Filtert die angeforderten Daten für . . .
`DBInstanceIdentifier`	Eine angegebene DB-Instance.
`DBClusterIdentifier`	Ein angegebener Aurora-DB-Cluster.
`DBClusterIdentifier, Role`	Ein bestimmter Aurora-DB-Cluster, der die Metrik nach Instance-Rolle zusammenfasst (WRITER/READER). Sie können beispielsweise Metriken für alle READER-Instances eines Clusters zusammenfassen.

Dimension	Filtert die angeforderten Daten für . . .
`DbClusterIdentifier, EngineName`	Eine spezifische Kombination von Aurora-DB-Cluster und Engine-Name. Sie können beispielsweise die `VolumeReadIOPs` -Metrik für den Cluster `ams1` und die Engine `aurora` anzeigen.
`DatabaseClass`	Alle Instances in einer Datenbankklasse. Sie können beispielsweise Metriken für alle Instances der Datenbankklasse zusammenfassen `db.r5.large` .
`EngineName`	Nur der identifizierte Engine-Name. Sie können beispielsweise Metriken für alle Instances mit dem Engine-Namen zusammenfassen `aurora-postgresql` .
`SourceRegion`	Nur die angegebene Region. Sie können beispielsweise Metriken für alle DB-Instances in der Region `us-east-1` zusammenfassen.

Verfügbarkeit von Aurora Metriken in der Amazon RDS Konsole

Nicht alle Metriken, die von Amazon Aurora bereitgestellt werden, sind in der Amazon-RDS-Konsole verfügbar. Sie können diese Metriken mithilfe von Tools wie der AWS CLI und der CloudWatch API anzeigen. Zudem werden einige Metriken in der Amazon-RDS-Konsole entweder für eine bestimmte Instance-Klasse oder mit verschiedenen Namen und Messeinheiten angezeigt.

Themen

- Aurora-Metriken, die in der Ansicht „Last Hour“ (Letzte Stunde) verfügbar sind
- Aurora Metriken in bestimmten Fällen verfügbar
- Aurora-Metriken, die nicht in der Konsole verfügbar sind

Aurora-Metriken, die in der Ansicht „Last Hour“ (Letzte Stunde) verfügbar sind

Sie können eine Teilmenge von kategorisierten Aurora-Metriken in der Standard-Ansicht für die letzte Stunde in der Amazon-RDS-Konsole anzeigen. Die folgende Tabelle listet die Kategorien

und zugehörigen Metriken auf, die in der Amazon RDS-Konsole für eine Aurora-Instance angezeigt werden.

Kategorie	Metriken

SQL	`ActiveTransactions`
	`BlockedTransactions`
	`BufferCacheHitRatio`
	`CommitLatency`
	`CommitThroughput`
	`DatabaseConnections`
	`DDLLatency`
	`DDLThroughput`
	`Deadlocks`
	`DMLLatency`
	`DMLThroughput`
	`LoginFailures`
	`ResultSetCacheHitRatio`
	`SelectLatency`
	`SelectThroughput`

System (System)	`AuroraReplicaLag`
	`AuroraReplicaLagMaximum`
	`AuroraReplicaLagMinimum`
	`CPUCreditBalance`

Kategorie	Metriken

	`CPUCreditUsage`
	`CPUUtilization`
	`FreeableMemory`
	`FreeLocalStorage` (Dies gilt nicht für Aurora Serverless v2.)
	`NetworkReceiveThroughput`

Bereitstellung	`AuroraReplicaLag`
	`BufferCacheHitRatio`
	`ResultSetCacheHitRatio`
	`SelectThroughput`

Aurora Metriken in bestimmten Fällen verfügbar

Zusätzlich werden einige Aurora-Metriken entweder für eine bestimmte Instance-Klasse oder nur für DB-Instances mit verschiedenen Namen und verschiedenen Messeinheiten angezeigt.

- Die Metriken `CPUCreditBalance` und `CPUCreditUsage` werden nur für Aurora MySQL-`db.t2`-Instance-Klassen und für Aurora PostgreSQL-`db.t3`-Instance-Klassen angezeigt.
- Eine Auflistung der Metriken, die mit verschiedenen Namen angezeigt werden:

Metrik	Anzeigename
`AuroraReplicaLagMaximum`	Maximalverzögerung des Replicas
`AuroraReplicaLagMinimum`	Minimalverzögerung des Replicas
`DDLThroughput`	DDL
`NetworkReceiveThroughput`	Netzwerkdurchsatz
`VolumeBytesUsed`	[Fakturiertes] Volumen der verwendeten Bytes

Metrik	Anzeigename
VolumeReadIOPs	[Fakturiertes] Volumen gelesene IOPS
VolumeWriteIOPs	[Fakturiertes] Volumen geschriebene IOPS

- Die folgenden Metriken gelten für das gesamte Aurora-DB-Cluster, werden jedoch nur angezeigt, wenn DB-Instances für ein Aurora-DB-Cluster in der Amazon RDS-Konsole angezeigt werden:
  - VolumeBytesUsed
  - VolumeReadIOPs
  - VolumeWriteIOPs
- Die folgenden Metriken werden in der Amazon RDS-Konsole in Megabytes, anstatt in Bytes angezeigt:
  - FreeableMemory
  - FreeLocalStorage
  - NetworkReceiveThroughput
  - NetworkTransmitThroughput
- Die folgenden Metriken gelten für einen Aurora PostgreSQL-DB-Cluster mit Aurora Optimized Reads:
  - AuroraOptimizedReadsCacheHitRatio
  - FreeEphemeralStorage
  - ReadIOPSEphemeralStorage
  - ReadLatencyEphemeralStorage
  - ReadThroughputEphemeralStorage
  - WriteIOPSEphemeralStorage
  - WriteLatencyEphemeralStorage
  - WriteThroughputEphemeralStorage

Aurora-Metriken, die nicht in der Konsole verfügbar sind

Die folgenden Aurora Metriken sind in der Amazon RDS Konsole nicht verfügbar:

- AuroraBinlogReplicaLag
- DeleteLatency

- DeleteThroughput
- EngineUptime
- InsertLatency
- InsertThroughput
- NetworkThroughput
- Queries
- UpdateLatency
- UpdateThroughput

CloudWatch Amazon-Metriken für Performance Insights

Performance Insights veröffentlicht automatisch einige Kennzahlen auf Amazon CloudWatch. Dieselben Daten können von Performance Insights abgefragt werden, aber wenn die Metriken vorhanden sind, ist es einfach, Alarme hinzuzufügen CloudWatch. CloudWatch Es macht es auch einfach, die Metriken zu bestehenden CloudWatch Dashboards hinzuzufügen.

Metrik	Beschreibung
DBLoad	Anzahl der aktiven Sitzungen für die DB-Engine In der Regel sind Sie an den Daten für die durchschnittliche Anzahl der aktiven Sitzungen interessiert. Diese Daten werden in Performan ce Insights als abgefrag `db.load.avg` .
DBLoadCPU	Anzahl aktiver Sitzungen mit dem Warteerei gnistyp CPU Diese Daten werden in Performan ce Insights als `db.load.avg` abgefragt, gefiltert durch den Warteereignistyp `CPU`.
DB-CPU LoadNon	Anzahl aktiver Sitzungen mit einem anderen Warteereignistyp als CPU

> **Note**
>
> Diese Metriken werden CloudWatch nur veröffentlicht, wenn die DB-Instance belastet ist.

Sie können diese Metriken mithilfe der CloudWatch Konsole AWS CLI, der oder der CloudWatch API untersuchen. Sie können auch andere Performance Insights Insights-Zählermetriken mithilfe einer speziellen mathematischen Metrikfunktion untersuchen. Weitere Informationen finden Sie unter Abfragen anderer Performance Insights Insights-Zählermetriken in CloudWatch.

Sie können beispielsweise die Statistiken für die `DBLoad` Metrik abrufen, indem Sie den get-metric-statisticsBefehl ausführen.

```
aws cloudwatch get-metric-statistics \
    --region us-west-2 \
    --namespace AWS/RDS \
    --metric-name DBLoad  \
    --period 60 \
    --statistics Average \
    --start-time 1532035185 \
    --end-time 1532036185 \
    --dimensions Name=DBInstanceIdentifier,Value=db-loadtest-0
```

Dieses Beispiel generiert eine Ausgabe wie die folgende.

```
{
  "Datapoints": [
  {
  "Timestamp": "2021-07-19T21:30:00Z",
  "Unit": "None",
  "Average": 2.1
  },
  {
  "Timestamp": "2021-07-19T21:34:00Z",
  "Unit": "None",
  "Average": 1.7
  },
  {
  "Timestamp": "2021-07-19T21:35:00Z",
  "Unit": "None",
  "Average": 2.8
```

```
},
{
"Timestamp": "2021-07-19T21:31:00Z",
"Unit": "None",
"Average": 1.5
},
{
"Timestamp": "2021-07-19T21:32:00Z",
"Unit": "None",
"Average": 1.8
},
{
"Timestamp": "2021-07-19T21:29:00Z",
"Unit": "None",
"Average": 3.0
},
{
"Timestamp": "2021-07-19T21:33:00Z",
"Unit": "None",
"Average": 2.4
}
],
"Label": "DBLoad"
}
```


Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

Abfragen anderer Performance Insights Insights-Zählermetriken in CloudWatch

Sie können RDS Performance Insights Insights-Metriken von abfragen, Alarme ausgeben und Grafiken erstellen CloudWatch. Sie können auf Informationen zu Ihrer zugreifen, indem Sie die `DB_PERF_INSIGHTS` metrische mathematische Funktion für verwenden CloudWatch. Mit dieser Funktion können Sie die Performance Insights Insights-Metriken verwenden, an die nicht direkt berichtet wird CloudWatch , um eine neue Zeitreihe zu erstellen.

Sie können die neue Metric Math-Funktion verwenden, indem Sie im Bildschirm Metrik auswählen in der CloudWatch Konsole auf das Drop-down-Menü Mathematik hinzufügen klicken. Sie können damit Alarme und Grafiken zu Performance Insights-Metriken oder zu Kombinationen von CloudWatch Performance Insights Insights-Metriken erstellen, einschließlich hochauflösender Alarme für Metriken unter einer Minute. Sie können die Funktion auch programmgesteuert verwenden, indem Sie den

Metric Math-Ausdruck in eine Anfrage aufnehmen. `get-metric-data` Weitere Informationen finden Sie unter Mathematische Syntax und Funktionen von Metriken und Erstellen eines Alarms für Performance Insights Insights-Zählermetriken aus einer AWS Datenbank.

Performance-Insights-Zählermetriken

Zählermetriken sind Betriebssystem- und Datenbank-Performance-Metriken im Performance-Insights-Dashboard. Um Leistungsprobleme zu identifizieren und zu analysieren, können Sie Zählermetriken mit der DB-Last korrelieren. Sie können der Metrik eine Statistikfunktion hinzufügen, um die Metrikwerte abzurufen. Die unterstützten Funktionen für die Metrik `os.memory.active` sind beispielsweise `.avg`, `.min`, `.max`,`.sum` und `.sample_count`.

Die Zählermetriken werden einmal pro Minute erfasst. Die Erfassung der Betriebssystemmetriken hängt davon ab, ob die erweiterte Überwachung aktiviert oder deaktiviert ist. Wenn die erweiterte Überwachung deaktiviert ist, werden die Betriebssystemmetriken einmal pro Minute erfasst. Ist die erweiterte Überwachung aktiviert, werden die Betriebssystemmetriken für den ausgewählten Zeitraum erfasst. Weitere Informationen zum Aktivieren und Deaktivieren der erweiterten Überwachung finden Sie unter Aktivieren und Deaktivieren von „Enhanced Monitoring“ (Erweiterte Überwachung).

Themen

- Performance Insights-Betriebssystemzähler
- Performance Insights-Zähler für Aurora MySQL
- Performance Insights-Zähler für Aurora PostgreSQL

Performance Insights-Betriebssystemzähler

Die folgenden Betriebssystemzähler, denen `os` vorangestellt ist, sind bei Performance Insights für Aurora PostgreSQL und Aurora MySQL verfügbar.

Sie können die `ListAvailableResourceMetrics`-API für die Liste der verfügbaren Zählermetriken für Ihre DB-Instance verwenden. Weitere Informationen finden Sie ListAvailableResourceMetricsim Amazon RDS Performance Insights API-Referenzhandbuch.

Zähler	Typ	Metrik	Beschreibung
Aktiv	Arbeitsspeicher	os.memory.active	Umfang des zugewiesenen

Zähler	Typ	Metrik	Beschreibung
			Arbeitsspeichers in Kilobyte.
Puffer	Arbeitsspeicher	os.memory.buffers	Umfang des verwendeten Arbeitsspeichers für die Pufferung von I/O-Anfragen vor dem Schreiben auf das Speichergerät, in Kilobyte.
Cached	Arbeitsspeicher	os.memory.cached	Die Größe des verwendeten Arbeitsspeichers für das Caching von Dateisystem-basierter I/O in Kilobyte.
DB Cache	Arbeitsspeicher	os.memory.db.cache	Die Größe des Arbeitsspeichers, die vom Datenbank prozess einschließlich tmpfs (shmem) für den Seiten-Cache verwendet wird, in Byte.

Zähler	Typ	Metrik	Beschreibung
DB Resident Set Size	Arbeitsspeicher	os.memory.db.resident SetSize	Die Größe des Arbeitsspeichers, die vom Datenbankprozess ohne tmpfs (shmem) für den anonymen Cache und den Swap-Cache verwendet wird, in Byte.
DB Swap	Arbeitsspeicher	os.memory.db.swap	Die Größe des Arbeitsspeichers, die vom Datenbankprozess für Swap verwendet wird, in Byte.
Dirty	Arbeitsspeicher	os.memory.dirty	Menge an Memory-Pages im RAM, die geändert, aber noch nicht in den entsprechenden Datenblock im Speicher geschrieben wurden, in Kilobyte.
Kostenfrei	Arbeitsspeicher	os.memory.free	Umfang des nicht zugewiesenen Arbeitsspeichers in Kilobyte.
Huge Pages frei	Arbeitsspeicher	os.memory.riesigPagesFree	Die Anzahl von freien "Huge Pages". "Huge Pages" sind eine Funktion des Linux-Kernel.

Zähler	Typ	Metrik	Beschreibung
Huge Pages reserviert	Arbeitsspeicher	os.memory.riesig PagesRsvd	Die Anzahl von gebundenen "Huge Pages".
Größe Huge Pages	Arbeitsspeicher	os.memory.riesig PagesSize	Die Größe für jede Huge Pages-Einheit, in Kilobyte.
Überschuss Huge Pages	Arbeitsspeicher	os.memory.riesig PagesSurp	Die Anzahl der verfügbaren überzähligen Huge Pages.
Huge Pages insgesamt	Arbeitsspeicher	os.memory.riesig PagesTotal	Die Gesamtzahl der Huge Pages.
Inaktiv	Arbeitsspeicher	os.memory.inactive	Umfang der am seltensten verwendeten Memory-Pages in Kilobyte.
Mapped	Arbeitsspeicher	os.memory.mapped	Die Gesamtmenge der Dateisysteminhalte, die Arbeitsspeicher in einem Prozess-Adressraum zugeordnet ist, in Kilobyte.s
Out of Memory Kill Count	Arbeitsspeicher	os.memory.outOfMemory KillCount	Die Anzahl der OOM-Kills im letzten Erfassungsintervall.

Zähler	Typ	Metrik	Beschreibung
Seitentabellen	Arbeitsspeicher	os.memory.pageTables	Umfang des von Page-Tabellen verwendeten Arbeitsspeichers in Kilobyte.
Slab	Arbeitsspeicher	os.memory.slab	Umfang der wiederverwendbaren Kernel-Datenstrukturen in Kilobyte.
Gesamt	Arbeitsspeicher	os.memory.total	Gesamtumfang des Arbeitsspeichers in Kilobyte.
Writeback	Arbeitsspeicher	os.memory.writeback	Gesamtumfang an modifizierten Speicherbereichen im RAM, die noch in den Sicherungsspeicher geschrieben werden, in Kilobyte.
Guest	CPU-Auslastung	os.cpuUtilization.guest	Der prozentuale Anteil der von Gastprogrammen verwendeten CPU.
Inaktiv	CPU-Auslastung	os.cpuUtilization.idle	Der prozentuale Anteil der CPU, der sich im Leerlauf befindet.
Irq	CPU-Auslastung	os.cpuUtilization.irq	Der prozentuale Anteil der von Software-Interrupts verwendeten CPU.

Zähler	Typ	Metrik	Beschreibung
Nice	CPU-Auslastung	os.cpuUtilization.nice	Der prozentuale Anteil der von Programmen mit niedrigster Priorität verwendeten CPU.
Steal	CPU-Auslastung	os.cpuUtilization.steal	Der prozentuale Anteil der von virtuellen Maschinen verwendeten CPU.
System (System)	CPU-Auslastung	os.cpuUtilization.system	Der prozentuale Anteil der vom Kernel verwendeten CPU.
Gesamt	CPU-Auslastung	os.cpuUtilization.total	Der prozentuale Anteil der insgesamt verwendeten CPU. Diese Angabe enthält den Nice-Wert.
Benutzer	CPU-Auslastung	os.cpuUtilization.user	Der prozentuale Anteil der von Benutzerprogrammen verwendeten CPU.
Wait	CPU-Auslastung	os.cpuUtilization.wait	Der Prozentsatz der unbenutzten CPU während des Wartens auf I/O-Zugriff.
Aurora Storage Aurora Storage Bytes Rx	Festplatten-IO	os.Diskio.AuroraStorage.Aurora RxStorageBytes	Die Anzahl der pro Sekunde für Aurora-Speicher empfangenen Byte.

Zähler	Typ	Metrik	Beschreibung
Aurora Storage Aurora Storage Bytes Tx	Festplatten-IO	StorageBytesos.Diskio.AuroraStorage.Aurora Tx	Die Anzahl der pro Sekunde für Aurora-Speicher hochgeladenen Byte.
Aurora Storage Disk Queue Depth	Festplatten-IO	os.Diskio.AuroraStorage.Disk QueueDepth	Die Länge der Aurora-Speicher-Festplattenwarteschlange.
Aurora Storage Read IOs PS	Festplatten-IO	os.diskIO.auroraStorage.readIOsPS	Die Anzahl der Lesevorgänge pro Sekunde.
Aurora Storage Read Latency	Festplatten-IO	os.diskIO.auroraStorage.readLatency	Die durchschnittliche Latenz einer I/O-Leseanforderung an den Aurora-Speicher in Millisekunden.
Aurora Storage Read Throughput	Festplatten-IO	os.diskIO.auroraStorage.readThroughput	Die Menge des Netzwerkdurchsatzes, der von Anforderungen an den DB-Cluster verwendet wird, in Bytes pro Sekunde.
Aurora Storage Write IOs PS	Festplatten-IO	os.diskIO.auroraStorage.writeIOsPS	Die Anzahl der Schreibvorgänge pro Sekunde.

Zähler	Typ	Metrik	Beschreibung
Aurora Storage Write Latency	Festplatten-IO	os.diskIO.auroraStorage.writeLatency	Die durchschnittliche Latenz einer I/O-Schreibanforderung an den Aurora-Speicher in Millisekunden.
Aurora Storage Write Throughput	Festplatten-IO	os.diskIO.auroraStorage.writeThroughput	Die Menge des Netzwerkdurchsatzes, der von Antworten vom DB-Cluster verwendet wird, in Bytes pro Sekunde.
Rdstemp Avg Queue Len	Festplatten-IO	os.DiskIO.rdstemp.avg QueueLen	Die Anzahl der Anfragen, die in der Warteschlange des I/O-Geräts warten.
Rdstemp Avg Req Sz	Festplatten-IO	os.DiskIO.rdstemp.avg ReqSz	Die Anzahl der Anfragen, die in der Warteschlange des I/O-Geräts warten.
Rdstemp Await	Festplatten-IO	os.diskIO.rdstemp.await	Die erforderliche Anzahl an Millisekunden für die Antwort auf Anfragen, einschließlich Warteschlangen- und Servicedauer.
Rdstemp Read IOs PS	Festplatten-IO	os.diskIO.rdstemp.readIOsPS	Die Anzahl der Lesevorgänge pro Sekunde.

Zähler	Typ	Metrik	Beschreibung
Rdstemp Read KB	Festplatten-IO	os.diskIO.rdstemp.readKb	Gesamtzahl der gelesenen Kilobyte.
Rdstemp Read KB PS	Festplatten-IO	os.diskIO.rdstemp.readKbPS	Die Anzahl der pro Sekunde gelesenen Kilobyte.
Rdstemp Rrqm PS	Festplatten-IO	os.diskIO.rdstemp.rrqmPS	Die Anzahl der zusammengeführten Leseanfragen in der Warteschlange pro Sekunde.
Rdstemp TPS	Festplatten-IO	os.diskIO.rdstemp.tps	Die Anzahl der I/O-Transaktionen pro Sekunde.
Rdstemp Util	Festplatten-IO	os.diskIO.rdstemp.util	Der Prozentsatz der CPU-Zeit, während der Anfragen ausgegeben wurden.
Rdstemp Write IOs PS	Festplatten-IO	os.diskIO.rdstemp.writeIOsPS	Die Anzahl der Schreibvorgänge pro Sekunde.
Rdstemp Write KB	Festplatten-IO	os.diskIO.rdstemp.writeKb	Gesamtzahl der geschriebenen Kilobyte.
Rdstemp Write KB PS	Festplatten-IO	os.diskIO.rdstemp.writeKbPS	Die Anzahl der pro Sekunde geschriebenen Kilobyte.

Zähler	Typ	Metrik	Beschreibung
Rdstemp Wrqm PS	Festplatten-IO	os.diskIO.rdstemp.wrqmPS	Die Anzahl der zusammengeführten Schreibanfragen in der Warteschlange pro Sekunde.
Blocked	Aufgaben	os.tasks.blocked	Die Anzahl von blockierten Aufgaben.
In Ausführung	Aufgaben	os.tasks.running	Die Anzahl von laufenden Aufgaben.
Sleeping	Aufgaben	os.tasks.sleeping	Die Anzahl von Aufgaben im Ruhezustand.
Angehalten	Aufgaben	os.tasks.stopped	Die Anzahl von angehaltenen Aufgaben.
Gesamt	Aufgaben	os.tasks.total	Die Gesamtanzahl der Aufgaben.
Zombie	Aufgaben	os.tasks.zombie	Die Anzahl der untergeordneten Aufgaben, die unter einer aktiven übergeordneten Aufgabe inaktiv sind.
One	Durchschnittliche Auslastung Minute	os.load .one AverageMinute	Die Anzahl der Prozesse, die während der letzten Minute CPU-Zeit angefordert haben.

Zähler	Typ	Metrik	Beschreibung
Fifteen	Durchschnittliche Auslastung Minute	os.load AverageMinute .fifteen	Die Anzahl der Prozesse, die während der letzten 15 Minuten CPU-Zeit angefordert haben.
Five	Durchschnittliche Auslastung Minute	os.load AverageMinute .five	Die Anzahl der Prozesse, die während der letzten 5 Minuten CPU-Zeit angefordert haben.
Cached	Auslagerung	os.swap.cached	Umfang des Swap-Arbeitsspeichers, der als Cache-Speicher verwendet wird, in Kilobyte.
Kostenfrei	Auslagerung	os.swap.free	Die Menge des freien Swap-Arbeitsspeichers in Kilobyte.
In	Auslagerung	os.swap.in	Die Menge des von der Festplatte ausgelagerten Speichers in Kilobyte.
Out	Auslagerung	os.swap.out	Die Menge des auf die Festplatte ausgelagerten Speichers in Kilobyte.
Gesamt	Auslagerung	os.swap.total	Die Gesamtmenge des verfügbaren Swap-Arbeitsspeichers in Kilobyte.

Zähler	Typ	Metrik	Beschreibung
Max Files	Dateisystem	os.fileSys.maxFiles	Die maximale Anzahl an Dateien, die für das Dateisyst em erstellt werden können.
Used Files	Dateisystem	os.fileSys.usedFiles	Die Anzahl der Dateien im Dateisyst em.
Used File Percent	Dateisystem	os.FileSys.Used FilePercent	Der Prozentsatz von verfügbaren Dateien, die in Gebrauch sind.
Used Percent	Dateisystem	os.fileSys.usedPer cent	Der prozentuale Anteil des verwendeten Speicherplatzes für das Dateisystem.
Used	Dateisystem	os.fileSys.used	Der durch Dateien belegte Speicherp latz im Dateisystem in Kilobyte.
Gesamt	Dateisystem	os.fileSys.total	Die Gesamtmenge des für das Dateisyst em verfügbaren Speicherplatzes in Kilobyte.
Rx	Network (Netzwerk)	os.network.rx	Die Anzahl der pro Sekunde empfangen en Byte.

Zähler	Typ	Metrik	Beschreibung
Tx	Network (Netzwerk)	os.network.tx	Die Anzahl der pro Sekunde hochgelad enen Byte.
Acu Utilization	Allgemeines	os.general.acuUtil ization	Der Anteil der aktuellen Kapazität an der maximal konfiguri erten Kapazität in Prozent.
Max Configured Acu	Allgemeines	os.general.max ConfiguredAcu	Die vom Benutzer konfigurierte maximale Kapazität in ACUs.
Min Configured Acu	Allgemeines	os.general.min ConfiguredAcu	Die vom Benutzer konfigurierte Mindestkapazität in ACUs.
Num VCPUs	Allgemeines	os.general.numVCPU s	Die Anzahl der virtuellen CPUs für die DB-Instance.
Serverless Database Capacity	Allgemeines	os.general.serverlos DatabaseCapacity	Die aktuelle Kapazität der Instance in ACUs.

Performance Insights-Zähler für Aurora MySQL

Die folgenden Datenbankzähler sind bei Performance Insights für Aurora MySQL verfügbar.

Themen

- Native Zähler für Aurora MySQL
- Nicht-native Zähler für Aurora MySQL

Native Zähler für Aurora MySQL

Native Metriken werden von der Datenbank-Engine und nicht von Amazon Aurora definiert. Sie finden Definitionen dieser nativen Metriken unter Serverstatusvariablen in der MySQL-Dokumentation.

Zähler	Typ	Einheit	Metrik
Com_analyze	SQL	Abfragen pro Sekunde	db.SQL.Com_analyze
Com_optimize	SQL	Abfragen pro Sekunde	db.SQL.Com_optimize
Com_select	SQL	Abfragen pro Sekunde	db.SQL.Com_select
Innodb_rows_deleted	SQL	Zeilen pro Sekunde	db.SQL.Innodb_rows_deleted
Innodb_rows_inserted	SQL	Zeilen pro Sekunde	db.SQL.Innodb_rows_inserted
Innodb_rows_read	SQL	Zeilen pro Sekunde	db.SQL.Innodb_rows_read
Innodb_rows_updated	SQL	Zeilen pro Sekunde	db.SQL.Innodb_rows_updated
Abfragen	SQL	Abfragen pro Sekunde	db.SQL.Queries
Fragen	SQL	Abfragen pro Sekunde	db.SQL.Questions

Zähler	Typ	Einheit	Metrik
Select_full_join	SQL	Abfragen pro Sekunde	db.SQL.Select_full_join
Select_full_range_join	SQL	Abfragen pro Sekunde	db.SQL.Select_full_range_join
Bereich auswählen	SQL	Abfragen pro Sekunde	db.SQL.Select_range
Select_range_check	SQL	Abfragen pro Sekunde	db.SQL.Select_range_check
Select_scan	SQL	Abfragen pro Sekunde	db.SQL.Select_scan
Slow_queries	SQL	Abfragen pro Sekunde	db.SQL.Slow_queries
Sort_merge_passes	SQL	Abfragen pro Sekunde	db.SQL.Sort_merge_passes
Sort_range	SQL	Abfragen pro Sekunde	db.SQL.Sort_range
Sort_rows	SQL	Abfragen pro Sekunde	db.SQL.Sort_rows

Zähler	Typ	Einheit	Metrik
Sort_scan	SQL	Abfragen pro Sekunde	db.SQL.Sort_scan
Total_query_time	SQL	Millisekunden	db.SQL.Total_query_time
Table_locks_immediate	Sperren	Anforderungen pro Sekunde	db.Locks.Table_locks_immediate
Table_locks_waited	Sperren	Anforderungen pro Sekunde	db.Locks.Table_locks_waited
Innodb_row_lock_time	Sperren	Millisekunden (durchschnittlich)	db.Locks.Innodb_row_lock_time
Aborted_clients	Benutzer	Verbindungen	db.Users.Aborted_clients
Aborted_connects	Benutzer	Verbindungen	db.Users.Aborted_connects
Verbindungen	Benutzer	Verbindungen	db.Users.Connections
External_threads_connected	Benutzer	Verbindungen	db.Users.External_threads_connected
max_connections	Benutzer	Verbindungen	db.User.max_connections
Threads_connected	Benutzer	Verbindungen	db.Users.Threads_connected

Zähler	Typ	Einheit	Metrik
Threads_created	Benutzer	Verbindungen	db.Users.Threads_created
Threads_running	Benutzer	Verbindungen	db.Users.Threads_running
Created_tmp_disk_tables	Temporäre Dateien	Tabellen pro Sekunde	db.Temp.Created_tmp_disk_tables
Created_tmp_tables	Temporäre Dateien	Tabellen pro Sekunde	db.Temp.Created_tmp_tables
Innodb_buffer_pool_pages_data	Cache	Seiten	db.Cache.Innodb_buffer_pool_pages_data
Innodb_buffer_pool_pages_total	Cache	Seiten	db.Cache.Innodb_buffer_pool_pages_total
Innodb_buffer_pool_read_requests	Cache	Seiten pro Sekunde	db.Cache.Innodb_buffer_pool_read_requests
Innodb_buffer_pool_reads	Cache	Seiten pro Sekunde	db.Cache.Innodb_buffer_pool_reads
Opened_tables	Cache	Tabellen	db.Cache.Opened_tables
Opened_table_definitions	Cache	Tabellen	db.Cache.Opened_table_definitions
Qcache_hits	Cache	Abfragen	db.Cache.Qcache_hits

Nicht-native Zähler für Aurora MySQL

Nicht-native Zähler-Metriken sind durch Amazon RDS definierte Zähler. Eine nicht-native Metrik kann eine Metrik sein, die Sie mit einer bestimmten Abfrage erhalten. Eine nicht-native Metrik kann

auch eine abgeleitete Metrik sein, bei der zwei oder mehrere native Zähler bei Berechnungen von Verhältnissen, Trefferraten oder Latenzen verwendet werden.

Zähler	Typ	Metrik	Beschreibung	Definition
innodb_buffer_pool_hits	Cache	db.Cache.innoDB_buffer_pool_hits	Die Anzahl der Lesevorgänge, die InnoDB aus dem Pufferpool verarbeiten konnte.	`innodb_buffer_pool_read_requests - innodb_buffer_pool_reads`
innodb_buffer_pool_hit_rate	Cache	db.Cache.innoDB_buffer_pool_hit_rate	Der Prozentsatz der Lesevorgänge, den InnoDB aus dem Pufferpool verarbeiten konnte.	`100 * innodb_buffer_pool_read_requests / (innodb_buffer_pool_read_requests + innodb_buffer_pool_reads)`
innodb_buffer_pool_usage	Cache	db.Cache.innoDB_buffer_pool_usage	Die Prozentsatz des InnoDB-Pufferpools, der Daten (Seiten) enthält. **Note** Bei komprimierten Tabellen kann dieser Wert variieren. Weitere Informationen finden Sie in den Angaben	`Innodb_buffer_pool_pages_data / Innodb_buffer_pool_pages_total * 100.0`

Zähler	Typ	Metrik	Beschreibung	Definition
			zu `Innodb_buffer_pool_pages_data` und `Innodb_buffer_pool_pages_total` unter Serverstatusvariablen in der MySQL-Dokumentation.	
query_cache_hit_rate	Cache	db.Cache.query_cache_hit_rate	Die Trefferrate des MySQL-Ergebnissatz-Caches (Abfrage-Cache).	`Qcache_hits / (QCache_hits + Com_select) * 100`
innodb_rows_changed	SQL	db.SQL.innodb_rows_changed	Die Gesamtzahl von InnoDB-Zeilenvorgängen.	`db.SQL.Innodb_rows_inserted + db.SQL.Innodb_rows_deleted + db.SQL.Innodb_rows_updated`
active_transactions	Transaktionen	db.Transactions.active_transactions	Die Gesamtzahl aktiver Transaktionen.	`SELECT COUNT(1) AS active_transactions FROM INFORMATION_SCHEMA.INNODB_TRX`

Zähler	Typ	Metrik	Beschreibung	Definition
trx_rseg_history_len	Transaktionen	db.Transactions.trx_rseg_history_len	Eine Liste der Undo-Protokollseiten für übernommene Transaktionen, die vom InnoDB-Transaktionssystem verwaltet wird, um die Parallelitätskontrolle für mehrere Versionen zu implementieren. Weitere Informationen zu Undo-Protokolleinträgen finden Sie unter https://dev.mysql.com/doc/refman/8.0/en/innodb-multi-versioning.html in der MySQL-Dokumentation.	`SELECT COUNT AS trx_rseg_history_len FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='trx_rseg_history_len'`
innodb_deadlocks	Sperren	db.Locks.innodb_deadlocks	Die Gesamtzahl von Deadlocks.	`SELECT COUNT AS innodb_deadlocks FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_deadlocks'`

Zähler	Typ	Metrik	Beschreibung	Definition
innodb_lock_timeouts	Sperren	db.Locks.innodb_lock_timeouts	Die Gesamtanzahl von Deadlocks, die das Zeitlimit überschritten haben.	`SELECT COUNT AS innodb_lock_timeouts FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_timeouts'`
innodb_row_lock_waits	Sperren	db.Locks.innodb_row_lock_waits	Die Gesamtanzahl von Zeilensperren, die zu einer Wartezeit geführt haben.	`SELECT COUNT AS innodb_row_lock_waits FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_row_lock_waits'`

Performance Insights-Zähler für Aurora PostgreSQL

Die folgenden Datenbankzähler sind bei Performance Insights für Aurora PostgreSQL verfügbar.

Themen

- Native Zähler für Aurora PostgreSQL
- Nicht-native Zähler für Aurora PostgreSQL

Native Zähler für Aurora PostgreSQL

Native Metriken werden von der Datenbank-Engine und nicht von Amazon Aurora definiert. Definitionen dieser nativen Metriken finden Sie unter Anzeigen von Statistiken in der PostgreSQL-Dokumentation.

Zähler	Typ	Einheit	Metrik
tup_deleted	SQL	Tupel pro Sekunde	db.SQL.tup_deleted
tup_fetched	SQL	Tupel pro Sekunde	db.SQL.tup_fetched
tup_inserted	SQL	Tupel pro Sekunde	db.SQL.tup_inserted
tup_returned	SQL	Tupel pro Sekunde	db.SQL.tup_returned
tup_updated	SQL	Tupel pro Sekunde	db.SQL.tup_updated
blks_hit	Cache	Blöcke pro Sekunde	db.Cache.blks_hit
buffers_alloc	Cache	Blöcke pro Sekunde	db.Cache.buffers_alloc
buffers_checkpoint	Prüfpunkt	Blöcke pro Sekunde	db.Checkpoint.buffers_checkpoint
checkpoints_req	Prüfpunkt	Prüfpunkte pro Minute	db.Checkpoint.checkpoints_req
checkpoint_sync_time	Prüfpunkt	Millisekunden pro Prüfpunkt	db.Checkpoint.checkpoint_sync_time
checkpoints_timed	Prüfpunkt	Prüfpunkte pro Minute	db.Checkpoint.checkpoints_timed
checkpoint_write_time	Prüfpunkt	Millisekunden pro Prüfpunkt	db.Checkpoint.checkpoint_write_time
maxwritten_clean	Prüfpunkt	Bgwriter-Bereinigungsstopps pro Minute	db.Checkpoint.maxwritten_clean
Deadlocks	Gleichzeitigkeit	Deadlocks pro Minute	db.Concurrency.deadlocks
blk_read_time	I/O	Millisekunden	db.IO.blk_read_time

Zähler	Typ	Einheit	Metrik
blks_read	I/O	Blöcke pro Sekunde	db.IO.blks_read
buffers_backend	I/O	Blöcke pro Sekunde	db.IO.buffers_backend
buffers_backend_fsync	I/O	Blöcke pro Sekunde	db.IO.buffers_backend_fsync
buffers_clean	I/O	Blöcke pro Sekunde	db.IO.buffers_clean
temp_bytes	Temporäre Dateien	Bytes pro Sekunde	db.Temp.temp_bytes
temp_files	Temporäre Dateien	Dateien pro Minute	db.Temp.temp_files
xact_commit	Transaktionen	Commits pro Sekunde	db.Transactions.xact_commit
xact_rollback	Transaktionen	Rollbacks pro Sekunde	db.Transactions.xact_rollback
numbackends	Benutzer	Verbindungen	db.User.numbackends
archived_count	WAL	Dateien pro Minute	db.WAL.archived_count

Nicht-native Zähler für Aurora PostgreSQL

Nicht-native Zähler-Metriken sind durch Amazon Aurora definierte Zähler. Eine nicht-native Metrik kann eine Metrik sein, die Sie mit einer bestimmten Abfrage erhalten. Eine nicht-native Metrik kann auch eine abgeleitete Metrik sein, bei der zwei oder mehrere native Zähler bei Berechnungen von Verhältnissen, Trefferraten oder Latenzen verwendet werden.

Zähler	Typ	Metrik	Beschreibung	Definition
checkpoint_sync_latency	Prüfpunkt	db.Checkpoint.checkpoint_sync_latency	Die Gesamtzeit, die auf den Teil der Prüfpunkt verarbeitung aufgewendet wurde, bei dem Dateien auf der Festplatte synchronisiert werden.	`checkpoint_sync_time / (checkpoints_timed + checkpoints_req)`
checkpoint_write_latency	Prüfpunkt	db.Checkpoint.checkpoint_write_latency	Die Gesamtzeit, die auf den Teil der Prüfpunkt verarbeitung aufgewendet wurde, bei dem Dateien auf die Festplatte geschrieben werden.	`checkpoint_write_time / (checkpoints_timed + checkpoints_req)`
local_blks_read	I/O	db.IO.local_blks_read	Gesamtzahl der gelesenen lokalen Blöcke	–
local_blk_read_time	I/O	db.IO.local_blk_read_time	Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit für das Lesen von lokalen Datendateiblöcken in Millisekunden aufgezeichnet. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.	–
orcache_blks_hit	I/O	db.IO.orcache_blks_hit	Gesamtzahl der Treffer von gemeinsam genutzten Blöcken aus dem Cache für optimierte Lesevorgänge	–

Zähler	Typ	Metrik	Beschreibung	Definition
orcache_blk_read_time	I/O	db.IO.orcache_blk_read_time	Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit für das Lesen von Datendateiblöcken aus dem Cache für optimierte Lesevorgänge in Millisekunden aufgezeichnet. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.	-
read_latency	I/O	db.IO.read_latency	Die Zeit, die für das Lesen von Datendateiblöcken durch Backends in dieser Instance aufgewendet wurde.	`blk_read_time / blks_read`
storage_blks_read	I/O	db.IO.storage_blks_read	Gesamtzahl der gemeinsam genutzten Blöcke, die aus dem Aurora-Speicher gelesen wurden	-

Zähler	Typ	Metrik	Beschreibung	Definition
storage_blk_read_time	I/O	db.IO.storage_blk_read_time	Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit für das Lesen von Datendateiblöcken aus dem Aurora-Speicher in Millisekunden aufgezeichnet. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.	–
idle_in_transaction_aborted_count	Status	db.state.idle_in_transaction_aborted_count	Die Anzahl der Sitzungen im Bundesstaat. `idle in transaction (aborted)`	–
idle_in_transaction_count	Status	db.state.idle_in_transaction_count	Die Anzahl der Sitzungen im Bundesstaat. `idle in transaction`	–
idle_in_transaction_max_time	Status	db.state.idle_in_transaction_max_time	Die Dauer der am längsten laufenden Transaktion im Bundesstaat in Sekunden. `idle in transaction`	–
logical_reads	SQL	db.SQL.logical_reads	Gesamtzahl der Blöcke, auf die zugegriffen und die gelesen wurden.	`blks_hit + blks_read`
queries_started	SQL	db.SQL.queries	Die Anzahl der gestarteten Abfragen.	–

Zähler	Typ	Metrik	Beschreibung	Definition
queries_finished	SQL	db.SQL.queries	Die Anzahl der abgeschlossenen Abfragen.	–
total_query_time	SQL	db.SQL.total_query_time	Die Gesamtzeit, die für die Ausführung von Anweisungen aufgewendet wurde, in Millisekunden.	–
active_transactions	Transaktionen	db.Transactions.active_transactions	Die Anzahl der aktiven Transaktionen.	–
blocked_transactions	Transaktionen	db.Transactions.blocked_transactions	Die Anzahl der blockierten Transaktionen.	–
commit_latency	Transaktionen	db.Transactions.commit_latency	Die durchschnittliche Dauer von Commit-Vorgängen.	`db.Transactions.duration_commits / db.Transactions.xact_commit`
duration_commits	Transaktionen	db.Transactions.duration_commits	Die gesamte Transaktionszeit, die in der letzten Minute verbracht wurde, in Millisekunden.	–
max_used_xact_ids	Transaktionen	db.Transactions.max_used_xact_ids	Die Anzahl der Transaktionen, die nicht vakuiert wurden.	–

Zähler	Typ	Metrik	Beschreibung	Definition
oldest_inactive_logical_replication_slot_xid_age	Transaktionen	db.transactions.oldest_inactive_logical_replication_slot_xid_age	Das Alter der ältesten Transaktion in einem inaktiven logischen Replikationsslot.	–
oldest_active_logical_replication_slot_xid_age	Transaktionen	db.transactions.oldest_active_logical_replication_slot_xid_age	Das Alter der ältesten Transaktion in einem aktiven logischen Replikationsslot.	–
oldest_reader_feedback_xid_age	Transaktionen	db.transactions.oldest_reader_feedback_xid_age	Das Alter der ältesten Transaktion einer langandauernden Transaktion auf einer Aurora-Reader-Instance oder Aurora Global DB-Reader-Instance.	–
oldest_prepared_transaction_xid_age	Transaktionen	db.transactions.OLDEST_PREPARED_TRANSACTION_XID_AGE	Das Alter der ältesten vorbereiteten Transaktion.	–

Zähler	Typ	Metrik	Beschreibung	Definition
oldest_running_transaction_xid_age	Transaktionen	db.transactions.OLDEST_RUNNING_TRANSACTION_XID_AGE	Das Alter der ältesten laufenden Transaktion.	–
max_connections	Benutzer	db.User.max_connections	Die maximale Anzahl von Verbindungen, die für eine Datenbank zulässig sind, wie im `max_connections` Parameter konfiguriert.	–
total_auth_attempts	Benutzer	db.User.total_auth_attempts	Die Anzahl der Verbindungsversuche zu dieser Instanz.	–
archive_failed_count	WAL	db.WAL.archive_failed_count	Die Anzahl der fehlgeschlagenen Versuche, WAL-Dateien zu archivieren, in Dateien pro Minute.	–

SQL-Statistiken für Performance Insights

SQL-Statistiken sind leistungsbezogene Metriken zu SQL-Abfragen, die von Performance Insights gesammelt werden. Performance Insights sammelt Statistiken für jede Sekunde, in der eine Abfrage ausgeführt wird, und für jeden SQL-Aufruf. Die SQL-Statistiken bilden den Durchschnitt für den ausgewählten Zeitraum ab.

Ein SQL-Digest setzt sich aus allen Abfragen zusammen, die ein bestimmtes Muster haben, aber nicht unbedingt dieselben Literalwerte haben. Der Digest ersetzt Literalwerte durch ein Fragezeichen. Zum Beispiel `SELECT * FROM emp WHERE lname= ?`. Dieser Digest kann die folgenden untergeordneten Abfragen enthalten:

```
SELECT * FROM emp WHERE lname = 'Sanchez'
SELECT * FROM emp WHERE lname = 'Olagappan'
SELECT * FROM emp WHERE lname = 'Wu'
```

Alle Engines unterstützen SQL-Statistiken für Digest-Abfragen.

Informationen zur Unterstützung dieser Funktion nach Region, DB-Engine und Instance-Klasse finden Sie unter DB-Engine-, Regions- und Instance-Klassenunterstützung von Amazon Aurora für Performance-Insights-Funktionen.

Themen

- SQL-Statistiken für Aurora MySQL
- SQL-Statistiken für Aurora PostgreSQL

SQL-Statistiken für Aurora MySQL

Aurora MySQL sammelt SQL-Statistiken nur auf Digest-Ebene. Auf der Statement-Ebene werden keine Statistiken angezeigt.

Themen

- Digest-Statistiken für Aurora MySQL
- Statistiken für Aurora MySQL
- Statistiken für Aurora MySQL

Digest-Statistiken für Aurora MySQL

Performance Insights sammelt SQL-Digest-Statistiken aus der `events_statements_summary_by_digest`-Tabelle. Die `events_statements_summary_by_digest`-Tabelle wird von der Datenbank verwaltet.

Diese Tabelle verfügt nicht über eine Bereinigungsrichtlinie. Die folgende Meldung wird in der AWS Management Console angezeigt, wenn die Tabelle voll ist:

```
Performance Insights is unable to collect SQL Digest statistics on new queries because
 the table events_statements_summary_by_digest is full.
Please truncate events_statements_summary_by_digest table to clear the issue. Check the
 User Guide for more details.
```

In dieser Situation verfolgen Aurora MySQL nicht SQL-Abfragen. Um dieses Problem zu beheben, kürzt Performance Insights die Digest-Tabelle automatisch, wenn die folgenden Bedingungen beide erfüllt sind:

- Die Tabelle ist voll.
- Performance Insights verwaltet das Leistungsschema automatisch.

  Für die automatische Verwaltung muss der Parameter `performance_schema` auf den Wert `0` festgelegt werden und Source (Quelle) auf `user` eingestellt sein. Wenn Performance Insights die Leistung nicht automatisch verwaltet, finden Sie weitere Informationen unter Aktivieren des Leistungsschemas für Performance Insights in Aurora MySQL.

Überprüfen Sie in der AWS CLI die Quelle eines Parameterwerts, indem Sie den Befehl describe-db-parameters ausführen.

Statistiken für Aurora MySQL

Die folgenden SQL-Statistiken stehen für Aurora MySQL-DB-Cluster zur Verfügung.

Metrik	Einheit
db.sql_tokenized.stats.count_star_per_sec	Aufrufe pro Sekunde
db.sql_tokenized.stats.sum_timer_wait_per_sec	Durchschnitt der aktiven Ausführungen (Average active executions, AAE) pro Sekunde
db.sql_tokenized.stats.sum_select_full_join_per_sec	Vollständigen Join pro Sekunde auswählen
db.sql_tokenized.stats.sum_select_range_check_per_sec	Bereichsprüfung pro Sekunde auswählen
db.sql_tokenized.stats.sum_select_scan_per_sec	Scan pro Sekunde auswählen
db.sql_tokenized.stats.sum_sort_merge_passes_per_sec	Zusammenführungsdurchläufe pro Sekunde sortieren
db.sql_tokenized.stats.sum_sort_scan_per_sec	Scans pro Sekunde sortieren

Metrik	Einheit
db.sql_tokenized.stats.sum_sort_rang e_per_sec	Bereiche pro Sekunde sortieren
db.sql_tokenized.stats.sum_sort_rows_per_sec	Zeilen pro Sekunde sortieren
db.sql_tokenized.stats.sum_rows_affected_per_ sec	Betroffene Zeilen pro Sekunde
db.sql_tokenized.stats.sum_rows_exam ined_per_sec	Überprüfte Zeilen pro Sekunde
db.sql_tokenized.stats.sum_rows_sent_per_sec	Gesendete Zeilen pro Sekunde
db.sql_tokenized.stats.sum_created_tmp_disk_t ables_per_sec	Temporäre Datenträgertabellen pro Sekunde erstellt
db.sql_tokenized.stats.sum_created_tmp_tables _per_sec	Temporäre Tabellen pro Sekunde erstellt
db.sql_tokenized.stats.sum_lock_time_per_sec	Sperrzeit pro Sekunde (in ms)

Statistiken für Aurora MySQL

Die folgenden Metriken stellen Statistiken pro einzelnen Abruf für SQL-Anweisungen bereit.

Metrik	Einheit
db.sql_tokenized.stats.sum_timer_wait_per_call	Durchschnitt Latenz pro Aufruf (in ms)
db.sql_tokenized.stats.sum_select_full_join_p er_call	Vollständige Joins pro Aufruf auswählen
db.sql_tokenized.stats.sum_select_ra nge_check_per_call	Bereichsprüfung pro Aufruf auswählen
db.sql_tokenized.stats.sum_select_sc an_per_call	Scans pro Aufruf auswählen

Metrik	Einheit
db.sql_tokenized.stats.sum_sort_merge_passes_per_call	Zusammenführungsdurchläufe pro Aufruf sortieren
db.sql_tokenized.stats.sum_sort_scan_per_call	Scans pro Aufruf sortieren
db.sql_tokenized.stats.sum_sort_range_per_call	Bereiche pro Aufruf sortieren
db.sql_tokenized.stats.sum_sort_rows_per_call	Zeilen pro Aufruf sortieren
db.sql_tokenized.stats.sum_rows_affected_per_call	Betroffene Zeilen pro Aufruf
db.sql_tokenized.stats.sum_rows_examined_per_call	Überprüfte Zeilen pro Aufruf
db.sql_tokenized.stats.sum_rows_sent_per_call	Gesendete Zeilen pro Aufruf
db.sql_tokenized.stats.sum_created_tmp_disk_tables_per_call	Temporäre Datenträgertabellen pro Aufruf erstellt
db.sql_tokenized.stats.sum_created_tmp_tables_per_call	Temporäre Tabellen pro Aufruf erstellt
db.sql_tokenized.stats.sum_lock_time_per_call	Sperrzeit pro Aufruf (in ms)

SQL-Statistiken für Aurora PostgreSQL

Performance Insights sammelt für jeden SQL-Aufruf und für jede Sekunde, in der eine Abfrage ausgeführt wird, SQL-Statistiken. Alle Aurora-Engines sammeln Statistiken nur auf Digest-Ebene.

Im Folgenden finden Sie Informationen zu Statistiken auf Digest-Ebene für Aurora PostgreSQL

Themen

- Digest-Statistiken für Aurora PostgreSQL
- Sekundengenaue Digest-Statistiken für Aurora PostgreSQL
- Digest-Statistiken pro Aufruf für Aurora PostgreSQL

Digest-Statistiken für Aurora PostgreSQL

Um SQL Digest-Statistiken anzeigen zu können, muss die Bibliothek `pg_stat_statements` geladen sein. Diese Bibliothek wird für Aurora-PostgreSQL-DB-Cluster, die mit PostgreSQL 10 kompatibel sind, standardmäßig geladen. Für Aurora-PostgreSQL-DB-Cluster, die mit PostgreSQL 9.6 kompatibel sind, müssen Sie diese Bibliothek manuell aktivieren. Zur manuellen Aktivierung fügen Sie in der DB-Parametergruppe, die der DB-Instance zugeordnet ist, `pg_stat_statements` zu `shared_preload_libraries` hinzu. Starten Sie anschließend die DB-Instance neu. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen.

> **Note**
>
> Performance-Insights kann nur Statistiken für nicht abgeschnittene Abfragen in `pg_stat_activity` erfassen. Standardmäßig kürzen PostgreSQL-Datenbanken Abfragen, die länger als 1 024 Bytes sind. Um die Abfragegröße zu erhöhen, ändern Sie den Parameter `track_activity_query_size` in der DB-Parametergruppe, die mit Ihrer DB-Instance verknüpft ist. Wenn Sie diesen Parameter ändern, ist ein Neustart der DB-Instance erforderlich.

Sekundengenaue Digest-Statistiken für Aurora PostgreSQL

Die folgenden SQL Digest-Statistiken sind für Aurora PostgreSQL DB-Instances verfügbar.

Metrik	Einheit
db.sql_tokenized.stats.calls_per_sec	Aufrufe pro Sekunde
db.sql_tokenized.stats.rows_per_sec	Zeilen pro Sekunde
db.sql_tokenized.stats.total_time_per_sec	Durchschnitt der aktiven Ausführungen (Average active executions, AAE) pro Sekunde
db.sql_tokenized.stats.shared_blks_hit_per_sec	Blocktreffer pro Sekunde
db.sql_tokenized.stats.shared_blks_read_per_sec	Blocklesevorgänge pro Sekunde

Metrik	Einheit
db.sql_tokenized.stats.shared_blks_dirtied_per_sec	Blöcke kontaminiert pro Sekunde
db.sql_tokenized.stats.shared_blks_written_per_sec	Blockschreibvorgänge pro Sekunde
db.sql_tokenized.stats.local_blks_hit_per_sec	Lokale Blocktreffer pro Sekunde
db.sql_tokenized.stats.local_blks_read_per_sec	Lokale Blocklesevorgänge pro Sekunde
db.sql_tokenized.stats.local_blks_dirtied_per_sec	Lokale Blockkontaminierungen pro Sekunde
db.sql_tokenized.stats.local_blks_written_per_sec	Lokale Blockschreibvorgänge pro Sekunde
db.sql_tokenized.stats.temp_blks_written_per_sec	Temporäre Schreibvorgänge pro Sekunde
db.sql_tokenized.stats.temp_blks_read_per_sec	Temporäre Lesevorgänge pro Sekunde
db.sql_tokenized.stats.blk_read_time_per_sec	Durchschnitt gleichzeitige Lesevorgänge pro Sekunde
db.sql_tokenized.stats.blk_write_time_per_sec	Durchschnitt gleichzeitige Schreibvorgänge pro Sekunde

Digest-Statistiken pro Aufruf für Aurora PostgreSQL

Die folgenden Metriken stellen Statistiken pro einzelnen Abruf für SQL-Anweisungen bereit.

Metrik	Einheit
db.sql_tokenized.stats.rows_per_call	Zeilen pro Aufruf
db.sql_tokenized.stats.avg_latency_per_call	Durchschnitt Latenz pro Aufruf (in ms)

Metrik	Einheit
db.sql_tokenized.stats.shared_blks_hit_per_call	Blocktreffer pro Aufruf
db.sql_tokenized.stats.shared_blks_read_per_call	Blocklesevorgänge pro Aufruf
db.sql_tokenized.stats.shared_blks_written_per_call	Blockschreibvorgänge pro Aufruf
db.sql_tokenized.stats.shared_blks_dirtied_per_call	Blöcke kontaminiert pro Aufruf
db.sql_tokenized.stats.local_blks_hit_per_call	Lokale Blocktreffer pro Aufruf
db.sql_tokenized.stats.local_blks_read_per_call	Lokale Blocklesevorgänge pro Aufruf
db.sql_tokenized.stats.local_blks_dirtied_per_call	Lokale Blockkontaminierungen pro Aufruf
db.sql_tokenized.stats.local_blks_written_per_call	Lokale Blockschreibvorgänge pro Aufruf
db.sql_tokenized.stats.temp_blks_written_per_call	Temporäre Blockschreibvorgänge pro Aufruf
db.sql_tokenized.stats.temp_blks_read_per_call	Temporäre Blocklesevorgänge pro Aufruf
db.sql_tokenized.stats.blk_read_time_per_call	Lesezeit pro Aufruf (in ms)
db.sql_tokenized.stats.blk_write_time_per_call	Schreibzeit pro Aufruf (in ms)

Weitere Informationen zu diesen Metriken finden Sie unter pg_stat_statements in der PostgreSQL-Dokumentation.

Betriebssystemmetriken im „Enhanced Monitoring“ (Erweiterte Überwachung)

Amazon Aurora stellt in Echtzeit Metriken für das Betriebssystem (BS) bereit, auf dem Ihr DB-Cluster ausgeführt wird. Aurora stellt die Metriken von Enhanced Monitoring für Ihr Amazon- CloudWatch Logs-Konto bereit. In den folgenden Tabellen sind die Betriebssystemmetriken aufgeführt, die mit Amazon CloudWatch Logs verfügbar sind.

Themen

Betriebssystemmetriken für Aurora

Gruppe	Metrik	Name der Konsole	Beschreibung
`General`	`engine`	Nicht zutreffend	Die Datenbank-Engine für die DB-Instance.
	`instanceID`	Nicht zutreffend	Die DB-Instance-Kennung.
	`instanceResourceID`	Nicht zutreffend	Ein unveränderlicher Bezeichner für die DB-Instance, der für eine AWS-Region eindeutig ist und auch als Protokolldatenstrom-ID verwendet wird.
	`numVCPUs`	Nicht zutreffend	Die Anzahl der virtuellen CPUs für die DB-Instance.
	`timestamp`	Nicht zutreffend	Die Uhrzeit, zu der die Metriken erfasst wurden.
	`uptime`	Nicht zutreffend	Die Zeitdauer, für die die DB-Instance aktiv war.
	`version`	Nicht zutreffend	Die Version des JSON-Formats für den Stream der Betriebssystem-Metriken.

Gruppe	Metrik	Name der Konsole	Beschreibung
`cpuUtilization`	`guest`	CPU Gast	Der prozentuale Anteil der von Gastprogrammen verwendeten CPU.
	`idle`	CPU Leerlauf	Der prozentuale Anteil der CPU, der sich im Leerlauf befindet.
	`irq`	CPU IRQ	Der prozentuale Anteil der von Software-Interrupts verwendeten CPU.
	`nice`	CPU Nice	Der prozentuale Anteil der von Programmen mit niedrigster Priorität verwendeten CPU.
	`steal`	CPU Steal	Der prozentuale Anteil der von virtuellen Maschinen verwendeten CPU.
	`system`	CPU-System	Der prozentuale Anteil der vom Kernel verwendeten CPU.
	`total`	CPU insgesamt	Der prozentuale Anteil der insgesamt verwendeten CPU. Diese Angabe enthält den Wert `nice`.
	`user`	CPU Benutzer	Der prozentuale Anteil der von Benutzerprogrammen verwendeten CPU.
	`wait`	CPU Warten	Der Prozentsatz der unbenutzten CPU während des Wartens auf I/O-Zugriff.
`diskIO`	`avgQueueLen`	Durchschn. Warteschlangengröße	Die Anzahl der Anfragen, die in der Warteschlange des I/O-Geräts warten.
	`avgReqSz`	Durchschn. Anforderungsgröße	Die durchschnittliche Anfragegröße in Kilobyte.

Gruppe	Metrik	Name der Konsole	Beschreibung
	`await`	Festplatten-I/O-Warten	Die erforderliche Anzahl an Millisekunden für die Antwort auf Anfragen, einschließlich Warteschlangen- und Servicedauer.
	`device`	Nicht zutreffend	Die Kennung des verwendeten Datenträgers.
	`readIOsPS`	Gelesene IO/s	Die Anzahl der Lesevorgänge pro Sekunde.
	`readKb`	Insgesamt gelesen	Gesamtzahl der gelesenen Kilobyte.
	`readKbPS`	Gelesene KB/s	Die Anzahl der pro Sekunde gelesenen Kilobyte.
	`readLatency`	Lese-Latenz	Die verstrichene Zeit zwischen dem Senden einer Lese-I/O-Anforderung und deren Abschluss in Millisekunden. Diese Metrik ist nur für Amazon Aurora verfügbar.
	`readThroughput`	Lesedurchsatz	Die Menge des Netzwerkdurchsatzes, der von Anforderungen an den DB-Cluster verwendet wird, in Bytes pro Sekunde. Diese Metrik ist nur für Amazon Aurora verfügbar.
	`rrqmPS`	Rrqms	Die Anzahl der zusammengeführten Leseanfragen in der Warteschlange pro Sekunde.
	`tps`	TPS	Die Anzahl der I/O-Transaktionen pro Sekunde.
	`util`	Datenträger-I/O-Util	Der Prozentsatz der CPU-Zeit, während der Anfragen ausgegeben wurden.

Gruppe	Metrik	Name der Konsole	Beschreibung
	writeIOsPS	Geschriebene IO/s	Die Anzahl der Schreibvorgänge pro Sekunde.
	writeKb	Insgesamt geschrieben	Gesamtzahl der geschriebenen Kilobyte.
	writeKbPS	Geschriebene KB/s	Die Anzahl der pro Sekunde geschriebenen Kilobyte.
	writeLatency	Schreib-Latenz	Die durchschnittliche verstrichene Zeit zwischen dem Senden einer Schreib-I/O-Anforderung und deren Abschluss in Millisekunden. Diese Metrik ist nur für Amazon Aurora verfügbar.
	writeThroughput	Schreibdurchsatz	Die Menge des Netzwerkdurchsatzes, der von Antworten vom DB-Cluster verwendet wird, in Bytes pro Sekunde. Diese Metrik ist nur für Amazon Aurora verfügbar.
	wrqmPS	Wrqms	Die Anzahl der zusammengeführten Schreibanfragen in der Warteschlange pro Sekunde.
fileSys	maxFiles	Max Inodes	Die maximale Anzahl an Dateien, die für das Dateisystem erstellt werden können.
	mountPoint	Nicht zutreffend	Der Pfad zum Dateisystem.
	name	Nicht zutreffend	Der Name des Dateisystems.

Gruppe	Metrik	Name der Konsole	Beschreibung
	`total`	Dateisystem insgesamt	Die Gesamtmenge des für das Dateisystem verfügbaren Speicherplatzes in Kilobyte.
	`used`	Verwendetes Dateisystem	Der durch Dateien belegte Speicherplatz im Dateisystem in Kilobyte.
	`usedFilePercent`	Gebrauchte Inodes	Der Prozentsatz von verfügbaren Dateien, die in Gebrauch sind.
	`usedFiles`	Used%	Die Anzahl der Dateien im Dateisystem.
	`usedPercent`	Verwendetes Dateisystem	Der prozentuale Anteil des verwendeten Speicherplatzes für das Dateisystem.
`loadAverageMinute`	`fifteen`	Last Durchschn. 15 Min	Die Anzahl der Prozesse, die während der letzten 15 Minuten CPU-Zeit angefordert haben.
	`five`	Laden Durchschn. 5 Min	Die Anzahl der Prozesse, die während der letzten 5 Minuten CPU-Zeit angefordert haben.
	`one`	Laden Durchschn. 1 Min	Die Anzahl der Prozesse, die während der letzten Minute CPU-Zeit angefordert haben.
`memory`	`active`	Aktiver Speicher	Umfang des zugewiesenen Arbeitsspeichers in Kilobyte.

Gruppe	Metrik	Name der Konsole	Beschreibung
	`buffers`	Gepufferter Speicher	Umfang des verwendeten Arbeitsspeichers für die Pufferung von I/O-Anfragen vor dem Schreiben auf das Speichergerät, in Kilobyte.
	`cached`	Zwischenspeicher	Umfang des verwendeten Arbeitsspeichers für Caching von Dateisystem-basierter I/O.
	`dirty`	Geänderter Speicher	Menge an Memory-Pages im RAM, die geändert, aber noch nicht in den entsprechenden Datenblock im Speicher geschrieben wurden, in Kilobyte.
	`free`	Freier Speicher	Umfang des nicht zugewiesenen Arbeitsspeichers in Kilobyte.
	`hugePagesFree`	Huge Pages frei	Die Anzahl von freien "Huge Pages". "Huge Pages" sind eine Funktion des Linux-Kernel.
	`hugePagesRsvd`	Huge Pages reserviert	Die Anzahl von gebundenen "Huge Pages".
	`hugePagesSize`	Größe Huge Pages	Die Größe für jede Huge Pages-Einheit, in Kilobyte.
	`hugePagesSurp`	Überschuss Huge Pages	Die Anzahl der verfügbaren überzähligen Huge Pages.
	`hugePagesTotal`	Huge Pages insgesamt	Die Gesamtzahl der Huge Pages.
	`inactive`	Inaktiver Speicher	Umfang der am seltensten verwendeten Memory-Pages in Kilobyte.

Gruppe	Metrik	Name der Konsole	Beschreibung
	`mapped`	Zugeordneter Speicher	Die Gesamtmenge der Dateisysteminhalte, die Arbeitsspeicher in einem Prozess-Adressraum zugeordnet ist, in Kilobyte.
	`pageTables`	Seitentabellen	Umfang des von Page-Tabellen verwendeten Arbeitsspeichers in Kilobyte.
	`slab`	Plattenspeicher	Umfang der wiederverwendbaren Kernel-Datenstrukturen in Kilobyte.
	`total`	Gesamtspeicher	Gesamtumfang des Arbeitsspeichers in Kilobyte.
	`writeback`	Writeback-Speicher	Gesamtumfang an modifizierten Speicherbereichen im RAM, die noch in den Sicherungsspeicher geschrieben werden, in Kilobyte.
`network`	`interface`	Nicht zutreffend	Die Kennung für die Netzwerkschnittstelle, die für die DB-Instance verwendet wird.
	`rx`	RX	Die Anzahl der pro Sekunde empfangenen Byte.
	`tx`	TX	Die Anzahl der pro Sekunde hochgeladenen Byte.
`processList`	`cpuUsedPc`	% CPU	Prozentsatz der vom Prozess benutzten CPU.
	`id`	Nicht zutreffend	Die ID des Prozesses.
	`memoryUsedPc`	RAM %	Prozentsatz des insgesamt vom Prozess benutzten Speichers.
	`name`	Nicht zutreffend	Der Name des Prozesses.

Gruppe	Metrik	Name der Konsole	Beschreibung
	`parentID`	Nicht zutreffend	Die Prozess-ID für den übergeordneten Prozess des aktuellen Prozesses.
	`rss`	RES	Umfang des dem Prozess zugeteilten RAM in Kilobyte.
	`tgid`	Nicht zutreffend	Die Thread-Gruppen-ID als Zahl, die die Prozess-ID darstellt, zu der ein Thread gehört. Diese Kennung wird verwendet, um Threads aus demselben Prozess zu gruppieren.
	`vss`	VIRT	Umfang des dem Prozess zugeteilten virtuellen Speichers in Kilobyte.
`swap`	`swap`	Auslagerung	Die Menge des verfügbaren Swap-Arbeitsspeichers in Kilobyte.
	`swap in`	Auslagerungen in	Die Menge des von der Festplatte ausgelagerten Speichers in Kilobyte.
	`swap out`	Auslagerungen aus	Die Menge des auf die Festplatte ausgelagerten Speichers in Kilobyte.
	`free`	Kostenlose Auslagerung	Die Menge des freien Swap-Arbeitsspeichers in Kilobyte.
	`committed`	Committed Auslagerung	Umfang des Swap-Arbeitsspeichers, der als Cache-Speicher verwendet wird, in Kilobyte.
`tasks`	`blocked`	Gesperrte Aufgaben	Die Anzahl von blockierten Aufgaben.
	`running`	Laufende Aufgaben	Die Anzahl von laufenden Aufgaben.

Gruppe	Metrik	Name der Konsole	Beschreibung
	`sleeping`	Ruhende Aufgaben	Die Anzahl von Aufgaben im Ruhezustand.
	`stopped`	Gestoppte Aufgaben	Die Anzahl von angehaltenen Aufgaben.
	`total`	Aufgaben insgesamt	Die Gesamtanzahl der Aufgaben.
	`zombie`	Aufgaben Zombie	Die Anzahl der untergeordneten Aufgaben, die unter einer aktiven übergeordneten Aufgabe inaktiv sind.

Überwachen von Ereignissen, Protokollen und Streams in einem Amazon Aurora-DB-Cluster

Wenn Sie Ihre Aurora Aurora-Datenbanken und Ihre anderen AWS Lösungen überwachen, ist es Ihr Ziel, Folgendes aufrechtzuerhalten:

- Zuverlässigkeit
- Verfügbarkeit
- Leistung
- Sicherheit

Überwachung von Metriken in einem Amazon-Aurora-Cluster erklärt, wie Sie den Cluster mithilfe von Metriken überwachen. Eine Komplettlösung muss auch Datenbankereignisse, Protokolldateien und Aktivitätsströme überwachen. AWS bietet Ihnen die folgenden Überwachungstools:

- Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, oftware-as-a S-Service (SaaS) - Anwendungen und AWS Diensten. EventBridge leitet diese Daten an Ziele weiter wie AWS Lambda. Auf diese Weise können Sie Ereignisse überwachen, die in Services auftreten, und ereignisgesteuerte Architekturen erstellen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.
- Amazon CloudWatch Logs bietet eine Möglichkeit, Ihre Protokolldateien von Aurora Aurora-Instances und anderen Quellen zu überwachen AWS CloudTrail, zu speichern und darauf zuzugreifen. Amazon CloudWatch Logs kann Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden AWS-Konto. CloudTrail übermittelt die Protokolldateien an einen Amazon S3 S3-Bucket, den Sie angeben. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

- Datenbankaktivitätsstreams ist eine Amazon-Aurora-Funktion, die einen Beinahe-Echtzeitdatenstrom der Aktivität in Ihrem DB-Cluster. bietet. Amazon Aurora sendet Aktivitäten per Push an einen Amazon Kinesis Data Stream. Der Kinesis Stream wird automatisch erstellt. Von Kinesis aus können Sie AWS Dienste wie Amazon Data Firehose konfigurieren und AWS Lambda den Stream nutzen und die Daten speichern.

Themen

Anzeigen von Protokollen, Ereignissen und Streams in der Amazon-RDS-Konsole

Amazon RDS lässt sich in AWS-Services integrieren, um Informationen zu Protokollen, Ereignissen und Datenbankaktivitäts-Streams in der RDS-Konsole anzuzeigen.

Die Registerkarte Logs·&·events (Protokolle und Ereignisse) für den Aurora-DB-Cluster zeigt die folgenden Informationen an:

- Auto-Scaling-Richtlinien und -Aktivitäten – Zeigt Richtlinien und Aktivitäten in Bezug auf die Aurora-Auto-Scaling-Funktion an. Diese Informationen werden nur auf der Registerkarte Logs·&·events (Protokolle und Ereignisse) auf Clusterebene angezeigt.
- Amazon-CloudWatch-Alarme – Zeigt alle metrischen Alarme, die Sie für die DB-Instance konfiguriert haben, in Ihrem Aurora-Cluster an. Wenn Sie keine Alarme konfiguriert haben, können Sie sie in der RDS-Konsole erstellen.
- Aktuelle Ereignisse – Zeigt eine Übersicht über Ereignisse (Umgebungsänderungen) für Ihre Aurora--DB-Instance oder Cluster an. Weitere Informationen finden Sie unter Anzeigen von Amazon RDS-Ereignissen.

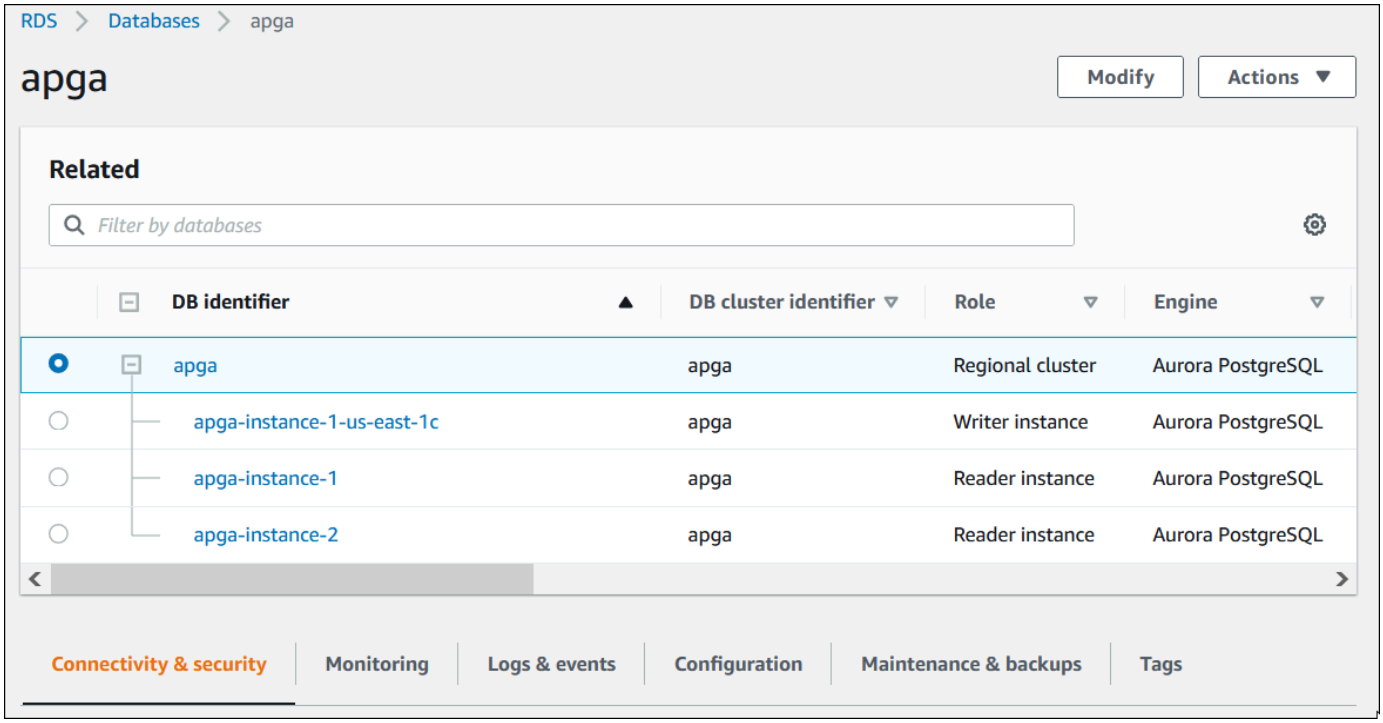
- Protokolle – Zeigt Datenbankprotokolldateien an, die von einer DB-Instance in Ihrem Aurora-Cluster generiert wurden. Weitere Informationen finden Sie unter Überwachen von Amazon Aurora-Protokolldateien.

Die Registerkarte Konfiguration zeigt Informationen über Datenbankaktivitäts-Streams an.

Zeigen Sie Protokolle, Ereignisse und Streams für Ihre Aurora-DB--Cluster in der RDS-Konsole wie folgt an:

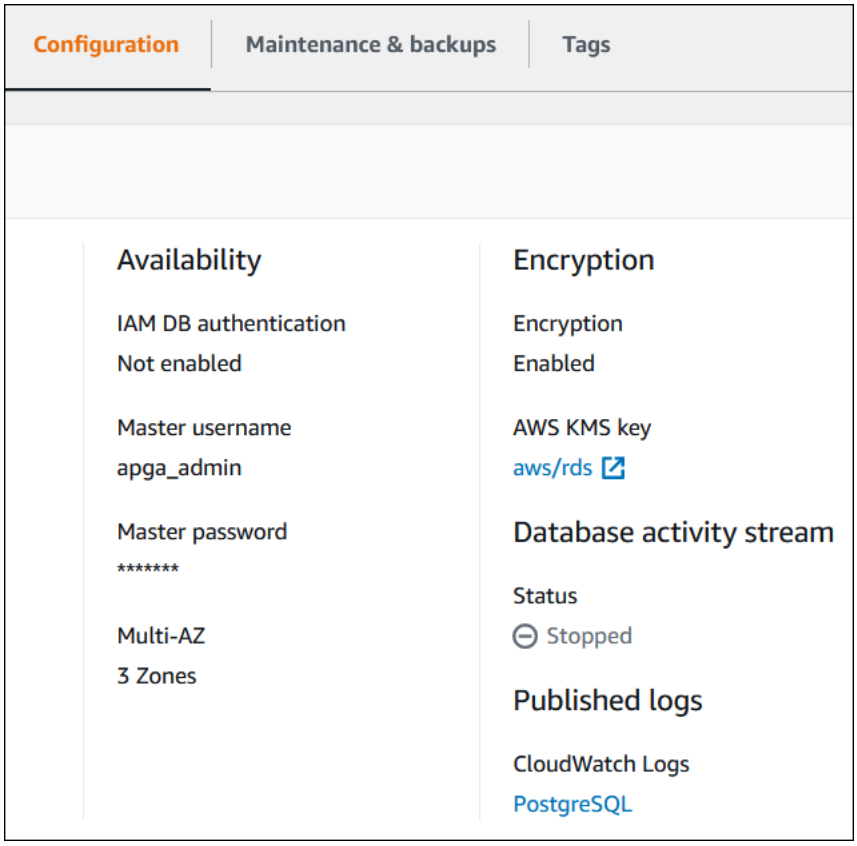
1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den Namen des Aurora-DB--Cluster an, das Sie überwachen möchten.

   Der Bereich Datenbanken wird angezeigt. Das folgende Beispiel zeigt eine Amazon-Aurora-PostgreSQL-DB-Cluster namens apga an.



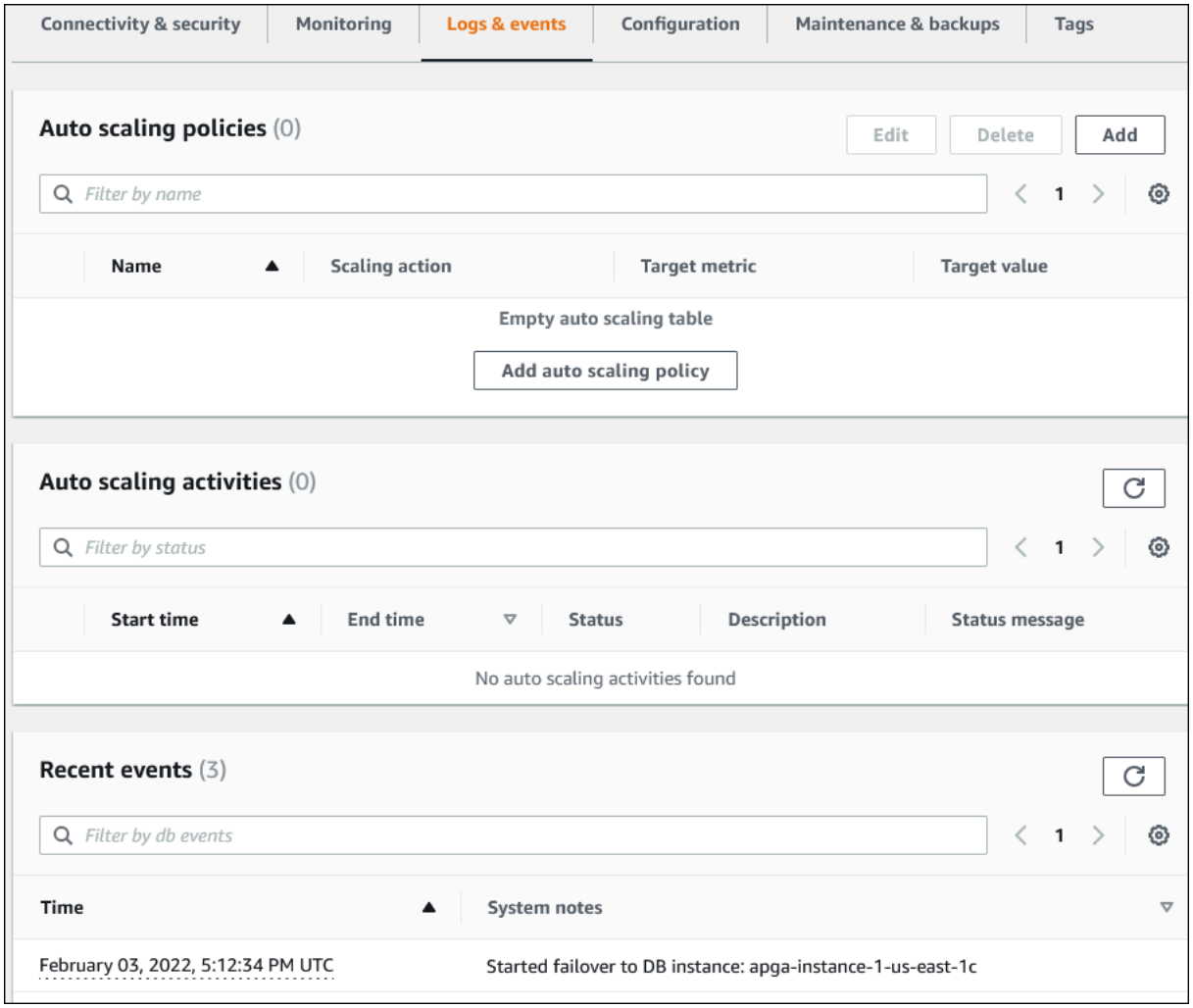
4. Scrollen Sie nach unten und wählen Sie Konfiguration aus.

   Das folgende Beispiel zeigt den Status der Datenbankaktivitäts-Streams für Ihren Cluster an.



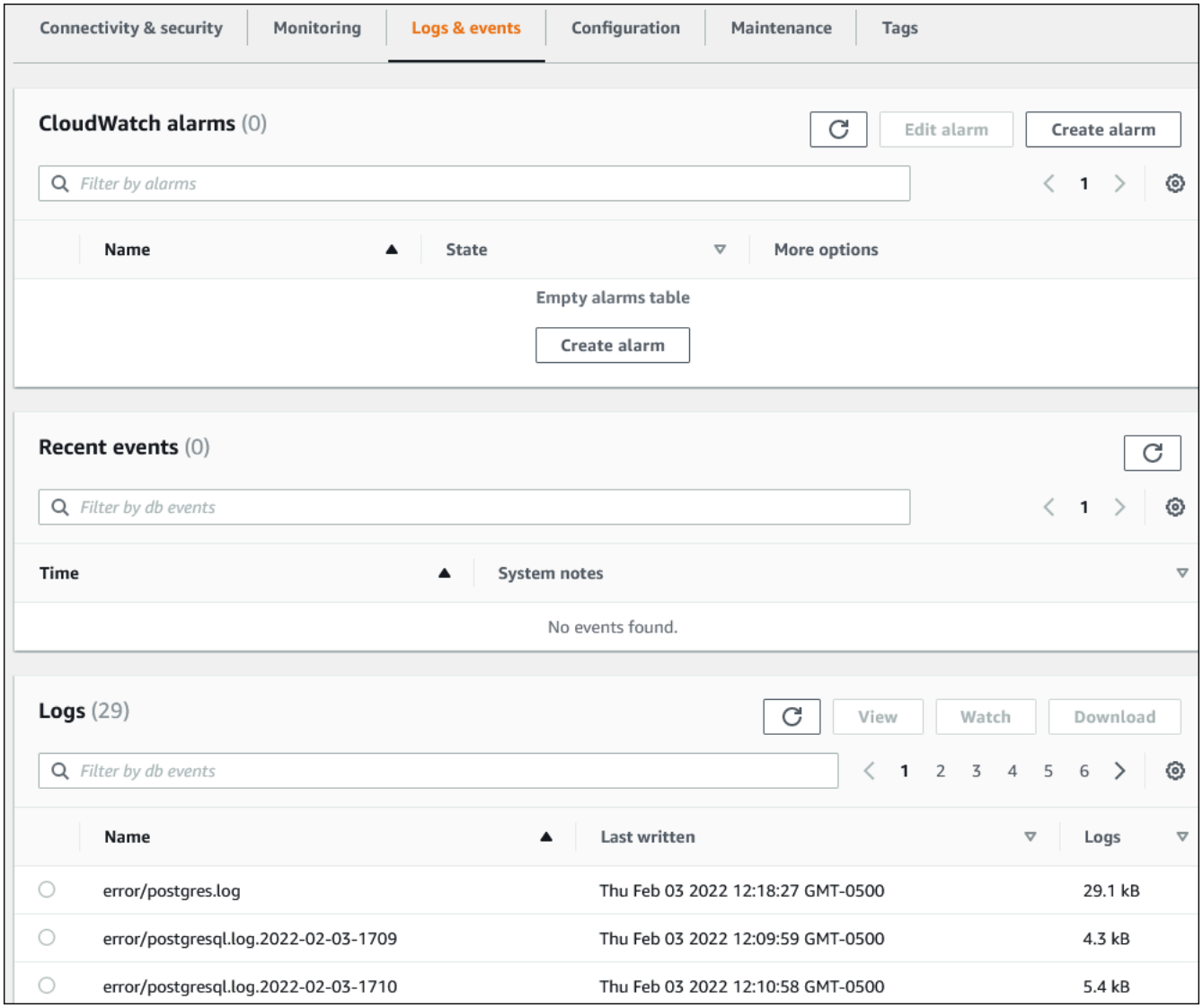
5. Wählen Sie Logs & Events (Protokolle und Ereignisse).

   Der Abschnitt Logs & Events (Protokolle und Ereignisse) wird angezeigt.



6. Wählen Sie eine DB-Instance in Ihrem Aurora-Cluster und dann Logs & Events (Protokolle & Ereignisse) für die Instance.

   Das folgende Beispiel zeigt, dass der Inhalt zwischen der DB-Instance-Seite und der DB-Cluster-Seite unterschiedlich ist. Auf der Seite der DB-Instance werden Protokolle und Alarme angezeigt.


Connectivity & security
Monitoring
Logs & events
Configuration
Maintenance
Tags
CloudWatch alarms (0)
Edit alarm
Create alarm
Filter by alarms
1
Name
State
More options
Empty alarms table
Create alarm
Recent events (0)
Filter by db events
1
Time
System notes
No events found.
Logs (29)
View
Watch
Download
Filter by db events
1 2 3 4 5 6
Name
Last written
Logs
error/postgres.log
Thu Feb 03 2022 12:18:27 GMT-0500
29.1 kB
error/postgresql.log.2022-02-03-1709
Thu Feb 03 2022 12:09:59 GMT-0500
4.3 kB
error/postgresql.log.2022-02-03-1710
Thu Feb 03 2022 12:10:58 GMT-0500
5.4 kB

Überwachung von Amazon Aurora-Ereignissen

Ein Ereignis weist auf eine Änderung in einer Umgebung hin. Dabei kann es sich um eine AWS-Umgebung, SaaS-Partnerservices oder -Anwendungen oder Ihre eigenen benutzerdefinierten Anwendungen oder Services handeln. Beschreibungen der Aurora-Ereignisse finden Sie unter Amazon RDS-Ereigniskategorien und Ereignisnachrichten für Aurora.

Themen

Überblick über Ereignisse für Aurora

Ein RDS event (RDS-Ereignis) weist auf eine Änderung der Aurora-Umgebung hin. Beispielsweise generiert Amazon Aurora ein Ereignis, wenn ein DB-Cluster gepatcht wird ausgeführt ändert. Amazon Aurora liefert Ereignisse nahezu EventBridge in Echtzeit.

> **Note**
>
> Amazon RDS sendet Ereignisse nach bestem Bemühen aus. Wir empfehlen Ihnen, keine Programme zu schreiben, die von der Reihenfolge oder dem Vorhandensein von Benachrichtigungsereignissen abhängen, da diese möglicherweise nicht in der richtigen Reihenfolge vorliegen oder fehlen.

Amazon RDS zeichnet Ereignisse auf, die sich auf die folgenden Ressourcen beziehen:

- DB-Cluster

  Eine Liste der Cluster-Ereignisse finden Sie unter DB-Cluster-Ereignisse.
- DB-Instances

  Eine Liste der DB-Instance-Ereignisse finden Sie unter DB-Instance-Ereignisse.
- DB-Parametergruppen

Eine Liste der Ereignisse der DB-Parametergruppe finden Sie unter DB-Parametergruppenereignisse.

- DB-Sicherheitsgruppen

  Eine Liste der Ereignisse der DB-Sicherheitsgruppe finden Sie unter DB-Sicherheitsgruppenereignisse.

- DB-Cluster-Snapshots

  Eine Liste der DB-Cluster-Snapshot-Ereignisse finden Sie unter DB-Cluster-Snapshot-Ereignisse.

- RDS-Proxy-Ereignisse

  Eine Liste der RDS-Proxy-Ereignisse finden Sie unter RDS-Proxy-Ereignisse.

- Blau/Grün-Bereitstellungsereignisse

  Eine Liste der Blau/Grün-Bereitstellungsereignisse finden Sie unter Blau/Grün-Bereitstellungsereignisse.

Diese Informationen beinhalten Folgendes:

- Das Datum und die Uhrzeit der Veranstaltung
- Der Quellname und der Quelltyp des Ereignisses
- Eine Nachricht, die mit dem Ereignis verknüpft ist
- Ereignisbenachrichtigungen enthalten Tags zum Zeitpunkt, an dem die Nachricht gesendet wurde, und geben möglicherweise nicht die Tags zum Zeitpunkt des Eintritts des Ereignisses wieder.

Anzeigen von Amazon RDS-Ereignissen

Sie können die folgenden Ereignisinformationen für Ihre Amazon Aurora-Ressourcen abrufen:

- Ressourcenname
- Ressourcentyp
- Zeitpunkt des Ereignisses
- Zusammenfassung der Ereignisbenachrichtigung

Greifen Sie über das auf die Ereignisse zu AWS Management Console, in dem Ereignisse der letzten 24 Stunden angezeigt werden. Sie können Ereignisse auch mithilfe des AWS CLI Befehls describe-events oder der DescribeEventsRDS-API-Operation abrufen. Wenn Sie die AWS CLI oder die RDS-API zum Anzeigen von Ereignissen verwenden, können Sie Ereignisse der letzten 14 Tage abrufen.

> **Note**
>
> Wenn Sie Ereignisse für längere Zeiträume speichern müssen, können Sie Amazon RDS-Ereignisse an senden EventBridge. Weitere Informationen finden Sie unter Erstellen einer Regel, die bei einem Amazon Aurora-Ereignis ausgelöst wird.

Beschreibungen der Amazon-Aurora-Ereignisse finden Sie unter Amazon RDS-Ereigniskategorien und Ereignisnachrichten für Aurora.

Ausführliche Informationen über Ereignisse mithilfe von AWS CloudTrail Anforderungsparametern finden Sie unterCloudTrail-Ereignisse.

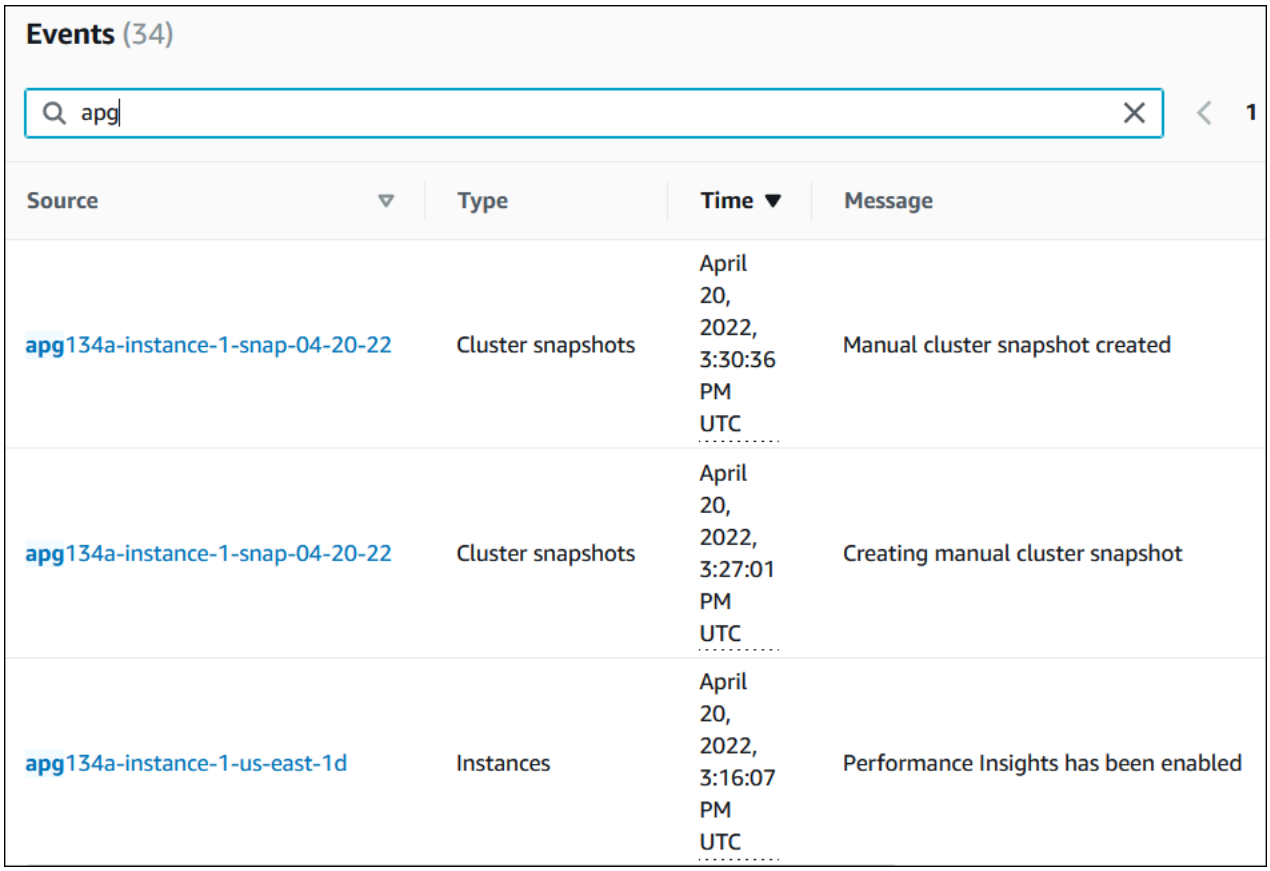
Konsole

So können Sie alle Amazon-RDS-Ereignisse der letzten 24 Stunden ansehen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Events.

   Die verfügbaren Ereignisse erscheinen in einer Liste.
3. (Optional) Geben Sie einen Suchbegriff ein, um Ihre Ergebnisse zu filtern.

Das folgende Beispiel zeigt eine Liste von Ereignissen, die nach den Zeichen **apg** gefiltert sind.



AWS CLI

Wenn Sie alle Ereignisse anzeigen möchten, die in der letzten Stunde generiert wurden, rufen Sie describe-events ohne Parameter auf.

```
aws rds describe-events
```

Die folgende Beispielausgabe zeigt, dass eine DB-Cluster-Instance gestoppt wurde.

```
{
    "Events": [
        {
            "EventCategories": [
                "recovery"
            ],
            "SourceType": "db-instance",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:mycluster-instance-1",
```

```
            "Date": "2022-04-20T15:02:38.416Z",
            "Message": "Recovery of the DB instance has started. Recovery time will
 vary with the amount of data to be recovered.",
            "SourceIdentifier": "mycluster-instance-1"
        }, ...
```

Um alle Amazon RDS-Ereignisse der letzten 10080 Minuten (7 Tage) anzuzeigen, rufen Sie den AWS CLI Befehl describe-events auf und setzen Sie den `--duration` Parameter auf. `10080`

```
aws rds describe-events --duration 10080
```

Das folgende Beispiel zeigt die Ereignisse im angegebenen Zeitraum für die DB-Instance *`test-instance`*.

```
aws rds describe-events \
    --source-identifier test-instance \
    --source-type db-instance \
    --start-time 2022-03-13T22:00Z \
    --end-time 2022-03-13T23:59Z
```

Die folgende Beispielausgabe zeigt den Status eines Backups.

```
{
    "Events": [
        {
            "SourceType": "db-instance",
            "SourceIdentifier": "test-instance",
            "EventCategories": [
                "backup"
            ],
            "Message": "Backing up DB instance",
            "Date": "2022-03-13T23:09:23.983Z",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance"
        },
        {
            "SourceType": "db-instance",
            "SourceIdentifier": "test-instance",
            "EventCategories": [
                "backup"
            ],
            "Message": "Finished DB Instance backup",
            "Date": "2022-03-13T23:15:13.049Z",
```

```
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance"
        }
    ]
}
```

API

Sie können alle Amazon RDS-Instance-Ereignisse der letzten 14 Tage anzeigen, indem Sie den DescribeEventsRDS-API-Vorgang aufrufen und den `Duration` Parameter auf setzen`20160`.

Arbeiten mit Amazon-RDS-Ereignisbenachrichtigungen

Amazon RDS verwendet Amazon Simple Notification Service (Amazon SNS), um Benachrichtigungen zu senden, wenn ein Amazon RDS-Ereignis stattfindet. Diese Benachrichtigungen können jedes von Amazon SNS für eine AWS-Region unterstützte Format aufweisen, wie zum Beispiel eine E-Mail, eine SMS oder ein Anruf an einen HTTP-Endpunkt.

Themen

Überblick über die Amazon RDS-Ereignisbenachrichtigung

Amazon RDS gruppiert Ereignisse in Kategorien, die Sie abonnieren können, damit Sie benachrichtigt werden, wenn ein Ereignis in dieser Kategorie eintritt.

Themen

RDS-Ressourcen, die für ein Ereignisabonnement in Frage kommen

Bei Amazon Aurora treten Ereignisse sowohl auf Ebene des DB-Clusters als auch auf Ebene der DB-Instance auf. Sie können eine Veranstaltungskategorie für die folgenden Ressourcen abonnieren:

- DB-Instance
- DB-Cluster
- DB-Cluster-Snapshot
- DB-Parametergruppe
- DB-Sicherheitsgruppe
- RDS-Proxy
- Kundenspezifische Motorversionen

Wenn Sie zum Beispiel die Backup-Kategorie für eine bestimmte DB-Instance abonnieren, werden Sie immer dann benachrichtigt, wenn ein Backup-bezogenes Ereignis eintritt, das die DB-Instance betrifft. Wenn Sie eine Konfigurationsänderungskategorie für eine DB-Instance abonnieren, werden Sie benachrichtigt, sobald die DB-Instance geändert wird. Außerdem erhalten Sie eine Benachrichtigung, wenn ein Abonnement für Ereignisbenachrichtigungen geändert wird.

Möglicherweise möchten Sie mehrere verschiedene Abonnements erstellen. Sie könnten beispielsweise ein Abonnement erstellen, das alle Ereignisbenachrichtigungen für alle DB-Instances empfängt, und ein anderes, das nur kritische Ereignisse für eine Teilmenge der DB-Instances enthält. Geben Sie für das zweite Abonnement eine oder mehrere DB-Instances im Filter an.

Grundlegendes Verfahren zum Abonnieren von Amazon RDS-Ereignisbenachrichtigungen

Gehen Sie wie folgt vor, um Amazon RDS-Ereignisbenachrichtigungen zu abonnieren:

1. Sie erstellen ein Abonnement für Amazon RDS-Ereignisbenachrichtigungen mithilfe der Amazon RDS-Konsole oder API. AWS CLI

   Amazon RDS verwendet den ARN eines Amazon SNS-Themas, um die einzelnen Abonnements zu ermitteln. Die Amazon RDS-Konsole erstellt einen ARN für Sie, wenn Sie ein Abonnement erstellen. Erstellen Sie den ARN mithilfe der Amazon SNS SNS-Konsole AWS CLI, der oder der Amazon SNS SNS-API.
2. Amazon RDS sendet eine Bestätigungs-E-Mail oder SMS-Nachricht an die Adressen, die Sie mit Ihrem Abonnement übermittelt haben.

3. Klicken Sie auf den Link in der erhaltenen Benachrichtigung, um das Abonnement zu bestätigen.
4. Die Amazon-RDS-Konsole aktualisiert den Abschnitt My Event Subscriptions (Meine Ereignisabonnements) mit dem Status Ihres Abonnements.
5. Amazon RDS sendet Benachrichtigungen an die Adressen, die Sie beim Erstellen des Abonnements angegeben haben.

Informationen über Identity and Access Management bei Verwendung von Amazon SNS finden Sie unterIdentity and Access Management in Amazon SNSimAmazon Simple Notification Service-Entwicklerhandbuchaus.

Sie können es verwenden AWS Lambda , um Ereignisbenachrichtigungen von einer DB-Instance aus zu verarbeiten. Weitere Informationen finden Sie unter Using AWS Lambda with Amazon RDS im AWS Lambda Developer Guide.

Zustellung von RDS-Ereignisbenachrichtigungen

Amazon RDS sendet Benachrichtigungen an die Adressen, die Sie beim Erstellen des Abonnements angeben. Die Benachrichtigung kann Nachrichtenattribute mit einschließen, die strukturierte Metadaten zu der Nachricht zur Verfügung stellen. Weitere Informationen über Nachrichtenattribute finden Sie unter Amazon RDS-Ereigniskategorien und Ereignisnachrichten für Aurora.

Es kann bis zu fünf Minuten dauern, bis Ereignisbenachrichtigungen zugestellt werden.

> **Important**
>
> Amazon RDS garantiert nicht die Reihenfolge der Ereignisse, die in einem Ereignisstrom gesendet werden. Die Reihenfolge der Ereignisse kann sich ändern.

Wenn Amazon SNS eine Benachrichtigung an einen abonnierten HTTP- oder HTTPS-Endpunkt sendet, enthält der Nachrichtentext der POST-Nachricht, die an den Endpunkt gesendet wurde, ein JSON-Dokument. Weitere Informationen finden Sie unter Amazon SNS-Nachrichten- und -JSON-Formate im Amazon Simple Notification Service-Entwicklerhandbuch.

Sie können SNS so konfigurieren, dass Sie mit Textnachrichten benachrichtigt werden. Weitere Informationen finden Sie unter Mobile Textnachrichten (SMS) im Amazon Simple Notification Service Developer Guide.

Um Benachrichtigungen zu deaktivieren, ohne ein Abonnement zu löschen, wählen SieNeinfürEnabledin der Amazon RDS-Konsole. Oder Sie können den `Enabled` Parameter so einstellen, dass er die AWS CLI oder die Amazon RDS-API `false` verwendet.

Fakturierung für Amazon-RDS-Ereignisbenachrichtigungen

Die Fakturierung für Amazon-RDS-Ereignisbenachrichtigungen erfolgt über Amazon SNS. Bei Verwendung von Ereignisbenachrichtigungen fallen Amazon-SNS-Gebühren an. Weitere Informationen zur Abrechnung von Amazon SNS finden Sie unter Preise für Amazon Simple Notification Service.

Beispiele für Aurora mit Amazon EventBridge

Die folgenden Beispiele veranschaulichen verschiedene Arten von Aurora-Ereignissen im JSON-Format. Ein Tutorial, das veranschaulicht, wie Sie Ereignisse im JSON-Format erfassen und anzeigen, finden Sie unter Tutorial: Statusänderungen der DB-Instance mithilfe von Amazon protokollieren EventBridge.

Themen

- Beispiel für ein DB-Cluster-Ereignis
- Beispiel für ein Ereignis der DB-Parametergruppe
- Beispiel für ein DB-Cluster-Snapshot-Ereignis

Beispiel für ein DB-Cluster-Ereignis

Es folgt das Beispiel eines DB-Cluster-Ereignisses im JSON-Format. Das Ereignis zeigt, dass der Cluster mit dem Namen `my-db-cluster` gepatcht wurde. Die Ereignis-ID ist `RDS-EVENT-0173`.

```
{
  "version": "0",
  "id": "844e2571-85d4-695f-b930-0153b71dcb42",
  "detail-type": "RDS DB Cluster Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-10-06T12:26:13Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:rds:us-east-1:123456789012:cluster:my-db-cluster"
  ],
```

```
  "detail": {
    "EventCategories": [
      "notification"
    ],
    "SourceType": "CLUSTER",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:my-db-cluster",
    "Date": "2018-10-06T12:26:13.882Z",
    "Message": "Database cluster has been patched",
    "SourceIdentifier": "my-db-cluster",
    "EventID": "RDS-EVENT-0173"
  }
}
```

Beispiel für ein Ereignis der DB-Parametergruppe

Der folgende Code ist ein Beispiel für ein DB-Parametergruppenereignis im JSON-Format. Das Ereignis zeigt, dass der Parameter `time_zone` in der Parametergruppe `my-db-param-group` aktualisiert wurde. Die Ereignis-ID lautet RDS-EVENT-0037.

```
{
  "version": "0",
  "id": "844e2571-85d4-695f-b930-0153b71dcb42",
  "detail-type": "RDS DB Parameter Group Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-10-06T12:26:13Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:rds:us-east-1:123456789012:pg:my-db-param-group"
  ],
  "detail": {
    "EventCategories": [
      "configuration change"
    ],
    "SourceType": "DB_PARAM",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:pg:my-db-param-group",
    "Date": "2018-10-06T12:26:13.882Z",
    "Message": "Updated parameter time_zone to UTC with apply method immediate",
    "SourceIdentifier": "my-db-param-group",
    "EventID": "RDS-EVENT-0037"
  }
}
```

Beispiel für ein DB-Cluster-Snapshot-Ereignis

Es folgt das Beispiel eines DB-Cluster-Snapshot-Ereignisses im JSON-Forma. Das Ereignis zeigt das Erstellen des Snapshots mit dem Namen `my-db-cluster-snapshot`. Die Ereignis-ID lautet RDS-EVENT-0074.

```
{
  "version": "0",
  "id": "844e2571-85d4-695f-b930-0153b71dcb42",
  "detail-type": "RDS DB Cluster Snapshot Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-10-06T12:26:13Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:rds:us-east-1:123456789012:cluster-snapshot:rds:my-db-cluster-snapshot"
  ],
  "detail": {
    "EventCategories": [
      "backup"
    ],
    "SourceType": "CLUSTER_SNAPSHOT",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster-snapshot:rds:my-db-
cluster-snapshot",
    "Date": "2018-10-06T12:26:13.882Z",
    "SourceIdentifier": "my-db-cluster-snapshot",
    "Message": "Creating manual cluster snapshot",
    "EventID": "RDS-EVENT-0074"
  }
}
```

Erteilen von Berechtigungen zum Veröffentlichen von Benachrichtigungen in einem Amazon-SNS-Thema

Erteilen Sie Amazon RDS Berechtigungen zum Veröffentlichen von Benachrichtigungen an ein Amazon Simple Notification Service (Amazon SNS)-Thema, indem Sie dem Zielthema eine AWS Identity and Access Management (IAM)-Richtlinie anfügen. Weitere Informationen zu Berechtigungen finden Sie unter Beispielfälle für die Zugriffskontrolle von Amazon Simple Notification Service im Entwicklerhandbuch für Amazon Simple Notification .

Standardmäßig verfügt ein Amazon-SNS-Thema über eine Richtlinie, die es allen Amazon-RDS-Ressourcen innerhalb desselben Kontos ermöglicht, Benachrichtigungen darin zu veröffentlichen. Sie können eine benutzerdefinierte Richtlinie anfügen, um kontoübergreifende Benachrichtigungen zuzulassen oder den Zugriff auf bestimmte Ressourcen einzuschränken.

Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die Sie dem Amazon-SNS-Zielthema anfügen. Sie beschränkt das Thema auf DB-Instances mit Namen, die dem angegebenen Präfix entsprechen. Geben Sie die folgenden Werte an, um diese Richtlinie zu verwenden:

- `Resource` – Den Amazon-Ressourcennamen (ARN) für das Amazon-SNS-Thema
- `SourceARN` – Ihren RDS-Ressourcen-ARN
- `SourceAccount` – Ihre AWS-Konto-ID

Eine Liste von Ressourcentypen und deren ARNs finden Sie unter Von Amazon RDS definierte Ressourcen in der Service-Autorisierungs-Referenz.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "events.rds.amazonaws.com"
      },
      "Action": [
        "sns:Publish"
      ],
      "Resource": "arn:aws:sns:us-east-1:123456789012:topic_name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:rds:us-east-1:123456789012:db:prefix-*"
```

```
        },
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

Abonnieren von Amazon RDS-Ereignisbenachrichtigungen

Am einfachsten lässt sich ein Abonnement mit der RDS-Konsole erstellen. Wenn Sie Abonnements für Ereignisbenachrichtigungen mithilfe der CLI oder API erstellen möchten, müssen Sie ein Amazon Simple Notification Service-Thema erstellen und dieses Thema über die Amazon SNS-Konsole oder Amazon SNS-API abonnieren. Sie müssen sich auch den Amazon-Ressourcennamen (ARN) des Themas notieren, da dieser beim Übermitteln von CLI-Befehlen oder API-Operationen verwendet wird. Weitere Informationen zum Erstellen und Abonnieren eines SNS-Themas finden Sie unter Erste Schritte mit Amazon SNS im Amazon Simple Notification Service-Entwicklerhandbuch.

Sie können den Quelltyp festlegen, zu dem Sie Benachrichtigungen erhalten möchten, sowie die die Amazon-RDS-Quelle, die das Ereignis auslöst:

Source type (Quellentyp)

Der Quelltyp. Beispiel: Source type (Quellentyp) könnte Instances sein. Sie müssen einen Quellentyp auswählen.

Resources to include (Einzuschließende Ressourcen)

Die Amazon-RDS-Ressourcen, die die Ereignisse generieren. Sie könnten beispielsweise Select specific instances (Spezifische Instances auswählen) und dannmyDBInstance1 auswählen.

In der folgenden Tabelle wird das Ergebnis erläutert für den Fall, dass Sie ***Resources*** to include (Einzuschließende Ressourcen) auswählen bzw. nicht auswählen.

Einzuschließende Ressourcen	Beschreibung	Beispiel
Angegeben	RDS benachrichtigt Sie nur über alle Ereignisse für die angegebene Ressource.	Wenn der Source type (Quellentyp) Instances lautet und Ihre Ressource myDBInstance1 ist, informiert Sie RDS nur über alle Ereignisse für myDBInstance1.
Nicht angegeben	Sie erhalten eine Benachrichtigung von RDS über die Ereignisse für den	Wenn Ihr Source type (Quellentyp) Instances lautet, informiert Sie RDS über alle Ereignisse in

Einzuschl ießende Ressourcen	Beschreibung	Beispiel
	angegebenen Quellentyp für alle Ihre Amazon-RDS-Ressourcen.	Verbindung mit der Instance in Ihrem Konto.

Standardmäßig erhalten Abonnenten von Amazon-SNS-Themen jede Nachricht, die zum Thema veröffentlicht wird. Um eine Teilmenge der Nachrichten zu erhalten, müssen Abonnenten dem Themen-Abonnement eine Filterrichtlinie zuweisen. Weitere Informationen zur SNS-Nachrichtenfilterung finden Sie unter Amazon-SNS-Nachrichtenfilterung im Entwicklerhandbuch zu Amazon Simple Notification Service.

Konsole

So abonnieren Sie RDS-Ereignisbenachrichtigungen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Event subscriptions (Ereignisabonnements).
3. Wählen Sie im Bereich Ereignisabonnements Ereignisabonnement erstellen aus.
4. Geben Sie Ihre Abonnementdetails wie folgt ein:

    a. Geben Sie unter Name einen Namen für das Abonnement für Ereignisbenachrichtigungen ein.

    b. Führen Sie für den Abschnitt Send notifications to (Benachrichtigung senden an) einen der folgenden Schritte aus:

    - Wählen Sie New email topic (Neues E-Mail-Thema) aus. Geben Sie einen Namen für Ihr E-Mail-Thema und eine Liste der Empfänger ein. Wir empfehlen, dass Sie die Ereignisabonnements mit derselben E-Mail-Adresse konfigurieren wie Ihren primären Kontokontakt. Die Empfehlungen, Serviceereignisse und persönlichen Zustandsnachrichten werden über verschiedene Kanäle gesendet. Die Abonnements für dieselbe E-Mail-Adresse stellen sicher, dass alle Nachrichten an einem Ort zusammengefasst werden.

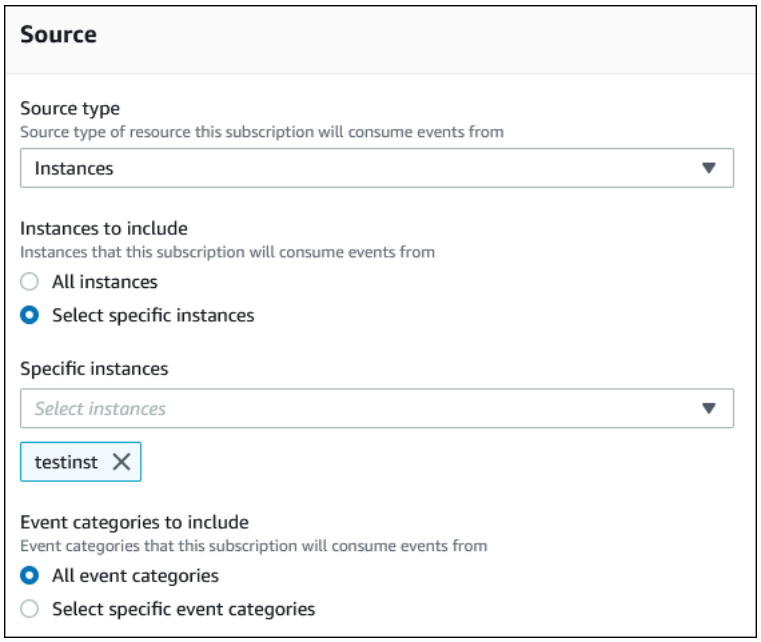
- Wählen Sie Amazon Resource Name (ARN) (Amazon-Ressourcenname (ARN)) aus. Wählen Sie dann einen vorhandenen Amazon-SNS-ARN für ein Amazon-SNS-Thema aus.

  Wenn Sie ein Thema verwenden möchten, das für die serverseitige Verschlüsselung (SSE) aktiviert wurde, gewähren Sie Amazon RDS die erforderlichen Berechtigungen für den Zugriff auf AWS KMS key. Weitere Informationen finden Sie unter Ermöglichen der Kompatibilität zwischen Ereignisquellen aus AWS-Services und verschlüsselten Themen im Entwicklerhandbuch für Amazon Simple Notification Service.

c. Wählen Sie unter Quelltyp einen Quelltyp aus. Wählen Sie beispielsweise Clusters (Cluster) oder Cluster snapshots (Cluster-Snapshots) aus.

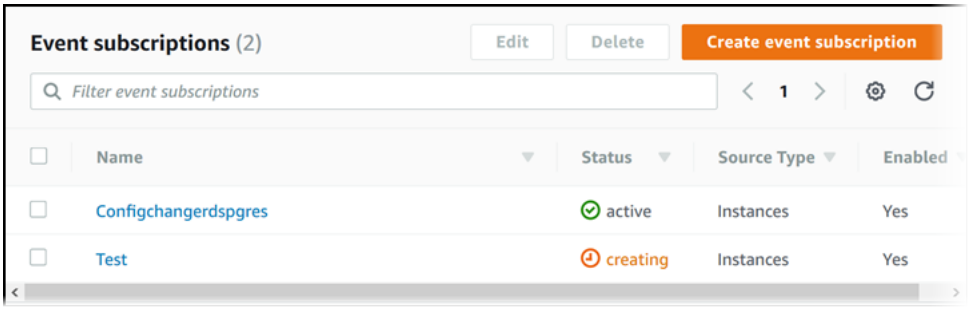
d. Wählen Sie die Ereigniskategorien und Ressourcen aus, für die Sie Ereignisbenachrichtigungen erhalten möchten.

   Im folgenden Beispiel werden Ereignisbenachrichtigungen für die DB-Instance mit dem Namen `testinst` konfiguriert.



e. Wählen Sie Create aus.

In der Amazon RDS-Konsole wird die Erstellung des Abonnements angezeigt.



AWS CLI

Um RDS-Ereignisbenachrichtigungen zu abonnieren, verwenden Sie den AWS CLI-Befehl `create-event-subscription`. Nutzen Sie die folgenden erforderlichen Parameter:

- `--subscription-name`
- `--sns-topic-arn`

Example

Für Linux, macOSoder Unix:

```
aws rds create-event-subscription \
    --subscription-name myeventsubscription \
    --sns-topic-arn arn:aws:sns:us-east-1:123456789012:myawsuser-RDS \
    --enabled
```

Windows:

```
aws rds create-event-subscription ^
    --subscription-name myeventsubscription ^
    --sns-topic-arn arn:aws:sns:us-east-1:123456789012:myawsuser-RDS ^
    --enabled
```

API

Rufen Sie die Amazon-RDS-API-Funktion `CreateEventSubscription` auf, um Amazon-RDS-Ereignisbenachrichtigungen zu abonnieren. Nutzen Sie die folgenden erforderlichen Parameter:

- `SubscriptionName`
- `SnsTopicArn`

Tags und Attribute von Amazon-RDS-Ereignisbenachrichtigungen

Wenn Amazon RDS eine Ereignisbenachrichtigung an Amazon Simple Notification Service (SNS) oder Amazon EventBridge sendet, enthält die Benachrichtigung Nachrichtenattribute und Ereignis-Tags. RDS sendet die Nachrichtenattribute separat mit der Nachricht, während sich die Ereignis-Tags im Nachrichtentext befinden. Verwenden Sie die Nachrichtenattribute und die Amazon-RDS-Tags, um Ihren Ressourcen Metadaten hinzuzufügen. Sie können diese Tags mit Ihren eigenen Notationen über die DB-Instances, Aurora-Clustern usw. ändern. Weitere Informationen über das Markieren von Amazon-RDS-Ressourcen mit Tags finden Sie unter Markieren von Amazon RDS-Ressourcen.

Standardmäßig empfangen Amazon SNS und Amazon EventBridge jede an sie gesendete Nachricht. SNS und EventBridge können die Nachricht filtern und die Benachrichtigungen an den bevorzugten Kommunikationsmodus senden, z. B. eine E-Mail, eine SMS oder einen Aufruf eines HTTP-Endpunkts.

> **Note**
>
> Die Benachrichtigung, die in einer E-Mail oder einer SMS gesendet wird, enthält keine Ereignis-Tags.

Die folgende Tabelle zeigt die Nachrichtenattribute für RDS-Ereignisse, die an den Themen-Subscriber gesendet wurden.

Amazon-RDS-Ereignisattribut	Beschreibung
EventID	Kennung der RDS-Ereignisnachricht, z. B. RDS-EVENT-0006.
Ressource	Die ARN-ID für die Ressource, die das Ereignis aussendet, z. B. `arn:aws:rds:ap-southeast-2:123456789012:db:database-1` .

Die RDS-Tags liefern Daten über die Ressource, die vom Serviceereignis betroffen war. RDS fügt den aktuellen Status der Tags im Nachrichtentext hinzu, wenn die Benachrichtigung an SNS oder EventBridge gesendet wird.

Weitere Informationen zur Nachrichtenfilterung für SNS finden Sie unter Amazon-SNS-Nachrichtenfilterung im Entwicklerhandbuch zu Amazon Simple Notification Service.

Weitere Informationen zum Filtern von Ereignis-Tags für EventBridge finden Sie unter Inhaltsfilterung in Amazon-EventBridge-Ereignismustern im Amazon-EventBridge-Benutzerhandbuch.

Weitere Informationen zum Filtern von nutzlastbasierten Tags für SNS finden Sie unter https://aws.amazon.com/blogs/compute/introducing-payload-based-message-filtering-for-amazon-sns/.

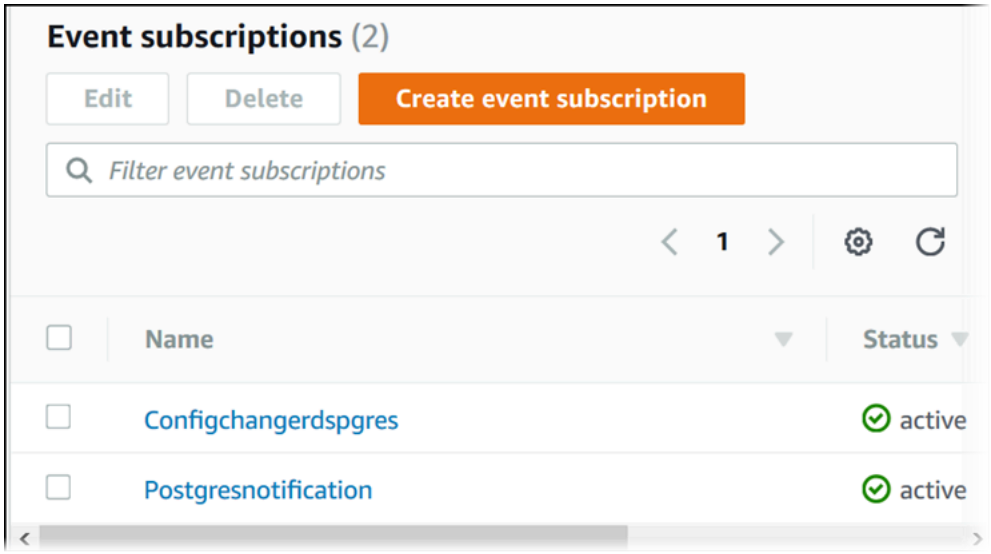
Auflisten von Abonnements für Amazon RDS-Ereignisbenachrichtigungen

Sie können Ihre aktuellen Abonnements für Amazon RDS-Ereignisbenachrichtigungen in einer Liste anzeigen.

Konsole

So zeigen Sie Ihre aktuellen Abonnements für Amazon RDS-Ereignisbenachrichtigungen in einer Liste an

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Ereignisabonnements aus. Im Bereich Ereignisabonnements werden all Ihre Abonnements für Ereignisbenachrichtigungen angezeigt.



AWS CLI

Verwenden Sie den AWS CLI-Befehl `describe-event-subscriptions`, um Ihre aktuellen Abonnements zu Amazon-RDS-Ereignisbenachrichtigungen auflisten zu lassen.

Example

Im folgenden Beispiel werden alle Ereignisabonnements beschrieben.

```
aws rds describe-event-subscriptions
```

Das folgende Beispiel beschreibt den Stack `myfirsteventsubscription`.

```
aws rds describe-event-subscriptions --subscription-name myfirsteventsubscription
```

API

Rufen Sie die Amazon-RDS-API-Aktion `DescribeEventSubscriptions` auf, um Ihre aktuellen Abonnements zu Amazon RDS-Ereignisbenachrichtigungen auflisten zu lassen.

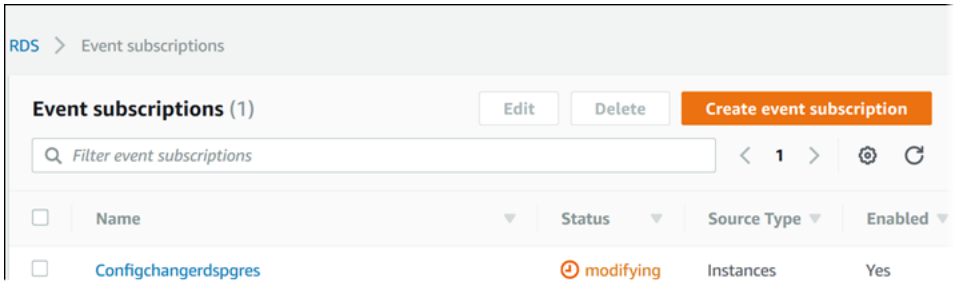
Ändern eines Abonnements für Amazon RDS-Ereignisbenachrichtigungen

Nachdem Sie ein Abonnement erstellt haben, können Sie den Namen des Abonnements, die Quell-ID, Kategorien oder den Thema-ARN ändern.

Konsole

So ändern Sie ein Abonnement für Amazon RDS-Ereignisbenachrichtigungen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Ereignisabonnements aus.
3. Wählen Sie im Bereich Ereignisabonnements das Abonnement, das Sie modifizieren möchten, und klicken Sie auf Bearbeiten.
4. Nehmen Sie Ihre Änderungen am Abonnement im Bereich Ziel oder Quelle vor.
5. Wählen Sie Bearbeiten aus. In der Amazon RDS-Konsole wird die Änderung des Abonnements angezeigt.



AWS CLI

Verwenden Sie den AWS CLI-Befehl `modify-event-subscription`, um ein Abonnement für Amazon-RDS-Ereignisbenachrichtigungen zu ändern. Verwenden Sie den folgenden erforderlichen Parameter:

- `--subscription-name`

Example

Mit folgendem Code wird aktivier `myeventsubscription`.

Für Linux, macOSoder Unix:

```
aws rds modify-event-subscription \
    --subscription-name myeventsubscription \
    --enabled
```

Windows:

```
aws rds modify-event-subscription ^
    --subscription-name myeventsubscription ^
    --enabled
```

API

Um ein Amazon RDS-Ereignis zu ändern, rufen Sie die Amazon RDS-API-Operation auf `ModifyEventSubscription`. Verwenden Sie den folgenden erforderlichen Parameter:

- `SubscriptionName`

Hinzufügen einer Quell-ID zu einem Abonnement für Amazon RDS-Ereignisbenachrichtigungen

Sie können einem vorhandenen Abonnement eine Quell-ID (die Amazon RDS-Quelle, von der das Ereignis generiert wird) hinzufügen.

Konsole

Sie können Quell-IDs einfach über die Amazon RDS-Konsole hinzufügen oder entfernen, indem Sie diese beim Ändern eines Abonnements aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Ändern eines Abonnements für Amazon RDS-Ereignisbenachrichtigungen.

AWS CLI

Verwenden Sie den AWS CLI-Befehl `add-source-identifier-to-subscription`, um einen „Quellenidentifizierer" zu einem Abonnement für Amazon-RDS-Ereignisbenachrichtigungen hinzuzufügen. Nutzen Sie die folgenden erforderlichen Parameter:

- `--subscription-name`
- `--source-identifier`

Example

Im folgenden Beispiel wird die Quell-ID `mysqldb` zum Abonnement `myrdseventsubscription` hinzugefügt.

Für Linux, macOSoder Unix:

```
aws rds add-source-identifier-to-subscription \
    --subscription-name myrdseventsubscription \
    --source-identifier mysqldb
```

Windows:

```
aws rds add-source-identifier-to-subscription ^
    --subscription-name myrdseventsubscription ^
    --source-identifier mysqldb
```

API

Rufen Sie die Amazon RDS-API auf, um eine Quell-ID zu einem Abonnement für Amazon RDS-Ereignisbenachrichtigungen hinzuzufügen `AddSourceIdentifierToSubscription`. Nutzen Sie die folgenden erforderlichen Parameter:

- `SubscriptionName`
- `SourceIdentifier`

Entfernen einer Quell-ID aus einem Abonnement für Amazon RDS-Ereignisbenachrichtigungen

Sie können eine Quell-ID (die Amazon RDS-Quelle, von der das Ereignis generiert wird) aus einem Abonnement entfernen, wenn Sie keine weiteren Benachrichtigungen mehr über Ereignisse für diese Quelle erhalten möchten.

Konsole

Sie können Quell-IDs einfach über die Amazon RDS-Konsole hinzufügen oder entfernen, indem Sie diese beim Ändern eines Abonnements aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Ändern eines Abonnements für Amazon RDS-Ereignisbenachrichtigungen.

AWS CLI

Verwenden Sie den AWS CLI-Befehl `remove-source-identifier-from-subscription`, um einen „Source Quellenidentifizierer" aus einem Abonnement für Amazon-RDS-Ereignisbenachrichtigungen zu entfernen. Nutzen Sie die folgenden erforderlichen Parameter:

- `--subscription-name`
- `--source-identifier`

Example

Im folgenden Beispiel wird die Quell-ID `mysqldb` aus dem Abonnement `myrdseventsubscription` entfernt.

Für Linux, macOSoder Unix:

```
aws rds remove-source-identifier-from-subscription \
    --subscription-name myrdseventsubscription \
    --source-identifier mysqldb
```

Windows:

```
aws rds remove-source-identifier-from-subscription ^
    --subscription-name myrdseventsubscription ^
    --source-identifier mysqldb
```

API

Verwenden Sie den Amazon RDS-API-Befehl `RemoveSourceIdentifierFromSubscription`, um einen „Source Identifier” aus einem Abonnement für Amazon RDS-Ereignisbenachrichtigungen zu entfernen. Nutzen Sie die folgenden erforderlichen Parameter:

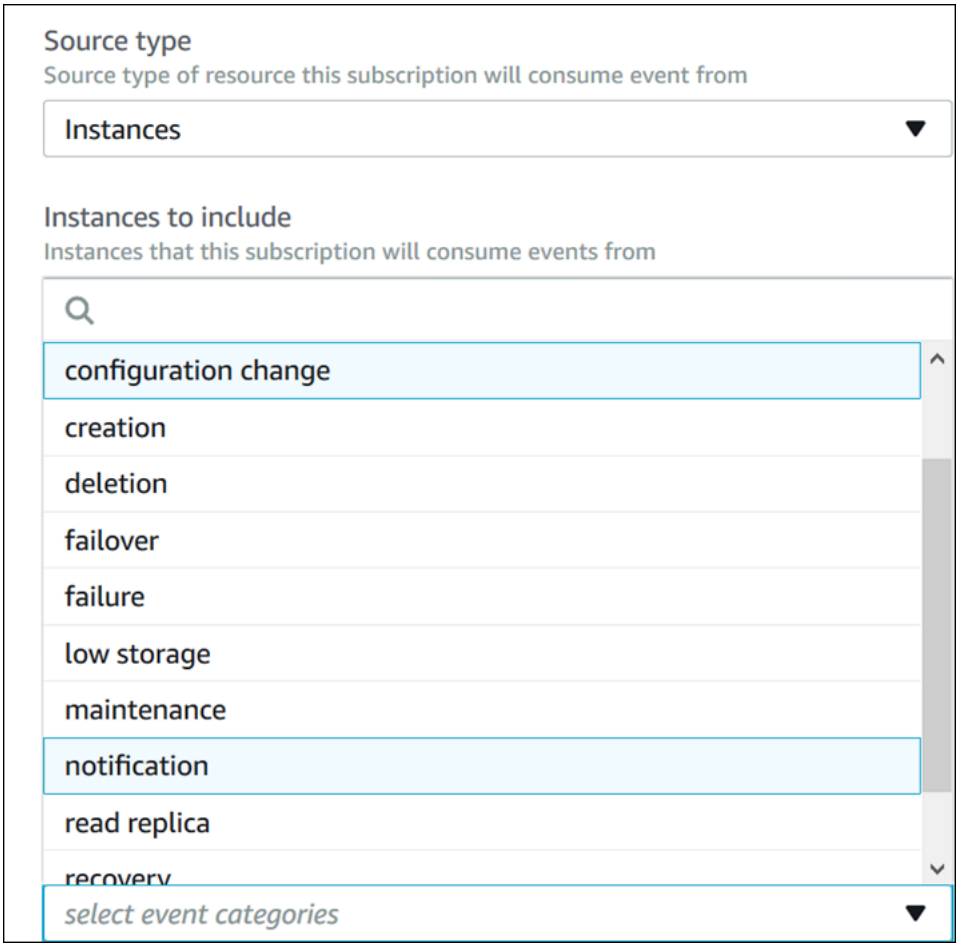
- `SubscriptionName`
- `SourceIdentifier`

Auflisten von Kategorien für Amazon RDS-Ereignisbenachrichtigungen

Alle Ereignisse für einen Ressourcentyp sind in Kategorien gruppiert. Gehen Sie wie folgt vor, um die verfügbaren Kategorien in einer Liste anzuzeigen.

Konsole

Wenn Sie ein Abonnement für Ereignisbenachrichtigungen erstellen oder ändern, werden die Ereigniskategorien in der Amazon RDS-Konsole angezeigt. Weitere Informationen finden Sie unter Ändern eines Abonnements für Amazon RDS-Ereignisbenachrichtigungen.



AWS CLI

Verwenden Sie den AWS CLI-Befehl `describe-event-categories`, um die Amazon-RDS-Ereignisbenachrichtigungskategorien auflisten zu lassen. Dieser Befehl hat keine erforderlichen Parameter.

Example

```
aws rds describe-event-categories
```

API

Verwenden Sie den Amazon RDS-API-Befehl `DescribeEventCategories`, um die Amazon RDS-Ereignisbenachrichtigungskategorien auflisten zu lassen. Dieser Befehl hat keine erforderlichen Parameter.

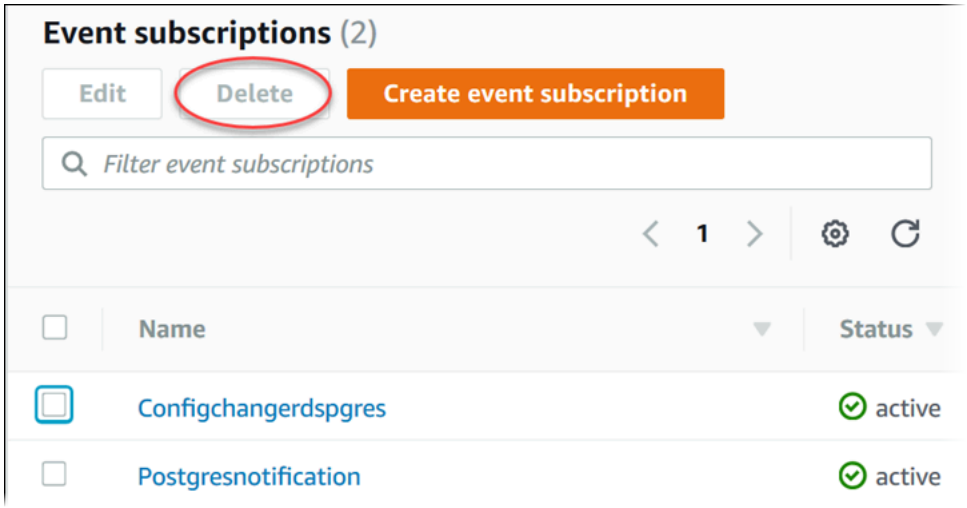
Löschen eines Abonnements für Amazon RDS-Ereignisbenachrichtigungen

Sie können ein Abonnement löschen, wenn Sie es nicht mehr benötigen. Alle Abonnenten des Themas erhalten dann keine weiteren Ereignisbenachrichtigungen, die über dieses Abonnement ausgegeben wurden.

Konsole

So löschen Sie ein Abonnement für Amazon RDS-Ereignisbenachrichtigungen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich DB Event Subscriptions (DB-Ereignisabonnements) aus.
3. Wählen Sie im Bereich My DB Event Subscriptions (Meine DB-Ereignisabonnements) das Abonnement aus, das Sie löschen möchten.
4. Wählen Sie Löschen.
5. In der Amazon RDS-Konsole wird die Löschung des Abonnements angezeigt.



AWS CLI

Verwenden Sie den AWS CLI-Befehl `delete-event-subscription`, um ein Abonnement für Amazon-RDS-Ereignisbenachrichtigungen zu löschen. Verwenden Sie den folgenden erforderlichen Parameter:

- `--subscription-name`

Example

Im folgenden Beispiel wird das Abonnement gelösch `myrdssubscription`.

```
aws rds delete-event-subscription --subscription-name myrdssubscription
```

API

Verwenden Sie den RDS-API-Befehl `DeleteEventSubscription`, um ein Abonnement für Amazon RDS-Ereignisbenachrichtigungen zu löschen. Verwenden Sie den folgenden erforderlichen Parameter:

- `SubscriptionName`

Erstellen einer Regel, die bei einem Amazon Aurora-Ereignis ausgelöst wird

Mit Amazon EventBridge können Sie AWS Services automatisieren und auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen reagieren.

Themen

Tutorial: Statusänderungen der DB-Instance mithilfe von Amazon protokollieren EventBridge

In diesem Tutorial erstellen Sie eine AWS Lambda Funktion, die die Statusänderungen für eine protokolliert. Anschließend erstellen Sie eine Regel, die die Funktion ausführt, sobald eine Statusänderung einer vorhandenen RDS-DB-Instance stattfindet. Das Tutorial geht davon aus, dass Sie eine kleine laufende Test-Instance haben, die Sie vorübergehend herunterfahren können.

> **Important**
>
> Führen Sie dieses Tutorial nicht für eine laufende Produktions-DB-Instance durch.

Themen

Schritt 1: Erstellen Sie eine AWS Lambda Funktion

Erstellen Sie eine Lambda-Funktion, um die Statusänderungsereignisse zu protokollieren. Sie geben diese Funktion beim Erstellen der Regel an.

So erstellen Sie eine Lambda-Funktion:

1. Öffnen Sie die AWS Lambda Konsole unter https://console.aws.amazon.com/lambda/.
2. Wenn Sie noch nicht mit Lambda gearbeitet haben, wird Ihnen eine Willkommensseite angezeigt. Wählen Sie Get Started Now. Andernfalls, wählen Sie Create function (Funktion erstellen) aus.
3. Wählen Sie Von Grund auf neu schreiben aus.

4. Gehen Sie auf der Seite Create function (Funktion erstellen) wie folgt vor:

   a. Geben Sie einen Namen und eine Beschreibung für die Lambda-Funktion ein. Geben Sie der Funktion beispielsweise den Namen **`RDSInstanceStateChange`**.

   b. Wählen Sie in Runtime Node.js 16x aus.

   c. Wählen Sie für Architecture (Architektur) x86_64 aus.

   d. Führen Sie für Execution role (Ausführungsrolle) einen der folgenden Schritte aus:

      - Wählen Sie Create a new role with basic Lambda permissions (Eine neue Rolle mit den grundlegenden Lambda-Berechtigungen erstellen) aus.
      - Wählen Sie für Execution role (Ausführungsrolle) die Option Use an existing role (Vorhandene Rolle verwenden) aus. Wählen Sie die Rolle aus.

   e. Wählen Sie Funktion erstellen.

5. Gehen Sie auf der InstanceStateChangeRDS-Seite wie folgt vor:

   a. In Code-Quelle wählen Sie index.js.

   b. Im Ausschnitt index.js löschen Sie den vorhandenen Code.

   c. Geben Sie den folgenden Code ein:

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('Received event:', JSON.stringify(event));
};
```

   d. Wählen Sie Deploy (Bereitstellen) aus.

Schritt 2: Erstellen einer Regel

Erstellen Sie eine Regel, damit die Lambda-Funktion ausgeführt wird, wenn Sie eine Amazon RDS-Instance starten.

Um die EventBridge Regel zu erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules aus.
3. Wählen Sie Regel erstellen aus.

4. Geben Sie einen Namen und eine Beschreibung für die Regel ein. Geben Sie z. B. ei **`RDSInstanceStateChangeRule`**.
5. Wählen Sie Rule with an event pattern 8Regel mit einem Ereignismuster) und dann Next (Weiter) aus.
6. Wählen Sie als Quelle für Ereignisse die Option AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.
7. Scrollen Sie nach unten zum Abschnitt Event pattern (Ereignismuster).
8. Wählen Sie für Ereignisquelle die Option AWS-Services aus.
9. Wählen Sie für AWS -Service die Option Relational Database Service (RDS) aus.
10. Für Ereignistyp wählen Sie RDS DB-Instance-Ereignis.
11. Übernehmen Sie das Standard-Ereignismuster. Wählen Sie anschließend Weiter.
12. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.
13. Für Select a target (Ein Ziel auswählen), wählen die Option Lambda function (Lambda-Funktion) aus.
14. Wählen Sie für Function (Funktion) die Lambda-Funktion aus, die Sie erstellt haben. Wählen Sie anschließend Weiter.
15. Wählen Sie in Configure tags (Tags konfigurieren) Next (Weiter) aus.
16. Überprüfen Sie die Schritte in Ihrer Regel. Wählen Sie dann Create rule (Regel erstellen) aus.

Schritt 3: Testen der Regel

Um Ihre Regel zu testen, fahren Sie eine RDS-DB-Instance herunter. Warten Sie einige Minuten, bis die Instance heruntergefahren wurde, und prüfen Sie dann, ob Ihre Lambda-Funktion aufgerufen wurde.

Testen der Regel durch Anhalten einer DB-Instance

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Stopp einer RDS-DB-Instance.
3. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
4. Wählen Sie im Navigationsbereich Rules (Regeln), den Namen der von Ihnen erstellten Regel aus.
5. Wählen Sie unter Regeldetails die Option Überwachung aus.

Sie werden zur CloudWatch Amazon-Konsole weitergeleitet. Wenn Sie nicht weitergeleitet werden, klicken Sie auf Metriken anzeigen in CloudWatch.

6. In Alle Metriken wählen Sie den Namen der Regel aus, die Sie erstellt haben.

   Das Diagramm sollte darauf hinweisen, dass die Regel aufgerufen wurde.

7. Wählen Sie im Navigationsbereich Log groups (Protokollgruppen) aus.
8. Wählen Sie den Namen der Protokollgruppe für die Lambda-Funktion aus (/aws/lambda/***function-name***).
9. Wählen Sie den Namen des Protokoll-Streams aus, um die von der Funktion für die von Ihnen gestartete Instance bereitgestellten Daten anzuzeigen. Das empfangene Ergebnis sollte in etwa wie folgt aussehen:

```
{
    "version": "0",
    "id": "12a345b6-78c9-01d2-34e5-123f4ghi5j6k",
    "detail-type": "RDS DB Instance Event",
    "source": "aws.rds",
    "account": "111111111111",
    "time": "2021-03-19T19:34:09Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:rds:us-east-1:111111111111:db:testdb"
    ],
    "detail": {
        "EventCategories": [
            "notification"
        ],
        "SourceType": "DB_INSTANCE",
        "SourceArn": "arn:aws:rds:us-east-1:111111111111:db:testdb",
        "Date": "2021-03-19T19:34:09.293Z",
        "Message": "DB instance stopped",
        "SourceIdentifier": "testdb",
        "EventID": "RDS-EVENT-0087"
    }
}
```

Weitere Beispiele für RDS-Ereignisse im JSON-Format finden Sie unter Überblick über Ereignisse für Aurora.

10. (Optional) Zum Abschluss können Sie die Amazon RDS-Konsole öffnen und die von Ihnen gestoppte Instance starten.

Amazon RDS-Ereigniskategorien und Ereignisnachrichten für Aurora

Amazon RDS generiert eine beträchtliche Anzahl von Ereignissen in Kategorien, die Sie über die Amazon RDS-Konsole oder die API abonnieren können. AWS CLI

Themen

DB-Cluster-Ereignisse

Die folgende Tabelle zeigt den Ereignistyp sowie eine Liste der Ereignisse für den Fall, dass ein DB-Cluster der Quelltyp ist.

> **Note**
>
> Im DB-Cluster-Ereignistyp ist keine Ereigniskategorie für Aurora Serverless vorhanden. Die Aurora Serverless-Ereignisse reichen von RDS-EVENT-0141 bis RDS-EVENT-0149.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Konfigurationsänderung	RDS-EVENT-0016	Die Anmeldeinformationen des Hauptbenutzers werden zurückgesetzt.	
Konfigurationsänderung	RDS-EVENT-0179	Database Activity Streams wird auf Ihrem Datenbank-Cluster gestartet.	Weitere Informationen finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Konfigurationsänderung	RDS-EVENT-0180	Database Activity Streams wird auf Ihrem Datenbank-Cluster angehalten.	Weitere Informationen finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.
Erstellung	RDS-EVENT-0170	DB-Cluster erstellt.	
Löschung	RDS-EVENT-0171	DB-Cluster gelöscht.	
Failover	RDS-EVENT-0069	Das Cluster-Failover ist fehlgeschlagen. Überprüfen Sie den Zustand Ihrer Cluster-Instances und versuchen Sie es erneut.	
Failover	RDS-EVENT-0070	Erneutes Hochstufen der vorherigen primären Instance: *Name*.	
Failover	RDS-EVENT-0071	Failover auf die DB-Instance abgeschlossen: *Name*.	
Failover	RDS-EVENT-0072	Dasselbe AZ-Failover auf die DB-Instance gestartet: *Name*.	
Failover	RDS-EVENT-0073	Übergreifendes AZ-Failover auf die DB-Instance gestartet: *Name*.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Ausfall	RDS-EVENT-0083	Amazon RDS konnte keine Anmeldeinformationen für den Zugriff auf Ihren Amazon-S3-Bucket für Ihren DB-Cluster *Name* erstellen. Dies liegt daran, dass die IAM-Rolle für die S3-Snapshot-Erfassung in Ihrem Konto nicht richtig konfiguriert ist oder der angegebene Amazon-S3-Bucket nicht gefunden werden kann. Weitere Informationen finden Sie im Abschnitt zur Fehlerbehebung in der Amazon-RDS-Dokumentation.	Weitere Informationen finden Sie unter Physische Migration von MySQL mithilfe von Percona XtraBackup und Amazon S3 .
Ausfall	RDS-EVENT-0143	Der DB-Cluster konnte aus diesem Grund nicht von *Einheiten* zu *Einheiten* skalieren: *Grund*.	Skalierung fehlgeschlagen für den Aurora Serverless-DB-Cluster.
Ausfall	RDS-EVENT-0354	Sie können den DB-Cluster aufgrund inkompatibler Ressourcen nicht erstellen. *Nachricht* .	Die *Nachricht* enthält Details über den Fehler.
Ausfall	RDS-EVENT-0355	Der DB-Cluster kann aufgrund unzureichender Ressourcenlimits nicht erstellt werden. *Nachricht* .	Die *Nachricht* enthält Details über den Fehler.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Globales Failover	RDS-EVENT-0181	Die globale Umstellung auf den DB-Cluster *Name* in der Region *Name* wurde gestartet.	Dieses Ereignis bezieht sich auf einen Umstellungsvorgang (früher als „verwaltetes geplantes Failover“ bezeichnet). Der Prozess kann verzögert werden, da andere Vorgänge auf dem DB-Cluster ausgeführt werden.
Globales Failover	RDS-EVENT-0182	Der alte primäre DB-Cluster *Name* in der Region *Name* wurde erfolgreich heruntergefahren.	Dieses Ereignis bezieht sich auf einen Umstellungsvorgang (früher als „verwaltetes geplantes Failover“ bezeichnet). Die alte primäre Instance in der globalen Datenbank akzeptiert keine Schreibvorgänge. Alle Volumes sind synchronisiert.
Globales Failover	RDS-EVENT-0183	Es wird auf die Datensynchronisierung zwischen den globalen Clustermitgliedern gewartet. Der aktuelle Stand liegt hinter dem primären DB-Cluster zurück: *Grund*.	Dieses Ereignis bezieht sich auf einen Umstellungsvorgang (früher als „verwaltetes geplantes Failover“ bezeichnet). Während der Synchronisierungsphase des globalen Datenbank-Failovers tritt eine Replikationsverzögerung auf.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Globales Failover	RDS-EVENT-0184	Der neue primäre DB-Cluster *Name* in der Region *Name* wurde erfolgreich hochgestuft.	Dieses Ereignis bezieht sich auf einen Umstellungsvorgang (früher als „verwaltetes geplantes Failover“ bezeichnet). Die Volumentopologie der globalen Datenbank wird mit dem neuen primären Volume wiederhergestellt.
Globales Failover	RDS-EVENT-0185	Die globale Umstellung auf den DB-Cluster *Name* in der Region *Name* wurde beendet.	Dieses Ereignis bezieht sich auf einen Umstellungsvorgang (früher als „verwaltetes geplantes Failover“ bezeichnet). Die globale Datenbankumstellung wurde auf dem primären DB-Cluster abgeschlossen. Nach Abschluss des Failovers kann es lange dauern, bis Replikate online sind.
Globales Failover	RDS-EVENT-0186	Die globale Umstellung auf den DB-Cluster *Name* in der Region *Name* wurde abgebrochen.	Dieses Ereignis bezieht sich auf einen Umstellungsvorgang (früher als „verwaltetes geplantes Failover“ bezeichnet).
Globales Failover	RDS-EVENT-0187	Die globale Umstellung auf den DB-Cluster *Name* in der Region *Name* ist fehlgeschlagen.	Dieses Ereignis bezieht sich auf einen Umstellungsvorgang (früher als „verwaltetes geplantes Failover“ bezeichnet).

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Globales Failover	RDS-EVENT-0238	Das globale Failover auf den DB-Cluster *Name* in der Region *Name* ist abgeschlossen.	
Globales Failover	RDS-EVENT-0239	Das globale Failover auf den DB-Cluster *Name* in der Region *Name* wurde gestartet.	
Globales Failover	RDS-EVENT-0240	Die erneute Synchronisierung der Mitglieder des DB-Clusters *Name* in der Region *Name* nach dem globalen Failover wurde gestartet.	
Globales Failover	RDS-EVENT-0241	Die erneute Synchronisierung der Mitglieder des DB-Clusters *Name* in der Region *Name* nach dem globalen Failover wurde beendet.	
Wartung	RDS-EVENT-0156	Der DB-Cluster verfügt über ein Upgrade der DB-Engine für kleinere Versionen.	
Wartung	RDS-EVENT-0173	Die Version der Datenbank-Cluster-Engine wurde aktualisiert.	Das Patchen des DB-Clusters ist abgeschlossen.
Wartung	RDS-EVENT-0176	Die Hauptversion der Datenbank-Cluster-Engine wurde aktualisiert.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Wartung	RDS-EVENT-0286	Das Upgrade der Version der Datenbank-Cluster-Engine wurde gestartet.	
Wartung	RDS-EVENT-0287	Es wurde festgestellt, dass ein Betriebssystem-Upgrade erforderlich ist.	
Wartung	RDS-EVENT-0288	Das Upgrade des Cluster-Betriebssystems wird gestartet.	
Wartung	RDS-EVENT-0289	Das Upgrade des Cluster-Betriebssystems wurde abgeschlossen.	
Wartung	RDS-EVENT-0363	*Das Upgrade wird gerade vorbereitet: cluster_name*	Die Upgrade-Vorabprüfungen für den DB-Cluster wurden gestartet.
Benachrichtigung	RDS-EVENT-0076	Fehler bei der Migration von *Name* zu *Name*. Grund: *Grund*.	Migration zu einem Aurora-DB-Cluster fehlgeschlagen.
Benachrichtigung	RDS-EVENT-0077	*Name*.*Name* konnte nicht in InnoDB konvertiert werden. Grund: *Grund*.	Während der Migration zu einem Aurora-DB-Cluster ist der Versuch fehlgeschlagen, ein Tabellenformular aus der Quelldatenbank in InnoDB zu konvertieren.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Benachrichtigung	RDS-EVENT-0085	Der DB-Cluster *Name* kann nicht aktualisiert werden, da die Instance *Name* den Status *Name* hat. Beheben Sie das Problem oder löschen Sie die Instance und versuchen Sie es erneut.	Beim Versuch, den Aurora DB-Cluster zu patchen, ist ein Fehler aufgetreten. Überprüfen Sie Ihren Instance-Status, lösen Sie das Problem und versuchen Sie es erneut. Weitere Informationen finden Sie unter Warten eines Amazon Aurora-DB-Clusters.
Benachrichtigung	RDS-EVENT-0141	Skalieren des DB-Clusters von *Einheiten* zu *Einheiten* aus diesem Grund: *Grund*.	Skalierung initiiert für den Aurora Serverless-DB-Cluster.
Benachrichtigung	RDS-EVENT-0142	Der DB-Cluster hat von *Einheiten* zu *Einheiten* skaliert.	Skalierung abgeschlossen für den Aurora Serverless-DB-Cluster.
Benachrichtigung	RDS-EVENT-0144	Der DB-Cluster wird angehalten.	Für den DB-Cluster von Aurora Serverless wurde eine automatische Pause eingeleitet.
Benachrichtigung	RDS-EVENT-0145	Der Cluster wird angehalten.	Der DB-Cluster von Aurora Serverless wurde angehalten.
Benachrichtigung	RDS-EVENT-0146	Das Anhalten des DB-Clusters wurde abgebrochen.	Das Anhalten des DB-Clusters von Aurora Serverless wurde abgebrochen.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Benachrichtigung	RDS-EVENT-0147	Der Betrieb des DB-Clusters wird fortgesetzt.	Für den DB-Cluster von Aurora Serverless wurde eine Fortsetzungsoperation eingeleitet.
Benachrichtigung	RDS-EVENT-0148	Der Betrieb des DB-Clusters wird fortgesetzt.	Die Fortsetzungsoperation für den DB-Cluster von Aurora Serverless ist abgeschlossen.
Benachrichtigung	RDS-EVENT-0149	Der DB-Cluster hat von *Einheiten* zu *Einheiten* skaliert, aber die Skalierung verlief aus diesem Grund nicht reibungslos: *Grund*.	Die nahtlose Skalierung des mit Durchsetzungsoption für den Aurora Serverless-DB-Cluster wurde abgeschlossen. Verbindungen wurden möglicherweise unterbrochen, wenn erforderlich.
Benachrichtigung	RDS-EVENT-0150	Der DB-Cluster wurde gestoppt.	
Benachrichtigung	RDS-EVENT-0151	Der DB-Cluster wurde gestartet.	
Benachrichtigung	RDS-EVENT-0152	Das Stoppen des DB-Clusters ist fehlgeschlagen.	
Benachrichtigung	RDS-EVENT-0153	Der DB-Cluster wird gestartet, da er die maximal zulässige Anhaltezeit überschritten hat.	
Benachrichtigung	RDS-EVENT-0172	Der Cluster wurde von *Name* in *Name* umbenannt.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Benachrichtigung	RDS-EVENT-0234	Exportaufgabe fehlgeschlagen.	Bei der Aufgabe zum Exportieren des DB-Clusters ist ein Fehler aufgetreten.
Benachrichtigung	RDS-EVENT-0235	Exportaufgabe abgebrochen.	Die Aufgabe zum Exportieren des DB-Clusters wurde abgebrochen.
Benachrichtigung	RDS-EVENT-0236	Exportaufgabe abgeschlossen.	Die Aufgabe zum Exportieren des DB-Clusters ist abgeschlossen.

DB-Instance-Ereignisse

In der folgenden Tabelle werden die Ereigniskategorie und die Ereignisse für den Quelltyp "DB-Instance" aufgeführt.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Verfügbarkeit	RDS-EVENT-0004	DB-Instance-Shutdown.	
Verfügbarkeit	RDS-EVENT-0006	Die DB-Instance wurde neu gestartet.	
Verfügbarkeit	RDS-EVENT-0022	Fehler beim Neustart von mysql: *Meldung*.	Während des Neustarts von Aurora MySQLRDS für MariaDB ist ein Fehler aufgetreten.
Backtrack (Rückverfolgung)	RDS-EVENT-0131	Das eigentliche Rückverfolgungsfenster kann kleiner als das von Ihnen angegebene Zielfenster der Rückverfolgung sein. Erwägen Sie, die Anzahl	Weitere Informationen zur Rückverfolgung finden Sie unter Rückverfolgen eines Aurora-DB-Clusters.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
		von Stunden im Zielfenster der Rückverfolgung zu reduzieren.	
Backtrack (Rückverfolgung)	RDS-EVENT-0132	Das tatsächliche Rückverfolgungsfenster entspricht dem Zielfenster der Rückverfolgung.	
Konfigurationsänderung	RDS-EVENT-0011	Es wurde aktualisiert, um den ParameterGroup *Datenbanknamen* zu verwenden.	
Konfigurationsänderung	RDS-EVENT-0012	Die Änderung wird auf die Datenbank-Instance-Klasse angewendet.	
Konfigurationsänderung	RDS-EVENT-0014	Die Änderung wurde auf die DB-Instance-Klasse angewendet.	
Konfigurationsänderung	RDS-EVENT-0017	Die Änderung wurde auf den zugewiesenen Speicher angewendet.	
Konfigurationsänderung	RDS-EVENT-0025	Die Änderung zur Konvertierung in eine Multi-AZ-DB-Instance wurde angewendet.	
Konfigurationsänderung	RDS-EVENT-0029	Die Änderung zur Konvertierung in eine standardmäßige (Single-AZ-)DB-Instance wurde angewendet.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Konfigurationsänderung	RDS-EVENT-0033	Es gibt *Zahl* Benutzer, die dem Hauptbenutzernamen entsprechen; es wird nur der Benutzer zurückgesetzt, der nicht an einen bestimmten Host gebunden ist.	
Konfigurationsänderung	RDS-EVENT-0067	Ihr Passwort konnte nicht zurückgesetzt werden. Fehlerinformation: *Meldung*.	
Konfigurationsänderung	RDS-EVENT-0078	Das Überwachungsintervall wurde auf *Zahl* geändert.	Die Konfiguration von „Enhanced Monitoring“ (Erweiterte Überwachung) wurde geändert.
Konfigurationsänderung	RDS-EVENT-0092	Die Aktualisierung der DB-Parametergruppe ist abgeschlossen.	
Erstellung	RDS-EVENT-0005	Die DB-Instance wurde erstellt.	
Löschung	RDS-EVENT-0003	Die DB-Instance wurde gelöscht.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Ausfall	RDS-EVENT-0035	Die Datenbank-Instance wurde in *Status* versetzt. *Nachricht* .	Einige Parameter der DB-Instance sind ungültig. Wenn beispielsweise die DB-Instance nicht gestartet werden konnte, da der Wert eines speicherbezogenen Parameters zu hoch für diese Instance-Klasse ist, sollten Sie den Speicherparameter ändern und die DB-Instance neu starten.
Ausfall	RDS-EVENT-0036	Die Datenbank-Instance ist *Status*. *Nachricht* .	Die DB-Instance befindet sich in einem inkompatiblen Netzwerk. Einige der angegebenen Subnetz-IDs sind ungültig oder nicht vorhanden.
Ausfall	RDS-EVENT-0079	Amazon RDS konnte keine Anmeldeinformationen für die erweiterte Überwachung erstellen und diese Funktion wurde deaktiviert. Dies liegt wahrscheinlich daran, dass es in Ihrem Konto rds-monitoring-role nicht vorhanden und nicht korrekt konfiguriert ist. Weitere Informationen finden Sie im Abschnitt zur Fehlerbehebung in der Amazon-RDS-Dokumentation.	Die erweiterte Überwachung kann nicht ohne die IAM-Rolle für erweiterte Überwachung aktiviert werden. Weitere Informationen zum Erstellen der IAM-Rolle finden Sie unter So erstellen Sie eine IAM-Rolle für „Enhanced Monitoring“ (Erweiterte Überwachung) in Amazon RDS.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Ausfall	RDS-EVENT-0080	Amazon RDS konnte die erweiterte Überwachung auf Ihrer Instance nicht konfigurieren: *Name*. Diese Funktion wurde deaktivie rt. Dies liegt wahrschei nlich daran, dass Ihr Konto rds-monitoring-role nicht korrekt vorhanden und konfiguriert ist. Weitere Informationen finden Sie im Abschnitt zur Fehlerbeh ebung in der Amazon-RDS-Dokumentation.	Die erweiterte Überwachu ng wurde aufgrund eines Fehlers während der Konfigurationsänderung deaktiviert. Wahrschei nlich ist die IAM-Rolle für erweiterte Überwachung falsch konfiguriert. Weitere Informationen über das Erstellen der IAM-Rolle für erweiterte Überwachu ng finden Sie unter So erstellen Sie eine IAM-Rolle für „Enhanced Monitorin g“ (Erweiterte Überwachu ng) in Amazon RDS.
Ausfall	RDS-EVENT-0082	Amazon RDS konnte keine Anmeldeinformationen für den Zugriff auf Ihren Amazon-S3-Bucket für Ihre DB-Instance *Name* erstellen . Dies liegt daran, dass die IAM-Rolle für die S3-Snapshot-Erfassung in Ihrem Konto nicht richtig konfiguriert ist oder der angegebene Amazon-S3 -Bucket nicht gefunden werden kann. Weitere Informationen finden Sie im Abschnitt zur Fehlerbeh ebung in der Amazon-RDS-Dokumentation.	Aurora konnte die Sicherungsdaten aus einem Amazon S3-Bucket nicht kopieren. Wahrschei nlich sind die Berechtig ungen für Aurora zum Zugriff auf den Amazon S3-Bucket falsch konfiguri ert. Weitere Informationen finden Sie unter Physische Migration von MySQL mithilfe von Percona XtraBackup und Amazon S3 .

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Ausfall	RDS-EVENT-0254	Das zugrunde liegende Speicherkontingent für dieses Kundenkonto hat das Limit überschri tten. Bitte erhöhen Sie das zulässige Speicherk ontingent, damit die Skalierung auf der Instance durchgeführt werden kann.	
Ausfall	RDS-EVENT-0353	Die DB-Instance kann aufgrund unzureich ender Ressourcenlimits nicht erstellt werden. *Nachricht* .	Die *Nachricht* enthält Details über den Fehler.
Wenig Speicherplatz	RDS-EVENT-0007	Der zugewiesene Speicherplatz ist ausgeschöpft. Weisen Sie zusätzlichen Speicherp latz zu, um das Problem zu lösen.	Der Speicherplatz, der für die DB-Instance zugewiese n wurde, ist aufgebrau cht. Sie sollten der DB-Instance weiteren Speicher zuordnen, um dieses Problem zu lösen. Weitere Informationen finden Sie unter RDS FAQ. Sie können den Speicherplatz für eine DB-Instance mit der Metrik Freier Speicherp latz überwachen.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Wenig Speicherplatz	RDS-EVENT-0089	Die freie Speicherkapazität für DB-Instance: *Name* ist mit *Prozentsatz* des bereitgestellten Speichers gering [Bereitgestellter Speicher: *Größe*, freier Speicher: *Größe*]. Erhöhen Sie ggf. den bereitgestellten Speicher, um dieses Problem zu beheben.	Die DB-Instance hat mehr als 90% ihres zugewiesenen Speichers verbraucht. Sie können den Speicherplatz für eine DB-Instance mit der Metrik Freier Speicherplatz überwachen.
Wenig Speicherplatz	RDS-EVENT-0227	Der Speicherplatz Ihres Aurora-Clusters ist gefährlich knapp, da nur noch *Betrag* Terabyte verbleiben. Bitte ergreifen Sie Maßnahmen, um die Speicherlast auf Ihrem Cluster zu reduzieren.	Das Aurora-Speicher-Subsystem hat wenig Speicherplatz.
Wartung	RDS-EVENT-0026	Es werden Offline-Patches auf die DB-Instance angewendet.	Die Offline-Wartung der DB-Instance wird gerade durchgeführt. Die DB-Instance ist zurzeit nicht verfügbar.
Wartung	RDS-EVENT-0027	Es wurden Offline-Patches auf die DB-Instance angewendet.	Die Offline-Wartung der DB-Instance ist abgeschlossen. Die DB-Instance ist nun verfügbar.
Wartung	RDS-EVENT-0047	Die Datenbank-Instance wurde gepatcht.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Wartung	RDS-EREIGNIS-0155	Die DB-Instance verfügt über ein Upgrade der DB-Engine für kleinere Versionen.	
Benachrichtigung	RDS-EVENT-0044	*message*	Dies ist eine vom Betreiber ausgegebene Benachrichtigung. Weitere Informationen finden Sie in der Ereignismeldung.
Benachrichtigung	RDS-EVENT-0048	Das Upgrade der Datenbank-Engine verzögert sich, da diese Instance über Lesereplikate verfügt, die zuerst aktualisiert werden müssen.	Patchen der DB-Instance wurde verzögert.
Benachrichtigung	RDS-EVENT-0087	Die DB-Instance wurde gestoppt.	
Benachrichtigung	RDS-EVENT-0088	Die DB-Instance wurde gestartet.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Read Replica	RDS-EVENT-0045	Die Replikation wurde gestoppt.	Die Replikation in Ihrer DB-Instance wurde aufgrund von zu wenig Speicher gestoppt. Skalieren Sie den Speicher oder reduzieren Sie die maximale Größe Ihrer Redo-Protokolle, damit die Replikation fortgesetzt werden kann. *Um Redo-Logs mit einer Größe von MiB aufnehmen zu können, benötigen Sie mindestens eine Menge MiB freien Speicherplatz.*
Read Replica	RDS-EVENT-0046	Die Replikation für das Lesereplikat wurde fortgesetzt.	Diese Meldung wird beim ersten Erstellen eines Lesereplikats sowie als Überwachungsmeldung zur Bestätigung der ordnungsgemäßen Replikationsausführung angezeigt. Falls diese Meldung auf die Benachrichtigung `RDS-EVENT-0045` folgt, wurde die Replikation (nach einem Fehler oder nachdem sie gestoppt wurde) fortgesetzt.
Read Replica	RDS-EVENT-0057	Das Replikationsstreaming wurde beendet.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Wiederherstellung	RDS-EVENT-0020	Wiederherstellung der DB-Instance wurde gestartet. Die Wiederherstellungsdauer variiert je nach zu wiederherstellender Datenmenge.	
Wiederherstellung	RDS-EVENT-0021	Wiederherstellung der DB-Instance ist abgeschlossen.	
Wiederherstellung	RDS-EVENT-0023	Aufkommende Snapshot-Anfrage: *Nachricht* .	Ein manuelles Backup wurde angefordert, jedoch erstellt Amazon RDS gerade einen DB-Snapshot. Senden Sie die Anforderung erneut, nachdem Amazon RDS den DB-Snapshot abgeschlossen hat.
Wiederherstellung	RDS-EVENT-0052	Die Wiederherstellung der Multi-AZ-Instance wurde gestartet.	Die Wiederherstellungsdauer variiert je nach zu wiederherstellender Datenmenge.
Wiederherstellung	RDS-EVENT-0053	Die Wiederherstellung der Multi-AZ-Instance wurde abgeschlossen. Failover oder Aktivierung steht noch aus.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Wiederherstellung	RDS-EVENT-0361	Die Wiederherstellung der Standby-DB-Instance wurde gestartet.	Die Standby-DB-Instance wird während des Wiederherstellungsvorgangs neu erstellt. Die Datenbankleistung wird während des Wiederherstellungsprozesses beeinträchtigt.
Wiederherstellung	RDS-EVENT-0362	Die Wiederherstellung der Standby-DB-Instance ist abgeschlossen.	Die Standby-DB-Instance wird während des Wiederherstellungsvorgangs neu erstellt. Die Datenbankleistung wird während des Wiederherstellungsprozesses beeinträchtigt.
Wiederherstellung	RDS-EVENT-0019	DB-Instance *Name* wurde zu *Name* wiederhergestellt.	Die DB-Instance wurde aus einem point-in-time Backup wiederhergestellt.
Ausführen von Sicherheits-Patches	RDS-EVENT-0230	Für Ihre DB-Instance ist ein System-Update verfügbar. Informationen zum Anwenden von Updates finden Sie unter „Warten einer DB-Instance“ im RDS-Benutzerhandbuch.	Ein neuer Betriebssystem-Patch ist verfügbar. Eine neues Nebenversions-Update des Betriebssystems ist für Ihre DB-Instance verfügbar. Informationen zum Anwenden von Aktualisierungen finden Sie unter Arbeiten mit Betriebssystem-Updates.

DB-Parametergruppenereignisse

In der folgenden Tabelle werden die Ereigniskategorie und die Ereignisse für den Quelltyp "DB-Parametergruppe" aufgeführt.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Konfigurationsänderung	RDS-EVENT-0037	Der *Name* des Parameters wurde mit der Methode *Methode* auf *Wert* aktualisiert.	

DB-Sicherheitsgruppenereignisse

In der folgenden Tabelle werden die Ereigniskategorie und die Ereignisse für den Quelltyp "DB-Sicherheitsgruppe" aufgeführt.

> **Note**
>
> DB-Sicherheitsgruppen sind Ressourcen für EC2-Classic. EC2-Classic wurde am 15. August 2022 außer Betrieb genommen. Wir empfehlen Ihnen, so bald wie möglich zu migrieren, falls noch nicht von EC2-Classic zu einer VPC migriert. Weitere Informationen finden Sie unter Migration von EC2-Classic zu einer VPC im Benutzerhandbuch für Amazon EC2 und im Blog EC2-Classic Networking is Retiring – Here's How to Prepare (EC2-Classic Networking geht in den Ruhestand – So bereiten Sie sich vor).

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Konfigurationsänderung	RDS-EVENT-0038	Die Änderung wurde auf die Sicherheitsgruppe angewendet.	
Ausfall	RDS-EVENT-0039	Die Autorisierung als *Benutzer* wird widerrufen.	Die Sicherheitsgruppe, deren Besitzer *Benutzer* ist,

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
			existiert nicht. Die Autorisierung für die Sicherheitsgruppe wurde widerrufen, weil sie ungültig ist.

DB-Cluster-Snapshot-Ereignisse

In der folgenden Tabelle werden die Ereigniskategorie und die Ereignisse für den Quelltyp „DB-Cluster-Snapshot“ aufgeführt.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
backup	RDS-EVENT-0074	Ein manueller Cluster-Snapshot wird erstellt.	
backup	RDS-EVENT-0075	Ein manueller Cluster-Snapshot wurde erstellt.	
Benachrichtigung	RDS-EVENT-0162	Bei der Aufgabe zum Exportieren von Cluster-Snapshots ist ein Fehler aufgetreten.	
Benachrichtigung	RDS-EVENT-0163	Die Aufgabe zum Exportieren von Cluster-Snapshots wurde abgebrochen.	
Benachrichtigung	RDS-EVENT-0164	Die Aufgabe zum Exportieren von Cluster-Snapshots ist abgeschlossen.	
backup	RDS-EVENT-0168	Erstellen eines automatisierten Cluster-Snapshots.	
Backup	RDS-EVENT-0169	Automatisierter Cluster-Snapshot erstellt.	

RDS-Proxy-Ereignisse

Die folgende Tabelle zeigt die Ereigniskategorie und eine Liste von Ereignissen für den Fall, dass ein RDS Proxy der Quelltyp ist.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Konfigurationsänderung	RDS-EVENT-0204	RDS hat den DB-Proxy *Name* geändert.	
Konfigurationsänderung	RDS-EVENT-0207	RDS hat den Endpunkt des DB-Proxys *Name* geändert.	
Konfigurationsänderung	RDS-EVENT-0213	RDS hat das Hinzufügen der DB-Instance erkannt und sie automatisch zur Zielgruppe des DB-Proxys *Name* hinzugefügt.	
Konfigurationsänderung	RDS-EVENT-0213	RDS hat das Löschen der DB-Instance *Name* erkannt und sie automatisch der Zielgruppe *Name* des DB-Proxys *Name* hinzugefügt.	
Konfigurationsänderung	RDS-EVENT-0214	RDS hat das Löschen der DB-Instance *Name* erkannt und sie automatisch aus der Zielgruppe *Name* des DB-Proxys *Name* entfernt.	
Konfigurationsänderung	RDS-EVENT-0215	RDS hat das Löschen des DB-Clusters *Name* erkannt und ihn automatisch aus der Zielgruppe *Name* des DB-Proxys *Name* entfernt.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Erstellung	RDS-EVENT-0203	RDS hat den DB-Proxy *Name* erstellt.	
Erstellung	RDS-EVENT-0206	RDS hat den Endpunkt *Name* für den DB-Proxy *Name* erstellt.	
Löschung	RDS-EVENT-0205	RDS hat den DB-Proxy *Name* erstellt.	
Löschung	RDS-EVENT-0208	RDS hat den Endpunkt *Name* für den DB-Proxy *Name* gelöscht.	
Ausfall	RDS-EVENT-0243	RDS konnte keine Kapazität für den Proxy *Name* bereitstellen, da in Ihren Subnetzen nicht genügend IP-Adressen verfügbar sind: *Name*. Stellen Sie sicher, dass Ihre Subnetze die Mindestanzahl unbenutzter IP-Adressen aufweisen, wie in der RDS-Proxy-Dokumentation empfohlen.	Informationen zur Bestimmung der empfohlenen Anzahl für Ihre Instance-Klasse finden Sie unter Planen der Kapazität von IP-Adressen.
Ausfall	RDS-EVENT-0275	*RDS hat einige Verbindungen zum DB-Proxynamen gedrosselt.* Die Anzahl der gleichzeitigen Verbindungsanfragen vom Client zum Proxy hat das Limit überschritten.	

Blau/Grün-Bereitstellungsereignisse

Die folgende Tabelle zeigt den Ereignistyp sowie eine Liste der Ereignisse für den Fall, dass der Quelltyp „Blau/Grün-Bereitstellung“ ist.

Weitere Informationen zu blauen/grünen Bereitstellungen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

Kategorie	Amazon RDS-Ereignis-ID	Fehlermeldung	Hinweise
Erstellung	RDS-EVENT-0244	Die Blau/Grün-Bereitstellungsaufgaben sind abgeschlossen. Sie können weitere Änderungen an den Datenbanken der grünen Umgebung vornehmen oder die Bereitstellung umstellen.	
Ausfall	RDS-EVENT-0245	Die Erstellung der Blau/Grün-Bereitstellung ist fehlgeschlagen, da (Quell-/Ziel-) DB-(Instance/Cluster) nicht gefunden wurde.	
Löschung	RDS-EVENT-0246	Die Blau/Grün-Bereitstellung wurde gelöscht.	
Benachrichtigung	RDS-EVENT-0247	Die Umstellung von *Blau* zu *Grün* wurde gestartet.	
Benachrichtigung	RDS-EVENT-0248	Die Umstellung der Blau/Grün-Bereitstellung ist abgeschlossen.	
Ausfall	RDS-EVENT-0249	Die Umstellung der Blau/Grün-Bereitstellung wurde abgebrochen.	

Kategorie	Amazon RDS-Ereignis-ID	Fehlermeldung	Hinweise
Benachrichtigung	RDS-EVENT-0259	Die Umstellung von -DB-Cluster *Blau* zu *Grün* wurde gestartet.	
Benachrichtigung	RDS-EVENT-0260	Die Umstellung von -DB-Cluster *Blau* zu *Grün* wurde abgeschlossen. *Blau* wurde in *Blau-alt* und *Grün* in *Blau* umbenannt.	
Ausfall	RDS-EVENT-0261	Die Umstellung von -DB-Cluster *Blau* zu *Grün* wurde aufgrund von *reason* abgebrochen.	
Benachrichtigung	RDS-EVENT-0311	Die Sequenzsynchronisierung für die Umstellung von DB-Cluster *Blau* zu *Grün* wurde initiiert. Die Umstellung kann bei der Verwendung von Sequenzen zu längeren Ausfallzeiten führen.	
Benachrichtigung	RDS-EVENT-0312	Die Sequenzsynchronisierung für die Umstellung von DB-Cluster *Blau* zu *Grün* wurde abgeschlossen.	

Kategorie	Amazon RDS-Ereignis-ID	Fehlermeldung	Hinweise
Ausfall	RDS-EVENT-0314	Die Sequenzsynchronisierung für die Umstellung des DB-Clusters *Blau* zu *Grün* wurde abgebrochen, da die Sequenzen nicht synchronisiert werden konnten.	

Überwachen von Amazon Aurora-Protokolldateien

Jede RDS-Datenbank-Engine generiert Protokolle, auf die Sie für die Überwachung und Fehlerbehebung zugreifen können. Der Typ der Protokolle hängt von Ihrer Datenbank-Engine ab.

Auf Datenbankprotokolle können Sie mithilfe der AWS Management Console, der AWS Command Line Interface (AWS CLI) oder der Amazon-RDS-API zugreifen. Sie können keine Transaktionsprotokolle anzeigen, ansehen oder herunterladen.

> **Note**
>
> In einigen Fällen enthalten Protokolle versteckte Daten. Daher kann es sein, dass das AWS Management Console den Inhalt in einer Protokolldatei anzeigt, aber die Protokolldatei ist möglicherweise leer, wenn Sie sie herunterladen.

Themen

Anzeigen und Auflisten von Datenbank-Protokolldateien

Sie können Datenbank-Protokolldateien für Ihre Amazon-Aurora-DB-Engine mithilfe der AWS Management Console anzeigen. Sie können auflisten, welche Protokolldateien zum Herunterladen bzw. Überwachen verfügbar sind, indem Sie die AWS CLI oder die Amazon-RDS-API verwenden.

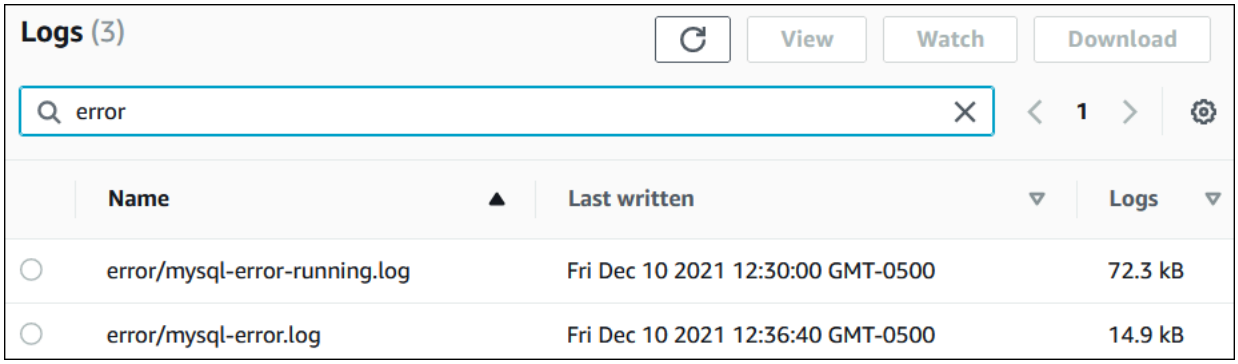
> **Note**
>
> Sie können die Protokolldateien für Aurora Serverless v1-DB-Cluster in der RDS-Konsole nicht anzeigen. Sie können sie jedoch in der Amazon-CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/ ansehen.

Konsole

So zeigen Sie eine Datenbank-Protokolldatei an

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Namen der DB-Instance, welche die anzuzeigende Protokolldatei enthält.
4. Wählen Sie die Registerkarte Logs & events (Protokolle und Ereignisse).
5. Scrollen Sie nach unten bis zum Abschnitt Protokolle.
6. (Optional) Geben Sie einen Suchbegriff ein, um Ihre Ergebnisse zu filtern.

   Im folgenden Beispiel werden Protokolle aufgeführt, die nach dem Text **`error`** gefiltert wurden.



7. Wählen Sie das gewünschte Protokoll und dann View (Anzeigen) aus.

AWS CLI

Um die verfügbaren Datenbank-Protokolldateien für eine DB-Instance aufzulisten, verwenden Sie den AWS CLI-Befehl `describe-db-log-files`.

Das folgende Beispiel gibt eine Liste von Protokolldateien für eine DB-Instance namens zurüc `my-db-instance`.

Example

```
aws rds describe-db-log-files --db-instance-identifier my-db-instance
```

RDS-API

Um die verfügbaren Datenbank-Protokolldateien für eine DB-Instance aufzulisten, verwenden Sie die Amazon RDS-API-Aktion `DescribeDBLogFiles`.

Herunterladen einer Datenbank-Protokolldatei

Sie können die AWS Management Console, AWS CLI oder API zum Herunterladen einer Datenbank-Protokolldatei verwenden.

Konsole

So laden Sie eine Datenbank-Protokolldatei herunter

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Namen der DB-Instance, welche die anzuzeigende Protokolldatei enthält.
4. Wählen Sie die Registerkarte Logs & events (Protokolle und Ereignisse).
5. Scrollen Sie nach unten bis zum Abschnitt Protokolle.
6. Klicken Sie im Bereich Protokolle auf die Schaltfläche neben dem gewünschten Protokoll und wählen Sie Herunterladen.
7. Öffnen Sie das Kontextmenü (rechte Maustaste) für den bereitgestellten Link und wählen Sie Save Link As (Link speichern unter) aus. Geben Sie den Speicherort für die Protokolldatei ein und klicken Sie dann auf Speichern.

AWS CLI

Verwenden Sie den AWS CLI-Befehl `download-db-log-file-portion`, um eine Datenbank-Protokolldatei herunterzuladen. Standardmäßig lädt dieser Befehl nur den neuesten Teil einer

Protokolldatei herunter. Sie können jedoch eine ganze Datei herunterladen, indem Sie den Parameter angebe `--starting-token 0`.

Das folgende Beispiel zeigt, wie man den Inhalt einer Protokolldatei namens log/ERROR.4 herunterlädt und in einer lokalen Datei namens errorlog.txt speichert.

Example

Für Linux, macOSoder Unix:

```
aws rds download-db-log-file-portion \
    --db-instance-identifier myexampledb \
    --starting-token 0 --output text \
    --log-file-name log/ERROR.4 > errorlog.txt
```

Windows:

```
aws rds download-db-log-file-portion ^
    --db-instance-identifier myexampledb ^
    --starting-token 0 --output text ^
    --log-file-name log/ERROR.4 > errorlog.txt
```

RDS-API

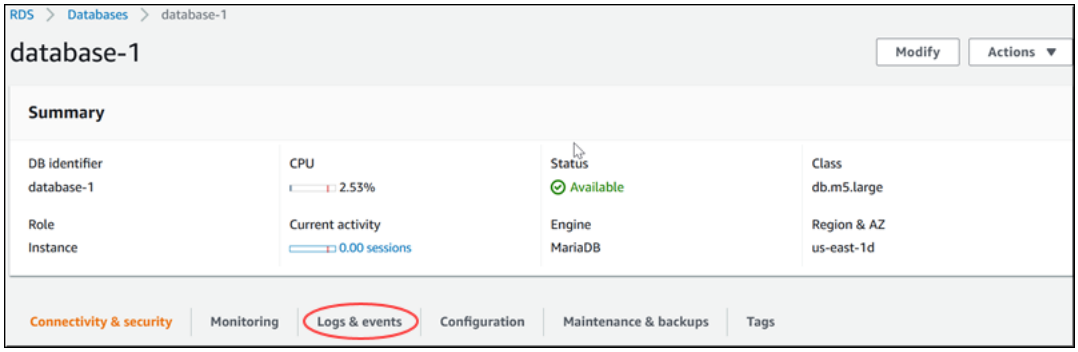
Verwenden Sie die Amazon RDS-API-Aktion `DownloadDBLogFilePortion`, um eine Datenbank-Protokolldatei herunterzuladen.

Überwachen einer Datenbank-Protokolldatei

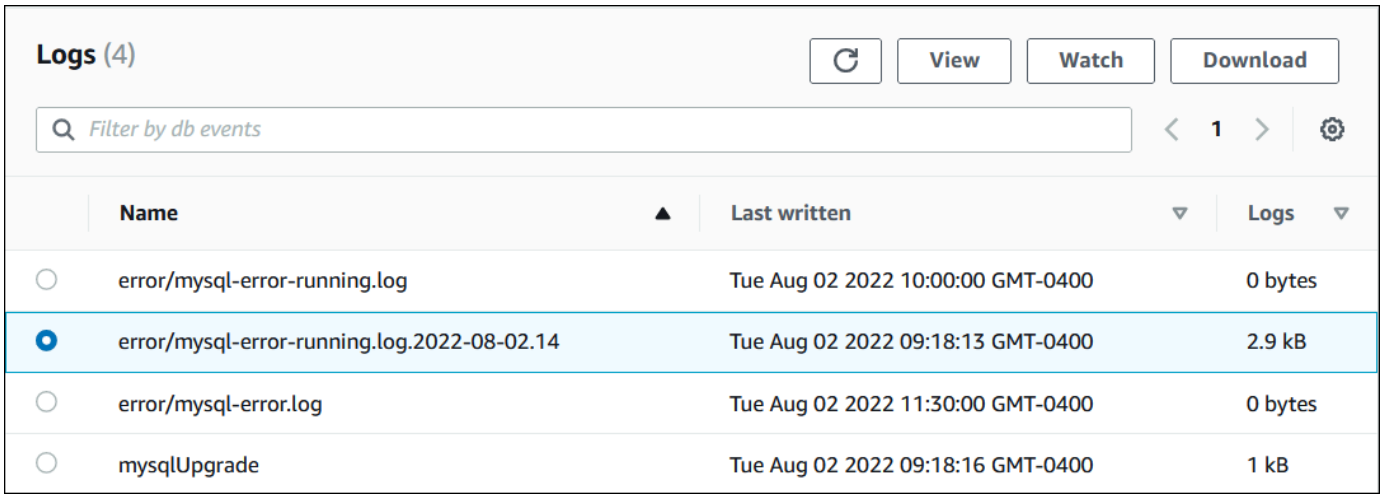
Das Überwachen einer Datenbank-Protokolldatei entspricht dem Verfolgen der Datei auf einem UNIX- oder Linux-System. Sie können eine Protokolldatei über die AWS Management Console überwachen. RDS aktualisiert das Ende des Protokolls alle 5 Sekunden.

So überwachen Sie eine Datenbank-Protokolldatei

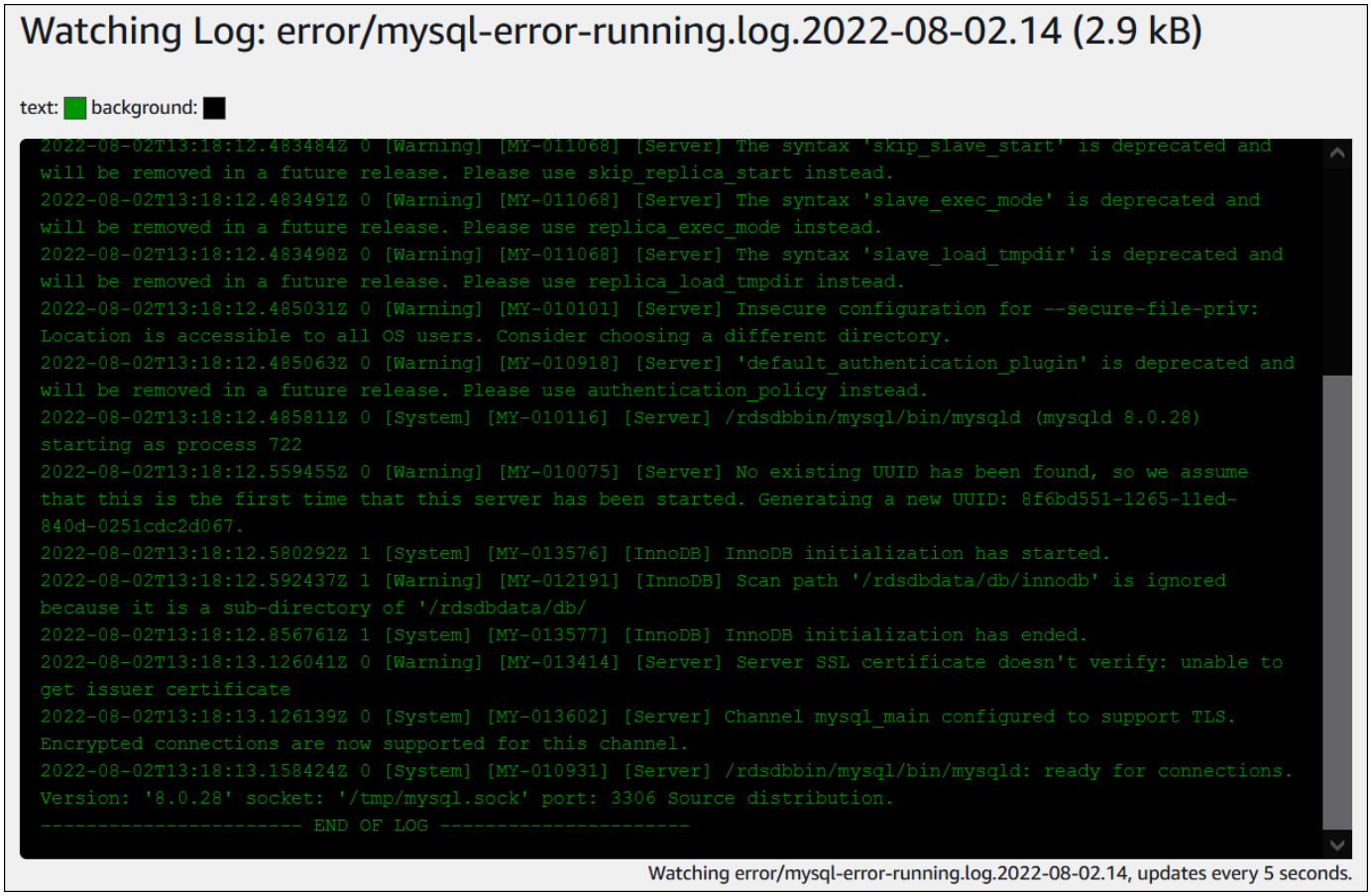
1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Namen der DB-Instance, welche die anzuzeigende Protokolldatei enthält.
4. Wählen Sie die Registerkarte Logs & events (Protokolle und Ereignisse).



5. Wählen Sie im Abschnitt Protokolle eine Protokolldatei und wählen Sie dann Watch (Beobachten).



RDS zeigt das Ende des Protokolls an, wie im folgenden MySQL-Beispiel gezeigt.



Veröffentlichen von Datenbankprotokollen in Amazon CloudWatch Logs

In einer On-Premises-Datenbank befinden sich die Datenbankprotokolle im Dateisystem. Amazon RDS bietet keinen Host-Zugriff auf die Datenbankprotokolle im Dateisystem Ihres DB-Clusters. Aus diesem Grund ermöglicht Amazon RDS das Exportieren von Datenbankprotokollen in Amazon CloudWatch Logs. Mit CloudWatch Logs können Sie Echtzeitanalysen der Protokolldaten durchführen. Sie können die Daten auch in einem Speicher mit hoher Beständigkeit speichern und mit dem CloudWatch-Logs-Agenten verwalten.

Themen

- Überblick über die RDS-Integration mit CloudWatch Logs
- Entscheiden, welche Protokolle in CloudWatch Logs veröffentlicht werden
- Angeben der Protokolle, die in CloudWatch Logs veröffentlicht werden sollen
- Suchen und Filtern Ihrer Protokolle in CloudWatch Logs

Überblick über die RDS-Integration mit CloudWatch Logs

In CloudWatch Logs ist ein Protokollstream eine Abfolge von Protokollereignissen, die dieselbe Quelle nutzen. Jede separate Quelle für Protokolle in CloudWatch Logs bildet einen separaten Protokollstream. Eine Protokollgruppe ist eine Gruppe von Protokollstreams, die dieselben Einstellungen für die Aufbewahrung, Überwachung und Zugriffskontrolle besitzen.

Amazon Aurora streamt kontinuierlich die Protokolldatensätze Ihres DB-Clusters in eine Protokollgruppe. Sie haben z. B. eine Protokollgruppe `/aws/rds/cluster/`*`cluster_name`*`/`*`log_type`* für jeden Protokolltyp, den Sie veröffentlichen. Diese Protokollgruppe befindet sich in derselben AWS-Region wie die Datenbank-Instance, die das Protokoll erzeugt.

AWS bewahrt Protokolldaten, die in CloudWatch Logs veröffentlicht wurden, auf unbegrenzte Dauer auf, wenn keine Aufbewahrungsfrist festgelegt wird. Weitere Informationen finden Sie unter Ändern der Aufbewahrungszeit von Protokolldaten in CloudWatch Logs.

Entscheiden, welche Protokolle in CloudWatch Logs veröffentlicht werden

Jede RDS-Datenbank-Engine unterstützt einen eigene Gruppe von Protokollen. Lesen Sie die folgenden Themen, um mehr über die Optionen für Ihre Datenbank-Engine zu erfahren:

- the section called “Aurora MySQL-Protokolle in CloudWatch Logs veröffentlichen”
- the section called “Veröffentlichen von Aurora-PostgreSQL-Protokollen in - CloudWatch Protokollen”

Angeben der Protokolle, die in CloudWatch Logs veröffentlicht werden sollen

Sie geben an, welche Protokolle in der Konsole veröffentlicht werden sollen. Stellen Sie sicher, dass eine servicegebundene Rolle in AWS Identity and Access Management (IAM) vorhanden ist. Weitere Informationen zu Service-verknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Aurora.

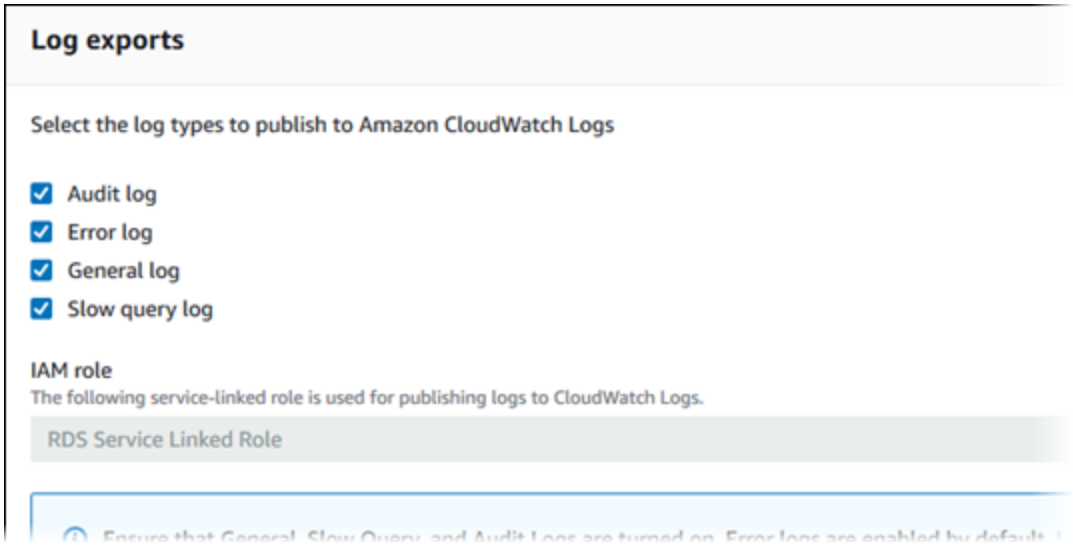
So geben Sie die Protokolle an, die veröffentlicht werden sollen

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Führen Sie eine der folgenden Aufgaben aus:

- Wählen Sie Create database (Datenbank erstellen) aus.
- Wählen Sie eine Datenbank in der Liste und dann Modify (Ändern) aus.

4. Wählen Sie in Logs exports (Protokollexporte) die Protokolle aus, die veröffentlicht werden sollen.

   Im folgenden Beispiel werden das Audit-Protokoll, Fehlerprotokolle, das allgemeine Protokoll und das Slow-Query-Protokoll angegeben.



Suchen und Filtern Ihrer Protokolle in CloudWatch Logs

Sie können mithilfe der Konsole von CloudWatch Logs nach den Protokolleinträgen suchen, die ein bestimmtes Kriterium erfüllen. Sie können auf die Protokolle entweder über die RDS-Konsole, die Sie zur CloudWatch-Logs-Konsole führt, oder direkt über die CloudWatch-Logs-Konsole zugreifen.

So suchen Sie Ihre RDS-Protokolle mithilfe der RDS-Konsole

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie ein DB-Cluster oder eine DB-Instance aus.
4. Wählen Sie Konfiguration.
5. Wählen Sie unter Published logs (Veröffentlichte Protokolle) das Datenbankprotokoll aus, das Sie anzeigen möchten.

So suchen Sie Ihre RDS-Protokolle mithilfe der CloudWatch-Logs-Konsole

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Log groups (Protokollgruppen) aus.
3. Geben Sie im Filterfeld **`/aws/rds`** ein.
4. Wählen Sie für Log Groups den Namen der Protokollgruppe mit dem Protokoll-Stream aus, nach dem gesucht werden soll.
5. Wählen Sie für Log Streams den Namen des zu suchenden Protokoll-Streams.
6. Geben Sie unter Protokollereignisse die zu verwendende Filtersyntax ein.

Weitere Informationen finden Sie unter Suchen und Filtern von Protokolldaten im Benutzerhandbuch von Amazon CloudWatch Logs. Ein Blog-Tutorial zur Überwachung von RDS-Protokollen finden Sie unter Erstellen Sie proaktive Datenbanküberwachung für Amazon RDS mit Amazon CloudWatch Logs, AWS Lambda und Amazon SNS.

Lesen der Protokolldateiinhalte mit REST

Amazon RDS bietet einen REST-Endpunkt, der den Zugriff auf die Protokolldateien der DB-Instance ermöglicht. Dies ist nützlich, wenn Sie eine Anwendung schreiben müssen, um Amazon RDS-Protokolldateiinhalte zu streamen.

Die Syntax lautet wie folgt:

```
GET /v13/downloadCompleteLogFile/DBInstanceIdentifier/LogFileName HTTP/1.1
Content-type: application/json
host: rds.region.amazonaws.com
```

Die folgenden Parameter sind erforderlich:

- *`DBInstanceIdentifier`*: der Name der DB-Instance, welche die Protokolldatei enthält, die Sie herunterladen möchten.
- *`LogFileName`*: der Name der Protokolldatei, die heruntergeladen werden soll.

Die Antwort enthält die Inhalte der angeforderten Protokolldatei als Stream zurück.

Im folgenden Beispiel wird die Protokolldatei namens log/ERROR.6 für die DB-Instance namens sample-sql in der Region us-west-2 heruntergeladen.

```
GET /v13/downloadCompleteLogFile/sample-sql/log/ERROR.6 HTTP/1.1
host: rds.us-west-2.amazonaws.com
X-Amz-Security-Token: AQoDYXdzEIH//////////
wEa0AIXLhngC5zp9CyB1R6abwKrXHVR5efnAVN3XvR7IwqKYalFSn6UyJuEFTft9nObglx4QJ+GXV9cpACkETq=
X-Amz-Date: 20140903T233749Z
X-Amz-Algorithm: AWS4-HMAC-SHA256
X-Amz-Credential: AKIADQKE4SARGYLE/20140903/us-west-2/rds/aws4_request
X-Amz-SignedHeaders: host
X-Amz-Content-SHA256: e3b0c44298fc1c229afbf4c8996fb92427ae41e4649b934de495991b7852b855
X-Amz-Expires: 86400
X-Amz-Signature: 353a4f14b3f250142d9afc34f9f9948154d46ce7d4ec091d0cdabbcf8b40c558
```

Wenn Sie eine nicht vorhandene DB-Instance angeben, besteht die Antwort aus dem folgenden Fehler:

- `DBInstanceNotFound: DBInstanceIdentifier` bezieht sich nicht auf eine vorhandene DB-Instance. (HTTP-Statuscode: 404)

Aurora-MySQL-Datenbank-Protokolldateien

Sie können die Aurora-MySQL-Protokolle direkt über die Amazon-RDS-Konsole, Amazon RDS API, AWS CLI oder AWS-SDKs überwachen. Sie können auf MySQL-Protokolle auch direkt zugreifen, indem Sie die Protokolle in eine Datenbank-Tabelle in der Hauptdatenbank weiterleiten und diese Tabelle abfragen. Mit dem Dienstprogramm "mysqlbinlog" können Sie ein binäres Protokoll herunterladen.

Weitere Informationen zum Anzeigen und Herunterladen von dateibasierten Datenbankprotokollen finden Sie unter Überwachen von Amazon Aurora-Protokolldateien.

Themen

Überblick über Aurora-MySQL-Datenbankprotokolle

Sie können die folgenden Arten von Aurora-MySQL-Protokolldateien überwachen:

- Fehler-log
- Slow-Query-Protokoll
- Allgemeines Protokoll
- Prüfungsprotokoll

Das Aurora-MySQL-Fehlerprotokoll wird standardmäßig generiert. Sie können die langsamen Abfrage- und allgemeinen Protokolle generieren, indem Sie Parameter in Ihrer DB-Parametergruppe festlegen.

Themen

- Protokollrotation und -aufbewahrung für Aurora MySQL

Aurora-MySQL-Fehlerprotokolle

Aurora MySQL schreibt Fehler in die `mysql-error.log`-Datei. An den Namen jeder Protokolldatei wird die Stunde ihrer Erstellung (in UTC) angefügt. Die Protokolldateien verfügen auch über einen Zeitstempel, anhand dessen Sie feststellen können, wann die Protokolleinträge geschrieben wurden.

Aurora MySQL schreibt das Fehlerprotokoll nur beim Startup, Herunterfahren und beim Auftreten von Fehlern. Eine DB-Instance kann Stunden oder Tage lang laufen, ohne dass neue Einträge in das Fehlerprotokoll geschrieben werden. Wenn Sie keine neuen Einträge sehen, sind im Server keine Fehler aufgetreten, die zu einem Eintrag in das Protokoll führen würden.

Konstruktionsbedingt werden die Fehlerprotokolle gefiltert, sodass nur unerwartete Ereignisse wie Fehler angezeigt werden. Die Fehlerprotokolle enthalten jedoch auch einige zusätzliche Datenbankinformationen, z. B. den Abfragefortschritt, die nicht angezeigt werden. Daher kann die Größe der Fehlerprotokolle auch ohne tatsächliche Fehler aufgrund laufender Datenbankaktivitäten zunehmen. Und auch wenn für die Fehlerprotokolle in der AWS Management Console ggf. eine bestimmte Größe in Byte oder Kilobyte angezeigt wird, enthalten die Protokolle möglicherweise 0 Byte, wenn Sie sie herunterladen.

Aurora MySQL schreibt `mysql-error.log` alle 5 Minuten auf die Festplatte. Es fügt den Inhalt des Protokolls `mysql-error-running.log` an.

Aurora MySQL rotiert die Datei `mysql-error-running.log` stündlich.

> **Note**
>
> Der Aufbewahrungszeitraum für das Protokoll ist zwischen Amazon RDS und unterschiedlich Aurora.

Aurora-MySQL-Protokolle für langsame Abfragen und allgemeine Protokolle

Das Slow-Query-Protokoll von Aurora MySQL und das allgemeine Protokoll können in eine Datei oder in eine Datenbanktabelle geschrieben werden. Legen Sie dazu die Parameter in Ihrer DB-Parametergruppe fest. Weitere Informationen zum Erstellen und Ändern einer DB-Parametergruppe finden Sie unter Arbeiten mit Parametergruppen. Sie müssen diese Parameter festlegen, bevor Sie

das Slow-Query-Protokoll oder das allgemeine Protokoll in der Amazon-RDS-Konsole bzw. mithilfe von Amazon-RDS-API, Amazon-RDS-CLI oder AWS SDKs sehen können.

Sie können Aurora-MySQL-Protokolle mithilfe der Parameter in dieser Liste kontrollieren:

- `slow_query_log` Um das Slow-Query-Protokoll zu erstellen, auf 1 setzen. Der Standardwert ist 0.
- `general_log` Um das allgemeine Protokoll zu erstellen, auf 1 setzen. Der Standardwert ist 0.
- `long_query_time`: Damit vermieden wird, dass schnell ausgeführte Abfragen im Slow-Query-Protokoll aufgenommen werden, legen Sie die kürzeste Laufzeit für eine zu protokollierende Abfrage in Sekunden fest. Der Standardwert liegt bei 10 Sekunden, der Mindestwert bei 0. Wenn log_output = FILE, können Sie einen Gleitkommawert angeben, der die Mikrosekundenauflösung festlegt. Wenn log_output = TABLE, können Sie einen Ganzzahlwert angeben, der die Sekundenauflösung festlegt. Nur Abfragen, deren Laufzeit den `long_query_time`-Wert übersteigt, werden im Protokoll aufgenommen. Wenn Sie beispielsweise `long_query_time` auf 0,1 setzen, verhindert dies Einträge von allen Abfragen, die weniger als 100 Millisekunden lang ausgeführt werden.
- `log_queries_not_using_indexes`: Um alle Abfragen, die keinen Index für das Slow-Query-Protokoll verwenden im Protokoll aufzunehmen, auf 1 setzen. Abfragen, die keinen Index verwenden, werden protokolliert, auch wenn ihre Laufzeit niedriger als der Wert des Parameters `long_query_time` ist. Der Standardwert ist 0.
- `log_output` *`option`*: Sie können eine der folgenden Optionen für den `log_output`-Parameter festlegen.
  - TABLE – schreibt allgemeine Abfragen in die `mysql.general_log`-Tabelle und langsame Abfragen in die `mysql.slow_log`-Tabelle.
  - FILE– schreibt Protokolle allgemeiner und langsamer Abfragen in das Dateisystem.
  - NONE– Die Protokollierung ist deaktiviert.

  Bei Aurora-MySQL-Version 2 ist der Standardwert für `log_output FILE`.

Weitere Informationen zu den Slow-Query- und allgemeinen Protokollen finden Sie in den folgenden Themen in der MySQL-Dokumentation:

- Das Slow-Query-Protokoll
- Das allgemeine Abfrageprotokoll

Aurora-MySQL-Prüfprotokoll

Die Auditprotokollierung für Aurora MySQL heißt Advanced Auditing. Zum Aktivieren von Advanced Auditing legen Sie bestimmte DB-Cluster-Parameter fest. Weitere Informationen finden Sie unter Verwenden von Advanced Auditing in einem Amazon Aurora MySQL DB-Cluster.

Protokollrotation und -aufbewahrung für Aurora MySQL

Wenn die Protokollierung aktiviert ist, rotiert oder löscht Amazon Aurora Protokolldateien in regelmäßigen Intervallen. Dies ist eine Vorsichtsmaßnahme, um möglichst zu vermeiden, dass eine umfangreiche Protokolldatei die Datenbanknutzung blockiert oder die Leistung beeinträchtigt. Aurora MySQL behandelt Rotation und Löschen wie folgt:

- Die Dateigrößen der Aurora-MySQL-Fehlerprotokolle sind auf maximal 15 Prozent des zugewiesenen Speicherplatzes für eine DB-Instance beschränkt. Um diesen Schwellenwert einzuhalten, werden die Protokolle automatisch stündlich gedreht. Aurora MySQL entfernt Protokolle nach 30 Tagen oder wenn 15 % des Festplattenspeichers belegt sind. Wenn die kombinierte Größe der Protokolle nach dem Löschen von alten Protokolldateien den Schwellwert überschreitet, werden die ältesten Protokolldateien gelöscht, bis die Größe den Schwellwert nicht mehr überschreitet.
- Aurora MySQL entfernt die Audit-, allgemeinen, langsamen Abfrage-Protokolle entweder nach 24 Stunden oder wenn 15 % des Speichers verbraucht wurden.
- Wenn die `FILE`-Protokollierung aktiviert ist, werden allgemeine Protokolldateien und Protokolldateien für langsame Abfragen stündlich geprüft und Protokolldateien, die älter als 24 Stunden sind, werden gelöscht. In einigen Fällen kann die Größe der verbleibenden kombinierten Protokolldatei nach dem Löschen die Schwelle von 15 % des lokalen Speicherplatzes für eine DB-Instance überschreiten. In diesen Fällen werden die ältesten Protokolldateien gelöscht, bis die Größe den Schwellenwert nicht mehr überschreitet.
- Wenn die `TABLE`-Protokollierung aktiviert ist, werden Protokolltabellen nicht rotiert oder gelöscht. Protokolltabellen werden abgeschnitten, wenn die Größe aller kombinierten Protokolle zu groß ist. Sie können das Ereignis `low_free_storage` abonnieren, um Benachrichtigungen zu erhalten, wenn Protokolltabellen manuell rotiert oder gelöscht werden sollen, um Speicherplatz freizugeben. Weitere Informationen finden Sie unter Arbeiten mit Amazon-RDS-Ereignisbenachrichtigungen.

  Sie können die `mysql.general_log`-Tabelle manuell rotieren, indem Sie die Prozedur `mysql.rds_rotate_general_log` aufrufen. Sie können die `mysql.slow_log`-Tabelle rotieren, wenn Sie die Prozedur `mysql.rds_rotate_slow_log` aufrufen.

Wenn Sie Protokolldateien manuell rotieren, wird die aktuelle Protokolltabelle in eine Sicherungsprotokolltabelle kopiert und die Einträge in der aktuellen Protokolltabelle werden entfernt. Sofern bereits eine Sicherungsprotokolltabelle vorhanden ist, wird diese gelöscht, bevor die aktuelle Protokolltabelle ins Backup kopiert wird. Sie können die Sicherungsprotokolltabelle abfragen, wenn dies nötig ist. Die Backup-Protokolltabelle für die `mysql.general_log`-Tabelle ist als `mysql.general_log_backup` benannt. Die Backup-Protokolltabelle für die `mysql.slow_log`-Tabelle ist als `mysql.slow_log_backup` benannt.

- Die Aurora-MySQL-Überwachungsprotokolle werden rotiert, wenn die Dateigröße 100 MB erreicht, und nach 24 Stunden entfernt.

Um mit den Protokollen über die Amazon RDS-Konsole, Amazon RDS-API, Amazon RDS-CLI, oder AWS SDKs zu arbeiten, setzen Sie den Parameter `log_output` auf FILE. Diese Protokolldateien werden wie das Aurora-MySQL-Fehlerprotokoll stündlich rotiert. Die Protokolldateien, die während der vorherigen 24 Stunden angelegt wurden, werden aufbewahrt. Beachten Sie, dass der Aufbewahrungszeitraum bei Amazon RDS und Aurora jeweils unterschiedlich ist.

Veröffentlichen von Aurora MySQL-Protokollen in Amazon CloudWatch Logs

Sie können die Aurora MySQL-DB-Cluster so konfigurieren, dass Protokolldaten in einer Protokollgruppe in Amazon CloudWatch Logs veröffentlicht werden. Mit CloudWatch Logs können Sie Echtzeitanalysen der Protokolldaten durchführen, und mit CloudWatch können Sie Alarme und Metriken erstellen. Sie können CloudWatch Logs verwenden, um Ihre Protokolldatensätze in einem Speicher mit hoher Beständigkeit abzulegen. Weitere Informationen finden Sie unter Veröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs.

Verwalten tabellenbasierter Aurora-MySQL-Protokolle

Sie können die allgemeinen und Slow-Query-Protokolle an Tabellen in der DB-Instance weiterleiten, indem Sie eine DB-Parametergruppe erstellen und den `log_output`-Serverparameter auf `TABLE` setzen. Allgemeine Abfragen werden anschließend in der `mysql.general_log`-Tabelle und Slow-Queries in der`mysql.slow_log`-Tabelle protokolliert. Sie können die Tabellen abfragen, um auf Protokollinformationen zuzugreifen. Durch Aktivieren dieser Protokollierung wird die Datenmenge erhöht, die in die Datenbank geschrieben wird, was die Performance beeinträchtigen kann.

Das allgemeine Protokoll und das Slow-Query-Protokoll sind standardmäßig deaktiviert. Um die Protokollierung in Tabellen zu aktivieren, müssen Sie auch die Serverparameter `general_log` und `slow_query_log` auf 1 setzen.

Protokolltabellen wachsen stetig, bis die entsprechenden Protokollierungsaktivitäten ausgeschaltet werden, indem der entsprechende Parameter auf gesetzt wir `0`. Mit der Zeit sammelt sich häufig eine große Datenmenge an und belegt einen beträchtlichen Anteil Ihres zugeteilten Speicherplatzes. Amazon Aurora erlaubt Ihnen nicht, die Protokolltabellen zu kürzen, aber Sie können ihre Inhalte verschieben. Beim Rotieren einer Tabelle wird deren Inhalt in einer Sicherungstabelle gespeichert, und anschließend wird eine neue leere Protokolldatei angelegt. Sie können Protokolltabellen mithilfe der folgenden Befehlszeilenprozeduren manuell rotieren, wobei die Eingabeaufforderung mit bezeichnet is `PROMPT>`:

```
PROMPT> CALL mysql.rds_rotate_slow_log;
PROMPT> CALL mysql.rds_rotate_general_log;
```

Um alte Daten komplett zu entfernen und den Speicherplatz zurückzugewinnen, rufen Sie die entsprechende Prozedur zweimal nacheinander auf.

Konfiguration von Aurora MySQL

Das Binärprotokoll ist eine Reihe von Protokolldateien, die Informationen zu Datenänderungen enthalten, die an einer Aurora-MySQL-Server-Instance vorgenommen wurden. Das Binärprotokoll enthält Informationen wie die folgenden:

- Ereignisse, die Datenbankänderungen wie Tabellenerstellungen oder Zeilenänderungen beschreiben
- Informationen über die Dauer jeder Anweisung, durch die Daten aktualisiert wurden
- Ereignisse für Anweisungen, durch die Daten aktualisieren werden hätten können, aber nicht wurden

Das binäre Protokoll zeichnet Anweisungen auf, die während der Replikation gesendet werden. Es ist auch für einige Wiederherstellungsvorgänge erforderlich. Weitere Informationen finden Sie unter Das Binärprotokoll und Binärprotokoll – Übersicht in der MySQL-Dokumentation.

Binäre Protokolle sind nur von der primären DB-Instance aus zugänglich, nicht von den Replicas.

MySQL in Amazon Aurora unterstützt die binären Protokollformate row-based, statement-based und mixed. Wir empfehlen gemischt, sofern Sie kein spezifisches Format des Binärprotokolls benötigen. Einzelheiten zu den verschiedenen Aurora-MySQL-Binärprotokollformaten finden Sie in der MySQL-Dokumentation unter Binärprotokollierungsformate.

Zur Verwendung der Replikation ist das binäre Protokollierungsformat wichtig, da es den Datensatz der Datenänderungen bestimmt, der in der Quelle aufgezeichnet und an die Replikationsziele gesendet wird. Weitere Informationen über Vor- und Nachteile verschiedener binärer Protokollierungsformate finden Sie unter Vorteile und Nachteile einer auf Anweisungen und einer auf Zeilen basierenden Replikation in der MySQL-Dokumentation.

> **Important**
>
> Wenn das binäre Protokollierungsformat auf "row-based" eingestellt ist, kann das zu sehr umfangreichen binären Protokolldateien führen. Große binäre Protokolldateien verringern die Speichermenge, die einem DB--Cluster zur Verfügung steht, und können den Zeitaufwand für die Wiederherstellungsoperation eines DB--Clusters erhöhen.
> Die anweisungsbasierte Replikation kann zu Inkonsistenzen zwischen dem Quell-DB--Cluster und einem Lese-Replikat führen. Weitere Informationen finden Sie unterErkennen sicherer und nicht sicherer Anweisungen in der binären Protokollierung in der MySQL-Dokumentation.
> Durch die Aktivierung der binären Protokollierung wird die Anzahl der Write-Disk-I/O-Operationen für den DB-Cluster erhöht. Sie können die IOPS-Nutzung mit der `VolumeWriteIOPs` CloudWatch Metrik überwachen.

Stellen Sie das MySQL-binäres-Protokollierungsformat wie folgt ein:

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie die DB-Cluster-Parametergruppe aus, die dem zugeordnet ist und den Sie ändern möchten.

   Eine Standard-Parametergruppe kann nicht modifiziert werden. Erstellen Sie eine neue Parametergruppe und ordnen Sie diese dem DB--Cluster zu, wenn der DB--Cluster eine Standardparametergruppe verwendet.

   Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.
4. Wählen Sie unter Aktionen die Option Bearbeiten aus.
5. Legen Sie den Parameter `binlog_format` auf das binäre Protokollierungsformat Ihrer Wahl fest (`ROW`, `STATEMENT` oder `MIXED`). Sie können auch den Wert `OFF` verwenden, um die Binärprotokollierung zu deaktivieren.

> **Note**
>
> Die Einstellung `binlog_format` auf `OFF` in der DB-Cluster-Parametergruppe deaktiviert die `log_bin` Sitzungsvariable. Dadurch wird die binäre Protokollierung auf dem Aurora MySQL-DB-Cluster deaktiviert, wodurch wiederum die `binlog_format` Sitzungsvariable auf den Standardwert von `ROW` in der Datenbank zurückgesetzt wird.

6. Wählen Sie Save changes (Änderungen speichern), um die Aktualisierungen in dieser DB--Cluster-Parametergruppe zu speichern.

Nachdem Sie diese Schritte ausgeführt haben, müssen Sie die Writer-Instance im DB-Cluster neu starten, damit Ihre Änderungen übernommen werden. Wenn Sie in Aurora MySQL Version 2.09 und niedriger die Writer-Instance neu starten, werden auch alle Reader-Instances im DB-Cluster neu gestartet. In Aurora MySQL Version 2.10 und höher müssen Sie alle Reader-Instances manuell neu starten. Weitere Informationen finden Sie unter Neustart eines Amazon Aurora DB-Clusters oder einer Amazon Aurora DB-Instance.

> **Important**
>
> Das Ändern einer DB-Cluster-Parametergruppe wirkt sich auf alle DB-Cluster aus, die diese Parametergruppe verwenden. Wenn Sie unterschiedliche binäre Logging-Formate für verschiedene Aurora MySQL-DB-Cluster in einer AWS Region angeben möchten, müssen die DB-Cluster unterschiedliche DB-Cluster-Parametergruppen verwenden. Diese Parametergruppen identifizieren unterschiedliche Protokollierungsformate. Weisen Sie jedem DB-Cluster die entsprechende DB-Cluster-Parametergruppe zu. Weitere Informationen zu Aurora MySQL-Parametern finden Sie unter Aurora MySQL Konfigurationsparameter.

Zugriff auf MySQL-Binärprotokolle

Sie können das Dienstprogramm mysqlbinlog verwenden, um Binärprotokolle aus RDS-for-MySQL-DB-Instances herunterzuladen oder zu streamen. Das Binärprotokoll wird auf den lokalen Computer heruntergeladen, von wo aus Sie Aktionen, wie die Wiedergabe eines Protokolls mithilfe des Hilfsprogramms mysql ausführen können. Weitere Informationen über die Verwendung des Dienstprogramms mysqlbinlog finden Sie unter Verwenden von mysqlbinlog zum Sichern binärer Protokolldateien in der MySQL-Dokumentation.

Verwenden Sie zum Ausführen des Dienstprogramms mysqlbinlog mit einer Amazon RDS-Instance die folgenden Optionen:

- `--read-from-remote-server` – Erforderlich.
- `--host` – der DNS-Name vom Endpunkt der Instance.
- `--port` – der von der Instance verwendete Port.
- `--user` – ein MySQL-Benutzer, dem die Berechtigung `REPLICATION SLAVE` erteilt wurde.
- `--password` – das Passwort für den MySQL-Benutzer oder lassen Sie einen Passwortwert aus, damit das Dienstprogramm zur Eingabe eines Passworts auffordert.
- `--raw` – Laden Sie die Datei im Binärformat herunter.
- `--result-file` – die lokale Datei, die den raw-Output empfangen soll.
- `--stop-never` – Streamen Sie die binären Protokolldateien.
- `--verbose` – Wenn Sie das Binlog-Format `ROW` verwenden, schließen Sie diese Option ein, um die Zeilenereignisse als Pseudo-SQL-Anweisungen anzuzeigen. Weitere Informationen zur Option `--verbose` finden Sie unter mysqlbinlog row event display in der MySQL-Dokumentation.
- Geben Sie die Namen einer oder mehrerer Binärprotokolldateien an. Verwenden Sie den SQL-Befehl `SHOW BINARY LOGS`, um eine Liste der verfügbaren Protokolle abzurufen.

Weitere Informationen über mysqlbinlog-Optionen finden Sie unter mysqlbinlog – Hilfsprogramm für die Verarbeitung binärer Protokolldateien in der MySQL-Dokumentation.

Die folgenden Beispiele veranschaulichen die Verwendung des Dienstprogramms mysqlbinlog.

Für Linux, macOSoder Unix:

```
mysqlbinlog \
    --read-from-remote-server \
    --host=MySQLInstance1.cg034hpkmmjt.region.rds.amazonaws.com \
    --port=3306  \
    --user ReplUser \
    --password \
    --raw \
    --verbose \
    --result-file=/tmp/ \
    binlog.00098
```

Windows:

```
mysqlbinlog ^
    --read-from-remote-server ^
    --host=MySQLInstance1.cg034hpkmmjt.region.rds.amazonaws.com ^
    --port=3306  ^
    --user ReplUser ^
    --password ^
    --raw ^
    --verbose ^
    --result-file=/tmp/ ^
    binlog.00098
```

In der Regel bereinigt Amazon RDS binäre Protokolldateien so schnell wie möglich. Andererseits muss das binäre Protokoll immer noch auf der Instance verfügbar sein, auf die mysqlbinlog zugreifen soll. Verwenden Sie die gespeicherte Prozedur mysql.rds_set_configuration und geben Sie einen Zeitraum mit ausreichend Zeit für den Download der Protokolle an, um die Anzahl der Stunden zu bestimmen, die RDS zum Aufbewahren der Binärprotokolle beachten soll. Nachdem Sie den Aufbewahrungszeitraum festgelegt haben, überwachen Sie die Speichernutzung für die DB-Instance, um sicherzustellen, dass die aufbewahrten binären Protokolle nicht zu viel Speicherplatz beanspruchen.

Das folgende Beispiel setzt den Aufbewahrungszeitraum auf 1 Tag.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

Verwenden Sie die gespeicherte Prozedur mysql.rds_show_configuration, um die aktuelle Einstellung anzeigen zu lassen.

```
call mysql.rds_show_configuration;
```

Datenbank-Protokolldateien von Aurora PostgreSQL

Aurora PostgreSQL protokolliert Datenbankaktivitäten in der PostgreSQL-Standardprotokolldatei. Bei einer On-Premises PostgreSQL-DB-Instance werden diese Nachrichten in `log/postgresql.log` lokal gespeichert. Für einen DB-Cluster von Aurora PostgreSQL ist die Protokolldatei auf dem Aurora-Cluster verfügbar. Außerdem müssen Sie die Amazon-RDS-Konsole verwenden, um deren Inhalte anzusehen oder herunterzuladen. Die Standardprotokollierungsebene erfasst Anmeldefehler, schwerwiegende Serverfehler, Deadlocks und Abfragefehler.

Weitere Informationen zum Anzeigen, Herunterladen und Überwachen von dateibasierten Datenbankprotokollen finden Sie unter Überwachen von Amazon Aurora-Protokolldateien. Weitere Informationen zu PostgreSQL-Protokollen finden Sie unter Arbeiten mit Amazon RDS und Aurora-PostgreSQL-Protokollen: Teil 1 und Arbeiten mit Amazon RDS und Aurora-PostgreSQL-Protokollen: Teil 2.

Zusätzlich zu den in diesem Thema behandelten PostgreSQL-Standardprotokollen unterstützt Aurora PostgreSQL auch die PostgreSQL-Audit-Erweiterung (`pgAudit`). Die meisten regulierten Branchen und Regierungsbehörden müssen ein Auditprotokoll oder einen Audit-Trail für die Änderungen von Daten führen, um die gesetzlichen Bestimmungen zu erfüllen. Weitere Informationen zur Installation und Verwendung von pgAudit finden Sie unter Verwenden von pgAudit zur Protokollierung der Datenbankaktivität.

Themen

- Parameter, die das Protokollierungsverhalten beeinflussen
- Aktivieren der Abfrageprotokollierung für Ihren DB-Cluster von Aurora PostgreSQL

Parameter, die das Protokollierungsverhalten beeinflussen

Sie können das Protokollierungsverhalten für Ihren DB-Cluster von Aurora PostgreSQL anpassen, indem Sie verschiedene Parameter ändern. In der folgenden Tabelle finden Sie unter anderem die Parameter, die sich darauf auswirken, wie lange die Protokolle gespeichert werden, wann das Protokoll rotiert werden soll und ob das Protokoll im CSV-Format (Comma-Separated Value) ausgegeben werden soll. Außerdem ist abgesehen von anderen Einstellungen die Textausgabe angegeben, die an STDERR gesendet wurde. Wenn Sie die Einstellungen für die modifizierbaren Parameter ändern möchten, verwenden Sie eine benutzerdefinierte DB-Cluster -Parametergruppe für Ihren DB-Cluster von Aurora PostgreSQL. Weitere Informationen finden Sie unter Arbeiten mit

Parametergruppen. Wie in der Tabelle angegeben, kann der Wert `log_line_prefix` nicht geändert werden.

Parameter	Standard	Beschreibung
log_destination	stderr	Legt das Ausgabeformat für das Protokoll fest. Die Standardeinstellung ist `stderr`, aber Sie können auch das CSV-Format angeben, indem Sie der Einstellung `csvlog` hinzufügen. Weitere Informationen finden Sie unter Festlegen des Protokollziels (`stderr`, `csvlog`).
log_filename	postgresql.log.%Y-%m-%d-%H%M	Gibt das Muster für den Namen der Protokolldatei an. Zusätzlich zur Standardeinstellung unterstützt dieser Parameter `postgresql.log.%Y-%m-%d` und `postgresql.log.%Y-%m-%d-%H` für das Dateinamenmuster.
log_line_prefix	%t:%r:%u@%d:[%p]:	Definiert das Präfix für jede Protokollzeile, die in `stderr` geschrieben wird, um die Uhrzeit (%t), den Remote-Host (%r), den Benutzer (%u), die Datenbank (%d) und die Prozess-ID (%p) anzugeben. Sie können diesen Parameter nicht ändern.
log_rotation_age	60	Minuten, nach denen die Protokolldatei automatisch rotiert wird. Sie können diesen Wert im Bereich von 1 bis 1440 Minuten ändern. Weitere Informationen finden Sie unter Festlegen der Rotation der Protokolldatei.
log_rotation_size	–	Die Größe (kB), bei der das Protokoll automatisch rotiert wird. Sie können diesen Wert im Bereich von 50.000 bis 1.000.000 Kilobyte ändern. Weitere Informationen hierzu finden

Parameter	Standard	Beschreibung
		Sie unter Festlegen der Rotation der Protokoll datei.
rds.log_retention_ period	4320	PostgreSQL-Protokolle, die älter als die angegebene Anzahl von Minuten sind, werden gelöscht. Mit dem Standardwert von 4.320 Minuten werden Protokolldateien nach 3 Tagen gelöscht. Weitere Informationen finden Sie unter Festlegen des Aufbewahrungszeitraums für Protokolle.

Anwendungsprobleme können Sie identifizieren, indem Sie im Protokoll nach Abfragefehlern, Anmeldefehlern, Deadlocks und schwerwiegenden Serverfehlern suchen. Angenommen, Sie haben eine Legacy-Anwendung von Oracle in Aurora PostgreSQL konvertiert, wobei jedoch nicht alle Abfragen ordnungsgemäß umgewandelt wurden. Diese falsch formatierten Abfragen generieren Fehlermeldungen in den Protokollen, mit denen Sie Probleme identifizieren können. Weitere Informationen zur Protokollierung von Abfragen finden Sie unter Aktivieren der Abfrageprotokollierung für Ihren DB-Cluster von Aurora PostgreSQL.

In den folgenden Themen finden Sie Informationen darüber, wie Sie verschiedene Parameter festlegen, die die grundlegenden Details Ihrer PostgreSQL-Protokolle steuern.

Themen

- Festlegen des Aufbewahrungszeitraums für Protokolle
- Festlegen der Rotation der Protokolldatei
- Festlegen des Protokollziels (stderr, csvlog)
- Grundlagen des Parameters log_line_prefix

Festlegen des Aufbewahrungszeitraums für Protokolle

Der `rds.log_retention_period`-Parameter gibt an, wie lange Ihr DB-Cluster von Aurora PostgreSQL die entsprechenden Protokolldateien aufbewahrt. Die Standardeinstellung ist 3 Tage (4 320 Minuten). Sie können diese Einstellung jedoch auf einen beliebigen Wert zwischen 1 Tag (1 440 Minuten) und 7 Tagen (10 080 Minuten) festlegen. Stellen Sie sicher, dass Ihr DB-Cluster

von Aurora PostgreSQL über ausreichend Speicherplatz verfügt, um die Protokolldateien für diesen Zeitraum zu speichern.

Wir empfehlen, dass Sie Ihre Protokolle routinemäßig in Amazon CloudWatch Logs veröffentlichen, damit Sie Systemdaten noch lange nach dem Entfernen der Protokolle aus Ihrem Aurora PostgreSQL-DB-Cluster anzeigen und analysieren können. Weitere Informationen finden Sie unter Veröffentlichen von Aurora-PostgreSQL-Protokollen in Amazon CloudWatch Logs. Nachdem Sie die CloudWatch Veröffentlichung eingerichtet haben, löscht Aurora ein Protokoll erst, nachdem es in CloudWatch Logs veröffentlicht wurde.

Amazon Aurora komprimiert ältere PostgreSQL Protokolle, wenn der Speicher für die DB-Instance einen Schwellenwert erreicht. Aurora komprimiert die Dateien mit dem gzip-Komprimierungsprogramm. Weitere Informationen finden Sie auf der gzip-Website.

Wenn der Speicher für die DB-Instance niedrig ist und alle verfügbaren Protokolle komprimiert sind, erhalten Sie eine Warnung wie die folgende:

```
Warning: local storage for PostgreSQL log files is critically low for
this Aurora PostgreSQL instance, and could lead to a database outage.
```

Wenn nicht genügend Speicher vorhanden ist, löscht Aurora möglicherweise komprimierte PostgreSQL-Protokolle vor Ablauf des angegebenen Aufbewahrungszeitraums. In diesem Fall wird eine Meldung ähnlich der folgenden angezeigt:

```
The oldest PostgreSQL log files were deleted due to local storage constraints.
```

Festlegen der Rotation der Protokolldatei

Neue Protokolldateien werden von Aurora standardmäßig jede Stunde erstellt. Das Timing wird vom Parameter `log_rotation_age` kontrolliert. Dieser Parameter hat einen Standardwert von 60 (Minuten). Sie können ihn jedoch auf jeden beliebigen Wert zwischen 1 Minute und 24 Stunden (1 440 Minuten) festlegen. Wenn die Rotation ansteht, wird eine neue eindeutige Protokolldatei erstellt. Die Datei wird nach dem Muster benannt, das durch den Parameter `log_filename` angegeben wird.

Protokolldateien können auch entsprechend ihrer Größe gedreht werden, wie im Parameter `log_rotation_size` angegeben. Dieser Parameter gibt an, dass das Protokoll rotiert werden soll, wenn es die angegebene Größe (in Kilobyte) erreicht. Der Standardwert für `log_rotation_size`

ist 100 000 KB (Kilobyte) für einen DB-Cluster von Aurora PostgreSQL. Sie können diesen Parameter jedoch auf einen beliebigen Wert zwischen 50 000 und 1 000 000 Kilobyte festlegen.

Die Protokolldateinamen basieren auf dem Dateinamenmuster des Parameters `log_filename`. Die verfügbaren Einstellungen für diesen Parameter lauten wie folgt:

- `postgresql.log.%Y-%m-%d` – Standardformat für den Namen der Protokolldatei. Nimmt das Jahr, den Monat und das Datum in den Namen der Protokolldatei auf.
- `postgresql.log.%Y-%m-%d-%H` – Nimmt die Stunde in das Format des Protokolldateinamens auf.
- `postgresql.log.%Y-%m-%d-%H%M` – Nimmt die Stunde und die Minuten in das Format des Protokolldateinamens auf.

Wenn Sie den `log_rotation_age`-Parameter auf weniger als 60 Minuten festlegen, stellen Sie für den `log_filename`-Parameter das Minutenformat ein.

Weitere Informationen finden Sie unter `log_rotation_age` und `log_rotation_size` in der PostgreSQL-Dokumentation.

Festlegen des Protokollziels (**`stderr`**, **`csvlog`**)

Standardmäßig generiert Aurora PostgreSQL Protokolle im Standardfehlerformat (stderr). Dieses Format ist die Standardeinstellung des Parameters `log_destination`. Jede Nachricht erhält ein Präfix nach dem im `log_line_prefix`-Parameter angegebenen Muster. Weitere Informationen finden Sie unter Grundlagen des Parameters log_line_prefix.

Aurora PostgreSQL kann die Protokolle auch im `csvlog`-Format generieren. Das `csvlog`-Format ist nützlich, um die Protokolldaten als CSV-Daten zu analysieren. Angenommen, Sie verwenden die Erweiterung `log_fdw`, um mit Ihren Protokollen als Fremdtabellen zu arbeiten. Die Fremdtabelle, die für `stderr`-Protokolldateien erstellt wurde, enthält eine einzelne Spalte mit Protokollereignisdaten. Durch Hinzufügen von `csvlog` zum `log_destination`-Parameter erhalten Sie die Protokolldatei im CSV-Format mit Abgrenzungen für die verschiedenen Spalten der Fremdtabelle. Sie können Ihre Protokolle jetzt einfacher sortieren und analysieren.

Wenn Sie `csvlog` für diesen Parameter angeben, beachten Sie, dass sowohl `stderr`- als auch `csvlog`-Dateien generiert werden. Achten Sie auf den von den Protokollen verbrauchten Speicher und berücksichtigen Sie dabei die `rds.log_retention_period`und andere Einstellungen, die sich auf den Protokollspeicher und Turnover auswirken. Wenn Sie `stderr` und `csvlog` verwenden, verdoppelt sich der von den Protokollen verbrauchte Speicher.

Wenn Sie `csvlog` zu `log_destination` hinzufügen und zu `stderr` allein zurückkehren möchten, müssen Sie den Parameter zurücksetzen. Rufen Sie dazu die Amazon-RDS-Konsole auf und öffnen Sie die benutzerdefinierte DB-Cluster-Parametergruppe für Ihre Instance. Wählen Sie den `log_destination`-Parameter, die Option Edit parameter (Parameter bearbeiten) und dann Reset (Zurücksetzen) aus.

Weitere Informationen zum Konfigurieren der Protokollierung finden Sie unter Arbeiten mit Amazon-RDS- und Aurora-PostgreSQL-Protokollen: Teil 1.

Grundlagen des Parameters log_line_prefix

Das `stderr`-Protokollformat wird jeder Protokollnachricht wie folgt mit den Details vorangestellt, die durch den `log_line_prefix`-Parameter angegeben werden.

```
%t:%r:%u@%d:[%p]:t
```

Sie können diese Einstellung nicht ändern. Jeder Protokolleintrag, der an `stderr` gesendet wird, enthält die folgenden Informationen.

- `%t` – Zeitpunkt der Protokolleingabe
- `%r` – Adresse des Remote-Hosts
- `%u@%d` – Benutzername und Datenbankname
- `[%p]` – Prozess-ID, falls verfügbar

Aktivieren der Abfrageprotokollierung für Ihren DB-Cluster von Aurora PostgreSQL

Sie können detailliertere Informationen über Ihre Datenbankaktivitäten sammeln, einschließlich Abfragen, Abfragen, die auf Sperren warten, Prüfpunkte und viele andere Details, indem Sie einige der in der folgenden Tabelle aufgeführten Parameter festlegen. Dieses Thema konzentriert sich auf das Protokollieren von Abfragen.

Parameter	Standard	Beschreibung
log_connections	–	Protokolliert jede erfolgreiche Verbindung. Informationen zur Verwendung dieses Parameters mit `log_disconnections` zum Erkennen von Verbindungsproblem

Parameter	Standard	Beschreibung
		en finden Sie unter Verwalten von Aurora PostgreSQL Verbindungsabwanderung mit Pooling .
log_disconnections	–	Protokolliert das Ende jeder Sitzung und ihre Dauer. Informationen zur Verwendung dieses Parameters mit `log_connections` zum Erkennen von Verbindungsproblemen finden Sie unter Verwalten von Aurora PostgreSQL Verbindungsabwanderung mit Pooling .
log_checkpoints	1	Protokolliert jeden Prüfpunkt.
log_lock_waits	–	Protokolliert lange Sperrenwartezeiten. Dieser Parameter ist standardmäßig nicht festgelegt.
log_min_duration_sample	–	(ms) Legt die Mindestausführungszeit fest, jenseits der stichprobenartig Anweisungen protokolliert werden. Die Stichprobengröße wird mit dem `log_statement_sample_rate` - Parameter festgelegt.
log_min_duration_statement	–	Jede SQL-Anweisung, die mindestens für die angegebene Zeit oder länger ausgeführt wird, wird protokolliert. Dieser Parameter ist standardmäßig nicht festgelegt. Die Aktivierung dieses Parameters kann Sie dabei unterstützen, nicht optimierte Abfragen zu finden.

Parameter	Standard	Beschreibung
log_statement	–	Legt den Typ der protokollierten Anweisungen fest. Standardmäßig ist dieser Parameter nicht festgelegt, aber Sie können ihn in `all`, `ddl` oder `mod` ändern, um die Typen von SQL-Anweisungen anzugeben, die protokolliert werden sollen. Wenn Sie etwas anderes als `none` für diesen Parameter angeben, sollten Sie auch zusätzliche Maßnahmen ergreifen, um die Offenlegung von Passwörtern in den Protokolldateien zu verhindern. Weitere Informationen finden Sie unter Reduzieren des Risikos der Offenlegung von Passwörtern bei der Verwendung der Abfrageprotokollierung.
log_statement_sample_rate	–	Der Prozentsatz der Anweisungen, die die in `log_min_duration_sample` angegebene Zeit bei der Protokollierung überschreiten. Diese Angabe wird als Gleitkommawert zwischen 0,0 und 1,0 ausgedrückt.
log_statement_stats	–	Schreibt kumulative Leistungsstatistiken in das Serverprotokoll.

Verwendung der Protokollierung, um Abfragen mit langsamer Ausführung zu suchen

Sie können SQL-Anweisungen und Abfragen protokollieren, um Abfragen zu finden, die langsam ausgeführt werden. Sie aktivieren diese Funktion, indem Sie die Einstellungen der Parameter `log_statement` und `log_min_duration` wie in diesem Abschnitt beschrieben ändern. Bevor Sie die Abfrageprotokollierung für Ihren DB-Cluster von Aurora PostgreSQL aktivieren, sollten Sie sich der möglichen Offenlegung von Passwörtern in den Protokollen bewusst sein und wissen, wie Sie die Risiken minimieren können. Weitere Informationen finden Sie unter Reduzieren des Risikos der Offenlegung von Passwörtern bei der Verwendung der Abfrageprotokollierung.

Nachstehend finden Sie Referenzinformationen zu den Parametern `log_statement` und `log_min_duration`.

log_statement

Dieser Parameter gibt den Typ der SQL-Anweisungen an, die an das Protokoll gesendet werden sollen. Der Standardwert ist `none`. Wenn Sie diesen Parameter in `all`, `ddl` oder `mod` ändern, stellen Sie sicher, dass Sie die empfohlenen Maßnahmen ergreifen, um das Risiko einer Offenlegung von Passwörtern in den Protokollen zu reduzieren. Weitere Informationen finden Sie unter Reduzieren des Risikos der Offenlegung von Passwörtern bei der Verwendung der Abfrageprotokollierung.

all

Protokolliert alle Anweisungen. Diese Einstellung wird für Debugging-Zwecke empfohlen.

ddl

Protokolliert alle Data Definition Language (DDL)-Anweisungen wie CREATE, ALTER, DROP usw.

mod

Protokolliert alle DDL-Anweisungen und Data Manipulation Language (DML)-Anweisungen wie INSERT, UPDATE und DELETE, die die Daten modifizieren.

Keine

Es werden keine SQL-Anweisungen protokolliert. Wir empfehlen diese Einstellung, um das Risiko zu vermeiden, dass Passwörter in den Protokollen offengelegt werden.

log_min_duration_statement

Jede SQL-Anweisung, die mindestens für die angegebene Zeit oder länger ausgeführt wird, wird protokolliert. Dieser Parameter ist standardmäßig nicht festgelegt. Die Aktivierung dieses Parameters kann Sie dabei unterstützen, nicht optimierte Abfragen zu finden.

–1–2147483647

Die Laufzeit in Millisekunden (ms), in der eine Anweisung protokolliert wird.

So richten Sie die Abfrageprotokollierung ein

Bei diesen Schritten wird davon ausgegangen, dass Ihr DB-Custer von Aurora PostgreSQL eine benutzerdefinierte DB-Cluster-Parametergruppe verwendet.

1. Stellen Sie den Parameter `log_statement` auf `all` ein. Im folgenden Beispiel werden die Informationen gezeigt, die bei dieser Parametereinstellung in die Datei `postgresql.log` geschrieben werden.

```
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:LOG: statement:
 SELECT feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:LOG: QUERY
 STATISTICS
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:DETAIL: ! system
 usage stats:
! 0.017355 s user, 0.000000 s system, 0.168593 s elapsed
! [0.025146 s user, 0.000000 s system total]
! 36644 kB max resident size
! 0/8 [0/8] filesystem blocks in/out
! 0/733 [0/1364] page faults/reclaims, 0 [0] swaps
! 0 [0] signals rcvd, 0/0 [0/0] messages rcvd/sent
! 19/0 [27/0] voluntary/involuntary context switches
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:STATEMENT: SELECT
 feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;
2022-10-05 22:05:56 UTC:52.95.4.1(11335):postgres@labdb:[3639]:ERROR: syntax error
 at or near "ORDER" at character 1
2022-10-05 22:05:56 UTC:52.95.4.1(11335):postgres@labdb:[3639]:STATEMENT: ORDER BY
 s.confidence DESC;
---------------------- END OF LOG ----------------------
```

2. Legen Sie den Parameter `log_min_duration_statement` fest. Im folgenden Beispiel werden die Informationen gezeigt, die in die Datei `postgresql.log` geschrieben werden, wenn der Parameter auf 1 festgelegt wird.

   Abfragen, die die im `log_min_duration_statement`-Parameter angegebene Dauer überschreiten, werden protokolliert. Es folgt ein Beispiel. Sie können die Protokolldatei für Ihren DB-Cluster von Aurora PostgreSQL in der Amazon-RDS-Konsole anzeigen.

```
2022-10-05 19:05:19 UTC:52.95.4.1(6461):postgres@labdb:[6144]:LOG: statement: DROP
 table comments;
2022-10-05 19:05:19 UTC:52.95.4.1(6461):postgres@labdb:[6144]:LOG: duration:
 167.754 ms
2022-10-05 19:08:07 UTC::@:[355]:LOG: checkpoint starting: time
```

```
2022-10-05 19:08:08 UTC::@:[355]:LOG: checkpoint complete: wrote 11 buffers
 (0.0%); 0 WAL file(s) added, 0 removed, 0 recycled; write=1.013 s, sync=0.006 s,
 total=1.033 s; sync files=8, longest=0.004 s, average=0.001 s; distance=131028 kB,
 estimate=131028 kB
---------------------- END OF LOG ----------------------
```

Reduzieren des Risikos der Offenlegung von Passwörtern bei der Verwendung der Abfrageprotokollierung

Wir empfehlen, für `log_statement` die Einstellung `none` beizubehalten, um zu vermeiden, dass Passwörter offengelegt werden. Wenn Sie `log_statement` auf `all`, `ddl` oder `mod` festlegen, sollten Sie einen oder mehrere der folgenden Schritte auszuführen.

- Verschlüsseln Sie vertrauliche Informationen für den Client. Weitere Informationen finden Sie unter Verschlüsselungsoptionen der PostgreSQL-Dokumentation. Verwenden Sie die Optionen `ENCRYPTED` und `UNENCRYPTED` der `CREATE`- und `ALTER`-Anweisungen. Weitere Informationen finden Sie im Abschnitt CREATE USER der PostgreSQL-Dokumentation.
- Richten Sie für Ihren DB-Cluster von Aurora PostgreSQL die PostgreSQL Auditing (PGAudit)-Erweiterung ein und verwenden Sie sie. Diese Erweiterung redigiert sensible Informationen in CREATE- und ALTER-Anweisungen, die an das Protokoll gesendet werden. Weitere Informationen finden Sie unter Verwenden von pgAudit zur Protokollierung der Datenbankaktivität.
- Beschränken Sie den Zugriff auf die CloudWatch Protokolle.
- Verwenden Sie stärkere Authentifizierungsmechanismen wie IAM.

Überwachung von Amazon Aurora-API-Aufrufen in AWS CloudTrail

AWS CloudTrail ist ein AWS-Service, mit dem Sie Ihr AWS-Konto überprüfen können. AWS CloudTrail wird für Ihr AWS-Konto aktiviert, wenn Sie es erstellen. Weitere Informationen über CloudTrail finden Sie im AWS CloudTrail-Leitfaden.

Themen

Integration von CloudTrail in Amazon Aurora

Alle Amazon Aurora-Aktionen werden von CloudTrail protokolliert. CloudTrail bietet eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service in Amazon Aurora durchgeführten Aktionen.

CloudTrail-Ereignisse

CloudTrail erfasst API-Aufrufe für Amazon Aurora als Ereignisse. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. Zu Ereignissen gehören Aufrufe von der Amazon RDS-Konsole und von Code-Aufrufen der Amazon-RDS-API-Operationen.

Amazon Aurora-Aktivitäten werden in einem CloudTrail-Ereignis im Event history (Ereignisverlauf) aufgezeichnet. Sie können die CloudTrail-Konsole verwenden, um API-Aktivitäten und -Ereignisse der letzten 90 Tage in einer AWS-Region anzuzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-API-Ereignisverlauf.

CloudTrail-Trails

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für Amazon Aurora, erstellen Sie einen Trail. Ein Trail ist eine Konfiguration, die die Zustellung von Ereignissen an einen angegebenen Amazon-S3-Bucket ermöglicht. CloudTrail übermittelt Protokolldateien in der Regel innerhalb von 15 Minuten nach einer Kontoaktivität.

> **Note**
>
> Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen.

Sie können zwei Arten von Trails für ein AWS-Konto erstellen: einen Trail, der für alle Regionen gilt, oder einen Trail für eine Region. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle -Regionen.

Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Amazon Aurora-Protokolldateieinträge

CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. CloudTrail-Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der die Aktion `CreateDBInstance` demonstriert.

```
{
    "eventVersion": "1.04",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/johndoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "johndoe"
```

```
    },
    "eventTime": "2018-07-30T22:14:06Z",
    "eventSource": "rds.amazonaws.com",
    "eventName": "CreateDBInstance",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.15.42 Python/3.6.1 Darwin/17.7.0 botocore/1.10.42",
    "requestParameters": {
        "enableCloudwatchLogsExports": [
            "audit",
            "error",
            "general",
            "slowquery"
        ],
        "dBInstanceIdentifier": "test-instance",
        "engine": "mysql",
        "masterUsername": "myawsuser",
        "allocatedStorage": 20,
        "dBInstanceClass": "db.m1.small",
        "masterUserPassword": "****"
    },
    "responseElements": {
        "dBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance",
        "storageEncrypted": false,
        "preferredBackupWindow": "10:27-10:57",
        "preferredMaintenanceWindow": "sat:05:47-sat:06:17",
        "backupRetentionPeriod": 1,
        "allocatedStorage": 20,
        "storageType": "standard",
        "engineVersion": "8.0.28",
        "dbInstancePort": 0,
        "optionGroupMemberships": [
            {
                "status": "in-sync",
                "optionGroupName": "default:mysql-8-0"
            }
        ],
        "dBParameterGroups": [
            {
                "dBParameterGroupName": "default.mysql8.0",
                "parameterApplyStatus": "in-sync"
            }
        ],
        "monitoringInterval": 0,
```

```
        "dBInstanceClass": "db.m1.small",
        "readReplicaDBInstanceIdentifiers": [],
        "dBSubnetGroup": {
            "dBSubnetGroupName": "default",
            "dBSubnetGroupDescription": "default",
            "subnets": [
                {
                    "subnetAvailabilityZone": {"name": "us-east-1b"},
                    "subnetIdentifier": "subnet-cbfff283",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1e"},
                    "subnetIdentifier": "subnet-d7c825e8",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1f"},
                    "subnetIdentifier": "subnet-6746046b",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1c"},
                    "subnetIdentifier": "subnet-bac383e0",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1d"},
                    "subnetIdentifier": "subnet-42599426",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1a"},
                    "subnetIdentifier": "subnet-da327bf6",
                    "subnetStatus": "Active"
                }
            ],
            "vpcId": "vpc-136a4c6a",
            "subnetGroupStatus": "Complete"
        },
        "masterUsername": "myawsuser",
        "multiAZ": false,
        "autoMinorVersionUpgrade": true,
        "engine": "mysql",
```

```
        "cACertificateIdentifier": "rds-ca-2015",
        "dbiResourceId": "db-ETDZIIXHEWY5N7GXVC4SH7H5IA",
        "dBSecurityGroups": [],
        "pendingModifiedValues": {
            "masterUserPassword": "****",
            "pendingCloudwatchLogsExports": {
                "logTypesToEnable": [
                    "audit",
                    "error",
                    "general",
                    "slowquery"
                ]
            }
        },
        "dBInstanceStatus": "creating",
        "publiclyAccessible": true,
        "domainMemberships": [],
        "copyTagsToSnapshot": false,
        "dBInstanceIdentifier": "test-instance",
        "licenseModel": "general-public-license",
        "iAMDatabaseAuthenticationEnabled": false,
        "performanceInsightsEnabled": false,
        "vpcSecurityGroups": [
            {
                "status": "active",
                "vpcSecurityGroupId": "sg-f839b688"
            }
        ]
    },
    "requestID": "daf2e3f5-96a3-4df7-a026-863f96db793e",
    "eventID": "797163d3-5726-441d-80a7-6eeb7464acd4",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


Wie im vorangegangenen Beispiel im Element `userIdentity` gezeigt, enthält jeder Ereignis- oder Protokolleintrag Informationen darüber, wer die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.

- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen zu `userIdentity` finden Sie unter CloudTrail-userIdentity-Element. Weitere Informationen zu `CreateDBInstance` und anderen Amazon Aurora-Aktionen finden Sie in der Amazon RDS API Reference (Amazon-RDS-API-Referenz).

Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams

Mithilfe von Datenbankaktivitätsstreams können Sie nahezu in Echtzeit Datenbankaktivitätsstreams überwachen.

Themen

Übersicht über Datenbankaktivitätsstreams

Als Amazon-Aurora-Datenbankadministrator müssen Sie Ihre Datenbank schützen und Compliance- und regulatorische Anforderungen erfüllen. Eine Strategie besteht darin, Datenbankaktivitätsstrreams in Ihre Überwachungstools zu integrieren. Auf diese Weise überwachen und legen Sie Alarme für Prüfungsaktivitäten in Ihrem Amazon-Aurora-Cluster fest.

Sicherheitsbedrohungen sind sowohl extern als auch intern. Zum Schutz vor internen Bedrohungen können Sie den Administratorzugriff auf Datenströme durch die Konfiguration der Funktion „Datenbankaktivitätsstreams“ steuern. -DBAs haben keinen Zugriff auf die Erfassung, Übertragung, Speicherung und Verarbeitung der Streams.

Themen

Funktionsweise von Datenbankaktivitätsstreams

In Amazon Aurora starten Sie einen Datenbankaktivitäts-Stream auf Clusterebene. Für alle DB-Instances in Ihrem Cluster sind Datenbankaktivitätsstreams aktiviert.

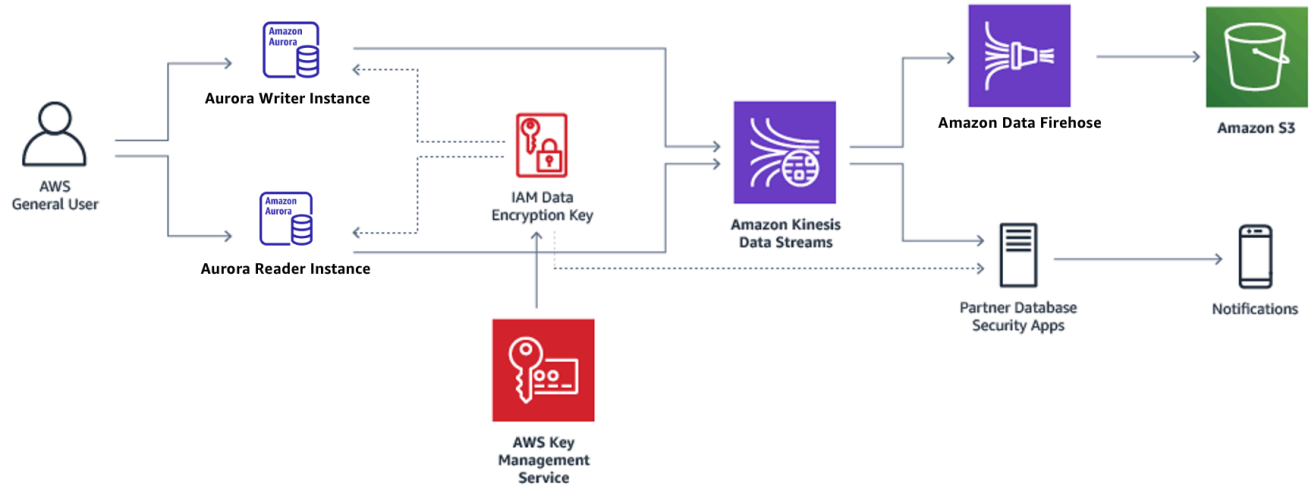
Ihr Aurora-DB-Cluster sendet Aktivitäten nahezu in Echtzeit per Push in einen Amazon Kinesis Data Stream. Der Kinesis Stream wird automatisch erstellt. Von Kinesis aus können Sie AWS Services wie Amazon Data Firehose und konfigurieren, AWS Lambda um den Stream zu nutzen und die Daten zu speichern.

> **Important**
>
> Die Verwendung der Datenbankaktivitätsstreams-Funktion in Amazon Aurora ist kostenlos, Amazon Kinesis erhebt jedoch Gebühren für einen Datenstrom. Weitere Informationen finden Sie unter Amazon Kinesis Data Streams – Preise.

Wenn Sie eine globale Aurora-Datenbank verwenden, starten Sie einen Datenbankaktivitäts-Stream separat auf jedem DB-Cluster. Jeder Cluster liefert Auditdaten innerhalb seiner eigenen AWS-Region an seinen eigenen Kinesis-Stream. Die Aktivitätsstreams funktionieren während eines Failovers nicht anders. Sie prüfen Ihre globale Datenbank weiterhin wie gewohnt.

Sie können Anwendungen für das Compliance-Management für den Verbrauch von Datenbankaktivitäts-Streams konfigurieren. Für Aurora PostgreSQL umfassen Compliance-Anwendungen IBM Security Guardium und Imperva SecureSphere Database Audit and Protection. Solche Anwendungen können den Datenstrom verwenden, um Warnungen zu generieren und Ihre Aurora-DB-Cluster- zu prüfen.

Die folgende Grafik zeigt einen Aurora-DB-Cluster, der mit Amazon Data Firehose konfiguriert ist.



Asynchroner und synchroner Modus für Datenbankaktivitätsstreams

Sie können festlegen, ob Datenbankaktivitätsereignisse in der Datenbanksitzung in einem der folgenden Modi behandelt werden sollen:

- Asynchroner Modus – Wenn eine Datenbanksitzung ein Aktivitätsstream-Ereignis generiert, kehrt die Sitzung sofort zu normalen Aktivitäten zurück. Im Hintergrund wird das Aktivitäts-Stream-Ereignis zu einem dauerhaften Datensatz gemacht. Wenn bei der Aufgabe im Hintergrund ein Fehler auftritt, wird ein RDS-Ereignis gesendet. Dieses Ereignis gibt Anfang und Ende der Zeitfenster an, in denen möglicherweise Datensätze des Aktivitäts-Stream-Ereignisses verloren gegangen sind.

  Der asynchrone Modus beschleunigt die Datenbankleistung, verschlechtert jedoch die Genauigkeit des Aktivitäts-Streams.

  > **Note**
  >
  > Der asynchrone Modus ist sowohl für Aurora PostgreSQL als auch Aurora MySQL verfügbar.

- Synchroner Modus – Wenn eine Datenbanksitzung im synchronen Modus ein Aktivitäts-Stream-Ereignis generiert, blockiert die Sitzung so lange andere Aktivitäten, bis das Ereignis dauerhaft gemacht wird. Falls es aus irgendeinem Grund nicht möglich ist, das Ereignis dauerhaft zu machen, kehrt die Datenbanksitzung zu normalen Aktivitäten zurück. Es wird allerdings ein RDS-

Ereignis gesendet, das darauf hinweist, dass Aktivitäts-Stream-Datensätze möglicherweise für einige Zeit verloren gehen. Wenn sich das System wieder in fehlerfreiem Zustand befindet, wird ein zweites RDS-Ereignis gesendet.

Der synchrone Modus fördert die Genauigkeit des Aktivitäts-Streams, verschlechtert jedoch die Datenbankleistung.

> **Note**
>
> Der synchrone Modus ist für Aurora PostgreSQL verfügbar. Sie können den synchronen Modus nicht mit Aurora MySQL verwenden.

Anforderungen und Einschränkungen für Datenbankaktivitätsstreams

In Aurora gelten für Datenbankaktivitätsstreams die folgenden Anforderungen und Einschränkungen:

- Amazon Kinesis ist für Datenaktivitätsstreams erforderlich.
- AWS Key Management Service (AWS KMS) ist für Datenbankaktivitäts-Streams erforderlich, da sie immer verschlüsselt sind.
- Das Anwenden zusätzlicher Verschlüsselung auf Ihren Amazon Kinesis Data Stream ist nicht mit Datenbankaktivitäts-Streams kompatibel, die bereits mit Ihrem - AWS KMS Schlüssel verschlüsselt sind.
- Starten Sie Ihren DatenbankaktivitätsStream auf DB-Cluster-Ebene. Wenn Sie Ihrem Cluster eine DB-Instance hinzufügen, müssen Sie keinen Aktivitätsstream auf der Instance starten: Sie wird automatisch überwacht.
- In einer globalen Aurora-Datenbank müssen Sie einen Datenbankaktivitäts-Stream separat auf jedem DB-Cluster starten. Jeder Cluster liefert Auditdaten innerhalb seiner eigenen AWS-Region an seinen eigenen Kinesis-Stream.
- Stellen Sie in Aurora PostgreSQL sicher, dass der Datenbank-Aktivitätsstream vor einem Upgrade gestoppt wird. Sie können den Datenbank-Aktivitätsstream starten, nachdem das Upgrade abgeschlossen ist.

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Aurora-Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen zur

Verfügbarkeit von Versionen und Regionen mit Aurora und Datenbank-Aktivitätsstreams finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Datenbankaktivitätsstreams.

Unterstützte DB-Instance-Klassen für Datenbankaktivitätsstreams

Für Aurora MySQL können Sie Datenbankaktivitätsstreams mit den folgenden DB-Instance-Klassen verwenden:

- db.r7g.*large
- db.r6g.*large
- db.r6i.*large
- db.r5.*large
- db.x2g.*

Für Aurora PostgreSQL können Sie Datenbankaktivitätsstreams mit den folgenden DB-Instance-Klassen verwenden:

- db.r7g.*large
- db.r6g.*large
- db.r6i.*large
- db.r6id.*large
- db.r5.*large
- db.r4.*large
- db.x2g.*

Netzwerkvoraussetzungen für Datenbankaktivitäts-Streams bei Aurora MySQL

Im folgenden Abschnitt erfahren Sie, wie Sie Ihre Virtual Private Cloud (VPC) für die Verwendung mit Datenbankaktivitäts-Streams konfigurieren.

> **Note**
>
> Die Netzwerkvoraussetzungen für Aurora MySQL gelten für die folgenden Engine-Versionen:

- Aurora MySQL Version 2, bis zu 2.11.3
- Aurora MySQL versie 2.12.0
- Aurora MySQL Version 3, bis zu 3.04.2

Themen

Voraussetzungen für Endgeräte AWS KMS

Instances in einem Aurora MySQL-Cluster, die Aktivitätsstreams verwenden, müssen auf AWS KMS Endpunkte zugreifen können. Stellen Sie sicher, dass diese Anforderung erfüllt ist, bevor Sie Datenbankaktivitäts-Streams für Ihren Aurora MySQL-Cluster aktivieren. Wenn der Aurora-Cluster öffentlich zugänglich ist, ist diese Anforderung automatisch erfüllt.

Important

Wenn der Aurora MySQL-DB-Cluster nicht auf den AWS KMS Endpunkt zugreifen kann, stoppt der Aktivitätsstream. In diesem Fall werden Sie von Aurora über dieses Problem mithilfe von RDS-Ereignissen benachrichtigt.

Voraussetzungen für die öffentliche Verfügbarkeit

Damit ein Aurora DB-Cluster öffentlich ist, muss es die folgenden Anforderungen erfüllen:

- Öffentlich zugänglich ist auf der AWS Management Console Cluster-Detailseite die Option Ja.
- Der DB-Cluster befindet sich in einem öffentlichen Amazon VPC-Subnetz. Weitere Informationen über öffentlich zugängliche DB-Instances finden Sie unter Arbeiten mit einer DB-Cluster in einer VPC. Weitere Informationen zu öffentlichen Amazon-VPC-Subnetzen finden Sie unter Ihre VPC und Subnetze.

Voraussetzungen für die private Verfügbarkeit

Wenn sich Ihr Aurora-DB-Cluster in einem öffentlichen VPC-Subnetz befindet und nicht öffentlich zugänglich ist, ist er privat. Um Ihren Cluster privat zu halten und ihn mit Datenbankaktivitätsströmen zu verwenden, haben Sie folgende Möglichkeiten:

- Konfigurieren Sie Network Address Translation (NAT) in Ihrer VPC. Weitere Informationen finden Sie unter NAT-Gateways.
- Erstellen Sie einen AWS KMS Endpunkt in Ihrer VPC. Diese Option wird empfohlen, weil sie einfacher zu konfigurieren ist.

So erstellen Sie einen AWS KMS Endpunkt in Ihrer VPC

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Klicken Sie auf Endpunkt erstellen.

   DieErstellen eines Endpunktswird angezeigt.
4. Gehen Sie wie folgt vor:
   - Wählen Sie in der Kategorie Dienste die Option AWS Dienste.
   - Wählen Sie unter Service Name die Option com.amazonaws aus. ***region*** .kms, wobei *Region* der Ort ist, AWS-Region an dem sich Ihr Cluster befindet.
   - Für VPC wählen Sie die VPC, in der sich Ihr Cluster befindet.
5. Klicken Sie auf Endpunkt erstellen.

Weitere Informationen über das Konfigurieren von VPC-Endpunkten finden Sie unter VPC-Endpunkte.

Starten eines Datenbankaktivitäts-Streams

Starten Sie einen Aktivitätsstream auf Clusterebene, um die Datenbankaktivität für alle Instances Ihres Aurora-DB-Clusters zu überwachen,. Alle DB-Instances, die Sie dem Cluster hinzufügen, werden ebenfalls automatisch überwacht. Wenn Sie eine globale Aurora-Datenbank verwenden, starten Sie einen Datenbankaktivitäts-Stream separat auf jedem DB-Cluster. Jeder Cluster liefert Auditdaten innerhalb seiner eigenen AWS-Region an seinen eigenen Kinesis-Stream.

Wenn Sie einen Aktivitätsstream starten, generiert jedes Datenbankaktivitätsereignis, das Sie in der Audit-Richtlinie konfiguriert haben, ein Ereignis im Aktivitätsstream. Zugriffsereignisse werden von SQL-Befehlen wie `CONNECT` und `SELECT` generiert. Änderungsereignisse werden von SQL-Befehlen wie `CREATE` und `INSERT` generiert.

Konsole

Starten eines Datenbankaktivitäts-Streams

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den DB-Cluster, für den/die Sie einen Aktivitätsstream starten möchten.
4. Wählen Sie für Actions (Aktionen) die Option Start activity stream (Aktivitäts-Stream starten) aus.

   Das Fenster Start database activity stream: *name* erscheint, wobei *name* Ihr DB-Cluster ist.
5. Geben Sie die folgenden Einstellungen ein:

   - Für AWS KMS key wählen Sie einen Schlüssel aus der Liste der AWS KMS keys.

     > **Note**
     >
     > Wenn Ihr Aurora-MySQL-Cluster nicht auf KMS-Schlüssel zugreifen kann, folgen Sie den Anweisungen unter Netzwerkvoraussetzungen für Datenbankaktivitäts-Streams bei Aurora MySQL, um diesen Zugriff zunächst zu aktivieren.

     Aurora verwendet den KMS-Schlüssel zur Verschlüsselung des Schlüssels, der wiederum die Datenbankaktivitäten verschlüsselt. Wählen Sie einen anderen KMS-Schlüssel als den Standardschlüssel. Weitere Informationen zu Verschlüsselungsschlüsseln und AWS KMS finden Sie unter Was ist AWS Key Management Service? im AWS Key Management Service-Entwicklerhandbuch.
   - Wählen Sie für Database activity stream mode (Datenbankaktivitäts-Stream-Modus) die Option Asynchronous (Asynchron) oder Synchronous (Synchron) aus.

> **Note**
>
> Diese Auswahl gilt nur für Aurora PostgreSQL. Bei Aurora MySQL können Sie nur den asynchronen Modus verwenden.

- Wählen Sie Sofort aus.

  Wenn Sie Sofort auswählen, wird der DB-Cluster sofort neu gestartet. Wenn Sie Während des nächsten Wartungsfensters auswählen, wird der DB-Cluster nicht sofort neu gestartet. In diesem Fall wird der Datenbankaktivitäts-Stream erst im nächsten Wartungsfenster gestartet.

6. Wählen Sie Start database activity stream (Datenbank-Aktivitätsstream starten) aus.

   Der Status für den DB-Cluster zeigt an, dass der Aktivitätsstream gestartet wird.

> **Note**
>
> Wenn Sie den Fehler `You can't start a database activity stream in this configuration` erhalten, überprüfen Sie Unterstützte DB-Instance-Klassen für Datenbankaktivitätsstreams, um festzustellen, ob Ihr DB-Cluster eine unterstützte Instance-Klasse verwendet.

AWS CLI

Um Datenbankaktivitäts-Streams für einen DB-Clustereine , konfigurieren Sie den DB-Clusterdie mit dem start-activity-stream AWS CLI Befehl .

- `--resource-arn` *`arn`* – Gibt den Amazon-Ressourcennamen (ARN) des DB-Clusters an.
- `--mode` *`sync-or-async`* – Gibt entweder den synchronen (`sync`) oder den asynchronen (`async`) Modus an. Bei Aurora PostgreSQL können Sie einen der beiden Werte wählen. Geben Sie bei Aurora MySQL `async` an.
- `--kms-key-id` *`key`* – Gibt die KMS-Schlüssel-ID für die Verschlüsselung von Nachrichten im Datenbankaktivitäts-Stream an. Der AWS KMS-Schlüsselbezeichner ist der Schlüssel-ARN, die Schlüssel-ID, der Alias-ARN oder der Alias-Name für den AWS KMS key.

Das folgende Beispiel startet einen Datenbankaktivitätsstream für einen DB-Cluster im asynchronen Modus.

Für Linux, macOSoder Unix:

```
aws rds start-activity-stream \
    --mode async \
    --kms-key-id my-kms-key-arn \
    --resource-arn my-cluster-arn \
    --apply-immediately
```

Windows:

```
aws rds start-activity-stream ^
    --mode async ^
    --kms-key-id my-kms-key-arn ^
    --resource-arn my-cluster-arn ^
    --apply-immediately
```

RDS-API

Um Datenbankaktivitäts-Streams für einen DB-Clustereine zu starten, konfigurieren Sie den Cluster mithilfe der -StartActivityStreamOperation.

Rufen Sie die Aktion mit den folgenden Parametern auf:

- `Region`
- `KmsKeyId`
- `ResourceArn`
- `Mode`

Abrufen des Status eines Datenbank-Aktivitätsstreams

Sie können den Status eines Aktivitätsstreams über die Konsole oder AWS CLI abrufen.

Konsole

Abrufen des Status eines Datenbank-Aktivitäts-Streams

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken und dann den Link des DB-Clusters aus.

3. Wählen Sie die Registerkarte Konfiguration aus und prüfen Sie die Statusangabe für Datenbank-Aktivitätsstream.

AWS CLI

Sie können die Aktivitätsstream-Konfiguration für einen DB-Cluster als Antwort auf eine CLI-Anforderung describe-db-clusters abrufen.

Das folgende Beispiel beschreibt *my-cluster*.

```
aws rds --region my-region describe-db-clusters --db-cluster-identifier my-cluster
```

Das folgende Beispiel zeigt eine JSON-Antwort. Die folgenden Felder werden angezeigt:

- `ActivityStreamKinesisStreamName`
- `ActivityStreamKmsKeyId`
- `ActivityStreamStatus`
- `ActivityStreamMode`
-

Diese Felder sind für Aurora PostgreSQL und Aurora MySQL identisch, außer dass `ActivityStreamMode` für Aurora MySQL immer `async` ist, während es für Aurora PostgreSQL `sync` oder `async` sein kann.

```
{
    "DBClusters": [
        {
      "DBClusterIdentifier": "my-cluster",
            ...
            "ActivityStreamKinesisStreamName": "aws-rds-das-cluster-
A6TSYXITZCZXJHIRVFUBZ5LTWY",
            "ActivityStreamStatus": "starting",
            "ActivityStreamKmsKeyId": "12345678-abcd-efgh-ijkl-bd041f170262",
            "ActivityStreamMode": "async",
            "DbClusterResourceId": "cluster-ABCD123456"
            ...
        }
    ]
}
```

RDS-API

Sie können die Aktivitätsstream-Konfiguration für einen DB-Cluster als Antwort auf einen DescribeDBClusters -Vorgang abrufen.

Stoppen eines Datenbankaktivitäts-Streams

Sie können den Status eines Aktivitäts-Streams über die Konsole oder AWS CLI abrufen.

Wenn Sie Ihren DB-Cluster löschen, wird der Aktivitätsstream gestoppt und der zugrunde liegende Amazon-Kinesis-Stream wird automatisch gelöscht.

Konsole

So deaktivieren Sie einen Aktivitäts-Stream:

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie das DB-Cluster aus, für das Sie den Datenbankaktivitäts-Stream stoppen möchten.
4. Wählen Sie für Actions (Aktionen) die Option Stop activity stream (Aktivitäts-Stream stoppen) aus. Das Fenster Database Activity Stream (Datenbankaktivitäts-Stream) wird aufgerufen.

    a. Wählen Sie Sofort aus.

    Wenn Sie Sofort auswählen, wird der DB-Cluster sofort neu gestartet. Wenn Sie Während des nächsten Wartungsfensters auswählen, wird der DB-Cluster nicht sofort neu gestartet. In diesem Fall wird der Datenbankaktivitäts-Stream erst im nächsten Wartungsfenster gestoppt.

    b. Klicken Sie auf Weiter.

AWS CLI

Um Datenbankaktivitäts-Streams für Ihren DB-ClusterIhre, konfigurieren Sie die DB-Cluster mit dem AWS CLI Befehl stop-activity-stream. Bestimmen Sie die AWS-Region für das DB-Cluster mit dem Parameter `--region`. Der Parameter `--apply-immediately` ist optional.

Für Linux, macOSoder Unix:

```
aws rds --region MY_REGION \
    stop-activity-stream \
```

```
    --resource-arn MY_CLUSTER_ARN \
    --apply-immediately
```

Windows:

```
aws rds --region MY_REGION ^
    stop-activity-stream ^
    --resource-arn MY_CLUSTER_ARN ^
    --apply-immediately
```

RDS-API

Um Datenbankaktivitäts-Streams für Ihren DB-Cluster , konfigurieren Sie die Cluster mithilfe der -StopActivityStreamOperation. Bestimmen Sie die AWS-Region für das DB-Cluster mit dem Parameter `Region`. Der Parameter `ApplyImmediately` ist optional.

Überwachen von Datenbankaktivitäts-Streams

Datenbankaktivitäts-Streams überwachen und melden Aktivitäten. Der Aktivitäts-Stream wird erfasst und an Amazon Kinesis übertragen. Von Kinesis aus können Sie den Aktivitäts-Stream überwachen, oder andere Dienste und Anwendungen können den Aktivitäts-Stream zur weiteren Analyse nutzen. Sie können den zugrunde liegenden Kinesis-Stream-Namen mithilfe des - AWS CLI Befehls `describe-db-clusters` oder der RDS-API-`DescribeDBClusters`Operation finden.

Aurora verwaltet den Kinesis Stream wie folgt:

- Aurora erzeugt den Kinesis Stream automatisch mit einem Aufbewahrungszeitraum von 24 Stunden.
- Aurora skaliert den Kinesis-Stream bei Bedarf.
- Wenn Sie den Datenbankaktivitäts-Stream stoppen oder den DB-Cluster löschen, löscht Aurora den Kinesis-Stream.

Die folgenden Kategorien von Aktivitäten werden überwacht und in das Prüfprotokoll des Aktivitäts-Streams aufgenommen:

- SQL-Befehle – Alle SQL-Befehle werden geprüft, ebenso vorbereitete Anweisungen, integrierte Funktionen und Funktionen in PL/SQL. Aufrufe von gespeicherten Prozeduren werden überprüft. Alle SQL-Anweisungen, die in gespeicherten Prozeduren oder Funktionen ausgegeben werden, werden ebenfalls überprüft.

- Sonstige Datenbankinformationen – Die überwachte Aktivität umfasst die vollständige SQL-Anweisung, die Zeilenzahl der betroffenen Zeilen aus DML-Befehlen, Objekte, auf die zugegriffen wurde, und den eindeutigen Datenbanknamen. Für Aurora PostgreSQL überwachen Datenbankaktivitäts-Streams auch die Bindevariablen und die Parameter der gespeicherten Prozedur.

  > **Important**
  >
  > Der vollständige SQL-Text jeder Anweisung ist im Prüfprotokoll des Aktivitäts-Streams sichtbar, inklusive aller sensiblen Daten. Datenbankbenutzerkennwörter werden jedoch redigiert, wenn Aurora sie wie in der folgenden SQL-Anweisung aus dem Kontext ermitteln kann.
  >
  > ```
  > ALTER ROLE role-name WITH password
  > ```

- Verbindungsinformationen – Die überwachte Aktivität umfasst Sitzungs- und Netzwerkinformationen, die Server-Prozess-ID und Beendigungscodes.

Wenn ein Aktivitätsstream während der Überwachung Ihrer DB-Instance fehlschlägt, werden Sie über RDS-Ereignisse benachrichtigt.

Themen

- Zugriff auf einen Aktivitäts-Stream von Kinesis aus
- Prüfungsprotokoll – Inhalte und Beispiele
- databaseActivityEventJSON-Array auflisten
- Verarbeiten eines Datenbankaktivitäts-Streams mit dem AWS SDK

Zugriff auf einen Aktivitäts-Stream von Kinesis aus

Wenn Sie einen Aktivitäts-Stream für einen DB-Cluster aktivieren, wird ein Kinesis-Stream für Sie erstellt. Von Kinesis aus können Sie die Datenbankaktivität in Echtzeit überwachen. Zur weiteren Analyse der Datenbankaktivität können Sie Ihren Kinesis-Stream mit Consumer-Anwendungen verbinden. Sie können den Stream auch mit Compliance-Management-Anwendungen wie IBM Security Guardium oder Imperva SecureSphere Database Audit and Protection verbinden.

Sie können entweder über die RDS- oder Kinesis-Konsole auf Ihren Kinesis-Stream zugreifen.

So greifen Sie über die RDS-Konsole auf einen Aktivitätsstream zu

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den/die DB-Cluster aus, auf der Sie einen Aktivitätsstream gestartet haben.
4. Wählen Sie Konfiguration.
5. Wählen Sie unter Database activity stream (Datenbank-Aktivitätsstream) den Link unter Kinesis stream (Kinesis-Stream) aus.
6. Wählen Sie in der Kinesis-Konsole Monitoring (Überwachung) aus, um mit der Überwachung der Datenbankaktivität zu beginnen.

So greifen Sie über die Kinesis-Konsole auf einen Aktivitätsstream von Kinesis zu

1. Öffnen Sie die Kinesis-Konsole unter.https://console.aws.amazon.com/kinesis.
2. Wählen Sie Ihren Aktivitäts-Stream aus der Liste der Kinesis-Streams aus.

   Der Name eines Aktivitäts-Streams besteht aus dem Präfix `aws-rds-das-cluster-` gefolgt von der Ressourcen-ID des DB-Clusters. Im Folgenden wird ein Beispiel gezeigt.

   ```
   aws-rds-das-cluster-NHVOV4PCLWHGF52NP
   ```

   Um die Amazon-RDS-Konsole zum Ermitteln der Ressourcen-ID für den DB-Cluster zu verwenden, wählen Sie Ihren DB-Cluster aus der Liste der Datenbanken aus und wählen dann die Registerkarte Konfiguration aus.

   Um den vollständigen Kinesis-Stream-Namen für einen Aktivitäts-Stream mit AWS CLI der zu finden, verwenden Sie eine describe-db-clusters CLI-Anfrage und notieren Sie sich den Wert von `ActivityStreamKinesisStreamName` in der Antwort.
3. Wählen Sie Monitoring (Überwachung) aus, um mit der Überwachung der Datenbankaktivität zu beginnen.

Weitere Informationen zur Verwendung von Amazon Kinesis finden Sie unter Was sind Amazon Kinesis Data Streams?.

Prüfungsprotokoll – Inhalte und Beispiele

Überwachte Ereignisse werden im Datenbankaktivitätsstream als JSON-Zeichenfolgen dargestellt. Die Struktur besteht aus einem JSON-Objekt mit einem `DatabaseActivityMonitoringRecord`, der wiederum ein Array von Aktivitätsereignissen `databaseActivityEventList` enthält.

Themen

Prüfungsprotokollbeispiele für Aktivitäts-Streams

Im Folgenden sehen Sie Beispiele für entschlüsselte JSON-Prüfprotokolle von Aktivitätsereignisdatensätzen.

Example Aktivitätsereignisdatensatz einer Aurora-PostgreSQL-CONNECT SQL-Anweisung

Im Folgenden sehen Sie einen Aktivitätsereignisdatensatz einer Anmeldung unter Verwendung einer `CONNECT`-SQL-Anweisung (`command`) durch einen psql-Client (`clientApplication`).


```
{
  "type":"DatabaseActivityMonitoringRecords",
  "version":"1.1",
  "databaseActivityEvents":
    {
      "type":"DatabaseActivityMonitoringRecord",
      "clusterId":"cluster-4HNY5V4RRNPKKYB7ICFKE5JBQQ",
      "instanceId":"db-FZJTMYKCXQBUUZ6VLU7NW3ITCM",
      "databaseActivityEventList":[
        {
          "startTime": "2019-10-30 00:39:49.940668+00",
          "logTime": "2019-10-30 00:39:49.990579+00",
          "statementId": 1,
          "substatementId": 1,
          "objectType": null,
          "command": "CONNECT",
          "objectName": null,
          "databaseName": "postgres",
          "dbUserName": "rdsadmin",
          "remoteHost": "172.31.3.195",
```

```
          "remotePort": "49804",
          "sessionId": "5ce5f7f0.474b",
          "rowCount": null,
          "commandText": null,
          "paramList": [],
          "pid": 18251,
          "clientApplication": "psql",
          "exitCode": null,
          "class": "MISC",
          "serverVersion": "2.3.1",
          "serverType": "PostgreSQL",
          "serviceName": "Amazon Aurora PostgreSQL-Compatible edition",
          "serverHost": "172.31.3.192",
          "netProtocol": "TCP",
          "dbProtocol": "Postgres 3.0",
          "type": "record",
          "errorMessage": null
        }
      ]
    },
   "key":"decryption-key"
}
```

Example Aktivitätsereignisdatensatz einer Aurora MySQL-CONNECT SQL-Anweisung

Im Folgenden sehen Sie einen Aktivitätsereignisdatensatz einer Anmeldung unter Verwendung einer CONNECT-SQL-Anweisung (`command`) durch einen mysql-Client (`clientApplication`).

```
{
  "type":"DatabaseActivityMonitoringRecord",
  "clusterId":"cluster-some_id",
  "instanceId":"db-some_id",
  "databaseActivityEventList":[
    {
      "logTime":"2020-05-22 18:07:13.267214+00",
      "type":"record",
      "clientApplication":null,
      "pid":2830,
      "dbUserName":"rdsadmin",
      "databaseName":"",
      "remoteHost":"localhost",
      "remotePort":"11053",
      "command":"CONNECT",
```

```
      "commandText":"",
      "paramList":null,
      "objectType":"TABLE",
      "objectName":"",
      "statementId":0,
      "substatementId":1,
      "exitCode":"0",
      "sessionId":"725121",
      "rowCount":0,
      "serverHost":"master",
      "serverType":"MySQL",
      "serviceName":"Amazon Aurora MySQL",
      "serverVersion":"MySQL 5.7.12",
      "startTime":"2020-05-22 18:07:13.267207+00",
      "endTime":"2020-05-22 18:07:13.267213+00",
      "transactionId":"0",
      "dbProtocol":"MySQL",
      "netProtocol":"TCP",
      "errorMessage":"",
      "class":"MAIN"
    }
  ]
}
```

Example Aktivitätsereignisdatensatz einer Aurora PostgreSQL CREATE TABLE-Anweisung

Im Folgenden sehen Sie ein Beispiel eines `CREATE TABLE`-Ereignisses für Aurora PostgreSQL.

```
{
  "type":"DatabaseActivityMonitoringRecords",
  "version":"1.1",
  "databaseActivityEvents":
    {
      "type":"DatabaseActivityMonitoringRecord",
      "clusterId":"cluster-4HNY5V4RRNPKKYB7ICFKE5JBQQ",
      "instanceId":"db-FZJTMYKCXQBUUZ6VLU7NW3ITCM",
      "databaseActivityEventList":[
        {
          "startTime": "2019-05-24 00:36:54.403455+00",
          "logTime": "2019-05-24 00:36:54.494235+00",
          "statementId": 2,
          "substatementId": 1,
          "objectType": null,
          "command": "CREATE TABLE",
```

```
          "objectName": null,
          "databaseName": "postgres",
          "dbUserName": "rdsadmin",
          "remoteHost": "172.31.3.195",
          "remotePort": "34534",
          "sessionId": "5ce73c6f.7e64",
          "rowCount": null,
          "commandText": "create table my_table (id serial primary key, name
 varchar(32));",
          "paramList": [],
          "pid": 32356,
          "clientApplication": "psql",
          "exitCode": null,
          "class": "DDL",
          "serverVersion": "2.3.1",
          "serverType": "PostgreSQL",
          "serviceName": "Amazon Aurora PostgreSQL-Compatible edition",
          "serverHost": "172.31.3.192",
          "netProtocol": "TCP",
          "dbProtocol": "Postgres 3.0",
          "type": "record",
          "errorMessage": null
        }
      ]
    },
   "key":"decryption-key"
}
```

Example Aktivitätsereignisdatensatz einer Aurora-MySQL-CREATE TABLE-Anweisung

Das folgende Beispiel zeigt eine `CREATE TABLE`-Anweisung für Aurora MySQL. Die Operation wird als zwei separate Ereignisdatensätze dargestellt. Das eine Ereignis verfügt über einen Wert `"class":"MAIN"`. Das andere über einen Wert `"class":"AUX"`. Die Nachrichten können in beliebiger Reihenfolge eintreffen. Das `logTime`-Feld des `MAIN`-Ereignisses ist immer früher als die `logTime`-Felder der entsprechenden `AUX`-Ereignisse.

Im folgenden Beispiel wird das Ereignis mit einem `class`-Wert von `MAIN` gezeigt.

```
{
  "type":"DatabaseActivityMonitoringRecord",
  "clusterId":"cluster-some_id",
  "instanceId":"db-some_id",
  "databaseActivityEventList":[
```

```
    {
      "logTime":"2020-05-22 18:07:12.250221+00",
      "type":"record",
      "clientApplication":null,
      "pid":2830,
      "dbUserName":"master",
      "databaseName":"test",
      "remoteHost":"localhost",
      "remotePort":"11054",
      "command":"QUERY",
      "commandText":"CREATE TABLE test1 (id INT)",
      "paramList":null,
      "objectType":"TABLE",
      "objectName":"test1",
      "statementId":65459278,
      "substatementId":1,
      "exitCode":"0",
      "sessionId":"725118",
      "rowCount":0,
      "serverHost":"master",
      "serverType":"MySQL",
      "serviceName":"Amazon Aurora MySQL",
      "serverVersion":"MySQL 5.7.12",
      "startTime":"2020-05-22 18:07:12.226384+00",
      "endTime":"2020-05-22 18:07:12.250222+00",
      "transactionId":"0",
      "dbProtocol":"MySQL",
      "netProtocol":"TCP",
      "errorMessage":"",
      "class":"MAIN"
    }
  ]
}
```

Im folgenden Beispiel wird das entsprechende Ereignis mit einem `class`-Wert von AUX gezeigt.

```
{
  "type":"DatabaseActivityMonitoringRecord",
  "clusterId":"cluster-some_id",
  "instanceId":"db-some_id",
  "databaseActivityEventList":[
    {
      "logTime":"2020-05-22 18:07:12.247182+00",
```

```
      "type":"record",
      "clientApplication":null,
      "pid":2830,
      "dbUserName":"master",
      "databaseName":"test",
      "remoteHost":"localhost",
      "remotePort":"11054",
      "command":"CREATE",
      "commandText":"test1",
      "paramList":null,
      "objectType":"TABLE",
      "objectName":"test1",
      "statementId":65459278,
      "substatementId":2,
      "exitCode":"",
      "sessionId":"725118",
      "rowCount":0,
      "serverHost":"master",
      "serverType":"MySQL",
      "serviceName":"Amazon Aurora MySQL",
      "serverVersion":"MySQL 5.7.12",
      "startTime":"2020-05-22 18:07:12.226384+00",
      "endTime":"2020-05-22 18:07:12.247182+00",
      "transactionId":"0",
      "dbProtocol":"MySQL",
      "netProtocol":"TCP",
      "errorMessage":"",
      "class":"AUX"
    }
  ]
}
```

Example Aktivitätsereignisdatensatz einer Aurora PostgreSQL SELECT-Anweisung

Das folgende Beispiel zeigt ein SELECT-Ereignis .

```
{
  "type":"DatabaseActivityMonitoringRecords",
  "version":"1.1",
  "databaseActivityEvents":
    {
      "type":"DatabaseActivityMonitoringRecord",
      "clusterId":"cluster-4HNY5V4RRNPKKYB7ICFKE5JBQQ",
      "instanceId":"db-FZJTMYKCXQBUUZ6VLU7NW3ITCM",
```

```
      "databaseActivityEventList":[
        {
          "startTime": "2019-05-24 00:39:49.920564+00",
          "logTime": "2019-05-24 00:39:49.940668+00",
          "statementId": 6,
          "substatementId": 1,
          "objectType": "TABLE",
          "command": "SELECT",
          "objectName": "public.my_table",
          "databaseName": "postgres",
          "dbUserName": "rdsadmin",
          "remoteHost": "172.31.3.195",
          "remotePort": "34534",
          "sessionId": "5ce73c6f.7e64",
          "rowCount": 10,
          "commandText": "select * from my_table;",
          "paramList": [],
          "pid": 32356,
          "clientApplication": "psql",
          "exitCode": null,
          "class": "READ",
          "serverVersion": "2.3.1",
          "serverType": "PostgreSQL",
          "serviceName": "Amazon Aurora PostgreSQL-Compatible edition",
          "serverHost": "172.31.3.192",
          "netProtocol": "TCP",
          "dbProtocol": "Postgres 3.0",
          "type": "record",
          "errorMessage": null
        }
      ]
    },
   "key":"decryption-key"
}
```

```
{
    "type": "DatabaseActivityMonitoringRecord",
    "clusterId": "",
    "instanceId": "db-4JCWQLUZVFYP7DIWP6JVQ77O3Q",
    "databaseActivityEventList": [
        {
            "class": "TABLE",
            "clientApplication": "Microsoft SQL Server Management Studio - Query",
```

```
            "command": "SELECT",
            "commandText": "select * from [testDB].[dbo].[TestTable]",
            "databaseName": "testDB",
            "dbProtocol": "SQLSERVER",
            "dbUserName": "test",
            "endTime": null,
            "errorMessage": null,
            "exitCode": 1,
            "logTime": "2022-10-06 21:24:59.9422268+00",
            "netProtocol": null,
            "objectName": "TestTable",
            "objectType": "TABLE",
            "paramList": null,
            "pid": null,
            "remoteHost": "local machine",
            "remotePort": null,
            "rowCount": 0,
            "serverHost": "172.31.30.159",
            "serverType": "SQLSERVER",
            "serverVersion": "15.00.4073.23.v1.R1",
            "serviceName": "sqlserver-ee",
            "sessionId": 62,
            "startTime": null,
            "statementId": "0x03baed90412f564fad640ebe51f89b99",
            "substatementId": 1,
            "transactionId": "4532935",
            "type": "record",
            "engineNativeAuditFields": {
                "target_database_principal_id": 0,
                "target_server_principal_id": 0,
                "target_database_principal_name": "",
                "server_principal_id": 2,
                "user_defined_information": "",
                "response_rows": 0,
                "database_principal_name": "dbo",
                "target_server_principal_name": "",
                "schema_name": "dbo",
                "is_column_permission": true,
                "object_id": 581577110,
                "server_instance_name": "EC2AMAZ-NFUJJNO",
                "target_server_principal_sid": null,
                "additional_information": "",
                "duration_milliseconds": 0,
                "permission_bitmask": "0x00000000000000000000000000000001",
```

```
                "data_sensitivity_information": "",
                "session_server_principal_name": "test",
                "connection_id": "AD3A5084-FB83-45C1-8334-E923459A8109",
                "audit_schema_version": 1,
                "database_principal_id": 1,
                "server_principal_sid":
 "0x0105000000000005150000000bdc2795e2d0717901ba6998cf4010000",
                "user_defined_event_id": 0,
                "host_name": "EC2AMAZ-NFUJJNO"
            }
        }
    ]
}
```

Example Aktivitätsereignisdatensatz einer Aurora MySQL-SELECT-Anweisung

Das folgende Beispiel zeigt ein `SELECT`-Ereignis.

Im folgenden Beispiel wird das Ereignis mit einem `class`-Wert von `MAIN` gezeigt.

```
{
  "type":"DatabaseActivityMonitoringRecord",
  "clusterId":"cluster-some_id",
  "instanceId":"db-some_id",
  "databaseActivityEventList":[
    {
      "logTime":"2020-05-22 18:29:57.986467+00",
      "type":"record",
      "clientApplication":null,
      "pid":2830,
      "dbUserName":"master",
      "databaseName":"test",
      "remoteHost":"localhost",
      "remotePort":"11054",
      "command":"QUERY",
      "commandText":"SELECT * FROM test1 WHERE id < 28",
      "paramList":null,
      "objectType":"TABLE",
      "objectName":"test1",
      "statementId":65469218,
      "substatementId":1,
      "exitCode":"0",
      "sessionId":"726571",
      "rowCount":2,
```

```
      "serverHost":"master",
      "serverType":"MySQL",
      "serviceName":"Amazon Aurora MySQL",
      "serverVersion":"MySQL 5.7.12",
      "startTime":"2020-05-22 18:29:57.986364+00",
      "endTime":"2020-05-22 18:29:57.986467+00",
      "transactionId":"0",
      "dbProtocol":"MySQL",
      "netProtocol":"TCP",
      "errorMessage":"",
      "class":"MAIN"
    }
  ]
}
```

Im folgenden Beispiel wird das entsprechende Ereignis mit einem `class`-Wert von AUX gezeigt.

```
{
  "type":"DatabaseActivityMonitoringRecord",
  "instanceId":"db-some_id",
  "databaseActivityEventList":[
    {
      "logTime":"2020-05-22 18:29:57.986399+00",
      "type":"record",
      "clientApplication":null,
      "pid":2830,
      "dbUserName":"master",
      "databaseName":"test",
      "remoteHost":"localhost",
      "remotePort":"11054",
      "command":"READ",
      "commandText":"test1",
      "paramList":null,
      "objectType":"TABLE",
      "objectName":"test1",
      "statementId":65469218,
      "substatementId":2,
      "exitCode":"",
      "sessionId":"726571",
      "rowCount":0,
      "serverHost":"master",
      "serverType":"MySQL",
      "serviceName":"Amazon Aurora MySQL",
```

```
      "serverVersion":"MySQL 5.7.12",
      "startTime":"2020-05-22 18:29:57.986364+00",
      "endTime":"2020-05-22 18:29:57.986399+00",
      "transactionId":"0",
      "dbProtocol":"MySQL",
      "netProtocol":"TCP",
      "errorMessage":"",
      "class":"AUX"
    }
  ]
}
```

DatabaseActivityMonitoringRecords JSON-Objekt

Die Datenbank-Aktivitätsereignisdatensätze befinden sich in einem JSON-Objekt, das die folgenden Informationen enthält.

JSON-Feld	Datentyp	Beschreibung
`type`	string	Der Typ des JSON-Datensatzes. Der Wert ist `DatabaseActivityMonitoringRecords` .
`version`	string	Die Version der Datenbank-Aktivitätsüberwachungsdatensätze. Die Version der generierten Datenbank-Aktivitätsdatensätze hängt von der Engine-Version des DB-Clusters ab: • Datenbank-Aktivitätsdatensätze der Version 1.1 werden für Aurora PostgreSQL-DB-Cluster generiert, auf denen die Engine-Versionen 10.10 und höhere Nebenversionen sowie die Engine-Versionen 11.5 und höher ausgeführt werden. • Datenbank-Aktivitätsdatensätze der Version 1.0 werden für Aurora PostgreSQL-DB-Cluster generiert, auf denen

JSON-Feld	Datentyp	Beschreibung
		die Engine-Versionen 10.7 und 11.4 ausgeführt werden. Alle folgenden Felder befinden sich sowohl in Version 1.0 als auch in Version 1.1, sofern nicht ausdrücklich angegeben.
databaseActivityEvents	Zeichenfolge	Ein JSON-Objekt, das die Aktivitätsereignisse enthält.
Schlüssel	Zeichenfolge	Ein Verschlüsselungsschlüssel, den Sie zum Entschlüsseln des databaseActivityEventListe verwenden

databaseActivityEvents JSON-Objekt

Das `databaseActivityEvents`-JSON-Objekt enthält die folgenden Informationen.

Felder der obersten Ebene im JSON-Datensatz

Jedes Ereignis im Prüfprotokoll wird in einen Datensatz im JSON-Format verpackt. Dieser Datensatz enthält die folgenden Felder.

type

Dieses Feld hat immer den Wert `DatabaseActivityMonitoringRecords`.

Version

Dieses Feld stellt die Version des Datenprotokolls oder des Vertrags für die Datenbankaktivität dar. Es definiert, welche Felder verfügbar sind.

Version 1.0 stellt die Unterstützung der ursprünglichen Datenaktivitäts-Streams für die Aurora PostgreSQL-Versionen 10.7 und 11.4 dar. Version 1.1 stellt die Unterstützung der Datenaktivitäts-Streams für die Aurora PostgreSQL-Versionen ab 10.10 und ab Aurora PostgreSQL-Version 11.5 dar. Version 1.1 enthält die zusätzlichen Felder `errorMessage` und `startTime`. Version 1.2 stellt die Unterstützung der Datenaktivitäts-Streams für Aurora MySQL 2.08 und höher dar. Version 1.2 enthält die zusätzlichen Felder `endTime` und `transactionId`.

databaseActivityEvents

Eine verschlüsselte Zeichenfolge, die ein oder mehrere Aktivitätsereignisse darstellt. Sie wird als Base64-Byte-Array dargestellt. Wenn Sie die Zeichenfolge entschlüsseln, ist das Ergebnis ein Datensatz im JSON-Format mit Feldern, wie in den Beispielen in diesem Abschnitt gezeigt.

Schlüssel

Der verschlüsselte Datenschlüssel, der zum Verschlüsseln der `databaseActivityEvents`-Zeichenfolge verwendet wird. Dies ist dieselbe AWS KMS key , die Sie beim Starten des Datenbankaktivitäts-Streams angegeben haben.

Im folgenden Beispiel wird das Format dieses Datensatzes gezeigt.

```
{
  "type":"DatabaseActivityMonitoringRecords",
  "version":"1.1",
  "databaseActivityEvents":"encrypted audit records",
  "key":"encrypted key"
}
```

Führen Sie die folgenden Schritte aus, um den Inhalt des `databaseActivityEvents`-Feldes zu entschlüsseln:

1. Entschlüsseln Sie den Wert im JSON-Feld `key` mit dem KMS-Schlüssel, den Sie beim Starten des Datenbankaktivitätsstroms angegeben haben. Dadurch wird der Datenverschlüsselungsschlüssel im Klartext zurückgegeben.
2. Base64-dekodieren Sie den Wert im `databaseActivityEvents`-JSON-Feld, um den Verschlüsselungstext der Prüfungsnutzlast im Binärformat zu erhalten.
3. Entschlüsseln Sie den binären Verschlüsselungstext mit dem Datenverschlüsselungsschlüssel, den Sie im ersten Schritt dekodiert haben.
4. Dekomprimieren Sie die entschlüsselte Nutzlast.
   - Die verschlüsselte Nutzlast befindet sich im `databaseActivityEvents`-Feld.
   - Das `databaseActivityEventList`-Feld enthält ein Array von Prüfdatensätzen. Die `type`-Felder im Array können `record` oder sein `heartbeat`.

Der Prüfprotokoll-Aktivitätsereignisdatensatz ist ein JSON-Objekt mit folgenden Informationen.

JSON-Feld	Datentyp	Beschreibung
`type`	string	Der Typ des JSON-Datensatzes. Der Wert ist `DatabaseActivityMonitoringRecord` .
`clusterId`	string	Die Ressourcen-ID des DB-Clusters. Sie entspricht dem DB-Clusterattribut `DbClusterResourceId` .
`instanceId`	string	Die Ressourcen-ID der DB-Instance. Sie dem DB-Instance-Attribut `DbiResourceId` .
databaseActivityEventListe	string	Ein Array von Aktivitätsprüfdatensätzen oder Heartbeat-Nachrichten.

databaseActivityEventJSON-Array auflisten

Die Prüfprotokollnutzlast ist ein verschlüsseltes JSON-Array `databaseActivityEventList`. In der folgenden Tabelle sind die Felder für jedes Aktivitätsereignis im entschlüsselten Array `DatabaseActivityEventList` eines Prüfprotokolls alphabetisch aufgelistet. Die Felder unterscheiden sich je nachdem, ob Sie Aurora PostgreSQL oder Aurora MySQL verwenden. Näheres entnehmen Sie bitte der Tabelle, die für Ihre Datenbank-Engine gilt.

> **Important**
>
> Die Ereignisstruktur kann sich ändern. Aurora könnte in Zukunft neue Felder zu Aktivitätsereignissen hinzufügen. Stellen Sie bei Anwendungen, welche die JSON-Daten analysieren, sicher, dass Ihr Code unbekannte Feldnamen ignorieren oder entsprechende Aktionen durchführen kann.

databaseActivityEventAuflisten von Feldern für Aurora PostgreSQL

Feld	Datentyp	Beschreibung
`class`	string	Die Aktivitätsereignisklasse. Gültige Werte für Aurora PostgreSQL sind die folgenden: • `ALL`

Feld	Datentyp	Beschreibung
		• CONNECT – Ein Verbindungs- oder Verbindungstrennungsereignis. • DDL – eine DDL-Anweisung, die nicht in der Liste der Anweisungen für die Klasse ROLE enthalten ist. • FUNCTION – ein Funktionsaufruf oder ein DO-Block. • MISC – ein sonstiger Befehl wie z. B. DISCARD, FETCH, CHECKPOINT oder VACUUM. • NONE • READ – eine Anweisung SELECT oder COPY, wenn es sich bei der Quelle um eine Relation oder Abfrage handelt. • ROLE – eine Anweisung in Zusammenhang mit Rollen und Berechtigungen wie z. B. GRANT, REVOKE und CREATE/ALTER/DROP ROLE. • WRITE – eine Anweisung INSERT, UPDATE, DELETE, TRUNCATE, oder COPY, wenn das Ziel eine Relation ist.
clientApplication	string	Die Anwendung, die der Client laut Meldung für die Verbindung verwendet hat. Der Client muss diese Informationen nicht angeben, der Wert kann daher Null sein.
command	string	Der Name des SQL-Befehls ohne Befehlsdetails.

Feld	Datentyp	Beschreibung
`commandText`	string	Die vom Benutzer übergebene eigentliche SQL-Anweisung. Bei Aurora PostgreSQL ist der Wert identisch mit der ursprünglichen SQL-Anweisung. Dieses Feld wird für alle Arten von Datensätzen verwendet, mit Ausnahme von Verbindungs- oder Verbindungstrennungsdatensätzen, bei denen der Wert Null ist. **Important** Der vollständige SQL-Text jeder Anweisung ist im Prüfprotokoll des Aktivitäts-Streams sichtbar, inklusive aller sensiblen Daten. Datenbankbenutzerkennwörter werden jedoch redigiert, wenn Aurora sie wie in der folgenden SQL-Anweisung aus dem Kontext ermitteln kann. `ALTER ROLE role-name WITH password`
`databaseName`	string	Die Datenbank, zu der der Benutzer eine Verbindung hergestellt hat.
`dbProtocol`	string	Das Datenbankprotokoll, z. B. `Postgres 3.0`.
`dbUserName`	string	Der Datenbankbenutzer, mit dem sich der Client authentifiziert hat.

Feld	Datentyp	Beschreibung
`errorMessage` (nur Datenbank-Aktivitätsdatensätze der Version 1.1)	string	Wenn ein Fehler aufgetreten ist, wird dieses Feld mit der Fehlermeldung gefüllt, die vom DB-Server generiert worden wäre. Der `errorMessage` -Wert ist null für normale Anweisungen, die nicht zu einem Fehler geführt haben. Ein Fehler wird als jede Aktivität definiert, die ein vom Client sichtbares PostgreSQL-Fehlerprotokollereignis mit einem Schweregrad von `ERROR` oder höher erzeugen würde. Weitere Informationen finden Sie unter PostgreSQL-Nachrichtenschweregrade. Beispielsweise erzeugen Syntaxfehler und Abfrageabbrüche eine Fehlermeldung. Interne PostgreSQL-Serverfehler wie Hintergrund-Checkpointer-Prozessfehler erzeugen keine Fehlermeldung. Datensätze für solche Ereignisse werden jedoch weiterhin ausgegeben, unabhängig von der Einstellung des Schweregrads des Protokolls. Dadurch wird verhindert, dass Angreifer die Protokollierung deaktivieren, um eine Erkennung zu vermeiden. Siehe auch das Feld `exitCode`.
`exitCode`	int	Ein Wert, der für einen Sitzungsbeendigungs-Datensatz verwendet wird. Bei einer sauberen Beendigung ist hier der Beendigungscode enthalten. In manchen Fehlersituationen kann nicht immer ein Beendigungscode erhalten werden. Beispiele: `exit()` von PostgreSQL oder Ausführung eines Befehls wie `kill -9` durch einen Operator. Wenn ein Fehler aufgetreten ist, zeigt das `exitCode`-Feld den SQL-Fehlercode `SQLSTATE` an, wie in PostgreSQL-Fehlercodes aufgeführt. Siehe auch das Feld `errorMessage` .

Feld	Datentyp	Beschreibung
`logTime`	string	Ein Zeitstempel wie im Prüfcodepfad aufgezeichnet. Dies stellt die Endzeit der SQL-Anweisungsausführung dar. Siehe auch das Feld `startTime` .
`netProtocol`	string	Das Netzwerkkommunikationsprotokoll.
`objectName`	string	Der Name des Datenbankobjekts, wenn die SQL-Anweisung für eines ausgeführt wird. Dieses Feld wird nur verwendet, wenn die SQL-Anweisung für ein Datenbankobjekt ausgeführt wird. Falls die SQL-Anweisung nicht für ein Objekt ausgeführt wird, lautet dieser Wert Null.
`objectType`	string	Der Datenbankobjekttyp wie z. B. Tabelle, Index, Ansicht usw. Dieses Feld wird nur verwendet, wenn die SQL-Anweisung für ein Datenbankobjekt ausgeführt wird. Falls die SQL-Anweisung nicht für ein Objekt ausgeführt wird, lautet dieser Wert Null. Gültige Werte sind unter anderem: • `COMPOSITE TYPE` • `FOREIGN TABLE` • `FUNCTION` • `INDEX` • `MATERIALIZED VIEW` • `SEQUENCE` • `TABLE` • `TOAST TABLE` • `VIEW` • `UNKNOWN`
`paramList`	string	Ein Array durch Kommas getrennter Parameter, die an die SQL-Anweisung übergeben werden. Wenn die SQL-Anweisung keine Parameter beinhaltet, ist dieser Wert ein leeres Array.

Feld	Datentyp	Beschreibung
`pid`	int	Die Prozess-ID des Back-End-Prozesses, der für die Client-Verbindung zugewiesen wird.
`remoteHost`	string	Entweder die Client-IP-Adresse oder der Hostname. Was davon verwendet wird, ist bei Aurora PostgreSQL von der Parametereinstellung `log_hostname` der Datenbank abhängig.
`remotePort`	string	Die Portnummer des Clients.
`rowCount`	int	Die Anzahl der Zeilen, die von der SQL-Anweisung zurückgegeben werden. Wenn eine SELECT-Anweisung beispielsweise 10 Zeilen zurückgibt, beträgt rowCount 10. Für INSERT- oder UPDATE-Anweisungen ist der RowCount 0.
`serverHost`	string	Die Host-IP-Adresse des Datenbankservers.
`serverType`	string	Der Datenbankservertyp, z. B `PostgreSQL` .
`serverVersion`	string	Die Datenbankserver-Version, z. B. `2.3.1` für Aurora PostgreSQL.
`serviceName`	string	Der Name des Service, beispielsweise `Amazon Aurora PostgreSQL-Compatible edition` .
`sessionId`	int	Eine pseudoeindeutige Sitzungskennung.
`sessionId`	int	Eine pseudoeindeutige Sitzungskennung.
`startTime` (nur Datenbank-Aktivitätsdatensätze der Version 1.1)	string	Die Zeit, zu der die Ausführung für die SQL-Anweisung begann. Um die ungefähre Ausführungszeit der SQL-Anweisung zu berechnen, verwenden Sie `logTime - startTime` . Siehe auch das Feld `logTime`.

Feld	Datentyp	Beschreibung
`statementId`	int	Eine ID für die SQL-Anweisung des Clients. Dieser Zähler auf Sitzungsebene erhöht sich mit jeder vom Client eingegebenen SQL-Anweisung.
`substatementId`	int	Eine ID für eine SQL-Unteranweisung. Dieser Wert zählt die enthaltenen Unteranweisungen für jede über das Feld `statementId` angegebene SQL-Anweisung.
`type`	string	Der Ereignistyp. Gültige Werte sind `record` oder `heartbeat` .

databaseActivityEventAuflisten von Feldern für Aurora MySQL

Feld	Datentyp	Beschreibung
`class`	string	Die Aktivitätsereignisklasse. Gültige Werte für Aurora MySQL sind die folgenden: • `MAIN` – das primäre Ereignis, das eine SQL-Anweisung darstellt. • `AUX` – ein zusätzliches Ereignis, das zusätzliche Details enthält. Beispielsweise kann eine Anweisung, mit der ein Objekt umbenannt wird, ein Ereignis der Klasse `AUX` aufweisen, das den neuen Namen wiedergibt. Um `MAIN`- und `AUX`-Ereignisse zu finden, die derselben Anweisung entsprechen, suchen Sie nach verschiedenen Ereignissen, die dieselben Werte für das Feld `pid` und für das Feld `statementId` aufweisen.
`clientApplication`	string	Die Anwendung, die der Client laut Meldung für die Verbindung verwendet hat. Der Client muss diese Informationen nicht angeben, der Wert kann daher Null sein.

Feld	Datentyp	Beschreibung
command	string	Die allgemeine Kategorie der SQL-Anweisung. Die Werte für dieses Feld hängen vom Wert von a class. Wenn class MAIN ist, enthalten die Werte Folgendes: • CONNECT – wenn eine Client-Sitzung verbunden ist. • QUERY – eine SQL-Anweisung. Ebenfalls enthalten sind ein oder mehrere Ereignisse mit einem class-Wert von AUX. • DISCONNECT – wenn eine Client-Sitzung getrennt wird. • FAILED_CONNECT – wenn ein Client versucht, eine Verbindung herzustellen, dies aber nicht möglich ist. • CHANGEUSER – eine Statusänderung, die Teil des MySQL-Netzwerkprotokolls ist und nicht aus einer von Ihnen ausgegebenen Anweisung stammt. Wenn class AUX ist, enthalten die Werte Folgendes: • READ – eine Anweisung SELECT oder COPY, wenn es sich bei der Quelle um eine Relation oder Abfrage handelt. • WRITE – eine Anweisung INSERT, UPDATE, DELETE, TRUNCATE, oder COPY, wenn das Ziel eine Relation ist. • DROP – Löschen eines Objekts • CREATE – Erstellen eines Objekts. • RENAME – Umbenennen eines Objekts. • ALTER – Ändern der Eigenschaften eines Objekts.

Feld	Datentyp	Beschreibung
`commandText`	string	Bei Ereignissen mit dem `class`-Wert von `MAIN` stellt dieses Feld die tatsächliche, vom Benutzer eingegebene SQL-Anweisung dar. Dieses Feld wird für alle Arten von Datensätzen verwendet, mit Ausnahme von Verbindungs- oder Verbindungstrennungsdatensätzen, bei denen der Wert Null ist. Bei Ereignissen mit einem `class`-Wert von `AUX` enthält dieses Feld zusätzliche Informationen über die am Ereignis beteiligten Objekte. Bei Aurora MySQL wird Zeichen, z. B. Anführungszeichen, ein Backslash vorangestellt, der ein Escape-Zeichen darstellt. **Important** Der vollständige SQL-Text jeder Anweisung ist im Prüfprotokoll sichtbar, inklusive aller sensiblen Daten. Datenbankbenutzerkennwörter werden jedoch redigiert, wenn Aurora sie wie in der folgenden SQL-Anweisung aus dem Kontext ermitteln kann. `mysql> SET PASSWORD = 'my-password ';` **Note** Geben Sie aus Sicherheitsgründen ein anderes Passwort als hier angegeben an.
`databaseName`	Zeichenfolge	Die Datenbank, zu der der Benutzer eine Verbindung hergestellt hat.
`dbProtocol`	string	Das Datenbankprotokoll. Derzeit ist dieser Wert bei Aurora MySQL immer `MySQL`.

Feld	Datentyp	Beschreibung
`dbUserName`	string	Der Datenbankbenutzer, mit dem sich der Client authentifiziert hat.
`endTime` (nur Datenbank-Aktivitätsdatensätze der Version 1.2)	string	Die Zeit, zu der die Ausführung für die SQL-Anweisung endete. Sie wird im UTC-Format (Coordinated Universal Time) dargestellt. Um die Ausführungszeit der SQL-Anweisung zu berechnen, verwenden Sie `endTime - startTime` . Siehe auch das Feld `startTime` .
`errorMessage` (nur Datenbank-Aktivitätsdatensätze der Version 1.1)	string	Wenn ein Fehler aufgetreten ist, wird dieses Feld mit der Fehlermeldung gefüllt, die vom DB-Server generiert worden wäre. Der `errorMessage` -Wert ist null für normale Anweisungen, die nicht zu einem Fehler geführt haben. Ein Fehler wird als jede Aktivität definiert, die ein vom Client sichtbares MySQL-Fehlerprotokollereignis mit einem Schweregrad von `ERROR` oder höher erzeugen würde. Weitere Informationen finden Sie unter Fehlerprotokoll im MySQL-Referenzhandbuch. Beispielsweise erzeugen Syntaxfehler und Abfrageabbrüche eine Fehlermeldung. Interne MySQL-Serverfehler wie Hintergrund-Checkpointer-Prozessfehler erzeugen keine Fehlermeldung. Datensätze für solche Ereignisse werden jedoch weiterhin ausgegeben, unabhängig von der Einstellung des Schweregrads des Protokolls. Dadurch wird verhindert, dass Angreifer die Protokollierung deaktivieren, um eine Erkennung zu vermeiden. Siehe auch das Feld `exitCode`.

Feld	Datentyp	Beschreibung
`exitCode`	int	Ein Wert, der für einen Sitzungsbeendigungs-Datensatz verwendet wird. Bei einer sauberen Beendigung ist hier der Beendigungscode enthalten. In manchen Fehlersituationen kann nicht immer ein Beendigungscode erhalten werden. In solchen Fällen kann dieser Wert Null oder leer sein.
`logTime`	string	Ein Zeitstempel wie im Prüfcodepfad aufgezeichnet. Sie wird im UTC-Format (Coordinated Universal Time) dargestellt. Die genaueste Methode zum Berechnen der Anweisungsdauer finden Sie in den Feldern `startTime` und `endTime`.
`netProtocol`	string	Das Netzwerkkommunikationsprotokoll. Derzeit ist dieser Wert bei Aurora MySQL immer `TCP`.
`objectName`	string	Der Name des Datenbankobjekts, wenn die SQL-Anweisung für eines ausgeführt wird. Dieses Feld wird nur verwendet, wenn die SQL-Anweisung für ein Datenbankobjekt ausgeführt wird. Falls die SQL-Anweisung nicht für ein Objekt ausgeführt wird, ist dieser Wert leer. Um den vollständig qualifizierten Namen des Objekts zu erstellen, kombinieren Sie `databaseName` und `objectName`. Wenn die Abfrage mehrere Objekte umfasst, kann dieses Feld eine durch Komma getrennte Liste von Namen sein.
`objectType`	string	Der Datenbankobjekttyp, z. B. Tabelle, Index usw. Dieses Feld wird nur verwendet, wenn die SQL-Anweisung für ein Datenbankobjekt ausgeführt wird. Falls die SQL-Anweisung nicht für ein Objekt ausgeführt wird, lautet dieser Wert Null. Gültige Werte für Aurora MySQL sind unter anderem: • `INDEX` • `TABLE` • `UNKNOWN`

Feld	Datentyp	Beschreibung
`paramList`	string	Dieses Feld wird für Aurora MySQL nicht verwendet und ist immer Null.
`pid`	int	Die Prozess-ID des Back-End-Prozesses, der für die Client-Verbindung zugewiesen wird. Wenn der Datenbankserver neu gestartet wird, ändert sich die `pid` und der Zähler für das Feld `statementId` beginnt von vorn.
`remoteHost`	string	Entweder die IP-Adresse oder der Hostname des Clients, der die SQL-Anweisung ausgegeben hat. Was davon verwendet wird, ist bei Aurora MySQL von der Parametereinstellung `skip_name_resolve` der Datenbank abhängig. Der Wert `localhost` gibt die Aktivität des speziellen Benutzers `rdsadmin` an.
`remotePort`	string	Die Portnummer des Clients.
`rowCount`	int	Die Anzahl der Tabellenzeilen, die von der SQL-Anweisung betroffen sind bzw. abgerufen werden. Dieses Feld wird nur für SQL-Anweisungen verwendet, bei denen es sich um DML-Anweisungen (DML = Data Manipulation Language) handelt. Falls die SQL-Anweisung keine DML-Anweisung ist, lautet dieser Wert Null.
`serverHost`	string	Die Datenbankserver-Instance-ID. Dieser Wert wird bei Aurora MySQL anders dargestellt als bei Aurora PostgreSQL. Aurora PostgreSQL verwendet eine IP-Adresse anstelle einer ID.
`serverType`	string	Der Datenbankservertyp, z. B `MySQL`.
`serverVersion`	string	Die Version des Datenbankservers. Derzeit ist dieser Wert bei Aurora MySQL immer `MySQL 5.7.12`.
`serviceName`	string	Name des Service. Derzeit ist dieser Wert bei Aurora MySQL immer `Amazon Aurora MySQL`.

Feld	Datentyp	Beschreibung
`sessionId`	int	Eine pseudoeindeutige Sitzungskennung.
`startTime` (nur Datenbank-Aktivitätsdatensätze der Version 1.1)	string	Die Zeit, zu der die Ausführung für die SQL-Anweisung begann. Sie wird im UTC-Format (Coordinated Universal Time) dargestellt. Um die Ausführungszeit der SQL-Anweisung zu berechnen, verwenden Sie `endTime - startTime` . Siehe auch das Feld `endTime`.
`statementId`	int	Eine ID für die SQL-Anweisung des Clients. Der Zähler erhöht sich mit jeder vom Client eingegebenen SQL-Anweisung. Der Zähler wird zurückgesetzt, wenn die DB-Instance neu gestartet wird.
`substatementId`	int	Eine ID für eine SQL-Unteranweisung. Dieser Wert ist 1 für Ereignisse mit der Klasse `MAIN` und 2 für Ereignisse mit der Klasse `AUX`. Verwenden Sie das `statementId` -Feld, um alle Ereignisse zu identifizieren, die von derselben Anweisung generiert werden.
`transactionId` (nur Datenbank-Aktivitätsdatensätze der Version 1.2)	int	Eine ID für eine Transaktion.
`type`	string	Der Ereignistyp. Gültige Werte sind `record` oder `heartbeat` .

Verarbeiten eines Datenbankaktivitäts-Streams mit dem AWS SDK

Sie können einen Aktivitätsstream programmgesteuert verarbeiten, indem Sie das AWS SDK verwenden. Im Folgenden sehen Sie vollständig funktionsfähige Java- und Python-Beispiele für eine mögliche Verarbeitung des Kinesis-Datenstroms.

Java

```
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.net.InetAddress;
import java.nio.ByteBuffer;
import java.nio.charset.StandardCharsets;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.Security;
import java.util.HashMap;
import java.util.List;
import java.util.Map;
import java.util.UUID;
import java.util.zip.GZIPInputStream;

import javax.crypto.Cipher;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.SecretKeySpec;

import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CryptoInputStream;
import com.amazonaws.encryptionsdk.jce.JceMasterKey;
import
 com.amazonaws.services.kinesis.clientlibrary.exceptions.InvalidStateException;
import com.amazonaws.services.kinesis.clientlibrary.exceptions.ShutdownException;
import com.amazonaws.services.kinesis.clientlibrary.exceptions.ThrottlingException;
import com.amazonaws.services.kinesis.clientlibrary.interfaces.IRecordProcessor;
import
 com.amazonaws.services.kinesis.clientlibrary.interfaces.IRecordProcessorCheckpointer;
import
 com.amazonaws.services.kinesis.clientlibrary.interfaces.IRecordProcessorFactory;
import
 com.amazonaws.services.kinesis.clientlibrary.lib.worker.InitialPositionInStream;
```

```
import
 com.amazonaws.services.kinesis.clientlibrary.lib.worker.KinesisClientLibConfiguration;
import com.amazonaws.services.kinesis.clientlibrary.lib.worker.ShutdownReason;
import com.amazonaws.services.kinesis.clientlibrary.lib.worker.Worker;
import com.amazonaws.services.kinesis.clientlibrary.lib.worker.Worker.Builder;
import com.amazonaws.services.kinesis.model.Record;
import com.amazonaws.services.kms.AWSKMS;
import com.amazonaws.services.kms.AWSKMSClientBuilder;
import com.amazonaws.services.kms.model.DecryptRequest;
import com.amazonaws.services.kms.model.DecryptResult;
import com.amazonaws.util.Base64;
import com.amazonaws.util.IOUtils;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;
import com.google.gson.annotations.SerializedName;
import org.bouncycastle.jce.provider.BouncyCastleProvider;

public class DemoConsumer {

    private static final String STREAM_NAME = "aws-rds-das-[cluster-external-
resource-id]";
    private static final String APPLICATION_NAME = "AnyApplication"; //unique
 application name for dynamo table generation that holds kinesis shard tracking
    private static final String AWS_ACCESS_KEY =
 "[AWS_ACCESS_KEY_TO_ACCESS_KINESIS]";
    private static final String AWS_SECRET_KEY =
 "[AWS_SECRET_KEY_TO_ACCESS_KINESIS]";
    private static final String DBC_RESOURCE_ID = "[cluster-external-resource-id]";
    private static final String REGION_NAME = "[region-name]"; //us-east-1, us-
east-2...
    private static final BasicAWSCredentials CREDENTIALS = new
 BasicAWSCredentials(AWS_ACCESS_KEY, AWS_SECRET_KEY);
    private static final AWSStaticCredentialsProvider CREDENTIALS_PROVIDER = new
 AWSStaticCredentialsProvider(CREDENTIALS);

    private static final AwsCrypto CRYPTO = new AwsCrypto();
    private static final AWSKMS KMS = AWSKMSClientBuilder.standard()
            .withRegion(REGION_NAME)
            .withCredentials(CREDENTIALS_PROVIDER).build();

    class Activity {
        String type;
        String version;
        String databaseActivityEvents;
```

```
        String key;
    }

    class ActivityEvent {
        @SerializedName("class") String _class;
        String clientApplication;
        String command;
        String commandText;
        String databaseName;
        String dbProtocol;
        String dbUserName;
        String endTime;
        String errorMessage;
        String exitCode;
        String logTime;
        String netProtocol;
        String objectName;
        String objectType;
        List<String> paramList;
        String pid;
        String remoteHost;
        String remotePort;
        String rowCount;
        String serverHost;
        String serverType;
        String serverVersion;
        String serviceName;
        String sessionId;
        String startTime;
        String statementId;
        String substatementId;
        String transactionId;
        String type;
    }

    class ActivityRecords {
        String type;
        String clusterId;
        String instanceId;
        List<ActivityEvent> databaseActivityEventList;
    }

    static class RecordProcessorFactory implements IRecordProcessorFactory {
        @Override
```

```
        public IRecordProcessor createProcessor() {
            return new RecordProcessor();
        }
    }

    static class RecordProcessor implements IRecordProcessor {

        private static final long BACKOFF_TIME_IN_MILLIS = 3000L;
        private static final int PROCESSING_RETRIES_MAX = 10;
        private static final long CHECKPOINT_INTERVAL_MILLIS = 60000L;
        private static final Gson GSON = new
GsonBuilder().serializeNulls().create();

        private static final Cipher CIPHER;
        static {
            Security.insertProviderAt(new BouncyCastleProvider(), 1);
            try {
                CIPHER = Cipher.getInstance("AES/GCM/NoPadding", "BC");
            } catch (NoSuchAlgorithmException | NoSuchPaddingException |
NoSuchProviderException e) {
                throw new ExceptionInInitializerError(e);
            }
        }

        private long nextCheckpointTimeInMillis;

        @Override
        public void initialize(String shardId) {
        }

        @Override
        public void processRecords(final List<Record> records, final
IRecordProcessorCheckpointer checkpointer) {
            for (final Record record : records) {
                processSingleBlob(record.getData());
            }

            if (System.currentTimeMillis() > nextCheckpointTimeInMillis) {
                checkpoint(checkpointer);
                nextCheckpointTimeInMillis = System.currentTimeMillis() +
CHECKPOINT_INTERVAL_MILLIS;
            }
        }
```

```
        @Override
        public void shutdown(IRecordProcessorCheckpointer checkpointer,
ShutdownReason reason) {
            if (reason == ShutdownReason.TERMINATE) {
                checkpoint(checkpointer);
            }
        }

        private void processSingleBlob(final ByteBuffer bytes) {
            try {
                // JSON $Activity
                final Activity activity = GSON.fromJson(new String(bytes.array(),
StandardCharsets.UTF_8), Activity.class);

                // Base64.Decode
                final byte[] decoded =
Base64.decode(activity.databaseActivityEvents);
                final byte[] decodedDataKey = Base64.decode(activity.key);

                Map<String, String> context = new HashMap<>();
                context.put("aws:rds:dbc-id", DBC_RESOURCE_ID);

                // Decrypt
                final DecryptRequest decryptRequest = new DecryptRequest()

.withCiphertextBlob(ByteBuffer.wrap(decodedDataKey)).withEncryptionContext(context);
                final DecryptResult decryptResult = KMS.decrypt(decryptRequest);
                final byte[] decrypted = decrypt(decoded,
getByteArray(decryptResult.getPlaintext()));

                // GZip Decompress
                final byte[] decompressed = decompress(decrypted);
                // JSON $ActivityRecords
                final ActivityRecords activityRecords = GSON.fromJson(new
String(decompressed, StandardCharsets.UTF_8), ActivityRecords.class);

                // Iterate throught $ActivityEvents
                for (final ActivityEvent event :
activityRecords.databaseActivityEventList) {
                    System.out.println(GSON.toJson(event));
                }
            } catch (Exception e) {
                // Handle error.
                e.printStackTrace();
```

```
            }
        }

        private static byte[] decompress(final byte[] src) throws IOException {
            ByteArrayInputStream byteArrayInputStream = new
ByteArrayInputStream(src);
            GZIPInputStream gzipInputStream = new
GZIPInputStream(byteArrayInputStream);
            return IOUtils.toByteArray(gzipInputStream);
        }

        private void checkpoint(IRecordProcessorCheckpointer checkpointer) {
            for (int i = 0; i < PROCESSING_RETRIES_MAX; i++) {
                try {
                    checkpointer.checkpoint();
                    break;
                } catch (ShutdownException se) {
                    // Ignore checkpoint if the processor instance has been shutdown
(fail over).
                    System.out.println("Caught shutdown exception, skipping
checkpoint." + se);
                    break;
                } catch (ThrottlingException e) {
                    // Backoff and re-attempt checkpoint upon transient failures
                    if (i >= (PROCESSING_RETRIES_MAX - 1)) {
                        System.out.println("Checkpoint failed after " + (i + 1) +
"attempts." + e);
                        break;
                    } else {
                        System.out.println("Transient issue when checkpointing -
attempt " + (i + 1) + " of " + PROCESSING_RETRIES_MAX + e);
                    }
                } catch (InvalidStateException e) {
                    // This indicates an issue with the DynamoDB table (check for
table, provisioned IOPS).
                    System.out.println("Cannot save checkpoint to the DynamoDB table
used by the Amazon Kinesis Client Library." + e);
                    break;
                }
                try {
                    Thread.sleep(BACKOFF_TIME_IN_MILLIS);
                } catch (InterruptedException e) {
                    System.out.println("Interrupted sleep" + e);
                }
```

```
            }
        }
    }

    private static byte[] decrypt(final byte[] decoded, final byte[] decodedDataKey)
throws IOException {
        // Create a JCE master key provider using the random key and an AES-GCM
encryption algorithm
        final JceMasterKey masterKey = JceMasterKey.getInstance(new
SecretKeySpec(decodedDataKey, "AES"),
                "BC", "DataKey", "AES/GCM/NoPadding");
        try (final CryptoInputStream<JceMasterKey> decryptingStream =
CRYPTO.createDecryptingStream(masterKey, new ByteArrayInputStream(decoded));
             final ByteArrayOutputStream out = new ByteArrayOutputStream()) {
            IOUtils.copy(decryptingStream, out);
            return out.toByteArray();
        }
    }

    public static void main(String[] args) throws Exception {
        final String workerId = InetAddress.getLocalHost().getCanonicalHostName() +
":" + UUID.randomUUID();
        final KinesisClientLibConfiguration kinesisClientLibConfiguration =
                new KinesisClientLibConfiguration(APPLICATION_NAME, STREAM_NAME,
CREDENTIALS_PROVIDER, workerId);

kinesisClientLibConfiguration.withInitialPositionInStream(InitialPositionInStream.LATEST);
        kinesisClientLibConfiguration.withRegionName(REGION_NAME);
        final Worker worker = new Builder()
                .recordProcessorFactory(new RecordProcessorFactory())
                .config(kinesisClientLibConfiguration)
                .build();

        System.out.printf("Running %s to process stream %s as worker %s...\n",
APPLICATION_NAME, STREAM_NAME, workerId);

        try {
            worker.run();
        } catch (Throwable t) {
            System.err.println("Caught throwable while processing data.");
            t.printStackTrace();
            System.exit(1);
        }
        System.exit(0);
```

```
    }

    private static byte[] getByteArray(final ByteBuffer b) {
        byte[] byteArray = new byte[b.remaining()];
        b.get(byteArray);
        return byteArray;
    }
}
```

Python

```
import base64
import json
import zlib
import aws_encryption_sdk
from aws_encryption_sdk import CommitmentPolicy
from aws_encryption_sdk.internal.crypto import WrappingKey
from aws_encryption_sdk.key_providers.raw import RawMasterKeyProvider
from aws_encryption_sdk.identifiers import WrappingAlgorithm, EncryptionKeyType
import boto3

REGION_NAME = '<region>'                    # us-east-1
RESOURCE_ID = '<external-resource-id>'      # cluster-ABCD123456
STREAM_NAME = 'aws-rds-das-' + RESOURCE_ID  # aws-rds-das-cluster-ABCD123456

enc_client =
 aws_encryption_sdk.EncryptionSDKClient(commitment_policy=CommitmentPolicy.FORBID_ENCRYPT_AL

class MyRawMasterKeyProvider(RawMasterKeyProvider):
    provider_id = "BC"

    def __new__(cls, *args, **kwargs):
        obj = super(RawMasterKeyProvider, cls).__new__(cls)
        return obj

    def __init__(self, plain_key):
        RawMasterKeyProvider.__init__(self)
        self.wrapping_key =
 WrappingKey(wrapping_algorithm=WrappingAlgorithm.AES_256_GCM_IV12_TAG16_NO_PADDING,
                                       wrapping_key=plain_key,
 wrapping_key_type=EncryptionKeyType.SYMMETRIC)

    def _get_raw_key(self, key_id):
```

```
        return self.wrapping_key


def decrypt_payload(payload, data_key):
    my_key_provider = MyRawMasterKeyProvider(data_key)
    my_key_provider.add_master_key("DataKey")
    decrypted_plaintext, header = enc_client.decrypt(
        source=payload,

 materials_manager=aws_encryption_sdk.materials_managers.default.DefaultCryptoMaterialsManag
    return decrypted_plaintext


def decrypt_decompress(payload, key):
    decrypted = decrypt_payload(payload, key)
    return zlib.decompress(decrypted, zlib.MAX_WBITS + 16)


def main():
    session = boto3.session.Session()
    kms = session.client('kms', region_name=REGION_NAME)
    kinesis = session.client('kinesis', region_name=REGION_NAME)

    response = kinesis.describe_stream(StreamName=STREAM_NAME)
    shard_iters = []
    for shard in response['StreamDescription']['Shards']:
        shard_iter_response = kinesis.get_shard_iterator(StreamName=STREAM_NAME,
 ShardId=shard['ShardId'],

 ShardIteratorType='LATEST')
        shard_iters.append(shard_iter_response['ShardIterator'])

    while len(shard_iters) > 0:
        next_shard_iters = []
        for shard_iter in shard_iters:
            response = kinesis.get_records(ShardIterator=shard_iter, Limit=10000)
            for record in response['Records']:
                record_data = record['Data']
                record_data = json.loads(record_data)
                payload_decoded =
 base64.b64decode(record_data['databaseActivityEvents'])
                data_key_decoded = base64.b64decode(record_data['key'])
                data_key_decrypt_result =
 kms.decrypt(CiphertextBlob=data_key_decoded,
```

```
 EncryptionContext={'aws:rds:dbc-id': RESOURCE_ID})
                print (decrypt_decompress(payload_decoded,
 data_key_decrypt_result['Plaintext']))
            if 'NextShardIterator' in response:
                next_shard_iters.append(response['NextShardIterator'])
        shard_iters = next_shard_iters


if __name__ == '__main__':
    main()
```

Verwalten des Zugriffs auf Datenbankaktivitäts-Streams

Jeder Benutzer mit entsprechenden AWS Identity and Access Management-(IAM)-Rollenrechten für Datenbankaktivitäts-Streams kann die Einstellungen für einen Aktivitäts-Stream für einen DB-Cluster erstellen, starten, stoppen und dessen Einstellungen ändern. Diese Aktionen sind im Prüfprotokoll des Streams enthalten. Aus Compliance-Gründen empfehlen wir Ihnen, diese Berechtigungen nicht den DBAs zu erteilen.

Der Zugriff auf Datenbankaktivitäts-Streams wird mithilfe von IAM-Richtlinien festgelegt. Weitere Informationen zur Aurora--Authentifizierung finden Sie unter Identity and Access Management für Amazon Aurora. Weitere Informationen zum Erstellen von IAM-Richtlinien finden Sie unter Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff.

Example Richtlinie zum Zulassen der Konfiguration von Datenbankaktivitäts-Streams

Um Benutzern einen präzisen Zugriff auf die Änderung von Aktivitäts-Streams zu ermöglichen, verwenden Sie die servicespezifischen Operationskontextschlüssel `rds:StartActivityStream` und `rds:StopActivityStream` in einer IAM-Richtlinie. Das folgende IAM-Richtlinienbeispiel ermöglicht es einem Benutzer oder einer Rolle, Aktivitäts-Streams zu konfigurieren.

```
{
   "Version":"2012-10-17",
   "Statement":[
        {
            "Sid":"ConfigureActivityStreams",
            "Effect":"Allow",
            "Action": [
                "rds:StartActivityStream",
```

```
                "rds:StopActivityStream"
            ],
            "Resource":"*",
          }
     ]
}
```

Example Richtlinie zum Zulassen des Startens von Datenbankaktivitäts-Streams

Das folgende IAM-Richtlinienbeispiel ermöglicht es einem Benutzer oder einer Rolle, Aktivitäts-Streams zu starten.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AllowStartActivityStreams",
            "Effect":"Allow",
            "Action":"rds:StartActivityStream",
            "Resource":"*"
        }
    ]
}
```

Example Richtlinie zum Zulassen des Anhaltens von Datenbankaktivitäts-Streams

Das folgende IAM-Richtlinienbeispiel ermöglicht es einem Benutzer oder einer Rolle, Aktivitäts-Streams zu stoppen.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AllowStopActivityStreams",
            "Effect":"Allow",
            "Action":"rds:StopActivityStream",
            "Resource":"*"
        }
     ]
}
```

Example Richtlinie zum Ablehnen des Startens von Datenbankaktivitäts-Streams

Im folgenden IAM-Richtlinienbeispiel wird ein Benutzer oder eine Rolle daran gehindert, Aktivitäts-Streams zu starten.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"DenyStartActivityStreams",
            "Effect":"Deny",
            "Action":"rds:StartActivityStream",
            "Resource":"*"
        }
     ]
}
```

Example Richtlinie zum Ablehnen des Anhaltens von Datenbankaktivitäts-Streams

Im folgenden IAM-Richtlinienbeispiel wird ein Benutzer oder eine Rolle daran gehindert, Aktivitäts-Streams zu stoppen.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"DenyStopActivityStreams",
            "Effect":"Deny",
            "Action":"rds:StopActivityStream",
            "Resource":"*"
        }
    ]
}
```

Überwachung von Bedrohungen mit Amazon GuardDuty RDS Protection

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der Ihnen hilft, Ihre Konten, Container, Workloads und die Daten in Ihrer AWS Umgebung zu schützen. Mithilfe von Modellen für maschinelles Lernen (ML) und Funktionen zur Erkennung von Anomalien und Bedrohungen werden GuardDuty kontinuierlich verschiedene Protokollquellen und Laufzeitaktivitäten überwacht, um potenzielle Sicherheitsrisiken und böswillige Aktivitäten in Ihrer Umgebung zu identifizieren und zu priorisieren.

GuardDuty RDS Protection analysiert und profiliert Anmeldeereignisse im Hinblick auf potenzielle Zugriffsbedrohungen auf Ihre Amazon Aurora Aurora-Datenbanken. Wenn Sie RDS-Schutz aktivieren, GuardDuty werden RDS-Anmeldeereignisse aus Ihren Aurora-Datenbanken verarbeitet. RDS Protection überwacht diese Ereignisse und erstellt ein Profil für potenzielle interne Bedrohungen oder externe Akteure.

Weitere Informationen zur Aktivierung von GuardDuty RDS Protection finden Sie unter GuardDuty RDS Protection im GuardDuty Amazon-Benutzerhandbuch.

Wenn RDS Protection eine potenzielle Bedrohung erkennt, z. B. ein ungewöhnliches Muster bei erfolgreichen oder fehlgeschlagenen Anmeldeversuchen, GuardDuty generiert RDS Protection ein neues Ergebnis mit Details über die potenziell gefährdete Datenbank. Sie können die Details zu den Ergebnissen im Abschnitt Zusammenfassung der Ergebnisse in der GuardDuty Amazon-Konsole einsehen. Die Ergebnisdetails variieren je nach Ergebnistyp. Die primären Details, Ressourcentyp und Ressourcenrolle, bestimmen, welche Art von Informationen für jedes einzelne Ergebnis verfügbar ist. Weitere Informationen zu den allgemein verfügbaren Details zu Ergebnissen und den Findetypen finden Sie unter Finding details bzw. GuardDuty RDS Protection Finding Types im GuardDuty Amazon-Benutzerhandbuch.

Sie können die RDS-Schutzfunktion für jedes Gerät an jedem Ort ein- oder ausschalten, AWS-Konto in AWS-Region dem diese Funktion verfügbar ist. Wenn der RDS-Schutz nicht aktiviert ist, GuardDuty werden potenziell gefährdete Aurora-Datenbanken nicht erkannt und es werden keine Einzelheiten zur Gefährdung bereitgestellt.

Ein vorhandenes GuardDuty Konto kann RDS Protection mit einer 30-tägigen Testphase aktivieren. Für ein neues GuardDuty Konto ist RDS Protection bereits aktiviert und in der 30-tägigen kostenlosen Testphase enthalten. Weitere Informationen finden Sie unter GuardDuty Kostenschätzung im GuardDuty Amazon-Benutzerhandbuch.

Informationen zu dem AWS-Region s where, GuardDuty das RDS-Schutz noch nicht unterstützt, finden Sie unter Verfügbarkeit regionsspezifischer Funktionen im GuardDuty Amazon-Benutzerhandbuch.

Die folgende Tabelle enthält die Aurora-Datenbankversionen, die GuardDuty RDS Protection unterstützt:

Amazon-Aurora-DB-Engine	Unterstützte Engine-Versionen
Aurora MySQL	• 2.10.2 oder höher • 3.02.1 oder höher
Aurora PostgreSQL	• 10.17 oder höher • 11.12 oder höher • 12.7 oder höher • 13.3 oder höher • 14.3 oder höher • 15.2 oder höher • 16.1 oder später

Arbeiten mit Amazon Aurora MySQL

Amazon Aurora MySQL ist eine vollständig verwaltete, MySQL-kompatible, relationale Datenbank-Engine, die die Geschwindigkeit und Zuverlässigkeit kommerzieller hochwertiger Datenbanken mit der Einfachheit und Kosteneffizienz von Open-Source-Datenbanken kombiniert. Aurora MySQL ist ein Drop-In-Ersatz für MySQL und macht es einfach und kostengünstig, Ihre neuen und bestehenden MySQL-Implementierungen einzurichten, zu betreiben und zu skalieren, sodass Sie sich auf Ihr Unternehmen und Ihre Anwendungen konzentrieren können. Amazon RDS bietet Aurora die Verwaltung, indem es routinemäßige Datenbankaufgaben wie Bereitstellung, Patching, Sicherung, Wiederherstellung, Fehlererkennung und Reparatur übernimmt. Amazon RDS bietet auch Push-Button-Migrationstools zum Konvertieren Ihrer vorhandenen Amazon RDS für MySQL-Anwendungen in Aurora MySQL.

Themen

Übersicht über Amazon Aurora MySQL

In den folgenden Abschnitten finden Sie eine Übersicht über Amazon Aurora MySQL.

Themen

Amazon Aurora MySQL-Leistungserweiterungen

Amazon Aurora beinhaltet Leistungserweiterungen, um den verschiedenen Bedürfnissen von kommerziellen High-End-Datenbanken gerecht zu werden.

Schnelles Einfügen

Schnelles Einfügen beschleunigt parallele Insert-Vorgänge, geordnet nach Primärschlüssel, und wird speziell auf die Statements `LOAD DATA` und `INSERT INTO ... SELECT ...` angewandt. Schnelles Einfügen speichert die Position eines Cursors in einem Indexdurchlauf beim Ausführen des Statements zwischen. Dies verhindert ein unnötiges erneutes Durchlaufen des Index.

Schnelles Einfügen ist nur für reguläre InnoDB-Tabellen in Aurora MySQL Version 3.03.2 und höher aktiviert. Diese Optimierung funktioniert nicht für temporäre InnoDB-Tabellen. Es ist in Aurora MySQL Version 2 für alle Versionen 2.11 und 2.12 deaktiviert. Die schnelle Einfügeoptimierung funktioniert nur, wenn die adaptive Hash-Indexoptimierung deaktiviert ist.

Sie können die folgenden Metrik überwachen, um die Effektivität von schnellem Einfügen für Ihr DB-Cluster zu bestimmen:

- `aurora_fast_insert_cache_hits`: Ein Zähler, der erhöht wird, wenn der zwischengespeicherte Cursor erfolgreich abgerufen und bestätigt wurde.
- `aurora_fast_insert_cache_misses`: Ein Zähler, der erhöht wird, wenn der zwischengespeicherte Cursor nicht mehr gültig ist und Aurora einen normalen Index-Durchlauf durchführt.

Sie können den aktuellen Wert der Metriken von schnellem Einfügen mithilfe des folgenden Befehls abrufen:

```
mysql> show global status like 'Aurora_fast_insert%';
```

Sie erhalten eine Ausgabe, die dem Folgenden ähnelt:

```
+---------------------------------+-----------+
| Variable_name                   | Value     |
+---------------------------------+-----------+
| Aurora_fast_insert_cache_hits   | 3598300   |
| Aurora_fast_insert_cache_misses | 436401336 |
+---------------------------------+-----------+
```

Amazon Aurora MySQL und raumbezogene Daten

Die folgende Liste bietet eine Übersicht über die wichtigsten räumlichen Aurora MySQL-Funktionen und erläutert, wie diese den räumlichen Funktionen in MySQL entsprechen.

- Aurora MySQL Version 2 unterstützt dieselben räumlichen Datentypen und Funktionen für räumliche Beziehungen wie MySQL 5.7. Weitere Informationen zu diesen Datentypen und -Funktionen finden Sie unter Räumliche Datentypen und Geofunktionen in der MySQL 5.7-Dokumentation.
- Aurora MySQL Version 3 unterstützt dieselben räumlichen Datentypen und Funktionen für räumliche Beziehungen wie MySQL 8.0 Weitere Informationen zu diesen Datentypen und -Funktionen finden Sie unter Räumliche Datentypen und Geofunktionen in der MySQL 8.0-Dokumentation.
- Aurora MySQL unterstützt die räumliche Indizierung in InnoDB-Tabellen. Die räumliche Indizierung verbessert die Abfrageleistung in großen Datensätzen für Abfragen von räumlichen Daten. In MySQL ist die räumliche Indizierung für InnoDB-Tabellen in MySQL 5.7 und 8.0 verfügbar.

  Aurora MySQL verwendet einen anderen Ansatz für die räumliche Indizierung als MySQL für hohe Leistung bei räumlichen Abfragen. Die räumliche Aurora-Indeximplementierung verwendet die raumausfüllende Kurve eines B-Baums; dadurch soll eine höhere Leistung für räumliche Bereichsscans erzielt werden als mit einem R-Baum.

> **Note**
>
> In Aurora MySQL kann eine Transaktion in einer Tabelle mit einem räumlichen Index, der für eine Spalte mit einer räumlichen Referenz-ID (SRID) definiert ist, nicht in einen Bereich eingefügt werden, der für die Aktualisierung durch eine andere Transaktion ausgewählt wurde.

Die folgenden Anweisungen aus der Data Definition Language (DDL) bieten Unterstützung für das Erstellen von Indizes in Spalten, die raumbezogene Datentypen verwenden.

CREATE TABLE

Sie können die `SPATIAL INDEX`-Schlüsselwörter in einer `CREATE TABLE`-Anweisung verwenden, um einen räumlichen Index zu einer Spalte in einer neuen Tabelle hinzuzufügen. Im Folgenden sehen Sie ein Beispiel.

```
CREATE TABLE test (shape POLYGON NOT NULL, SPATIAL INDEX(shape));
```

ALTER TABLE

Sie können die `SPATIAL INDEX`-Schlüsselwörter in einer `ALTER TABLE`-Anweisung verwenden, um einen räumlichen Index zu einer Spalte in einer vorhandenen Tabelle hinzuzufügen. Im Folgenden sehen Sie ein Beispiel.

```
ALTER TABLE test ADD SPATIAL INDEX(shape);
```

CREATE INDEX

Sie können das `SPATIAL`-Schlüsselwort in einer `CREATE INDEX`-Anweisung verwenden, um einen räumlichen Index zu einer Spalte in einer vorhandenen Tabelle hinzuzufügen. Im Folgenden sehen Sie ein Beispiel.

```
CREATE SPATIAL INDEX shape_index ON test (shape);
```

Aurora mit MySQL Version 3 ist kompatibel mit MySQL 8.0

Sie können Aurora MySQL Version 3 verwenden, um die neuesten MySQL-kompatiblen Funktionen, Leistungsverbesserungen und Bugfixes zu erhalten. Im Folgenden erfahren Sie mehr über Aurora MySQL Version 3 mit MySQL 8.0 Kompatibilität. Sie können lernen, wie Sie Ihre Cluster und Anwendungen auf Aurora MySQL Version 3 aktualisieren.

Einige Aurora-Funktionen wie Aurora Serverless v2 erfordern Aurora MySQL Version 3.

Themen

Funktionen aus der Community Edition von MySQL 8.0

Die erste Version von Aurora MySQL Version 3 ist mit der Community Edition von MySQL 8.0.23 kompatibel. MySQL 8.0 führt mehrere neue Funktionen ein, darunter die folgenden:

- JSON-Funktionen Weitere Informationen zur Nutzung finden Sie unterJSON-FunktionenimMySQL-Referenzhandbuchaus.
- Fensterfunktionen. Weitere Informationen zur Nutzung finden Sie unterFensterfunktionenimMySQL-Referenzhandbuchaus.
- Gemeinsame Tabellenausdrücke (CTEs) unter Verwendung der`WITH`-Klausel. Weitere Informationen zur Nutzung finden Sie unterWITH (Allgemeine Tabellenausdrücke)imMySQL-Referenzhandbuchaus.
- Optimiert`ADD COLUMN`und`RENAME COLUMN`-Klauseln für`ALTER TABLE`statement. Diese Optimierungen werden „Instant DDL“ genannt. Aurora MySQL Version 3 ist mit der MySQL-Instant-DDL-Funktion der Community kompatibel. Die ehemalige Aurora Fast DDL-Funktion wird nicht

verwendet. Informationen zur Verwendung für Instant DDL finden Sie unterSofortige DDL (Aurora MySQL Version 3)aus.

- Absteigende, funktionale und unsichtbare Indizes. Weitere Informationen zur Nutzung finden Sie unterUnsichtbare Indizes,Absteigende Indizes, undCREATE INDEX-AnweisungimMySQL-Referenzhandbuchaus.
- Rollenbasierte Berechtigungen, die durch SQL-Anweisungen gesteuert werden. Weitere Informationen zu Änderungen am Berechtigungsmodell finden Sie unterRollenbasiertes Berechtigungsmodellaus.
- `NOWAIT`und`SKIP LOCKED`-Klauseln mit`SELECT ... FOR SHARE`Estatement. Diese Klauseln vermeiden es, darauf zu warten, dass andere Transaktionen Zeilensperren freigeben. Weitere Informationen zu Lesesperren finden Sie im MySQL-Referenzhandbuch.
- Verbesserungen der Binärprotokollreplikation (binlog). Die Aurora MySQL-Details finden Sie unterBinäre Protokoll-Replikationaus. Insbesondere können Sie eine gefilterte Replikation durchführen. Informationen zur Verwendung zur gefilterten Replikation finden Sie unterSo bewerten Server Replikationsfilterregeln imMySQL-Referenzhandbuchaus.
- Hinweise Einige der MySQL 8.0-kompatiblen Hinweise wurden bereits auf Aurora MySQL Version 2 zurückportiert. Weitere Informationen zur Sicherheit im Zusammenhang mit Aurora MySQL finden Sie unter Aurora-MySQL-Hinweise. Eine vollständige Liste der Hinweise in MySQL 8.0 finden Sie unterOptimierungshinweiseimMySQL-Referenzhandbuchaus.

Die vollständige Liste der Funktionen, die zur MySQL 8.0 Community Edition hinzugefügt wurden, finden Sie im BlogbeitragDie vollständige Liste der neuen Funktionen in MySQL 8.0aus.

Aurora MySQL Version 3 enthält auch Änderungen an Schlüsselwörtern für inklusive Sprache, die von der Community MySQL 8.0.26 zurückportiert wurden. Einzelheiten zu diesen Änderungen finden Sie unterInklusive Sprachänderungen für Aurora MySQL Version 3aus.

Aurora MySQL Version 3 als Voraussetzung für Aurora MySQL Serverless v2

Aurora MySQL Version 3 ist Voraussetzung für alle DB-Instances in einem Aurora-MySQL-Serverless-v2-Cluster. Aurora MySQL Serverless v2 enthält Unterstützung für Reader-Instances in einem DB-Cluster und andere Aurora-Funktionen, die für Aurora MySQL Serverless v1 nicht verfügbar sind. Diese Version bietet auch eine schnellere und stärker granulare Skalierung als Aurora MySQL Serverless v1.

Versionshinweise für Aurora MySQL Version 3

Die Versionshinweise für alle Versionen von Aurora MySQL Version 3 finden Sie unter Aktualisierungen der Datenbank-Engine für Amazon Aurora MySQL Version 3 in den Versionshinweisen für Aurora MySQL.

Neue -Optimierungen für parallele Abfragen

Die parallele Aurora-Abfrageoptimierung gilt nun für mehr SQL-Operationen:

- Die parallele Abfrage gilt jetzt für Tabellen, die die Datentypen enthaltenTEXT,BLOB,JSON,GEOMETRY, undVARCHARundCHARlänger als 768 Bytes.
- Parallele Abfragen können Abfragen mit partitionierten Tabellen optimieren.
- Eine parallele Abfrage kann Abfragen mit Aggregatfunktionsaufrufen in der Auswahlliste und derHAVING-Klausel.

Weitere Informationen zu Enhanced Monitoring finden Sie unter Upgrade paralleler Abfrage-Cluster auf Aurora-MySQL-Version 3. Allgemeine Informationen zu Aurora-Sicherungen finden Sie unter Arbeiten mit Parallel Query für Amazon Aurora MySQL.

Optimierungen reduzieren die Neustartzeit der Datenbank

Ihr Aurora-MySQL-DB-Cluster muss sowohl bei geplanten als auch bei ungeplanten Ausfällen hochverfügbar sein.

Datenbankadministratoren müssen gelegentlich Datenbankwartungen durchführen. Diese Wartungsmaßnahmen umfassen Datenbank-Patches, Upgrades, Änderungen von Datenbankparametern, die einen manuellen Neustart erfordern, die Durchführung eines Failovers, um den Zeitaufwand für Instance-Klassenänderungen zu reduzieren, usw. Solche geplanten Aktionen machen Ausfallzeiten erforderlich.

Ausfallzeiten können jedoch auch durch ungeplante Aktionen verursacht werden, beispielsweise durch einen unerwarteten Failover aufgrund eines zugrunde liegenden Hardwarefehlers oder durch die Drosselung von Datenbankressourcen. Alle diese geplanten und ungeplanten Aktionen führen zu einem Neustart der Datenbank.

In Aurora MySQL Version 3.05 und höher haben wir Optimierungen eingeführt, die die Neustartzeit der Datenbank reduzieren. Diese Optimierungen sorgen für bis zu 65 % weniger Ausfallzeiten

als ohne Optimierungen und weniger Unterbrechungen Ihrer Datenbank-Workloads nach einem Neustart.

Während des Datenbankstarts werden viele interne Speicherkomponenten initialisiert. Die größte dieser Komponenten ist der InnoDB-Pufferpool, der in Aurora MySQL standardmäßig 75 % der Instance-Speichergröße ausmacht. Unsere Tests haben ergeben, dass die Initialisierungszeit proportional zur Größe des InnoDB-Pufferpools ist und daher mit der Größe der DB-Instance-Klasse skaliert. Während dieser Initialisierungsphase kann die Datenbank keine Verbindungen akzeptieren, wodurch es zu längeren Ausfallzeiten bei Neustarts kommt. In der ersten Phase des schnellen Neustarts von Aurora MySQL wird die Initialisierung des Pufferpools optimiert, wodurch die Zeit für die Datenbankinitialisierung und damit die Gesamtneustartzeit reduziert werden kann.

Weitere Informationen finden Sie im Blog Reduce downtime with Amazon Aurora MySQL database restart time optimizations.

Neues temporäres Tabellenverhalten in Aurora-MySQL-Version 3

Aurora MySQL Version 3 behandelt temporäre Tabellen anders als frühere Aurora-MySQL-Versionen. Dieses neue Verhalten wird von der Community Edition von MySQL 8.0 geerbt. Es gibt zwei Arten von temporären Tabellen, die mit Aurora MySQL Version 3 erstellt werden können:

- Interne (oder implizite) temporäre Tabellen – werden von der Aurora-MySQL-Engine erstellt, um Vorgänge wie Sortieraggregation, abgeleitete Tabellen oder allgemeine Tabellenausdrücke (CTEs) zu behandeln.
- Vom Benutzer erstellte (oder explizite) temporäre Tabellen – werden von der Aurora-MySQL-Engine erstellt, wenn Sie die Anweisung `CREATE TEMPORARY TABLE` verwenden.

Es gibt zusätzliche Überlegungen sowohl für interne als auch für vom Benutzer erstellte temporäre Tabellen auf Aurora-Reader-DB-Instances. Diese werden in den folgenden Abschnitten erläutert.

Themen

- Speicher-Engine für interne (implizite) temporäre Tabellen
- Begrenzung der Größe interner temporärer Tabellen im Arbeitsspeicher
- Abschwächung von Füllungsgradproblemen bei internen temporären Tabellen auf Aurora Replicas
- Vom Benutzer erstellte (explizite) temporäre Tabellen auf Reader-DB-Instances
- Fehler bei der Erstellung temporärer Tabellen und Abhilfemaßnahmen

Speicher-Engine für interne (implizite) temporäre Tabellen

Beim Generieren von Zwischenergebnismengen versucht Aurora MySQL zunächst, in temporäre Tabellen im Arbeitsspeicher zu schreiben. Dies ist aufgrund inkompatibler Datentypen oder konfigurierter Grenzwerte möglicherweise nicht erfolgreich. In diesem Fall wird die temporäre Tabelle in eine temporäre Tabelle auf dem Datenträger konvertiert, anstatt im Arbeitsspeicher abgelegt zu werden. Weitere Informationen hierzu finden Sie unter Verwendung interner temporärer Tabellen in MySQL in der MySQL-Dokumentation.

In Aurora-MySQL-Version 3 unterscheidet sich die Funktionsweise interner temporärer Tabellen von früheren Aurora-MySQL-Versionen. Anstatt sich für solche temporären Tabellen zwischen den InnoDB- und MyISAM-Speicher-Engines zu entscheiden, wählen Sie jetzt zwischen den`TempTable`und InnoDB Storage-Engines.

Mit der`TempTable`Speicher-Engine können Sie eine zusätzliche Auswahl für den Umgang mit bestimmten Daten treffen. Die betroffenen Daten überlaufen den Speicherpool, der alle internen temporären Tabellen für die DB-Instance enthält.

Diese Optionen können die Leistung von Abfragen beeinflussen, die hohe Mengen an temporären Daten generieren, z. B. während der Durchführung von Aggregationen wie `GROUP BY` auf großen Tabellen.

> **Tip**
>
> Wenn Ihre Workload Abfragen enthält, die interne temporäre Tabellen generieren, bestätigen Sie, wie Ihre Anwendung mit dieser Änderung funktioniert, indem Sie Benchmarks ausführen und leistungsbezogene Metriken überwachen.
> In einigen Fällen passt die Menge an temporären Daten in`TempTable`Speicherpool oder überläuft den Speicherpool nur um einen kleinen Betrag. In diesen Fällen empfehlen wir die `TempTable`-Einstellung für interne temporäre Tabellen und speicherzugeordnete Dateien, um Überlaufdaten zu speichern. Dies ist die Standardeinstellung.

Die `TempTable`-Speicher-Engine ist die Standardeinstellung. `TempTable` verwendet einen gemeinsamen Speicherpool für alle temporären Tabellen, die diese Engine verwenden, anstelle eines maximalen Speicherlimits pro Tabelle. Die Größe dieses Speicherpools wird durch den Parameter temptable_max_ram angegeben. Der Wert dieses Parameters beträgt standardmäßig 1 GiB bei DB-Instances mit 16 oder mehr GiB Arbeitsspeicher und 16 MB bei DB-Instances mit weniger

als 16 GB Arbeitsspeicher. Die Größe des Speicherpools beeinflusst den Speicherverbrauch auf Sitzungsebene.

Bei Verwendung der Speicher-Engine `TempTable` kann es vorkommen, dass die temporären Daten die Größe des Speicherpools überschreiten. In diesem Fall speichert Aurora MySQL die Überlaufdaten mithilfe eines sekundären Mechanismus.

Sie können den Parameter temptable_max_mmap festlegen, um anzugeben, ob die Daten zu temporären Dateien im Arbeitsspeicher oder zu internen temporären Tabellen von InnoDB auf der Festplatte überlaufen werden. Die verschiedenen Datenformate und Überlaufkriterien dieser Überlaufmechanismen können sich auf die Abfrageleistung auswirken. Sie tun dies, indem sie die Menge der auf die Festplatte geschriebenen Daten und die Nachfrage nach Festplattenspeicherdurchsatz beeinflussen.

Aurora MySQL speichert die Überlaufdaten unterschiedlich, abhängig von der Wahl des Datenüberlaufziels und ob die Abfrage auf einer Writer- oder Reader-DB-Instance ausgeführt wird:

- In der Writer-Instanz werden Daten, die zu internen temporären Tabellen von InnoDB überlaufen, im Aurora-Cluster-Volume gespeichert.
- In der Writer-Instanz befinden sich Daten, die zu speicherzugeordneten temporären Dateien überlaufen, auf lokalem Speicher auf der Aurora MySQL-Version 3-Instanz.
- Bei Reader-Instanzen befinden sich Überlaufdaten immer auf speicherzugeordneten temporären Dateien auf lokalem Speicher. Dies liegt daran, dass schreibgeschützte Instances keine Daten auf dem Aurora-Cluster-Volume speichern können.

Die Konfigurationsparameter für interne temporäre Tabellen gelten unterschiedlich für die Writer- und Reader-Instanzes in Ihrem Cluster.

- Für Reader-Instances verwendet Aurora MySQL immer die Speicher–Engine `TempTable`.
- Die Größe für `temptable_max_mmap` beträgt für Writer- und Reader-Instances unabhängig von der Speichergröße der DB-Instance standardmäßig 1 GB. Sie können diesen Wert sowohl für Writer- als auch für Reader-Instances anpassen.
- Die Einstellung von `temptable_max_mmap` auf `0` deaktiviert die Verwendung von temporären Dateien mit Speicherzuordnung auf Writer-Instances.
- Sie können `0` auf Reader-Instances nicht auf `temptable_max_mmap` setzen.

> **Note**
>
> Es wird nicht empfohlen, den temptable_use_mmap-Parameter zu verwenden. Dieser ist veraltet, und es wird erwartet, dass die Unterstützung dafür in einer künftigen MySQL-Version entfernt wird.

Begrenzung der Größe interner temporärer Tabellen im Arbeitsspeicher

Wie in Speicher-Engine für interne (implizite) temporäre Tabellen erwähnt, können Sie temporäre Tabellenressourcen global steuern, indem Sie die Einstellungen temptable_max_ram und temptable_max_mmap verwenden.

Sie können die Größe jeder einzelnen internen temporären Tabelle im Arbeitsspeicher auch einschränken, indem Sie den DB-Parameter tmp_table_size verwendenParameter. Dieses Limit soll verhindern, dass einzelne Abfragen übermäßig viele globale temporäre Tabellenressourcen verbrauchen, was sich auf die Leistung gleichzeitiger Abfragen auswirken kann, die diese Ressourcen benötigen.

Der Parameter `tmp_table_size` definiert die maximale Größe temporärer Tabellen, die von der `MEMORY`-Speicher-Engine in Aurora-MySQL-Version 3 erstellt werden.

In Aurora-MySQL-Version 3.04 und höher definiert der Parameter `tmp_table_size` auch die maximale Größe temporärer Tabellen, die von der `TempTable`-Speicher-Engine erstellt werden, wenn der DB-Parameter `aurora_tmptable_enable_per_table_limit` auf `ON` festgelegt ist. Dieses Verhalten ist standardmäßig deaktiviert (`OFF`). Dies entspricht dem Verhalten von Aurora-MySQL-Version 3.03 und niedrigeren Versionen.

- Wenn `aurora_tmptable_enable_per_table_limit` `OFF` ist ,wird `tmp_table_size` nicht für interne temporäre Tabellen im Arbeitsspeicher berücksichtigt, die von der`TempTable`-Speicher-Engine erstellt wurden.

  Das globale `TempTable`-Ressourcenlimit gilt jedoch weiterhin. Aurora MySQL verhält sich wie folgt, wenn das globale `TempTable`-Ressourcenlimit erreicht wird:

  - Writer-DB-Instances – Aurora MySQL konvertiert die temporäre Tabelle im Arbeitsspeicher automatisch in eine temporäre InnoDB-Tabelle auf der Festplatte.
  - Reader-DB-Instances – Die Abfrage endet mit einem Fehler.

```
ERROR 1114 (HY000): The table '/rdsdbdata/tmp/#sqlxx_xxx' is full
```

- Wenn `aurora_tmptable_enable_per_table_limit` `ON` ist, verhält sich Aurora MySQL wie folgt, wenn das `tmp_table_size`-Limit erreicht wird:
  - Writer-DB-Instances – Aurora MySQL konvertiert die temporäre Tabelle im Arbeitsspeicher automatisch in eine temporäre InnoDB-Tabelle auf der Festplatte.
  - Reader-DB-Instances – Die Abfrage endet mit einem Fehler.

    ```
    ERROR 1114 (HY000): The table '/rdsdbdata/tmp/#sqlxx_xxx' is full
    ```

    In diesem Fall gelten sowohl das globale `TempTable`-Ressourcenlimit als auch das Limit pro Tabelle.

> **Note**
>
> Der `aurora_tmptable_enable_per_table_limit`-Parameter hat keine Auswirkungen, wenn interne_tmp_mem_storage_engine auf `MEMORY` eingestellt ist. In diesem Fall wird die maximale Größe einer temporären Tabelle im Arbeitsspeicher durch den Wert tmp_table_size oder max_heap_table_size definiert, je nachdem, welcher Wert kleiner ist.

Die folgenden Beispiele zeigen das Verhalten des `aurora_tmptable_enable_per_table_limit`-Parameters für Writer- und Reader-DB-Instances.

Example einer Writer-DB-Instance mit der Einstellung **`aurora_tmptable_enable_per_table_limit`** auf **`OFF`**

Die temporäre Tabelle im Arbeitsspeicher wird nicht in eine temporäre InnoDB-Tabelle auf dem Datenträger konvertiert.

```
mysql> set aurora_tmptable_enable_per_table_limit=0;
Query OK, 0 rows affected (0.00 sec)

mysql> select
 @@innodb_read_only,@@aurora_version,@@aurora_tmptable_enable_per_table_limit,@@temptable_max_r
```

```
+--------------------+------------------+-----------------------------------------
+---------------------+----------------------+
| @@innodb_read_only | @@aurora_version | @@aurora_tmptable_enable_per_table_limit |
 @@temptable_max_ram | @@temptable_max_mmap |
+--------------------+------------------+-----------------------------------------
+---------------------+----------------------+
|                  0 | 3.04.0           |                                        0 |
       1073741824 |           1073741824 |
+--------------------+------------------+-----------------------------------------
+---------------------+----------------------+
1 row in set (0.00 sec)

mysql> show status like '%created_tmp_disk%';
+-------------------------+-------+
| Variable_name           | Value |
+-------------------------+-------+
| Created_tmp_disk_tables | 0     |
+-------------------------+-------+
1 row in set (0.00 sec)

mysql> set cte_max_recursion_depth=4294967295;
Query OK, 0 rows affected (0.00 sec)

mysql> WITH RECURSIVE cte (n) AS (SELECT 1 UNION ALL SELECT n + 1 FROM cte WHERE n <
 60000000) SELECT max(n) FROM cte;
+----------+
| max(n)   |
+----------+
| 60000000 |
+----------+
1 row in set (13.99 sec)

mysql> show status like '%created_tmp_disk%';
+-------------------------+-------+
| Variable_name           | Value |
+-------------------------+-------+
| Created_tmp_disk_tables | 0     |
+-------------------------+-------+
1 row in set (0.00 sec)
```

Example einer Writer-DB-Instance mit der Einstellung **aurora_tmptable_enable_per_table_limit** auf **ON**

Die temporäre Tabelle im Arbeitsspeicher wird in eine temporäre InnoDB-Tabelle auf dem Datenträger konvertiert.

```
mysql> set aurora_tmptable_enable_per_table_limit=1;
Query OK, 0 rows affected (0.00 sec)

mysql> select
 @@innodb_read_only,@@aurora_version,@@aurora_tmptable_enable_per_table_limit,@@tmp_table_size;
+--------------------+-----------------+-----------------------------------------
+------------------+
| @@innodb_read_only | @@aurora_version | @@aurora_tmptable_enable_per_table_limit |
 @@tmp_table_size |
+--------------------+-----------------+-----------------------------------------
+------------------+
|                  0 | 3.04.0          |                                        1 |
      16777216 |
+--------------------+-----------------+-----------------------------------------
+------------------+
1 row in set (0.00 sec)

mysql> set cte_max_recursion_depth=4294967295;
Query OK, 0 rows affected (0.00 sec)

mysql> show status like '%created_tmp_disk%';
+-------------------------+-------+
| Variable_name           | Value |
+-------------------------+-------+
| Created_tmp_disk_tables | 0     |
+-------------------------+-------+
1 row in set (0.00 sec)

mysql> WITH RECURSIVE cte (n) AS (SELECT 1 UNION ALL SELECT n + 1 FROM cte WHERE n <
 6000000) SELECT max(n) FROM cte;
+---------+
| max(n)  |
+---------+
| 6000000 |
+---------+
1 row in set (4.10 sec)
```

```
mysql> show status like '%created_tmp_disk%';
+-------------------------+-------+
| Variable_name           | Value |
+-------------------------+-------+
| Created_tmp_disk_tables | 1     |
+-------------------------+-------+
1 row in set (0.00 sec)
```

Example einer Reader-DB-Instance mit der Einstellung **aurora_tmptable_enable_per_table_limit** auf **OFF**

Die Abfrage wird ohne Fehler beendet, weil `tmp_table_size` nicht zutrifft, und das globale `TempTable`-Ressourcenlimit wurde nicht erreicht.

```
mysql> set aurora_tmptable_enable_per_table_limit=0;
Query OK, 0 rows affected (0.00 sec)

mysql> select
 @@innodb_read_only,@@aurora_version,@@aurora_tmptable_enable_per_table_limit,@@temptable_max_r
+--------------------+-----------------+-----------------------------------------
+----------------------+----------------------+
| @@innodb_read_only | @@aurora_version | @@aurora_tmptable_enable_per_table_limit |
 @@temptable_max_ram | @@temptable_max_mmap |
+--------------------+-----------------+-----------------------------------------
+----------------------+----------------------+
|                  1 | 3.04.0          |                                        0 |
       1073741824 |           1073741824 |
+--------------------+-----------------+-----------------------------------------
+----------------------+----------------------+
1 row in set (0.00 sec)

mysql> set cte_max_recursion_depth=4294967295;
Query OK, 0 rows affected (0.00 sec)

mysql> WITH RECURSIVE cte (n) AS (SELECT 1 UNION ALL SELECT n + 1 FROM cte WHERE n <
 60000000) SELECT max(n) FROM cte;
+----------+
| max(n)   |
+----------+
| 60000000 |
+----------+
1 row in set (14.05 sec)
```

Example einer Reader-DB-Instance mit der Einstellung **aurora_tmptable_enable_per_table_limit** auf **OFF**

Diese Abfrage erreicht das globale TempTable-Ressourcenlimit, wobei `aurora_tmptable_enable_per_table_limit` auf OFF eingestellt ist. Die Abfrage endet mit einem Fehler auf den Reader-Instances.

```
mysql> set aurora_tmptable_enable_per_table_limit=0;
Query OK, 0 rows affected (0.00 sec)

mysql> select
 @@innodb_read_only,@@aurora_version,@@aurora_tmptable_enable_per_table_limit,@@temptable_max_r
+--------------------+------------------+-----------------------------------------
+---------------------+----------------------+
| @@innodb_read_only | @@aurora_version | @@aurora_tmptable_enable_per_table_limit |
 @@temptable_max_ram | @@temptable_max_mmap |
+--------------------+------------------+-----------------------------------------
+---------------------+----------------------+
|                  1 | 3.04.0           |                                        0 |
       1073741824 |           1073741824 |
+--------------------+------------------+-----------------------------------------
+---------------------+----------------------+
1 row in set (0.00 sec)

mysql> set cte_max_recursion_depth=4294967295;
Query OK, 0 rows affected (0.01 sec)

mysql> WITH RECURSIVE cte (n) AS (SELECT 1 UNION ALL SELECT n + 1 FROM cte WHERE n <
 120000000) SELECT max(n) FROM cte;
ERROR 1114 (HY000): The table '/rdsdbdata/tmp/#sqlfd_1586_2' is full
```

Example einer Reader-DB-Instance mit der Einstellung **aurora_tmptable_enable_per_table_limit** auf **ON**

Die Abfrage endet mit einem Fehler, wenn das `tmp_table_size`-Limit erreicht wird.

```
mysql> set aurora_tmptable_enable_per_table_limit=1;
Query OK, 0 rows affected (0.00 sec)

mysql> select
 @@innodb_read_only,@@aurora_version,@@aurora_tmptable_enable_per_table_limit,@@tmp_table_size;
+--------------------+------------------+-----------------------------------------
+------------------+
```

```
| @@innodb_read_only | @@aurora_version | @@aurora_tmptable_enable_per_table_limit |
 @@tmp_table_size |
+--------------------+------------------+------------------------------------------
+------------------+
|                  1 | 3.04.0           |                                        1 |
      16777216 |
+--------------------+------------------+------------------------------------------
+------------------+
1 row in set (0.00 sec)

mysql> set cte_max_recursion_depth=4294967295;
Query OK, 0 rows affected (0.00 sec)

mysql> WITH RECURSIVE cte (n) AS (SELECT 1 UNION ALL SELECT n + 1 FROM cte WHERE n <
 6000000) SELECT max(n) FROM cte;
ERROR 1114 (HY000): The table '/rdsdbdata/tmp/#sqlfd_8_2' is full
```

Abschwächung von Füllungsgradproblemen bei internen temporären Tabellen auf Aurora Replicas

Sie können Probleme mit der Größenbeschränkung für temporäre Tabellen vermeiden, indem Sie die Parameter `temptable_max_ram` und `temptable_max_mmap` auf einen kombinierten Wert festlegen, der die Anforderungen Ihrer Workloads erfüllen kann.

Seien Sie vorsichtig, wenn Sie den Wert des Parameters `temptable_max_ram` festlegen. Wenn Sie den Wert zu hoch einstellen, wird der verfügbare Arbeitsspeicher auf der Datenbank-Instance reduziert, was zu einer Out-of-Memory-Bedingung führen kann. Überwachen Sie den durchschnittlichen möglichen freien Arbeitsspeicher der DB-Instance. Ermitteln Sie dann einen geeigneten Wert für `temptable_max_ram`, damit Sie immer noch angemessenen freien Speicherplatz auf der Instance zur Verfügung haben. Weitere Informationen finden Sie unter Probleme mit freisetzbarem Speicher in Amazon Aurora.

Es ist auch wichtig, die Größe des lokalen Speichers und die Speicherplatzbelegung durch die temporäre Tabelle zu überwachen. Weitere Informationen zur Überwachung des lokalen Arbeitsspeichers auf einer Instance finden Sie im AWS-Wissenscenter-Artikel Was ist im Aurora-MySQL-kompatiblen lokalen Speicher gespeichert und wie kann ich lokale Speicherprobleme beheben?.

> **Note**
>
> Dieses Verfahren funktioniert nicht, wenn der `aurora_tmptable_enable_per_table_limit`-Parameter auf `ON` festgelegt ist.

Weitere Informationen finden Sie unter Begrenzung der Größe interner temporärer Tabellen im Arbeitsspeicher.

Example 1

Sie wissen, dass Ihre temporären Tabellen auf eine kumulative Größe von 20 GiB anwachsen. Sie möchten temporäre In-Memory-Tabellen auf 2 GiB festlegen und auf maximal 20 GiB auf der Festplatte anwachsen lassen.

Setzen Sie `temptable_max_ram` auf **`2,147,483,648`** und `temptable_max_mmap` auf **`21,474,836,480`**. Diese Werte werden in Byte angegeben.

Diese Parametereinstellungen stellen sicher, dass Ihre temporären Tabellen auf eine kumulative Summe von 22 GiB anwachsen können.

Example 2

Ihre aktuelle Instance-Größe ist 16xlarge oder größer. Sie kennen nicht die Gesamtgröße der temporären Tabellen, die Sie möglicherweise benötigen. Sie möchten bis zu 4 GiB im Arbeitsspeicher und den maximal verfügbaren Speicher auf der Festplatte nutzen können.

Setzen Sie `temptable_max_ram` auf **`4,294,967,296`** und `temptable_max_mmap` auf **`1,099,511,627,776`**. Diese Werte werden in Byte angegeben.

Hier legen Sie `temptable_max_mmap` auf 1 TiB fest, was weniger als der maximale lokale Speicher von 1,2 TiB auf einer Aurora-DB-Instance der Größe 16xlarge ist.

Passen Sie bei einer kleineren Instance-Größe den Wert `temptable_max_mmap` an, damit der verfügbare lokale Arbeitsspeicher nicht vollständig belegt wird. Bei einer 2xlarge-Instance stehen für den lokalen Speicher beispielsweise nur 160 GiB zur Verfügung. Daher empfehlen wir, den Wert auf weniger als 160 GiB einzustellen. Weitere Informationen über den verfügbaren lokalen Speicher für DB-Instance-Größen finden Sie unter Temporäre Speicherlimits für Aurora MySQL.

Vom Benutzer erstellte (explizite) temporäre Tabellen auf Reader-DB-Instances

Sie können explizite temporäre Tabellen erstellen, indem Sie das Schlüsselwort `TEMPORARY` in Ihrer Anweisung `CREATE TABLE` verwenden. Explizite temporäre Tabellen werden auf der Writer-DB-Instance in einem Aurora-DB-Cluster unterstützt. Sie können auch explizite temporäre Tabellen

für Reader DB-Instances verwenden. Die Tabellen können jedoch die Verwendung der InnoDB-Speicher-Engine nicht erzwingen.

Um Fehler beim Erstellen expliziter temporärer Tabellen auf Reader-DB-Instances von Aurora MySQL zu vermeiden, stellen Sie sicher, dass alle `CREATE TEMPORARY TABLE`-Anweisungen mit einer der folgenden Methoden ausgeführt werden:

- Verzichten Sie auf die Angabe der `ENGINE=InnoDB`-Klausel.
- Legen Sie den SQL-Modus nicht auf `NO_ENGINE_SUBSTITUTION` fest.

Fehler bei der Erstellung temporärer Tabellen und Abhilfemaßnahmen

Der Fehler, den Sie erhalten, ist unterschiedlich, je nachdem, ob Sie ein einfache `CREATE TEMPORARY TABLE`-Aussage oder die Variation `CREATE TEMPORARY TABLE AS SELECT` verwenden. Das folgende Beispiel zeigt die Reihenfolge der verschiedenen Typen:

Dieses temporäre Tabellenverhalten gilt nur für schreibgeschützte Instanzen. Dieses erste Beispiel bestätigt, dass es sich um die Art von Instanz handelt, mit der die Sitzung verbunden ist.

```
mysql> select @@innodb_read_only;
+--------------------+
| @@innodb_read_only |
+--------------------+
|                  1 |
+--------------------+
```

Für einfache `CREATE TEMPORARY TABLE`-Anweisungen schlägt die Anweisung fehl, wenn der `NO_ENGINE_SUBSTITUTION`-SQL-Modus aktiviert ist. Wenn `NO_ENGINE_SUBSTITUTION` deaktiviert wird (Standardeinstellung), wird die entsprechende Engine-Ersetzung vorgenommen und die temporäre Tabelle wird erfolgreich erstellt.

```
mysql> set sql_mode = 'NO_ENGINE_SUBSTITUTION';

mysql>  CREATE TEMPORARY TABLE tt2 (id int) ENGINE=InnoDB;
ERROR 3161 (HY000): Storage engine InnoDB is disabled (Table creation is disallowed).

mysql> SET sql_mode = '';

mysql> CREATE TEMPORARY TABLE tt4 (id int) ENGINE=InnoDB;
```

```
mysql> SHOW CREATE TABLE tt4\G
*************************** 1. row ***************************
       Table: tt4
Create Table: CREATE TEMPORARY TABLE `tt4` (
  `id` int DEFAULT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci
```

Für `CREATE TEMPORARY TABLE AS SELECT`-Anweisungen schlägt die Anweisung fehl, wenn der SQL-Modus `NO_ENGINE_SUBSTITUTION` aktiviert ist. Wenn `NO_ENGINE_SUBSTITUTION` deaktiviert wird (Standardeinstellung), wird die entsprechende Engine-Ersetzung vorgenommen und die temporäre Tabelle wird erfolgreich erstellt.

```
mysql> set sql_mode = 'NO_ENGINE_SUBSTITUTION';

mysql> CREATE TEMPORARY TABLE tt1 ENGINE=InnoDB AS SELECT * FROM t1;
ERROR 3161 (HY000): Storage engine InnoDB is disabled (Table creation is disallowed).

mysql> SET sql_mode = '';

mysql> show create table tt3;
+-------+-----------------------------------------------------------+
| Table | Create Table                                              |
+-------+-----------------------------------------------------------+
| tt3   | CREATE TEMPORARY TABLE `tt3` (
  `id` int DEFAULT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci |
+-------+-----------------------------------------------------------+
1 row in set (0.00 sec)
```

Weitere Informationen zu den Speicheraspekten und Leistungsauswirkungen temporärer Tabellen in Aurora-MySQL-Version 3 finden Sie im Blogbeitrag Verwenden der TempTable-Speicher-Engine in Amazon RDS für MySQL und Amazon Aurora MySQL.

Vergleich von Aurora-MySQL-Version 2 und Aurora-MySQL-Version 3

Verwenden Sie Folgendes, um mehr über Änderungen zu erfahren, die Sie beachten sollten, wenn Sie Ihren Aurora-MySQL-Version 2-Cluster auf Version 3 aktualisieren.

Themen

- Funktionsunterschiede zwischen Aurora MySQL Version 2 und 3
- Unterstützung für Instance-Klassen

- Parameteränderungen für Aurora MySQL Version 3
- Statusvariablen.
- Inklusive Sprachänderungen für Aurora MySQL Version 3
- AUTO_INCREMENT-Werte
- Binäre Protokoll-Replikation

Funktionsunterschiede zwischen Aurora MySQL Version 2 und 3

Die folgenden Amazon-Aurora-MySQL-Funktionen werden in Aurora MySQL for MySQL 5.7 unterstützt, in Aurora MySQL for MySQL 8.0 derzeit jedoch nicht.

- Sie können Aurora-MySQL-Version 3 nicht für Aurora Serverless v1-Cluster verwenden. Aurora-MySQL-Version 3 arbeitet mit Aurora Serverless v2.
- Der Labor-Modus gilt nicht für Aurora-MySQL-Version 3. In Aurora-MySQL-Version 3 gibt es keine Labormodusfunktionen. Instant DDL ersetzt die schnelle Online-DDL-Funktion, die früher im Labormodus verfügbar war. Ein Beispiel finden Sie unter Sofortige DDL (Aurora MySQL Version 3).
- Der Abfrage-Cache wird aus der Community MySQL 8.0 und auch aus Aurora MySQL Version 3 entfernt.
- Aurora MySQL Version 3 ist mit der MySQL-Hash-Join-Funktion der Community kompatibel. Die Aurora-spezifische Implementierung von Hash-Joins in Aurora MySQL Version 2 wird nicht verwendet. Informationen zur Verwendung von Hash-Joins mit Aurora-Parallelabfrage finden Sie unterHash-Join für parallele Abfrage-Cluster aktivierenundAurora-MySQL-Hinweiseaus. Allgemeine Nutzungsinformationen zu Hash-Joins finden Sie unterHash Join-OptimierungimMySQL-Referenzhandbuchaus.
- Diemysql.lambda_asyncDie gespeicherte Prozedur, die in Aurora MySQL Version 2 veraltet war, wird in Version 3 entfernt. Verwenden Sie für Version 3 die asynchrone Funktionlambda_asyncStattdessen.
- Der Standardzeichensatz in Aurora MySQL Version 3 istutf8mb4aus. In Aurora MySQL Version 2 war der Standardzeichensatzlatin1aus. Weitere Informationen zu diesem Zeichensatz finden Sie unterDer utf8mb4-Zeichensatz (UTF-8-Unicode-Kodierung mit 4 Bytes)imMySQL-Referenzhandbuchaus.

Einige Aurora MySQL-Funktionen sind für bestimmte Kombinationen von AWS Region und DB-Engine-Version verfügbar. Details hierzu finden Sie unter Unterstützte Funktionen in Amazon Aurora by AWS-Region und der Aurora-DB-Engine.

Unterstützung für Instance-Klassen

Aurora-MySQL-Version 3 unterstützt einen anderen Satz von Instance-Klassen als Aurora-MySQL-Version 2:

- Für größere Instances können Sie die modernen Instance-Klassen wie`db.r5`, `db.r6g` und `db.x2g` verwenden.
- Für kleinere Instances können Sie die modernen Instance-Klassen wie `db.t3` und `db.t4g` verwenden.

> **Note**
>
> Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter Verwendung von T-Instance-Klassen für Entwicklung und Tests.

Die folgenden Instance-Klassen aus Aurora-MySQL-Version 2 sind für Aurora-MySQL-Version 3 nicht verfügbar:

- `db.r4`
- `db.r3`
- `db.t3.small`
- `db.t2`

Überprüfen Sie Ihre Verwaltungsskripte auf CLI-Anweisungen, die DB-Instances von Aurora MySQL erstellen. Hardcode-Instance-Klassennamen, die für Aurora-MySQL-Version 3 nicht verfügbar sind. Ändern Sie ggf. die Namen der Instance-Klasse zu solchen, die Aurora-MySQL-Version 3 unterstützt.

> **Tip**
>
> Verwenden Sie den `describe-orderable-db-instance-options` AWS CLI Befehl, um die Instanzklassen zu überprüfen, die Sie für eine bestimmte Kombination aus Aurora MySQL-Version und AWS Region verwenden können.

Ausführliche Einzelheiten zu Aurora-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.

Parameteränderungen für Aurora MySQL Version 3

Aurora MySQL Version 3 enthält neue Konfigurationsparameter auf Clusterebene und Instanzebene. Aurora MySQL Version 3 entfernt auch einige Parameter, die in Aurora MySQL Version 2 vorhanden waren. Einige Parameternamen werden infolge der Initiative zur inklusiven Sprache geändert. Aus Gründen der Abwärtskompatibilität können Sie die Parameterwerte weiterhin entweder mit den alten Namen oder den neuen Namen abrufen. Sie müssen jedoch die neuen Namen verwenden, um Parameterwerte in einer benutzerdefinierten Parametergruppe anzugeben.

In Aurora MySQL Version 3 ist der Wert des`lower_case_table_names`-Parameter wird zum Zeitpunkt der Erstellung des Clusters dauerhaft festgelegt. Wenn Sie für diese Option einen nicht standardmäßigen Wert verwenden, richten Sie Ihre benutzerdefinierte Parametergruppe Aurora MySQL Version 3 vor dem Upgrade ein. Geben Sie dann die Parametergruppe während des Wiederherstellungsvorgangs „Cluster wiederherstellen“ oder „Snapshot wiederherstellen“ an.

> **Note**
>
> Bei einer auf Aurora MySQL basierenden globalen Aurora-Datenbank können Sie kein direktes Upgrade von Aurora-MySQL-Version 2 zu Version 3 durchführen, wenn der Parameter `lower_case_table_names` aktiviert ist. Verwenden Sie stattdessen die Snapshot-Wiederherstellungsmethode.

In Aurora-MySQL-Version 3 gelten die Parameter `init_connect` und `read_only` nicht für Benutzer, die über die `CONNECTION_ADMIN`-Berechtigung verfügen. Dies schließt den Aurora-Hauptbenutzer ein. Weitere Informationen finden Sie unter Rollenbasiertes Berechtigungsmodell.

Eine Liste aller Aurora-MySQL-Clusterparameter finden Sie unter Parameter auf Cluster-Ebene. Die Tabelle umfasst alle Parameter aus Aurora-MySQL-Version 2 und 3. Die Tabelle enthält Hinweise dazu, welche Parameter in Aurora-MySQL-Version 3 neu sind oder aus Aurora-MySQL-Version 3 entfernt wurden.

Eine vollständige Liste der Aurora-MySQL-Instance-Parameter finden Sie unter Parameter auf Instance-Ebene. Die Tabelle umfasst alle Parameter aus Aurora-MySQL-Version 2 und 3. Die Tabelle enthält Hinweise dazu, welche Parameter in Aurora-MySQL-Version 3 neu sind und welche Parameter aus Aurora-MySQL-Version 3 entfernt wurden. Sie enthält auch Hinweise dazu, welche Parameter in früheren Versionen modifizierbar waren, aber nicht Aurora-MySQL´-Version 3.

Weitere Informationen zu geänderten Parameternamen finden Sie unter Inklusive Sprachänderungen für Aurora MySQL Version 3.

Statusvariablen.

Informationen zu Statusvariablen, die nicht auf Aurora MySQL anwendbar sind, finden Sie unterMySQL-Statusvariablen, die nicht für Aurora MySQL geltenaus.

Inklusive Sprachänderungen für Aurora MySQL Version 3

Aurora MySQL Version 3 ist mit Version 8.0.23 aus der MySQL Community Edition kompatibel. Aurora MySQL Version 3 enthält auch Änderungen von MySQL 8.0.26 in Bezug auf Schlüsselwörter und Systemschemas für inklusive Sprache. Zum Beispiel, das`SHOW REPLICA STATUS`Befehl wird jetzt bevorzugt stattSHOW SLAVE STATUSaus.

Die folgenden CloudWatch Amazon-Metriken haben in Aurora MySQL Version 3 neue Namen.

In Aurora MySQL Version 3 sind nur die neuen Metriknamen verfügbar. Stellen Sie sicher, dass Sie alle Alarme oder andere Automatisierungen aktualisieren, die auf Metriknamen beruhen, wenn Sie auf Aurora MySQL Version 3 aktualisieren.

Alter Name	Neuer Name
`ForwardingMasterDMLLatency`	`ForwardingWriterDMLLatency`
`ForwardingMasterOpenSessions`	`ForwardingWriterOpenSessions`
`AuroraDMLRejectedMasterFull`	`AuroraDMLRejectedWriterFull`
`ForwardingMasterDMLThroughput`	`ForwardingWriterDMLThroughput`

Die folgenden Statusvariablen haben neue Namen in Aurora MySQL Version 3.

Aus Gründen der Kompatibilität können Sie beide Namen in der ersten Version 3 von Aurora MySQL verwenden. Die alten Statusvariablennamen sollen in einer zukünftigen Version entfernt werden.

Name, der entfernt werden soll	Neuer oder bevorzugter Name
`Aurora_fwd_master_dml_stmt_duration`	`Aurora_fwd_writer_dml_stmt_duration`
`Aurora_fwd_master_dml_stmt_count`	`Aurora_fwd_writer_dml_stmt_count`
`Aurora_fwd_master_select_stmt_duration`	`Aurora_fwd_writer_select_stmt_duration`
`Aurora_fwd_master_select_stmt_count`	`Aurora_fwd_writer_select_stmt_count`
`Aurora_fwd_master_errors_session_timeout`	`Aurora_fwd_writer_errors_session_timeout`
`Aurora_fwd_master_open_sessions`	`Aurora_fwd_writer_open_sessions`
`Aurora_fwd_master_errors_session_limit`	`Aurora_fwd_writer_errors_session_limit`
`Aurora_fwd_master_errors_rpc_timeout`	`Aurora_fwd_writer_errors_rpc_timeout`

Die folgenden Konfigurationsparameter haben neue Namen in Aurora MySQL Version 3.

Aus Gründen der Kompatibilität können Sie die Parameterwerte im `mysql`-Client unter Verwendung eines der beiden Namen in der ersten Version 3 von Aurora MySQL prüfen. Beim Ändern der Werte in einer benutzerdefinierten Parametergruppe können Sie nur die neuen Namen verwenden. Die alten Parameternamen werden in einer zukünftigen Version entfernt.

Name, der entfernt werden soll	Neuer oder bevorzugter Name
aurora_fwd_master_idle_timeout	aurora_fwd_writer_idle_timeout
aurora_fwd_master_max_connections_pct	aurora_fwd_writer_max_connections_pct
master_verify_checksum	source_verify_checksum
sync_master_info	sync_source_info
init_slave	init_replica
rpl_stop_slave_timeout	rpl_stop_replica_timeout
log_slow_slave_statements	log_slow_replica_statements
slave_max_allowed_packet	replica_max_allowed_packet
slave_compressed_protocol	replica_compressed_protocol
slave_exec_mode	replica_exec_mode
slave_type_conversions	replica_type_conversions
slave_sql_verify_checksum	replica_sql_verify_checksum
slave_parallel_type	replica_parallel_type
slave_preserve_commit_order	replica_preserve_commit_order

Name, der entfernt werden soll	Neuer oder bevorzugter Name	
log_slave_updates	log_replica_updates	
slave_allow_batching	replica_allow_batching	
slave_load_tmpdir	replica_load_tmpdir	
slave_net_timeout	replica_net_timeout	
sql_slave_skip_counter	sql_replica_skip_counter	
slave_skip_errors	replica_skip_errors	
slave_checkpoint_period	replica_checkpoint_period	
slave_checkpoint_group	replica_checkpoint_group	
slave_transaction_retries	replica_transaction_retries	
slave_parallel_workers	replica_parallel_workers	
slave_pending_jobs_size_max	replica_pending_jobs_size_max	
pseudo_slave_mode	pseudo_replica_mode	

Die folgenden gespeicherten Prozeduren haben neue Namen in Aurora MySQL Version 3.

Aus Gründen der Kompatibilität können Sie beide Namen in der ersten Version 3 von Aurora MySQL verwenden. Die alten Prozedurnamen sollen in einer zukünftigen Version entfernt werden.

Name, der entfernt werden soll	Neuer oder bevorzugter Name	
`mysql.rds_set_master_auto_position`	`mysql.rds_set_source_auto_position`	
`mysql.rds_set_external_master`	`mysql.rds_set_external_source`	
`mysql.rds_set_external_master_with_auto_position`	`mysql.rds_set_external_source_with_auto_position`	
`mysql.rds_reset_external_master`	`mysql.rds_reset_external_source`	
`mysql.rds_next_master_log`	`mysql.rds_next_source_log`	

AUTO_INCREMENT-Werte

In Aurora MySQL Version 3 bewahrt Aurora`AUTO_INCREMENT`Wert für jede Tabelle, wenn jede DB-Instance neu gestartet wird. In Aurora MySQL Version 2 wird`AUTO_INCREMENT`Der Wert wurde nach einem Neustart nicht beibehalten.

Der `AUTO_INCREMENT` Wert bleibt nicht erhalten, wenn Sie einen neuen Cluster einrichten, indem Sie aus einem Snapshot wiederherstellen, eine point-in-time Wiederherstellung durchführen und einen Cluster klonen. In diesen Fällen wird die`AUTO_INCREMENT`value wird basierend auf dem größten Spaltenwert in der Tabelle zum Zeitpunkt der Erstellung des Snapshots auf den Wert initialisiert. Dieses Verhalten ist anders als in RDS für MySQL 8.0, wo der `AUTO_INCREMENT`-Wert während dieser Vorgänge beibehalten wird.

Binäre Protokoll-Replikation

In der MySQL 8.0 Community Edition ist die Replikation des Binärprotokolls standardmäßig aktiviert. In Aurora MySQL Version 3 ist die Replikation des binären Protokolls standardmäßig deaktiviert.

> **Tip**
>
> Wenn Ihre Hochverfügbarkeitsanforderungen durch die integrierten Replikationsfunktionen von Aurora erfüllt werden, können Sie die Replikation von Binärprotokollen deaktiviert lassen. Auf diese Weise können Sie den Leistungsaufwand der Binärprotokollreplikation vermeiden. Sie können auch die zugehörige Überwachung und Fehlerbehebung vermeiden, die für die Verwaltung der Binärprotokollreplikation erforderlich sind.

Aurora unterstützt die Binärprotokollreplikation von einer MySQL 5.7 kompatiblen Quelle zu Aurora MySQL Version 3. Das Quellsystem kann ein Aurora MySQL-DB-Cluster, eine RDS für MySQL-DB-Instance oder eine lokale MySQL-DB-Instance sein.

Wie bei der Community MySQL unterstützt Aurora MySQL die Replikation von einer Quelle, auf der eine bestimmte Version ausgeführt wird, zu einem Ziel, auf dem dieselbe Hauptversion oder eine höhere Hauptversion ausgeführt wird. Beispielsweise wird die Replikation von einem MySQL 5.6 kompatiblen System auf Aurora MySQL Version 3 nicht unterstützt. Die Replikation von Aurora MySQL Version 3 auf ein mit MySQL 5.7 kompatibles oder MySQL 5.6—kompatibles System wird nicht unterstützt. Einzelheiten zur Verwendung der Binärprotokollreplikation finden Sie unterReplizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation)aus.

Aurora MySQL Version 3 enthält Verbesserungen der Binärprotokollreplikation in der Community MySQL 8.0, z. B. gefilterte Replikation. Weitere Informationen zu den Verbesserungen der Community MySQL 8.0 finden Sie unterSo bewerten Server Replikationsfilterregelnim MySQL-Referenzhandbuchaus.

Transaktionskomprimierung für die Binärprotokollreplikation

Informationen zur Verwendung zur Binärprotokollkomprimierung finden Sie unterBinärprotokoll-Transaktionskomprimierungim MySQL-Referenzhandbuch.

Die folgenden Einschränkungen gelten für die Binärprotokollkomprimierung in Aurora-MySQL-Version 3:

- Transaktionen, deren binäre Protokolldaten größer als die maximal zulässige Paketgröße sind, werden nicht komprimiert. Dies gilt unabhängig davon, ob die Einstellung für die Komprimierung des binären Protokolls in Aurora MySQL aktiviert ist. Solche Transaktionen werden repliziert, ohne komprimiert zu werden.

- Wenn Sie einen Konnektor für Change Data Capture (CDC) verwenden, der MySQL 8.0 noch nicht unterstützt, können Sie diese Funktion nicht verwenden. Es wird empfohlen, alle Konnektoren von Drittanbietern gründlich mit der Binärprotokollkomprimierung zu testen. Diese Tests sollten ausgeführt werden, bevor Sie die Binlog-Komprimierung in Systemen aktivieren, die Binlog-Replikation für CDC verwenden.

Vergleich von Aurora-MySQL-Version 3 und MySQL 8.0 Community Edition

Sie können die folgenden Informationen verwenden, um mehr über die Änderungen zu erfahren, die Sie beachten müssen, wenn Sie von einem anderen MySQL 8.0-kompatiblen System zu Aurora-MySQL-Version 3 konvertieren.

Im Allgemeinen unterstützt Aurora MySQL Version 3 den Feature-Set der Community MySQL 8.0.23. Einige neue Funktionen der MySQL 8.0 Community Edition gelten nicht für Aurora MySQL. Einige dieser Funktionen sind mit einigen Aurora-Aspekten, wie der Aurora-Speicherarchitektur, nicht kompatibel. Andere Funktionen sind nicht erforderlich, da der Amazon RDS-Verwaltungsservice gleichwertige Funktionen bietet. Die folgenden Funktionen in der Community MySQL 8.0 werden in Aurora-MySQL-Version 3 nicht unterstützt oder funktionieren anders.

Die Versionshinweise für alle Versionen von Aurora MySQL Version 3 finden Sie unter Aktualisierungen der Datenbank-Engine für Amazon Aurora MySQL Version 3 in den Versionshinweisen für Aurora MySQL.

Themen

MySQL-8.0-Funktionen sind in Aurora-MySQL-Version 3 nicht verfügbar

Die folgenden Funktionen der Community MySQL 8.0 sind in Aurora MySQL Version 3 nicht verfügbar oder funktionieren anders.

- Ressourcengruppen und zugehörige SQL-Anweisungen werden in Aurora MySQL nicht unterstützt.
- Aurora MySQL unterstützt keine benutzerdefinierten Undo-Tablespaces und zugehörige SQL-Anweisungen wie`CREATE UNDO TABLESPACE`, `ALTER UNDO TABLESPACE ... SET INACTIVE` und. `DROP UNDO TABLESPACE`

- Aurora MySQL unterstützt das Rückgängigmachen von Tablespace-Kürzungen für Aurora MySQL-Versionen unter 3.06 nicht. In Aurora MySQL Version 3.06 und höher wird die automatische Undo-Tablespace-Kürzung unterstützt.
- Sie können die Einstellungen von MySQL-Plugins nicht ändern.
- Das X-Plugin wird nicht unterstützt.
- Multisource-Replikation wird nicht unterstützt.

Rollenbasiertes Berechtigungsmodell

Mit Aurora MySQL Version 3 können Sie die Tabellen im`mysql`-Datenbank direkt. Insbesondere können Sie Benutzer nicht einrichten, indem Sie in die`mysql.user`-Tabelle Stattdessen verwenden Sie SQL-Anweisungen, um rollenbasierte Berechtigungen zu gewähren. Sie können auch keine anderen Objekte wie gespeicherte Prozeduren in der `mysql`-Datenbank erstellen. Sie können immer noch die `mysql`-Tabellen abfragen. Wenn Sie die Binärprotokollreplikation verwenden, werden Änderungen direkt am`mysql`Tabellen im Quellcluster werden nicht auf den Zielcluster repliziert.

In einigen Fällen verwendet Ihre Anwendung möglicherweise Verknüpfungen, um Benutzer oder andere Objekte zu erstellen, indem Sie sie in die`mysql`-Tabellen Wenn ja, ändern Sie Ihren Anwendungscode, um die entsprechenden Anweisungen wie `CREATE USER` zu verwenden. Wenn Ihre Anwendung gespeicherte Prozeduren oder andere Objekte in der `mysql`-Datenbank erstellt, verwenden Sie stattdessen eine andere Datenbank.

Um Metadaten für Datenbankbenutzer während der Migration aus einer externen MySQL-Datenbank zu exportieren, können Sie stattdessen einen MySQL-Shell-Befehl verwenden`mysqldump`. Weitere Informationen finden Sie unter Instance Dump Utility, Schema Dump Utility und Table Dump Utility.

Um die Verwaltung von Berechtigungen für viele Benutzer oder Anwendungen zu vereinfachen, können Sie`CREATE ROLE`-Anweisung zum Erstellen einer Rolle mit einer Reihe von Berechtigungen. Dann können Sie die`GRANT`und`SET ROLE`-Anweisungen und die`current_role`Funktion, um Benutzern oder Anwendungen Rollen zuzuweisen, die aktuelle Rolle zu wechseln und zu überprüfen, welche Rollen in Kraft sind. Weitere Informationen zum rollenbasierten Berechtigungssystem in MySQL 8.0 finden Sie unter Verwenden von Rollen im MySQL-Referenzhandbuch.

> **Important**
>
> Wir empfehlen Ihnen, den Hauptbenutzer nicht direkt in Ihren Anwendungen zu verwenden. Bleiben Sie stattdessen bei der bewährten Methode, einen Datenbankbenutzer zu

verwenden, der mit den Mindestberechtigungen erstellt wurde, die für Ihre Anwendung erforderlich sind.

Aurora-MySQL-Version 3 enthält eine spezielle Rolle, die alle folgenden Berechtigungen besitzt. Der Name der Rolle lautet `rds_superuser_role`. Dem primären Administratorbenutzer für jeden Cluster wurde diese Rolle bereits gewährt. Die`rds_superuser_role`enthält die folgenden Berechtigungen für alle Datenbankobjekte:

- `ALTER`
- `APPLICATION_PASSWORD_ADMIN`
- `ALTER ROUTINE`
- `CONNECTION_ADMIN`
- `CREATE`
- `CREATE ROLE`
- `CREATE ROUTINE`
- `CREATE TEMPORARY TABLES`
- `CREATE USER`
- `CREATE VIEW`
- `DELETE`
- `DROP`
- `DROP ROLE`
- `EVENT`
- `EXECUTE`
- `INDEX`
- `INSERT`
- `LOCK TABLES`
- `PROCESS`
- `REFERENCES`
- `RELOAD`
- `REPLICATION CLIENT`

- `REPLICATION SLAVE`
- `ROLE_ADMIN`
- `SET_USER_ID`
- `SELECT`
- `SHOW DATABASES`
- `SHOW_ROUTINE` (Aurora-MySQL-Version 3.04 und höher)
- `SHOW VIEW`
- `TRIGGER`
- `UPDATE`
- `XA_RECOVER_ADMIN`

Die Rollendefinition umfasst auch`WITH GRANT OPTION`damit ein Administratorbenutzer diese Rolle anderen Benutzern gewähren kann. Insbesondere muss der Administrator alle Berechtigungen erteilen, die zur Durchführung der Binärprotokollreplikation mit dem Aurora MySQL-Cluster als Ziel erforderlich sind.

> **Tip**
>
> Um die vollständigen Details der Berechtigungen anzuzeigen, geben Sie die folgenden Anweisungen ein.
>
> ```
> SHOW GRANTS FOR rds_superuser_role@'%';
> SHOW GRANTS FOR name_of_administrative_user_for_your_cluster@'%';
> ```

Aurora MySQL Version 3 enthält auch Rollen, mit denen Sie auf andere AWS Dienste zugreifen können. Sie können diese Rollen als Alternative zu`GRANT`-Anweisungen. Sie geben beispielsweise`GRANT AWS_LAMBDA_ACCESS TO user`INSTEAD OF`GRANT INVOKE LAMBDA ON *.* TO user`aus. Die Verfahren für den Zugriff auf andere AWS Dienste finden Sie unterIntegrieren von Amazon Aurora MySQL in anderen AWS-Services. Aurora MySQL Version 3 umfasst die folgenden Rollen im Zusammenhang mit dem Zugriff auf andere AWS Dienste:

- `AWS_LAMBDA_ACCESS`-Rolle, als Alternative zur`INVOKE LAMBDA`Privilegierte Daten. Weitere Informationen zur Nutzung finden Sie unter Aufrufen einer Lambda-Funktion aus einem Amazon Aurora MySQL-DB-Cluster.

- `AWS_LOAD_S3_ACCESS`-Rolle, als Alternative zur`LOAD FROM S3`Privilegierte Daten. Weitere Informationen zur Nutzung finden Sie unter Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket.
- `AWS_SELECT_S3_ACCESS`-Rolle, als Alternative zur`SELECT INTO S3`Privilegierte Daten. Weitere Informationen zur Nutzung finden Sie unter Speichern von Daten aus einem Amazon Aurora MySQL-DB-Cluster in Textdateien in einem Amazon S3-Bucket.
- `AWS_SAGEMAKER_ACCESS`-Rolle, als Alternative zur`INVOKE SAGEMAKER`Privilegierte Daten. Weitere Informationen zur Nutzung finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.
- `AWS_COMPREHEND_ACCESS`-Rolle, als Alternative zur`INVOKE COMPREHEND`Privilegierte Daten. Weitere Informationen zur Nutzung finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.

Wenn Sie Zugriff mithilfe von Rollen in Aurora MySQL Version 3 gewähren, aktivieren Sie die Rolle auch mithilfe der`SET ROLE` *`role_name`*oder`SET ROLE ALL`statement. Im folgenden Beispiel wird gezeigt, wie dies geschieht. Ersetzen Sie den entsprechenden Rollennamen für `AWS_SELECT_S3_ACCESS`.

```
# Grant role to user.
mysql> GRANT AWS_SELECT_S3_ACCESS TO 'user'@'domain-or-ip-address'

# Check the current roles for your user. In this case, the AWS_SELECT_S3_ACCESS role
 has not been activated.
# Only the rds_superuser_role is currently in effect.
mysql> SELECT CURRENT_ROLE();
+--------------------------+
| CURRENT_ROLE()           |
+--------------------------+
| `rds_superuser_role`@`%` |
+--------------------------+
1 row in set (0.00 sec)

# Activate all roles associated with this user using SET ROLE.
# You can activate specific roles or all roles.
# In this case, the user only has 2 roles, so we specify ALL.
mysql> SET ROLE ALL;
Query OK, 0 rows affected (0.00 sec)

# Verify role is now active
```

```
mysql> SELECT CURRENT_ROLE();
+-------------------------------------------------+
| CURRENT_ROLE()                                  |
+-------------------------------------------------+
| `AWS_SELECT_S3_ACCESS`@`%`,`rds_superuser_role`@`%` |
+-------------------------------------------------+
```

Authentifizierung

In Community MySQL 8.0 ist das Standard-Authentifizierungs-Plugin `caching_sha2_password`. Aurora MySQL Version 3 verwendet immer noch`mysql_native_password`-Plugin. Sie können die `default_authentication_plugin`-Einstellung nicht ändern.

Upgrade auf Aurora MySQL Version 3

Informationen zum Upgrade Ihrer Datenbank von Aurora MySQL Version 2 auf Version 3 finden Sie unter[Aktualisieren der Hauptversion eines DB-Clusters von Amazon Aurora MySQL](#).

Aurora-MySQL-Version 2, kompatibel mit MySQL 5.7

In diesem Thema werden die Unterschiede zwischen Aurora-MySQL-Version 2 und MySQL 5.7 Community Edition beschrieben.

In Aurora-MySQL-Version 2 nicht unterstützte Funktionen

Die folgenden Funktionen werden in MySQL 5.7 unterstützt, in Aurora MySQL Version 2 derzeit jedoch nicht:

- `CREATE TABLESPACE`-SQL-Anweisung
- Plugin für die Gruppenreplikation
- Größere Seitengröße
- Laden des InnoDB-Pufferpools beim Starten
- Plugin für den InnoDB-Volltext-Parser
- Replikation aus mehreren Quellen
- Größenanpassung des Online-Pufferpools
- Plugin zur Passwortüberprüfung – Sie können das Plugin installieren, es wird jedoch nicht unterstützt. Sie können das Plugin nicht anpassen.
- Plugins für die Umformulierung von Abfragen

- Replikationsfilter
- X Protocol

Weitere Informationen über diese Funktionen finden Sie in der MySQL 5.7 Dokumentation.

Temporäres Tabellenverhalten in Aurora-MySQL-Version 2

In MySQL 5.7 wird der temporäre Tabellenbereich automatisch erweitert und vergrößert sich nach Bedarf, um temporäre Tabellen auf der Festplatte unterzubringen. Wenn temporäre Tabellen gelöscht werden, kann der freigewordene Speicherplatz für neue temporäre Tabellen wiederverwendet werden, der temporäre Tabellenbereich behält jedoch die erweiterte Größe bei und wird nicht verkleinert. Der temporäre Tabellenbereich wird gelöscht und neu erstellt, wenn die Engine neu gestartet wird.

In Aurora MySQL Version 2 gilt das folgende Verhalten:

- Bei neuen DB-Clustern von Aurora MySQL, die mit Version 2.10 und höher erstellt wurden, wird der temporäre Tabellenbereich entfernt und neu erstellt, wenn Sie die Datenbank neu starten. Dadurch kann die Funktion zur dynamischen Größenanpassung Speicherplatz zurückgewinnen.
- Bei bestehenden DB-Clustern von Aurora MySQL, die auf folgende Versionen aktualisiert wurden:
  - Version 2.10 oder höher – Der temporäre Tabellenbereich wird entfernt und neu erstellt, wenn Sie die Datenbank neu starten. Dadurch kann die Funktion zur dynamischen Größenanpassung Speicherplatz zurückgewinnen.
  - Version 2.09 – Der temporäre Tabellenbereich wird nicht entfernt, wenn Sie die Datenbank neu starten.

Sie können die Größe des temporären Tabellenbereichs auf Ihrem DB-Cluster von Aurora MySQL Version 2 mithilfe der folgenden Abfrage überprüfen:

```
SELECT
    FILE_NAME,
    TABLESPACE_NAME,
    ROUND((TOTAL_EXTENTS * EXTENT_SIZE) / 1024 / 1024 / 1024, 4) AS SIZE
FROM
    INFORMATION_SCHEMA.FILES
WHERE
    TABLESPACE_NAME = 'innodb_temporary';
```

Weitere Informationen finden Sie unter Der temporäre Tabellenbereich in der MySQL-Dokumentation.

Speicher-Engine für temporäre Tabellen auf der Festplatte

Aurora MySQL Version 2 verwendet je nach Rolle der Instance unterschiedliche Speicher-Engines für interne temporäre Tabellen auf der Festplatte.

- Auf der Writer-Instance verwenden temporäre Tabellen auf der Festplatte standardmäßig die InnoDB-Speicher-Engine. Sie sind im temporären Tabellenbereich im Aurora-Cluster-Volume gespeichert.

  Sie können dieses Verhalten auf der Writer-Instance ändern, indem Sie den Wert für den DB-Parameter `internal_tmp_disk_storage_engine` ändern. Weitere Informationen finden Sie unter Parameter auf Instance-Ebene.
- Auf Reader-Instances nutzen temporäre Tabellen auf der Festplatte die MyISAM-Speicher-Engine, die lokalen Speicher verwendet. Dies liegt daran, dass schreibgeschützte Instances keine Daten auf dem Aurora-Cluster-Volume speichern können.

Sicherheit in Amazon Aurora MySQL

Die Sicherheit für Amazon Aurora MySQL wird auf drei Ebenen verwaltet:

- Um zu kontrollieren, wer Amazon RDS-Managementaktionen auf Aurora MySQL-DB-Clustern und DB-Instances ausführen kann, verwenden Sie AWS Identity and Access Management (IAM). Wenn Sie AWS mithilfe von IAM-Anmeldeinformationen eine Verbindung herstellen, muss Ihr AWS Konto über IAM-Richtlinien verfügen, die die für die Durchführung von Amazon RDS-Verwaltungsvorgängen erforderlichen Berechtigungen gewähren. Weitere Informationen finden Sie unter Identity and Access Management für Amazon Aurora.

  Wenn Sie IAM für den Zugriff auf die Amazon RDS-Konsole verwenden, stellen Sie sicher, dass Sie sich zuerst AWS Management Console mit Ihren IAM-Benutzeranmeldedaten bei der anmelden. Öffnen Sie dann die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

- Stellen Sie sicher, dass Sie Aurora-MySQL-DB-Cluster in einer Virtual Public Cloud (VPC) basierend auf dem Amazon-VPC-Service erstellen. Mithilfe einer VPC-Sicherheitsgruppe können Sie steuern, welche Geräte und Amazon-EC2-Instances Verbindungen zum Endpunkt und Port der DB-Instance für Aurora MySQL-DB-Cluster in einer VPC herstellen können. Diese Endpunkt- und Portverbindungen können mithilfe von Transport Layer Security (TLS) erstellt werden. Zusätzlich können Firewall-Regeln in Ihrem Unternehmen steuern, ob in Ihrem Unternehmen verwendete Geräte Verbindungen mit einer DB-Instance herstellen dürfen. Weitere Informationen zu VPCs finden Sie unter Amazon VPCs und Amazon Aurora.

  Die unterstützte VPC-Tenancy hängt von der DB-Instance-Klasse ab, die von Ihren Aurora MySQL DB-Clustern verwendet wird. Mit `default`-VPC-Tenancy, the VPC läuft der VPC auf gemeinsam genutzter Hardware. Mit der `dedicated`-VPC-Tenancy läuft die VPC auf einer dedizierten Hardware-Instance. Die DB-Instance-Klassen mit Spitzenlastleistung unterstützen nur die Standard-VPC-Tenancy. Die Burstable-Performance-DB-Instance-Klassen umfassen die DB-Instanzklassen db.t2, db.t3 und db.t4g. Alle anderen Aurora MySQL DB-Instance-Klassen unterstützen sowohl die Standard- als auch die dedizierte VPC-Mieterschaft.

  > **Note**
  >
  > Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter Verwendung von T-Instance-Klassen für Entwicklung und Tests.

Weitere Informationen zu Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen. Weitere Informationen über die `default`- und `dedicated`-VPC-Tenancy finden Sie unter Dedicated Instances im Amazon Elastic Compute Cloud-Benutzerhandbuch.

- Sie können eine der folgenden Anweisungen, oder eine Kombination davon, befolgen, um die Anmeldung und die Berechtigungen für ein Amazon Aurora MySQL-DB-Cluster zu bestätigen:
  - Sie können denselben Ansatz wie mit einer Stand-Alone Instance in MySQL wählen.

    Befehle wie `CREATE USER`, `RENAME USER`, `GRANT`, `REVOKE` und `SET PASSWORD` funktionieren genau wie auf lokalen Datenbanken, so wie auch das direkte Ändern von Datenbank-Schema-Tabellen. Weitere Informationen finden Sie unter Access Control and Account Management in der MySQL-Dokumentation.
  - Sie können auch die IAM-Datenbank-Authentifizierung verwenden.

    Mit der IAM-Datenbank-Authentifizierung können Sie mithilfe eines IAM-Benutzers, einer IAM-Rolle oder eines Authentifizierungstokens Ihr DB-Cluster bestätigen. Ein Authentifizierungstoken ist ein eindeutiger Wert, der mithilfe des Signatur-Version 4-Signiervorgangs erstellt wird. Mithilfe der IAM-Datenbankauthentifizierung können Sie dieselben Anmeldeinformationen verwenden, um den Zugriff auf Ihre AWS Ressourcen und Datenbanken zu kontrollieren. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung.

> **Note**
>
> Weitere Informationen finden Sie unter Sicherheit in Amazon Aurora.

Berechtigungen von Masterbenutzerkonten mit Amazon Aurora MySQL.

Wenn Sie eine DB-Instance von Amazon Aurora MySQL erstellen, verfügt der Hauptbenutzer standardmäßig über die Berechtigungen, die unter Berechtigungen von Hauptbenutzerkonten aufgeführt sind.

Um Verwaltungsservices für jeden DB-Cluster bereitzustellen, werden die `admin`- und `rdsadmin`-Benutzer erstellt, wenn der DB-Cluster erstellt wird. Ein Versuch, das Passwort auszulassen oder umzubenennen, oder Berechtigungen für das `rdsadmin` Konto zu ändern, führt zu einem Fehler.

In Aurora-MySQL-Version 2-DB-Clustern werden die `admin`- und `rdsadmin`-Benutzer erstellt, wenn der DB-Cluster erstellt wird. In Aurora-MySQL-Version 3-Clustern werden die `admin`-, `rdsadmin` und `rds_superuser_role`-Benutzer erstellt.

> **Important**
>
> Wir empfehlen Ihnen, den Hauptbenutzer nicht direkt in Ihren Anwendungen zu verwenden. Bleiben Sie stattdessen bei der bewährten Methode, einen Datenbankbenutzer zu verwenden, der mit den Mindestberechtigungen erstellt wurde, die für Ihre Anwendung erforderlich sind.

Für die Verwaltung des Aurora MySQL-DB-Clusters wurden die Standardbefehle `kill` und `kill_query` eingeschränkt. Verwenden Sie stattdessen die Amazon RDS-Befehle `rds_kill` und `rds_kill_query`, um Benutzersitzungen oder Abfragen in Ihren Aurora MySQL-DB-Instances zu beenden.

> **Note**
>
> Die Verschlüsselung einer Datenbank-Instance und von Snapshots wird für die Region China (Ningxia) nicht unterstützt.

Verwenden von TLS mit DB-Clustern von Aurora MySQL

DB-Cluster von Amazon Aurora MySQL unterstützen Transport Layer Security (TLS)-Verbindungen von Anwendungen mithilfe des gleichen Prozesses und öffentlichen Aktivierungsschlüssels wie DB-Instances von RDS für MySQL.

Amazon RDS erstellt ein TLS-Zertifikat und installiert das Zertifikat auf der DB-Instance, wenn Amazon RDS die Instance bereitstellt. Diese Zertifikate werden von einer Zertifizierungsstelle signiert. Das TLS-Zertifikat enthält den DB-Instance-Endpunkt als allgemeinen Namen (Common Name, CN) für das TLS-Zertifikat, um gegen Spoofing-Angriffe zu schützen. Dadurch können Sie nur den DB-Cluster-Endpunkt verwenden, um sich mit einem DB-Cluster mithilfe von TLS zu verbinden, wenn Ihr Client SAN (Subject Alternative Names) unterstützt. Andernfalls müssen Sie den Instance-Endpunkt einer Writer-Instance verwenden.

Informationen zum Herunterladen von Zertifikaten finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

Wir empfehlen den AWS JDBC-Treiber als Client, der SAN mit TLS unterstützt. Weitere Informationen zum AWS JDBC-Treiber und vollständige Anweisungen zu seiner Verwendung finden Sie im Amazon Web Services (AWS) JDBC-Treiber-Repository. GitHub

Themen

- Anfordern einer TLS-Verbindung mit einem DB-Cluster von Aurora MySQL
- TLS-Versionen für Aurora MySQL
- Konfigurieren von Cipher-Suites für Verbindungen mit Aurora-MySQL-DB-Clustern
- Verschlüsseln von Verbindungen zu einem Aurora MySQL-DB-Cluster

Anfordern einer TLS-Verbindung mit einem DB-Cluster von Aurora MySQL

Mit dem DB-Clusterparameter `require_secure_transport` können Sie es erforderlich machen, dass Benutzerverbindungen mit Ihrem DB-Cluster von Aurora MySQL TLS verwenden. Standardmäßig ist der `require_secure_transport`-Parameter auf `OFF` festgelegt. Sie können den Parameter `require_secure_transport` auf `ON` festlegen und damit erforderlich machen, dass Verbindungen mit Ihrem DB-Cluster TLS verwenden.

Sie können den Parameterwert `require_secure_transport` festlegen, indem Sie die Parametergruppe für Ihren DB-Cluster aktualisieren. Sie müssen Ihren DB-Cluster nicht neu starten, damit die Änderung wirksam wird. Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

> **Note**
>
> Der Parameter `require_secure_transport` ist nur für Aurora-MySQL-Version 2 und 3 verfügbar. Sie können diesen Parameter in einer benutzerdefinierten DB-Cluster-Parametergruppe festlegen. Der Parameter ist in DB-Instance-Parametergruppen nicht verfügbar.

Wenn der Parameter `require_secure_transport` für einen DB-Cluster auf `ON` festgelegt ist, kann ein Datenbankclient eine Verbindung zu ihm herstellen, wenn er eine verschlüsselte Verbindung herstellen kann. Andernfalls wird eine Fehlermeldung ähnlich der folgenden an den Client zurückgegeben:

```
MySQL Error 3159 (HY000): Connections using insecure transport are prohibited while --
require_secure_transport=ON.
```

TLS-Versionen für Aurora MySQL

Aurora MySQL unterstützt die Transport Layer Security (TLS)-Versionen 1.0, 1.1, 1.2 und 1.3. Ab Aurora-MySQL-Version 3.04.0 und höher können Sie das TLS-1.3-Protokoll verwenden, um Ihre Verbindungen zu schützen. In der folgenden Tabelle wird die TLS-Unterstützung für Aurora MySQL-Versionen gezeigt.

Aurora MySQL Version	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	Standard
Aurora-MySQL-Version 2	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt	Alle unterstützten TLS-Versionen
Aurora MySQL Version 3 (unter 3.04.0)	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt	Alle unterstützten TLS-Versionen
Aurora MySQL Version 3 (3.04.0 und höher)	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt	Alle unterstützten TLS-Versionen

Important

Wenn Sie benutzerdefinierte Parametergruppen für Ihre Aurora-MySQL-Cluster mit Version 2 und Versionen vor 3.04.0 verwenden, empfehlen wir die Verwendung von TLS 1.2, da TLS 1.0 und 1.1 weniger sicher sind. In der Community-Edition von MySQL 8.0.26 und Aurora MySQL 3.03 und ihren Unterversionen wurde die Unterstützung für die TLS-Versionen 1.1 und 1.0 eingestellt.

Die Community-Edition von MySQL 8.0.28 und die kompatiblen Aurora-MySQL-Versionen 3.04.0 und höher unterstützen TLS 1.1 und TLS 1.0 nicht. Wenn Sie Aurora-MySQL-Versionen 3.04.0 und höher verwenden, legen Sie das TLS-Protokoll in Ihrer benutzerdefinierten Parametergruppe nicht auf 1.0 oder 1.1 fest.
Für Aurora-MySQL-Versionen 3.04.0 und höher ist die Standardeinstellung TLS 1.3 und TLS 1.2.

Sie können den DB-Cluster-Parameter `tls_version` zur Angabe der zulässigen Protokollversionen verwenden. Vergleichbare Clientparameter sind für die meisten Client-Tools oder Datenbanktreiber verfügbar. Einige ältere Clients unterstützen möglicherweise keine neueren TLS-Versionen. Standardmäßig versucht der DB-Cluster, die höchste TLS-Protokollversion zu verwenden, die sowohl von der Server- als auch von der Clientkonfiguration zugelassen wird.

Legen Sie den `tls_version`-DB-Cluster-Parameter auf einen der folgenden Werte fest:

- `TLSv1.3`
- `TLSv1.2`
- `TLSv1.1`
- `TLSv1`

Sie können auch den Parameter `tls_version` auch als Zeichenfolge einer durch Kommas getrennten Liste einstellen. Wenn Sie sowohl die Protokolle TLS 1.2 als auch TLS 1.0 verwenden möchten, muss der Parameer `tls_version` alle Protokolle vom niedrigsten bis zum höchsten enthalten. In diesem Fall ist `tls_version` eingestellt als:

```
tls_version=TLSv1,TLSv1.1,TLSv1.2
```

Weitere Informationen zum Ändern von Parametern in einer DB-Cluster-Parametergruppe finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe. Wenn Sie AWS CLI den `tls_version` DB-Cluster-Parameter ändern, `ApplyMethod` muss der auf gesetzt sein`pending-reboot`. Wenn die Anwendungsmethode `pending-reboot` ist, werden Änderungen an Parametern angewendet, nachdem Sie die der Parametergruppe zugeordneten DB-Cluster gestoppt und neu gestartet haben.

Konfigurieren von Cipher-Suites für Verbindungen mit Aurora-MySQL-DB-Clustern

Durch die Verwendung von konfigurierbaren Chiffrier-Suiten können Sie mehr Kontrolle über die Sicherheit Ihrer Datenbankverbindungen haben. Sie können eine Liste von Verschlüsselungssammlungen angeben, die Sie zum Sichern von TLS-Verbindungen mit Ihrer Datenbank des Clients zulassen möchten. Mit konfigurierbaren Chiffrier-Suiten können Sie die Verbindungsverschlüsselung steuern, die Ihr Datenbankserver akzeptiert. Dadurch wird verhindert, dass unsichere oder veraltete Chiffren verwendet werden.

Konfigurierbare Verschlüsselungssuites werden in Aurora-MySQL-Version 3 und Aurora-MySQL-Version 2 unterstützt. Um die Liste der zulässigen Verschlüsselungsverfahren TLS 1.2, TLS 1.1, TLS 1.0 für die Verschlüsselung von Verbindungen anzugeben, ändern Sie den Cluster-Parameter `ssl_cipher`. Legen Sie den Wert für `ssl_cipher`-Parameter in einer Cluster-Parametergruppe mithilfe der AWS Management Console, der AWS CLI oder der RDS-API fest.

Legen Sie den Parameter `ssl_cipher` auf eine Zeichenfolge von kommagetrennten Verschlüsselungswerten für Ihre TLS-Version fest. Für die Clientanwendung können Sie die Chiffren angeben, die für verschlüsselte Verbindungen verwendet werden sollen, indem Sie beim Herstellen der Verbindung mit einer Datenbank die Option `--ssl-cipher` verwenden. Weitere Information zur Herstellung einer Verbindung mit Ihrer Datenbank finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora MySQL-DB-Cluster.

Ab Aurora-MySQL-Version 3.04.0 und höher können Sie TLS-1.3-Verschlüsselungssuiten angeben. Um die zulässigen TLS-1.3-Verschlüsselungssuites zu spezifizieren, ändern Sie den Parameter `tls_ciphersuites` in Ihrer Parametergruppe. TLS 1.3 hat die Anzahl der verfügbaren Verschlüsselungssuites reduziert, da die Benennungskonvention geändert wurde, wodurch der Schlüsselaustauschmechanismus und das verwendete Zertifikat entfernt werden. Legen Sie den Wert für `tls_ciphersuites` auf eine Zeichenfolge von kommagetrennten Verschlüsselungswerten für TLS 1.3 fest.

Die folgende Tabelle zeigt die unterstützten Chiffren zusammen mit dem TLS-Verschlüsselungsprotokoll und gültigen Aurora-MySQL-Engine-Versionen für jede Chiffre.

Verschlüsselungsverfahren	Verschlüsselungsprotokoll	Unterstützte Aurora-MySQL-Versionen
`DHE-RSA-AES128-SHA`	TLS 1.0	3.01.0 und höher, alle unter 2.11.0

Verschlüsselungsverfahren	Verschlüsselungsprotokoll	Unterstützte Aurora-MySQL-Versionen
DHE-RSA-AES128-SHA256	TLS 1.2	3.01.0 und höher, alle unter 2.11.0
DHE-RSA-AES128-GCM-SHA256	TLS 1.2	3.01.0 und höher, alle unter 2.11.0
DHE-RSA-AES256-SHA	TLS 1.0	3.03.0 und niedriger, alle unter 2.11.0
DHE-RSA-AES256-SHA256	TLS 1.2	3.01.0 und höher, alle unter 2.11.0
DHE-RSA-AES256-GCM-SHA384	TLS 1.2	3.01.0 und höher, alle unter 2.11.0
ECDHE-RSA-AES128-SHA	TLS 1.0	3.01.0 und höher, 2.09.3 und höher, 2.10.2 und höher
ECDHE-RSA-AES128-SHA256	TLS 1.2	3.01.0 und höher, 2.09.3 und höher, 2.10.2 und höher
ECDHE-RSA-AES128-GCM-SHA256	TLS 1.2	3.01.0 und höher, 2.09.3 und höher, 2.10.2 und höher
ECDHE-RSA-AES256-SHA	TLS 1.0	3.01.0 und höher, 2.09.3 und höher, 2.10.2 und höher
ECDHE-RSA-AES256-SHA384	TLS 1.2	3.01.0 und höher, 2.09.3 und höher, 2.10.2 und höher
ECDHE-RSA-AES256-GCM-SHA384	TLS 1.2	3.01.0 und höher, 2.09.3 und höher, 2.10.2 und höher
TLS_AES_128_GCM_SHA256	TLS 1.3	3.04.0 und höher

Verschlüsselungsverfahren	Verschlüsselungsprotokoll	Unterstützte Aurora-MySQL-Versionen
TLS_AES_256_GCM_SHA384	TLS 1.3	3.04.0 und höher
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	3.04.0 und höher

> **Note**
>
> DHE-RSA-Verschlüsselungen werden nur von Aurora-MySQL-Versionen vor 2.11.0 unterstützt. Versionen 2.11.0 und höher unterstützen nur ECDHE-Verschlüsselungen.

Weitere Informationen zum Ändern von Parametern in einer DB-Cluster-Parametergruppe finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe. Wenn Sie die CLI verwenden, um den DB-Cluster-Parameter `ssl_cipher` zu ändern, stellen Sie sicher, dass Sie die `ApplyMethod` auf `pending-reboot` festlegen. Wenn die Anwendungsmethode `pending-reboot` ist, werden Änderungen an Parametern angewendet, nachdem Sie die der Parametergruppe zugeordneten DB-Cluster gestoppt und neu gestartet haben.

Sie können auch den CLI-Befehl describe-engine-default-cluster-parameters verwenden, um zu ermitteln, welche Cipher Suites derzeit für eine bestimmte Parametergruppenfamilie unterstützt werden. Im folgenden Beispiel wird veranschaulicht, wie Sie die zulässigen Werte für `ssl_cipher`-Cluster-Parameter für Aurora-MySQL-Version 2 abrufen.

```
aws rds describe-engine-default-cluster-parameters --db-parameter-group-family aurora-
mysql5.7

        ...some output truncated...
 {
  "ParameterName": "ssl_cipher",
  "ParameterValue": "DHE-RSA-AES128-SHA,DHE-RSA-AES128-SHA256,DHE-RSA-AES128-GCM-
SHA256,DHE-RSA-AES256-SHA,DHE-RSA-AES256-SHA256,DHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-
AES128-SHA,ECDHE-RSA-AES128-SHA256,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES256-
SHA,ECDHE-RSA-AES256-SHA384,ECDHE-RSA-AES256-GCM-SHA384",
  "Description": "The list of permissible ciphers for connection encryption.",
  "Source": "system",
```

```
  "ApplyType": "static",
  "DataType": "list",
  "AllowedValues": "DHE-RSA-AES128-SHA,DHE-RSA-AES128-SHA256,DHE-RSA-AES128-GCM-
SHA256,DHE-RSA-AES256-SHA,DHE-RSA-AES256-SHA256,DHE-RSA-AES256-GCM-SHA384,ECDHE-
RSA-AES128-SHA,ECDHE-RSA-AES128-SHA256,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES256-
SHA,ECDHE-RSA-AES256-SHA384,ECDHE-RSA-AES256-GCM-SHA384",
  "IsModifiable": true,
  "SupportedEngineModes": [
   "provisioned"
  ]
 },
       ...some output truncated...
```

Weitere Informationen zu Chiffren finden Sie in der ssl_cipher-Variablen in der MySQL-Dokumentation. Weitere Informationen zu Chiffrier-Suite-Formaten finden Sie unter openssl-ciphers list format und openssl-ciphers string format-Dokumentation auf der OpenSSL-Website.

Verschlüsseln von Verbindungen zu einem Aurora MySQL-DB-Cluster

Um die vom Standard-`mysql`-Client verwendeten Verbindungen zu verschlüsseln, starten Sie den mysql-Client mithilfe des Parameters `--ssl-ca`, um auf den öffentlichen Schlüssel zu verweisen, beispielsweise:

Für MySQL 5.7 und 8.0:

```
mysql -h myinstance.123456789012.rds-us-east-1.amazonaws.com
--ssl-ca=full_path_to_CA_certificate --ssl-mode=VERIFY_IDENTITY
```

Für MySQL 5.6:

```
mysql -h myinstance.123456789012.rds-us-east-1.amazonaws.com
--ssl-ca=full_path_to_CA_certificate --ssl-verify-server-cert
```

Ersetzen Sie *`full_path_to_CA_certificate`* mit dem vollständigen Pfad zum Zertifikat Ihrer Zertifizierungsstelle (CA). Informationen zum Herunterladen von Zertifikaten finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

Sie können TLS-Verbindungen für bestimmte Benutzerkonten anfordern. Verwenden Sie beispielsweise eine der folgenden Anweisungen – abhängig von Ihrer MySQL-Version – um /TLS-Verbindungen für das Benutzerkonto `encrypted_user` erforderlich zu machen.

Für MySQL 5.7 und 8.0:

```
ALTER USER 'encrypted_user'@'%' REQUIRE SSL;
```

Für MySQL 5.6:

```
GRANT USAGE ON *.* TO 'encrypted_user'@'%' REQUIRE SSL;
```

Wenn Sie einen RDS-Proxy verwenden, stellen Sie eine Verbindung mit dem Proxyendpunkt anstelle des üblichen Cluster-Endpunkts her. Sie können SSL/TLS für Verbindungen mit dem Proxy auf die gleiche Weise wie für Verbindungen direkt mit dem Aurora-DB-Cluster als erforderlich oder optional festlegen. Informationen zur Verwendung von RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

> **Note**
>
> Weitere Informationen zu TLS-Verbindungen mit MySQL finden Sie in der MySQL-Dokumentation.

Aktualisieren von Anwendungen, um Verbindungen mit DB-Clustern von Aurora MySQL mithilfe neuer TLS-Zertifikate herzustellen

Am 13. Januar 2023 veröffentlichte Amazon RDS neue Zertifizierungsstellen-Zertifikate (Certificate Authority, CA) zum Herstellen von Verbindungen mit Ihren Aurora-DB-Clustern mithilfe von Transport Layer Security (TLS). Im Folgenden finden Sie Informationen dazu, wie Sie Ihre Anwendungen aktualisieren, um die neuen Zertifikate verwenden zu können.

In diesem Thema finden Sie Informationen dazu, wie Sie ermitteln, ob Client-Anwendungen für die Herstellung von Verbindungen mit Ihren DB-Clustern TLS verwenden. Wenn dies der Fall ist, können Sie weiter überprüfen, ob diese Anwendungen zur Herstellung von Verbindungen Zertifikatverifizierungen erfordern.

> **Note**
>
> Einige Anwendungen sind so konfiguriert, dass sie nur dann Verbindungen mit Aurora MySQL-DB-Clustern herstellen, wenn sie das Zertifikat auf dem Server erfolgreich identifizieren können.
> Für solche Anwendungen müssen Sie die Trust Stores Ihrer Client-Anwendung aktualisieren, damit diese die neuen CA-Zertifikate enthalten.

Nach der Aktualisierung der CA-Zertifikate in den Trust Stores Ihrer Client-Anwendungen können Sie die Zertifikate auf Ihren DB-Clustern rotieren. Es wird nachdrücklich empfohlen, diese Verfahren vor der Implementierung in Produktionsumgebungen in einer Entwicklungs- oder Testumgebung zu testen.

Weitere Informationen zur Zertifikatrotation finden Sie unter Rotieren Ihrer SSL/TLS-Zertifikate. Weitere Informationen zum Herunterladen von Zertifikaten finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer . Informationen zum Verwenden von TLS mit DB-Clustern von Aurora MySQL finden Sie unter Verwenden von TLS mit DB-Clustern von Aurora MySQL.

Themen

- Ermitteln, ob ein Client zum Herstellen von Verbindungen Zertifikatverifizierungen erfordert
- Aktualisieren des Trust Stores Ihrer Anwendung
- Java-Beispielcode für die Herstellung von TLS-Verbindungen

Ermitteln, ob Anwendungen Verbindungen mit Ihrem DB-Cluster von Aurora MySQL mithilfe von TLS herstellen

Wenn Sie Aurora MySQL Version 2 verwenden (kompatibel mit MySQL 5.7) und das Performance-Schema aktiviert ist, können Sie die folgende Abfrage ausführen, um zu prüfen, ob Verbindungen TLS verwenden. Informationen zum Aktivieren des Performance-Schemas finden Sie unter Performance Schema Quick Start in der MySQL-Dokumentation.

```
mysql> SELECT id, user, host, connection_type
       FROM performance_schema.threads pst
       INNER JOIN information_schema.processlist isp
       ON pst.processlist_id = isp.id;
```

In dieser Beispielausgabe können Sie sehen, dass sowohl Ihre eigene Sitzung (`admin`), als auch eine als `webapp1` angemeldete Anwendung TLS verwenden.

```
+----+-----------------+------------------+-----------------+
| id | user            | host             | connection_type |
+----+-----------------+------------------+-----------------+
|  8 | admin           | 10.0.4.249:42590 | SSL/TLS         |
|  4 | event_scheduler | localhost        | NULL            |
| 10 | webapp1         | 159.28.1.1:42189 | SSL/TLS         |
+----+-----------------+------------------+-----------------+
3 rows in set (0.00 sec)
```

Ermitteln, ob ein Client zum Herstellen von Verbindungen Zertifikatverifizierungen erfordert

Sie können überprüfen, ob JDBC-Clients und MySQL-Clients zum Herstellen von Verbindungen Zertifikatverifizierungen erfordern.

JDBC

Das folgende Beispiel mit MySQL Connector/J 8.0 zeigt eine Möglichkeit, wie Sie die JDBC-Verbindungseigenschaften einer Anwendung überprüfen können, um zu ermitteln, ob zum erfolgreichen Herstellen von Verbindungen ein gültiges Zertifikat benötigt wird. Weitere Informationen zu allen JDBC-Verbindungsoptionen für MySQL finden Sie unter Configuration Properties in der MySQL-Dokumentation.

Wenn MySQL Connector/J 8.0 verwendet wird, erfordert eine TLS-Verbindung die Verifizierung anhand des CA-Serverzertifikats, wenn in den Verbindungseigenschaften `sslMode` auf `VERIFY_CA` oder `VERIFY_IDENTITY` festgelegt ist, wie im folgenden Beispiel gezeigt.

```
Properties properties = new Properties();
properties.setProperty("sslMode", "VERIFY_IDENTITY");
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);
```

> **Note**
>
> Wenn Sie entweder den MySQL Java Connector v5.1.38 oder höher oder den MySQL Java Connector v8.0.9 oder höher verwenden, um eine Verbindung mit Ihren Datenbanken herzustellen, verwenden diese Clienttreiber selbst dann standardmäßig TLS, wenn Sie Ihre Anwendungen nicht explizit zur Verwendung von TLS beim Verbinden mit Ihren Datenbanken konfiguriert haben. Darüber hinaus führen sie bei Verwendung von TLS eine teilweise Zertifikatüberprüfung durch und stellen keine Verbindung her, wenn das Datenbankserverzertifikat abgelaufen ist.

MySQL

Die folgenden Beispiele mit dem MySQL-Client zeigen zwei Möglichkeiten, wie Sie die MySQL-Verbindung eines Skripts überprüfen, um zu ermitteln, ob zum Herstellen von Verbindungen ein gültiges Zertifikat erforderlich ist. Weitere Informationen zu allen Verbindungsoptionen mit dem MySQL-Client finden Sie unter Client-Side Configuration for Encrypted Connections in der MySQL-Dokumentation.

Wenn der MySQL-5.7- oder MySQL-8.0-Client verwendet wird, erfordert eine TLS-Verbindung die Verifizierung anhand des CA-Serverzertifikats, wenn Sie für die Option `--ssl-mode` den Wert `VERIFY_CA` oder `VERIFY_IDENTITY` angeben, wie im folgenden Beispiel gezeigt.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem
 --ssl-mode=VERIFY_CA
```

Wenn der MySQL 5.6-Client verwendet wird, erfordert eine SSL-Verbindung die Verifizierung anhand des CA-Serverzertifikats, wenn Sie die Option `--ssl-verify-server-cert` angeben wie im folgenden Beispiel gezeigt.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem
 --ssl-verify-server-cert
```

Aktualisieren des Trust Stores Ihrer Anwendung

Informationen zum Aktualisieren des Trust Stores für MySQL-Anwendungen finden Sie unter Installing SSL Certificates in der MySQL-Dokumentation.

> **Note**
>
> Wenn Sie den Trust Store aktualisieren, können Sie ältere Zertifikate beibehalten und die neuen Zertifikate einfach hinzufügen.

Aktualisieren des Trust Stores Ihrer Anwendung für JDBC

Sie können den Trust Store für Anwendungen aktualisieren, die JDBC für TLS-Verbindungen verwenden.

Informationen zum Herunterladen des Stammverzeichnisses finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

Beispiele für Skripte, die Zertifikate importieren, finden Sie unter Beispielskript für den Import von Zertifikaten in Ihren Trust Store.

Wenn Sie den JDBC-Treiber von MySQL in einer Anwendung verwenden, legen Sie in der Anwendung die folgenden Eigenschaften fest.

```
System.setProperty("javax.net.ssl.trustStore", certs);
System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

> **Note**
>
> Geben Sie aus Sicherheitsgründen ein anderes Passwort als hier angegeben an.

Legen Sie während des Startens der Anwendung die folgenden Eigenschaften fest.

```
java -Djavax.net.ssl.trustStore=/path_to_truststore/MyTruststore.jks -
Djavax.net.ssl.trustStorePassword=my_truststore_password com.companyName.MyApplication
```

Java-Beispielcode für die Herstellung von TLS-Verbindungen

Im folgenden Codebeispiel wird gezeigt, wie Sie die SSL-Verbindung einrichten, die das Serverzertifikat mithilfe von JDBC validiert.

```
public class MySQLSSLTest {

        private static final String DB_USER = "user name";
        private static final String DB_PASSWORD = "password";
        // This key store has only the prod root ca.
        private static final String KEY_STORE_FILE_PATH = "file-path-to-keystore";
        private static final String KEY_STORE_PASS = "keystore-password";

    public static void test(String[] args) throws Exception {
        Class.forName("com.mysql.jdbc.Driver");


        System.setProperty("javax.net.ssl.trustStore", KEY_STORE_FILE_PATH);
        System.setProperty("javax.net.ssl.trustStorePassword", KEY_STORE_PASS);

        Properties properties = new Properties();
        properties.setProperty("sslMode", "VERIFY_IDENTITY");
        properties.put("user", DB_USER);
        properties.put("password", DB_PASSWORD);

        Connection connection = DriverManager.getConnection("jdbc:mysql://jagdeeps-ssl-
test.cni62e2e7kwh.us-east-1.rds.amazonaws.com:3306",properties);
        Statement stmt=connection.createStatement();

        ResultSet rs=stmt.executeQuery("SELECT 1 from dual");

        return;
```

```
    }
}
```

> **Important**
>
> Nachdem Sie festgestellt haben, dass Ihre Datenbankverbindungen TLS verwenden, und Ihren Anwendungsvertrauensspeicher aktualisiert haben, können Sie Ihre Datenbank aktualisieren, um die rds-ca-rsa2048-g1-Zertifikate zu verwenden. Anweisungen hierzu finden Sie in Schritt 3 unter Aktualisierung Ihres CA-Zertifikats durch Änderung Ihrer DB-Instance .

Verwenden der Kerberos-Authentifizierung für Aurora MySQL

Sie können die Kerberos-Authentifizierung verwenden, um Benutzer zu authentifizieren, wenn diese sich mit Ihrem DB-Cluster von Aurora MySQL verbinden. Konfigurieren Sie Ihren DB-Cluster dazu so, dass AWS Directory Service for Microsoft Active Directory für die Kerberos-Authentifizierung verwendet wird. AWS Directory Service for Microsoft Active Directory wird auch als AWS Managed Microsoft AD bezeichnet. Es ist eine Funktion, die mit AWS Directory Service verfügbar ist. Weitere Informationen finden Sie unter Was ist AWS Directory Service? im Administratorhandbuch für AWS Directory Service.

Zunächst erstellen Sie ein AWS Managed Microsoft AD-Verzeichnis, um Benutzeranmeldeinformationen zu speichern. Anschließend stellen Sie Ihrem DB-Cluster von Aurora MySQL die Active Directory Domain und weitere Informationen zur Verfügung. Wenn sich Benutzer beim DB-Cluster von Aurora MySQL authentifizieren, werden Authentifizierungsanforderungen an das AWS Managed Microsoft AD-Verzeichnis weitergeleitet.

Wenn Sie alle Ihre Anmeldeinformationen im selben Verzeichnis aufbewahren, können Sie Zeit und Mühe sparen. Mit diesem Ansatz haben Sie einen zentralen Ort für die Speicherung und Verwaltung von Anmeldeinformationen für mehrere DB-Cluster. Die Verwendung eines Verzeichnisses kann auch Ihr allgemeines Sicherheitsprofil verbessern.

Außerdem können Sie von Ihrem eigenen On-Premises Microsoft Active Directory auf Anmeldeinformationen zugreifen. Dazu erstellen Sie eine vertrauensvolle Domain-Beziehung, damit das AWS Managed Microsoft AD-Verzeichnis Ihrem On-Premises Microsoft Active Directory vertraut. Auf diese Weise können Ihre Benutzer auf Ihre DB-Cluster von Aurora SQL mit derselben Windows Single Sign-On-Oberfläche (SSO) zugreifen, die sie auch für den Zugriff auf Workloads in Ihrem lokalen Netzwerk verwenden.

Eine Datenbank kann Kerberos, AWS Identity and Access Management (IAM) oder sowohl Kerberos- als auch IAM-Authentifizierung nutzen. Da die Kerberos- und IAM-Authentifizierung jedoch unterschiedliche Authentifizierungsmethoden bereitstellen, kann sich ein bestimmter Benutzer nur mit der einen oder anderen Authentifizierungsmethode bei einer Datenbank anmelden, jedoch nicht mit beiden. Weitere Informationen zur IAM-Authentifizierung finden Sie unter IAM-Datenbankauthentifizierung.

Inhalt

Übersicht über die Kerberos-Authentifizierung für DB-Cluster von Aurora MySQL

Wenn Sie die Kerberos-Authentifizierung für einen DB-Cluster von Aurora MySQL einrichten möchten, führen Sie die folgenden allgemeinen Schritte aus. Diese Schritte werden später ausführlich beschrieben.

1. Verwenden Sie AWS Managed Microsoft AD zum Erstellen eines AWS Managed Microsoft AD-Verzeichnisses. Zur Erstellung des Verzeichnisses können Sie AWS Management Console, AWS CLI oder AWS Directory Service verwenden. Ausführliche Anweisungen dazu finden Sie unter Erstellen Ihres AWS Managed Microsoft AD-Verzeichnisses im AWS Directory Service-Administratorhandbuch.

2. Erstellen Sie eine AWS Identity and Access Management-(IAM)-Rolle, die die verwaltete IAM-Richtlinie `AmazonRDSDirectoryServiceAccess` verwendet. Die Rolle erlaubt Amazon Aurora, Aufrufe an Ihr Verzeichnis zu senden.

   Damit die Rolle Zugriff gewährt, muss der AWS Security Token Service (AWS STS)-Endpunkt in der AWS-Region für Ihr AWS-Konto aktiviert sein. AWS STS-Endpunkte sind standardmäßig in allen AWS-Regionen aktiv und Sie können sie ohne weitere Maßnahmen nutzen. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von AWS STS in einer AWS-Region im IAM-Benutzerhandbuch.
3. Erstellen und konfigurieren Sie Benutzer im Verzeichnis AWS Managed Microsoft AD mithilfe der Tools aus dem Microsoft Active Directory. Weitere Informationen zum Erstellen von Benutzern in Ihrem Active Directory finden Sie unter Verwalten von Benutzern und Gruppen in AWS Managed Microsoft AD im AWS Directory Service Administrationshandbuch.
4. Erstellen oder ändern Sie einen DB-Cluster von Aurora MySQL. Wenn Sie entweder die CLI oder die RDS-API für die Erstellungsanforderung verwenden, geben Sie eine Domänen-ID mit dem Parameter `Domain` an. Verwenden Sie die `d-*`-ID, die bei der Erstellung Ihres Verzeichnisses generiert wurde, und den Namen der von Ihnen erstellten IAM-Rolle.

   Wenn Sie einen vorhandenen DB-Cluster von Aurora MySQL so ändern, dass er die Kerberos-Authentifizierung verwendet, legen Sie die Parameter für die Domain und die IAM-Rolle für den DB-Cluster fest. Suchen Sie den DB-Cluster in derselben VPC wie das Domain-Verzeichnis.
5. Verwenden Sie die Hauptbenutzer-Anmeldeinformationen von Amazon RDS, um sich mit dem DB-Cluster von Aurora MySQL zu verbinden. Erstellen Sie den Datenbankbenutzer in Aurora MySQL gemäß den Anweisungen in Schritt 6: Erstellen von Aurora-MySQL-Benutzern, die die Kerberos-Authentifizierung verwenden.

   Benutzer, die Sie auf diese Weise anlegen, können sich mit der Kerberos-Authentifizierung beim DB-Cluster von Aurora MySQL anmelden. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Aurora MySQL mit Kerberos-Authentifizierung.

Wenn Sie die Kerberos-Authentifizierung mit einem On-Premises oder einem selbst gehosteten Microsoft Active Directory verwenden möchten, erstellen Sie eine Gesamtstruktur-Vertrauensstellung. Eine Gesamtstruktur-Vertrauensstellung ist eine Vertrauensbeziehung zwischen zwei Gruppen von Domains. Die Vertrauensstellung kann uni- oder bidirektional sein. Weitere Informationen zur Einrichtung einer gesamtstrukturbasierten Vertrauensstellung mit AWS Directory Service finden Sie unter ?Wann sollte eine Vertrauensstellung erstellt werden im AWS Directory Service-Administrationshandbuch.

Einschränkungen bei der Kerberos-Authentifizierung für Aurora MySQL

Die folgenden Einschränkungen gelten für die Kerberos-Authentifizierung für Aurora MySQL:

- Die Kerberos-Authentifizierung wird für Aurora MySQL Version 3.03 und höher unterstützt.

  Weitere Informationen zur AWS-Region-Unterstützung finden Sie unter Kerberos-Authentifizierung mit Aurora MySQL.
- Um die Kerberos-Authentifizierung mit Aurora MySQL zu verwenden, muss Ihr MySQL-Client oder Connector Version 8.0.26 oder höher auf Unix-Plattformen bzw. 8.0.27 oder höher unter Windows verwenden. Andernfalls ist das clientseitige `authentication_kerberos_client`-Plugin nicht verfügbar und Sie können sich nicht authentifizieren.
- Nur AWS Managed Microsoft AD wird in Aurora MySQL unterstützt. Sie können jedoch DB-Cluster von Aurora MySQL zu gemeinsam genutzten verwalteten Microsoft-AD-Domains zusammenführen, die verschiedenen Konten in derselben AWS-Region gehören.

  Außerdem können Sie ein eigenes On-Premises Active Directory verwenden. Weitere Informationen finden Sie unter Schritt 2: (Optional) Erstellen einer Vertrauensstellung für ein On-Premise-Active-Directory.
- Wenn Kerberos verwendet wird, um einen Benutzer zu authentifizieren, der sich von MySQL-Clients oder von Treibern auf dem Windows-Betriebssystem aus mit dem Aurora-MySQL-Cluster verbindet, muss die Groß-/Kleinschreibung des Datenbankbenutzernamens standardmäßig mit der Groß-/Kleinschreibung des Benutzers im Active Directory übereinstimmen. Wenn der Benutzer im Active Directory beispielsweise als `Admin` angezeigt wird, muss der Datenbankbenutzername `Admin` lauten.

  Mit dem Plug-in `authentication_kerberos` können Sie jetzt jedoch den Benutzernamenvergleich ohne Berücksichtigung der Groß-/Kleinschreibung verwenden. Weitere Informationen finden Sie unter Schritt 8: (Optional) Konfigurieren eines Benutzernamenvergleichs ohne Berücksichtigung der Groß-/Kleinschreibung.
- Sie müssen die Reader-DB-Instances neu starten, nachdem Sie die Funktion zur Installation des `authentication_kerberos`-Plugins aktiviert haben.
- Die Replikation auf DB-Instances, die das `authentication_kerberos`-Plugin nicht unterstützen, kann zu einem Replikationsfehler führen.
- Damit globale Aurora-Datenbanken die Kerberos-Authentifizierung verwenden können, müssen Sie diese für jeden DB-Cluster in der globalen Datenbank konfigurieren.

- Der Domain-Name muss weniger als 62 Zeichen lang sein.
- Ändern Sie den DB-Cluster-Port nicht, nachdem Sie die Kerberos-Authentifizierung aktiviert haben. Wenn Sie den Port ändern, funktioniert die Kerberos-Authentifizierung nicht mehr.

Einrichten der Kerberos-Authentifizierung für DB-Cluster von Aurora MySQL

Verwenden Sie AWS Managed Microsoft AD, die Kerberos-Authentifizierung für einen DB-Cluster von Aurora MySQL einzurichten. Um die Kerberos-Authentifizierung einzurichten, führen Sie die folgenden Schritte aus.

Themen

Schritt 1: Erstellen eines Verzeichnisses mit AWS Managed Microsoft AD

AWS Directory Service erstellt ein vollständig verwaltetes Active Directory in der AWS Cloud. Wenn Sie ein AWS Managed Microsoft AD-Verzeichnis erstellen, erstellt AWS Directory Service zwei Domänencontroller und DNS-Server (Domain Name System) in Ihrem Namen. Die Verzeichnisserver werden in verschiedenen Subnetzen in einer VPC erstellt. Diese Redundanz trägt dazu bei, dass Ihr Verzeichnis auch im Fehlerfall erreichbar bleibt.

Wenn Sie ein AWS Managed Microsoft AD-Verzeichnis erstellen, führt AWS Directory Service die folgenden Aufgaben in Ihrem Namen aus:

- Einrichten eines Active Directory innerhalb der VPC.
- Erstellt ein Konto für den Verzeichnisadministrator mit dem Benutzernamen `Admin` und dem angegebenen Passwort. Mit diesem Konto verwalten Sie das Verzeichnis.

> **Note**
>
> Stellen Sie sicher, dass Sie dieses Passwort speichern. AWS Directory Service speichert es nicht. Sie können es zurücksetzen, aber Sie können es nicht abrufen.

- Erstellt eine Sicherheitsgruppe für die Verzeichniscontroller.

Wenn Sie AWS Managed Microsoft AD starten, erstellt AWS eine Organisationseinheit (OU), die alle Objekte Ihres Verzeichnisses enthält. Diese OU erhält den NetBIOS-Namen, den Sie beim Erstellen des Verzeichnisses eingegeben haben. Sie befindet sich im Stammverzeichnis der Domain, das sich im Besitz und Verwaltungsbereich von AWS befindet.

Das `Admin`-Konto, das mit Ihrem AWS Managed Microsoft AD-Verzeichnis erstellt wurde, hat Berechtigungen für die häufigsten administrativen Aktivitäten für Ihre OU, einschließlich:

- Erstellen, Aktualisieren oder Löschen von Benutzern
- Hinzufügen von Ressourcen zu Ihrer Domain, etwa Datei- oder Druckserver, und anschließendes Gewähren der zugehörigen Ressourcenberechtigungen für Benutzer in der OU
- Erstellen weiterer OUs und Container
- Delegieren von Befugnissen
- Wiederherstellen von gelöschten Objekten aus dem Active Directory-Papierkorb
- Ausführen von AD- und DNS-Windows- PowerShell Modulen auf dem Active Directory Web Service

Das `Admin`-Konto hat auch die Berechtigung, die folgenden domänenweiten Aktivitäten durchzuführen:

- Verwalten von DNS-Konfigurationen (Hinzufügen, Entfernen oder Aktualisieren von Datensätzen, Zonen und Weiterleitungen)
- Aufrufen von DNS-Ereignisprotokollen
- Anzeigen von Sicherheitsereignisprotokollen

So erstellen Sie ein Verzeichnisses mit AWS Managed Microsoft AD

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Directory Service-Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Wählen Sie im Navigationsbereich Directories (Verzeichnisse) aus. Wählen Sie denn Set up Directory (Verzeichnis einrichten) aus.
3. Wählen Sie AWS Managed Microsoft AD aus. AWS Managed Microsoft AD ist die einzige Option, die Sie derzeit mit Amazon RDS verwenden können.
4. Geben Sie die folgenden Informationen ein:

   DNS-Name des Verzeichnisses

   Den vollständig qualifizierten Namen für das Verzeichnis, z. B. **`corp.example.com`**.

   NetBIOS-Name des Verzeichnisses

   Die kurzen Namen für das Verzeichnis, z. B. **`CORP`**.

   Verzeichnisbeschreibung

   (Optional) Eine Beschreibung für das Verzeichnis.

   Administratorpasswort

   Das Passwort für den Verzeichnisadministrator. Während des Verzeichniserstellungsprozesses wird ein Administratorkonto mit dem Benutzernamen Admin und diesem Passwort angelegt.

   Das Passwort für den Verzeichnisadministrator das nicht das Wort "admin" enthalten. Beachten Sie beim Passwort die Groß- und Kleinschreibung und es muss 8 bis 64 Zeichen lang sein. Zudem muss es mindestens ein Zeichen aus dreien der vier folgenden Kategorien enthalten:

   - Kleinbuchstaben (a–z)
   - Großbuchstaben (A–Z)
   - Zahlen (0–9)
   - Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

   Passwort bestätigen

   Das wiederholte Administrator-Passwort.
5. Wählen Sie Weiter aus.

6. Geben Sie die folgenden Informationen in den Abschnitt Networking ein. Wählen Sie dann Next (Weiter) aus:

   VPC

   Die VPC für das Verzeichnis. Erstellen Sie den DB-Cluster von Aurora MySQL in derselben VPC.

   Subnetze

   Subnetze für die Verzeichnisserver. Die beiden Subnetze müssen zu verschiedenen Availability-Zonen gehören.

7. Prüfen Sie die Verzeichnisinformationen und nehmen Sie ggf. Änderungen vor. Wenn die Informationen richtig sind, wählen Sie Create directory (Verzeichnis erstellen).

Es dauert einige Minuten, bis das Verzeichnis erstellt wird. Wenn es erfolgreich erstellt wurde, ändert sich der Wert Status in Active (Aktiv).

Um Informationen über Ihr Verzeichnis anzuzeigen, wählen Sie den Verzeichnisnamen in der Verzeichnisliste aus. Notieren Sie sich den Wert Verzeichnis-ID. Sie benötigen diesen Wert, wenn Sie Ihren DB-Cluster von Aurora MySQL erstellen oder ändern.

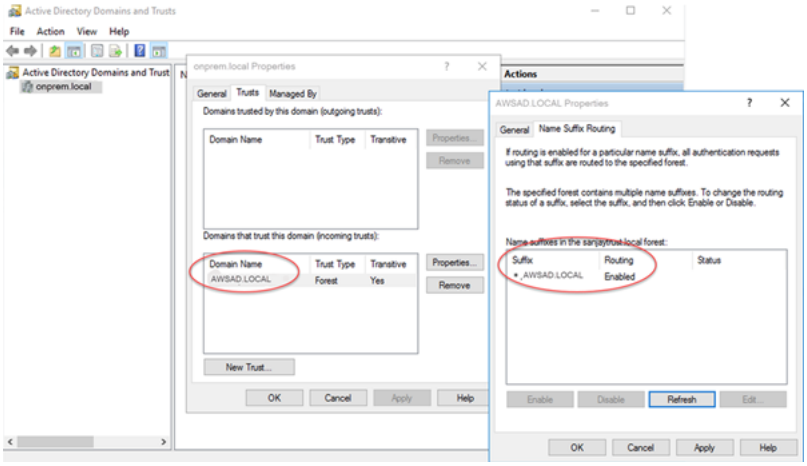
Schritt 2: (Optional) Erstellen einer Vertrauensstellung für ein On-Premise-Active-Directory

Wenn Sie Ihr eigenes lokales Microsoft Active Directory nicht verwenden möchten, fahren Sie mit for Schritt 3: Erstellen einer IAM-Rolle zur Verwendung durch Amazon Aurora.

Um die Kerberos-Authentifizierung mit Ihrem lokalen Active Directory zu verwenden, müssen Sie mittels Gesamtstruktur-Vertrauensstellung eine vertrauenswürdige Domain-Beziehung zwischen Ihrem lokalen Microsoft Active Directory und dem AWS Managed Microsoft AD-Verzeichnis (erstellt in Schritt 1: Erstellen eines Verzeichnisses mit AWS Managed Microsoft AD) erstellen. Die Vertrauensstellung kann einseitig erfolgen, wobei das AWS Managed Microsoft AD-Verzeichnis dem lokalen Microsoft Active Directory vertraut. Die Vertrauensstellung kann auch bidirektional erfolgen, wobei beide Active Directories einander vertrauen. Weitere Informationen zur Einrichtung einer gesamtstrukturbasierten Vertrauensstellung mit AWS Directory Service finden Sie unter Wann sollte eine Vertrauensstellung erstellt werden im AWS Directory Service-Administrationshandbuch.

> **Note**
>
> Verwendung eines lokalen Microsoft Active Directory:
>
> - Windows-Clients müssen eine Verbindung mithilfe des Domänennamens des AWS Directory Service auf dem Endpunkt statt rds.amazonaws.com herstellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Aurora MySQL mit Kerberos-Authentifizierung.
> - Windows-Clients können keine Verbindung über benutzerdefinierten Aurora-Endpunkte herstellen. Weitere Informationen hierzu finden Sie unter Amazon Aurora-Verbindungsverwaltung.
> - Globale Datenbanken:
>   - Windows-Clients können sich nur über Instance- oder Cluster-Endpunkte in der primären AWS-Region der globalen Datenbank verbinden.
>   - Windows-Clients können sich nicht über Cluster-Endpunkte in sekundären AWS-Regionen verbinden.

Stellen Sie sicher, dass der lokale Microsoft Active Directory-Domänenname ein DNS-Suffix-Routing enthält, das der neu erstellten Vertrauensstellung entspricht. Im folgenden Screenshot wird ein Beispiel gezeigt.



Schritt 3: Erstellen einer IAM-Rolle zur Verwendung durch Amazon Aurora

Damit Amazon Aurora AWS Directory Service für Sie aufrufen kann, ist eine AWS Identity and Access Management (IAM)-Rolle erforderlich, die die verwaltete IAM-Richtlinie

`AmazonRDSDirectoryServiceAccess` verwendet. Diese Rolle ermöglicht es Aurora, Aufrufe an AWS Directory Service durchzuführen.

Wenn Sie einen DB-Cluster mit der AWS Management Console erstellen und über die Berechtigung `iam:CreateRole` verfügen, erstellt die Konsole diese Rolle automatisch. In diesem Fall lautet der Rollenname `rds-directoryservice-kerberos-access-role`. Andernfalls müssen Sie die IAM-Rolle manuell erstellen. Wenn Sie diese IAM-Rolle erstellen, wählen Sie `Directory Service`, und hängen die von AWS verwaltete Richtlinie `AmazonRDSDirectoryServiceAccess` an.

Weitere Informationen über das Erstellen von IAM-Rollen für einen Service finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Optional können Sie Richtlinien mit den erforderlichen Berechtigungen erstellen, anstatt die verwaltete IAM-Richtlinie zu verwende `AmazonRDSDirectoryServiceAccess`. In diesem Fall muss die IAM-Rolle die folgende IAM-Vertrauensrichtlinie haben.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die Rolle muss auch über die folgende IAM-Rollenrichtlinie verfügen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
```

```
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
  ]
}
```

Schritt 4: Anlegen und Konfigurieren von Benutzern

Sie können Benutzer mit dem Tool "Active Directory-Benutzer und -Computer" erstellen. Dieses Tool ist Teil der Tools Active Directory Domain Services und Active Directory Lightweight Directory Services. „Benutzer“ sind Einzelpersonen oder Entitäten, die Zugriff auf Ihr Verzeichnis haben.

Wenn Sie Benutzer in einem AWS Directory Service-Verzeichnis erstellen möchten, verwenden Sie eine On-Premises oder Amazon-EC2-Instance auf der Basis von Microsoft Windows, die mit Ihrem AWS Directory Service-Verzeichnis verbunden ist. Gleichzeitig müssen Sie bei der Instance als Benutzer angemeldet sein, der über Berechtigungen zum Erstellen von Benutzern verfügt. Weitere Informationen finden Sie unter Verwalten von Benutzern und GruppenAWS Managed Microsoft AD imAWS Directory-Service-Administrationshandbuch.

Schritt 5: Erstellen oder Ändern eines DB-Clusters von Aurora MySQL

Erstellen oder ändern Sie einen DB-Cluster von Aurora MySQL zur Verwendung mit Ihrem Verzeichnis. Sie können die Konsole, AWS CLI oder RDS-API verwenden, um einen DB-Cluster einem Verzeichnis zuzuordnen. Sie können diese Aufgabe mit einer der folgenden Methoden durchführen:

- Erstellen Sie einen neuen Aurora MySQL-DB-Cluster mithilfe der Konsole, des create-db-cluster CLI-Befehls oder der RDS-API-Operation CreateDBCluster.

  Anweisungen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.
- Ändern Sie einen vorhandenen Aurora MySQL-DB-Cluster mithilfe der Konsole, des modify-db-cluster CLI-Befehls oder der ModifyDBCluster-RDS-API-Operation.

  Anweisungen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.
- Stellen Sie einen DB-Cluster von Aurora MySQL aus einem DB-Snapshot mithilfe der Konsole, des CLI-Befehls restore-db-cluster-from-snapshot oder der RestoreDBClusterFromSnapshot.

Anweisungen finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.

- Stellen Sie einen DB-Cluster von Aurora MySQL point-in-time mithilfe der Konsole, des CLI-Befehls restore-db-cluster-to-point-in-time oder der RDS-API-Operation RestoreDBClusterToPointInTime in einem wieder her.

  Anweisungen finden Sie unter Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit.

Die Kerberos-Authentifizierung wird nur für DB-Cluster von Aurora MySQL in einer VPC unterstützt. Der DB-Cluster kann sich in derselben VPC wie das Verzeichnis oder in einer anderen VPC befinden. Die VPC des DB-Clusters muss über eine VPC-Sicherheitsgruppe verfügen, die ausgehende Kommunikation mit Ihrem Verzeichnis zulässt.

Konsole

Wenn Sie die Konsole zum Erstellen, Ändern oder Wiederherstellen eines DB-Clusters verwenden, wählen Sie Kerberos-Authentifizierung im Datenbank-Authentifizierung-Abschnitt. Wählen Sie Verzeichnis durchsuchen und dann das Verzeichnis aus, oder klicken Sie auf Neues Verzeichnis erstellen.

AWS CLI

Wenn Sie die AWS CLI oder die RDS-API verwenden, verknüpfen Sie einen DB-Cluster mit einem Verzeichnis. Die folgenden Parameter sind erforderlich, damit der DB-Cluster das von Ihnen erstellte Domain-Verzeichnis verwendet:

- Für den `--domain`-Parameter verwenden Sie den Domänenbezeichner („d-*“-Bezeichner), der beim Erstellen des Verzeichnisses generiert wurde.
- Verwenden Sie für den `--domain-iam-role-name`-Parameter die von Ihnen erstellte Rolle, die die verwaltete IAM-Richtlinie `AmazonRDSDirectoryServiceAccess` verwendet.

Beispielsweise ändert der folgende CLI-Befehl einen DB-Cluster so, dass er ein Verzeichnis verwendet.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --domain d-ID \
```

```
    --domain-iam-role-name role-name
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --domain d-ID ^
    --domain-iam-role-name role-name
```

> **Important**
>
> Wenn Sie einen DB-Cluster ändern, um die Kerberos-Authentifizierung zu aktivieren, starten Sie die Reader-DB-Instances neu, nachdem Sie die Änderung vorgenommen haben.

Schritt 6: Erstellen von Aurora-MySQL-Benutzern, die die Kerberos-Authentifizierung verwenden

Der DB-Cluster ist der AWS Managed Microsoft AD-Domain beigetreten. Auf diese Weise können Sie Aurora-MySQL-Benutzer aus den Active-Directory-Benutzern Ihrer Domain bereitstellen. Die Datenbankberechtigungen werden durch Standardberechtigungen von Aurora MySQL verwaltet, die diesen Benutzern gewährt und entzogen werden.

Sie können einem Active-Directory-Benutzer erlauben, sich bei Aurora MySQL zu authentifizieren. Dazu verwenden Sie zunächst die Hauptbenutzer-Anmeldeinformationen von Amazon RDS, um sich mit der DB-Instance von Aurora MySQL sowie mit jedem anderen DB-Cluster zu verbinden. Nachdem Sie angemeldet sind, erstellen Sie einen extern authentifizierten Benutzer mit Kerberos-Authentifizierung in Aurora MySQL wie folgt:

```
CREATE USER user_name@'host_name' IDENTIFIED WITH 'authentication_kerberos' BY
 'realm_name';
```

- Ersetzen Sie *user_name* durch den Benutzernamen. Benutzer (sowohl Menschen als auch Anwendungen) aus Ihrer Domain können sich nun über einen der Domain beigetretenen Client per Kerberos-Authentifizierung mit dem DB-Cluster verbinden.
- Ersetzen Sie *host_name* durch den Hostnamen. Sie können % als Platzhalter verwenden. Sie können auch bestimmte IP-Adressen für den Hostnamen verwenden.

- Ersetzen Sie *realm_name* durch den Verzeichnisbereichsnamen der Domain. Der Bereichsname entspricht normalerweise dem DNS-Domain-Namen in Großbuchstaben, z. B. `CORP.EXAMPLE.COM`. Ein Bereich ist eine Gruppe von Systemen, die dasselbe Kerberos Key Distribution Center verwenden.

Im folgenden Beispiel wird ein Datenbankbenutzer mit dem Namen `Admin` erstellt, der sich gegenüber dem Active Directory mit dem Bereichsnamen `MYSQL.LOCAL` authentifiziert.

```
CREATE USER Admin@'%' IDENTIFIED WITH 'authentication_kerberos' BY 'MYSQL.LOCAL';
```

Ändern einer vorhandenen Aurora-MySQL-Anmeldung

Sie können auch eine vorhandene Aurora-MySQL-Anmeldung ändern, um die Kerberos-Authentifizierung zu verwenden. Nutzen Sie dazu die folgende Syntax:

```
ALTER USER user_name IDENTIFIED WITH 'authentication_kerberos' BY 'realm_name';
```

Schritt 7: Konfigurieren eines MySQL-Clients

Gehen Sie folgendermaßen vor, um einen MySQL-Client zu konfigurieren:

1. Erstellen Sie eine `krb5.conf`-Datei (oder eine vergleichbare Datei), um auf die Domain zu verweisen.
2. Stellen Sie sicher, dass der Datenverkehr zwischen dem Client-Host und fließen kan AWS Directory Service. Verwenden Sie ein Netzwerk-Dienstprogramm wie Netcat für die folgenden Aufgaben:
   - Überprüfen Sie den Datenverkehr über DNS für Port 53.
   - Überprüfen Sie den Datenverkehr über TCP/UDP an Port 53 und für Kerberos (Ports 88 und 464 für AWS Directory Service.
3. Stellen Sie sicher, dass der Datenverkehr zwischen dem Client-Host und der DB-Instance über den Datenbank-Port fließen kann. Verwenden Sie beispielsweise `mysql`, um eine Verbindung herzustellen und auf die Datenbank zuzugreifen.

Im Folgenden finden Sie Beispielinhalte der Datei `krb5.conf` für AWS Managed Microsoft AD.

```
[libdefaults]
```

```
 default_realm = EXAMPLE.COM
[realms]
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

Nachfolgend ist ein Beispiel für den Inhalt von `krb5.conf` für ein On-Premises Microsoft Active Directory aufgeführt.

```
[libdefaults]
 default_realm = EXAMPLE.COM
[realms]
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
 ONPREM.COM = {
  kdc = onprem.com
  admin_server = onprem.com
 }
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
 .onprem.com = ONPREM.COM
 onprem.com = ONPREM.COM
 .rds.amazonaws.com = EXAMPLE.COM
 .amazonaws.com.cn = EXAMPLE.COM
 .amazon.com = EXAMPLE.COM
```

Schritt 8: (Optional) Konfigurieren eines Benutzernamenvergleichs ohne Berücksichtigung der Groß-/Kleinschreibung

Standardmäßig muss die Groß-/Kleinschreibung des MySQL-Datenbankbenutzernamens mit der Groß-/Kleinschreibung der Active-Directory-Anmeldung übereinstimmen. Mit dem Plug-in `authentication_kerberos` können Sie jetzt jedoch den Benutzernamenvergleich ohne Berücksichtigung der Groß-/Kleinschreibung verwenden. Setzen Sie dazu den Parameter `authentication_kerberos_caseins_cmp` des DB-Clusters auf `true`.

So verwenden Sie den Benutzernamenvergleich ohne Berücksichtigung der Groß-/Kleinschreibung

1. Erstellen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe. Folgen Sie den Verfahren in Erstellen einer DB-Cluster-Parametergruppe.
2. Bearbeiten Sie die neue Parametergruppe, um den Wert für `authentication_kerberos_caseins_cmp` auf `true` zu setzen. Folgen Sie den Verfahren in Ändern von Parametern in einer DB-Cluster-Parametergruppe.
3. Ordnen Sie die DB-Clusterparametergruppe dem DB-Cluster von Aurora MySQL zu. Folgen Sie den Verfahren in Zuordnen einer DB-Cluster-Parametergruppe zu einem DB-Cluster.
4. Starten Sie den DB-Cluster neu.

Herstellen einer Verbindung mit Aurora MySQL mit Kerberos-Authentifizierung

Um Fehler zu vermeiden, verwenden Sie einen MySQL-Client mit Version 8.0.26 oder höher auf Unix-Plattformen, 8.0.27 oder höher unter Windows.

Verwenden der Kerberos-Anmeldung von Aurora MySQL, um eine Verbindung mit dem DB-Cluster herzustellen

Wenn Sie eine Verbindung mit Aurora MySQL mit Kerberos-Authentifizierung herstellen möchten, melden Sie sich als Datenbankbenutzer an, den Sie gemäß den Anweisungen unter Schritt 6: Erstellen von Aurora-MySQL-Benutzern, die die Kerberos-Authentifizierung verwenden erstellt haben.

Stellen Sie über die Eingabeaufforderung eine Verbindung mit einem der Endpunkte her, die mit Ihrem DB-Cluster von Aurora MySQL verbunden sind. Wenn Sie zur Eingabe des Passworts aufgefordert werden, geben Sie das mit diesem Benutzernamen verknüpfte Kerberos-Passwort ein.

Wenn Sie sich bei Kerberos authentifizieren, wird ein Ticket-Granting Ticket (TGT) generiert, falls noch keines existiert. Das `authentication_kerberos`-Plugin verwendet das TGT, um ein Serviceticket zu erhalten, das dann dem Aurora-MySQL-Datenbankserver vorgelegt wird.

Sie können den MySQL-Client verwenden, um sich mit Kerberos-Authentifizierung unter Windows oder Unix mit Aurora MySQL zu verbinden.

Unix

Sie können die Verbindung mit einer der folgenden Methoden herstellen:

- Rufen Sie das TGT manuell ab. In diesem Fall müssen Sie dem MySQL-Client das Passwort nicht nennen.
- Stellen Sie das Passwort für die Active-Directory-Anmeldung direkt dem MySQL-Client zur Verfügung.

Das clientseitige Plugin wird auf Unix-Plattformen für MySQL-Client-Versionen ab 8.0.26 unterstützt.

So stellen Sie eine Verbindung her, indem Sie das TGT manuell abrufen

1. Verwenden Sie an der Befehlszeilenschnittstelle den folgenden Befehl, um das TGT abzurufen.

   ```
   kinit user_name
   ```

2. Verwenden Sie den folgenden `mysql`-Befehl, um sich beim DB-Instance-Endpunkt Ihres DB-Clusters anzumelden.

   ```
   mysql -h DB_instance_endpoint -P 3306 -u user_name -p
   ```

   > **Note**
   >
   > Die Authentifizierung kann fehlschlagen, wenn der Keytab auf der DB-Instance rotiert wird. Rufen Sie in diesem Fall ein neues TGT ab, indem Sie `kinit` erneut ausführen.

So stellen Sie eine direkte Verbindung her

1. Verwenden Sie an der Befehlszeilenschnittstelle den folgenden `mysql`-Befehl, um sich beim DB-Instance-Endpunkt Ihres DB-Clusters anzumelden.

   ```
   mysql -h DB_instance_endpoint -P 3306 -u user_name -p
   ```

2. Geben Sie das Passwort für den Active-Directory-Benutzer an.

Windows

Unter Windows erfolgt die Authentifizierung normalerweise bei der Anmeldung, sodass Sie das TGT nicht manuell abrufen müssen, um eine Verbindung mit dem DB-Cluster von Aurora MySQL herzustellen. Die Groß- und Kleinschreibung des Datenbankbenutzernamens muss mit der Groß-/

Kleinschreibung des Benutzers im Active Directory übereinstimmen. Wenn der Benutzer im Active Directory beispielsweise als `Admin` angezeigt wird, muss der Datenbankbenutzername `Admin` lauten.

Das clientseitige Plugin wird unter Windows für MySQL-Client-Versionen ab 8.0.27 unterstützt.

So stellen Sie eine direkte Verbindung her

- Verwenden Sie an der Befehlszeilenschnittstelle den folgenden `mysql`-Befehl, um sich beim DB-Instance-Endpunkt Ihres DB-Clusters anzumelden.

```
mysql -h DB_instance_endpoint -P 3306 -u user_name
```

Kerberos-Authentifizierung mit globalen Aurora-Datenbanken

Die Kerberos-Authentifizierung für Aurora MySQL wird für globale Aurora-Datenbanken unterstützt. Wenn Sie Benutzer im sekundären DB-Cluster mithilfe des Active Directory des primären DB-Clusters authentifizieren möchten, replizieren Sie das Active Directory auf die sekundäre AWS-Region. Sie aktivieren die Kerberos-Authentifizierung auf dem sekundären Cluster mit derselben Domain-ID wie für den primären Cluster. Die AWS Managed Microsoft AD-Replikation wird nur mit der Enterprise-Version von Active Directory unterstützt. Weitere Informationen finden Sie unter Regionsübergreifende Replikation im AWS Directory Service-Administratorhandbuch.

Migration von RDS für MySQL zu Aurora MySQL

Nachdem Sie von RDS für MySQL mit aktivierter Kerberos-Authentifizierung zu Aurora MySQL migriert haben, ändern Sie Benutzer, die mit dem `auth_pam`-Plugin erstellt wurden, so, dass sie das `authentication_kerberos`-Plugin verwenden. Beispiele:

```
ALTER USER user_name IDENTIFIED WITH 'authentication_kerberos' BY 'realm_name';
```

Verhindern einer Zwischenspeicherung von Tickets

Wenn beim Start der MySQL-Client-Anwendung kein gültiges TGT vorhanden ist, kann die Anwendung das TGT abrufen und zwischenspeichern. Wenn Sie verhindern möchten, dass das TGT zwischengespeichert wird, legen Sie in der Datei `/etc/krb5.conf` einen Konfigurationsparameter fest.

> **Note**
>
> Diese Konfiguration gilt nur für Client-Hosts, auf denen Unix ausgeführt wird, nicht für Windows.

So verhindern Sie das Zwischenspeichern von TGTs

- Fügen Sie `/etc/krb5.conf` wie folgt einen `[appdefaults]`-Abschnitt hinzu:

```
[appdefaults]
  mysql = {
    destroy_tickets = true
  }
```

Protokollieren für die Kerberos-Authentifizierung

Die Umgebungsvariable `AUTHENTICATION_KERBEROS_CLIENT_LOG` legt die Protokollierungsebene für die Kerberos-Authentifizierung fest. Sie können die Protokolle für das clientseitige Debugging verwenden.

Die zulässigen Werte sind 1–5. Protokollmeldungen werden in die Standardfehlerausgabe geschrieben. In der folgenden Tabelle ist jede Protokollierungsebene beschrieben.

Protokollierungsstufe	Beschreibung
1 oder nicht festgelegt	Keine Protokollierung
2	Fehlermeldungen
3	Fehler- und Warnmeldungen
4	Fehler-, Warn- und Informationsmeldungen
5	Fehler-, Warn-, Informations- und Debug-Meldungen

Verwalten eines DB-Clusters in einer Domäne

Sie können die AWS CLI oder die RDS-API verwenden, um Ihren DB-Cluster und seine Beziehung zu Ihrem verwalteten Active Directory zu verwalten. Sie können z. B. ein Active Directory für die Kerberos-Authentifizierung zuordnen und ein Active Directory trennen, um die Kerberos-Authentifizierung zu deaktivieren. Sie können auch einen DB-Cluster, der extern von einem Active Directory authentifiziert werden soll, in ein anderes Active Directory verschieben.

Sie können z. B. mithilfe der Amazon RDS-API Folgendes tun:

- Um erneut zu versuchen, die Kerberos-Authentifizierung für eine fehlgeschlagene Mitgliedschaft zu aktivieren, verwenden Sie die API-Operation `ModifyDBInstance` und geben Sie die Verzeichnis-ID der aktuellen Mitgliedschaft an.
- Um den IAM-Rollennamen für die Mitgliedschaft zu aktualisieren, verwenden Sie die `ModifyDBInstance`-API-Operation und geben Sie die Verzeichnis-ID der aktuellen Mitgliedschaft und die neue IAM-Rolle an.
- Wenn Sie die Kerberos-Authentifizierung in einem DB-Cluster deaktivieren möchten, verwenden Sie die API-Operation `ModifyDBInstance` und geben Sie `none` als Domänenparameter an.
- Um einen DB-Cluster von einer Domäne in eine andere zu verschieben, verwenden Sie die API-Operation `ModifyDBInstance`. Geben Sie die Domänen-ID der neuen Domäne als Domänenparameter an.
- Wenn Sie die Mitgliedschaft für jeden DB-Cluster auflisten möchten, verwenden Sie die API-Operation `DescribeDBInstances`.

Grundlegendes zur Domänenmitgliedschaft

Nachdem Sie Ihren DB-Cluster erstellt oder geändert haben, wird er Mitglied der Domäne. Sie können den Status der Domänenmitgliedschaft für den DB-Cluster anzeigen, indem Sie den CLI-Befehl describe-db-clusters verwenden. Der Status des DB-Clusters kann einer der folgenden sein:

- `kerberos-enabled`: Für den DB-Cluster ist die Kerberos-Authentifizierung aktiviert.
- `enabling-kerberos`: AWS ist dabei, die Kerberos-Authentifizierung auf diesem DB-Cluster zu aktivieren.
- `pending-enable-kerberos`: Das Aktivieren der Kerberos-Authentifizierung in diesem DB-Cluster steht aus.

- `pending-maintenance-enable-kerberos`: AWS versucht, die Kerberos-Authentifizierung auf dem DB-Cluster während des nächsten geplanten Wartungsfensters zu aktivieren.
- `pending-disable-kerberos`: Das Deaktivieren der Kerberos-Authentifizierung in diesem DB-Cluster steht aus.
- `pending-maintenance-disable-kerberos`: AWS versucht, die Kerberos-Authentifizierung auf dem DB-Cluster während des nächsten geplanten Wartungsfensters zu deaktivieren.
- `enable-kerberos-failed`: Ein Konfigurationsproblem hat AWS daran gehindert, die Kerberos-Authentifizierung auf dem DB-Cluster zu aktivieren. Überprüfen und korrigieren Sie Ihre Konfiguration, bevor Sie den Befehl zum Ändern des DB-Clusters erneut ausführen.
- `disabling-kerberos`: AWS ist dabei, die Kerberos-Authentifizierung auf diesem DB-Cluster zu deaktivieren.

Eine Anfrage zur Aktivierung der Kerberos-Authentifizierung kann wegen eines Netzwerkverbindungsproblems oder einer falschen IAM-Rolle fehlschlagen. Angenommen, Sie erstellen einen DB-Cluster oder ändern einen vorhandenen DB-Cluster und der Versuch, die Kerberos-Authentifizierung zu aktivieren, schlägt fehl. Wenn dies geschieht, führen Sie den Befehl zum Ändern erneut aus oder ändern Sie den neu erstellte DB-Cluster, um der Domäne beizutreten.

Migrieren von Daten zu einem Amazon Aurora MySQL-DB-Cluster

Sie haben mehrere Möglichkeiten, Daten aus einer vorhandenen Datenbank in einen Amazon Aurora MySQL-DB-Cluster zu migrieren. Die verfügbaren Migrationsoptionen sind auch von der Quelldatenbank und der Menge der zu migrierenden Daten abhängig.

Es gibt zwei verschiedene Migrationstypen: physisch und logisch. Bei der physischen Migration werden physische Kopien von Datenbankdateien verwenden, um die Datenbank zu migrieren. Bei der logischen Migration erfolgt die Migration durch Anwendung logischer Datenbankänderungen, wie beispielsweise Einfügungen, Aktualisierungen und Löschungen.

Die physische Migration hat die folgenden Vorteile:

- Die physische Migration ist schneller als die logische Migration, insbesondere für große Datenbanken.
- Die Datenbankleistung leidet nicht, wenn für eine physische Migration eine Sicherung durchgeführt wird.
- Die physische Migration kann alles in der Quelldatenbank migrieren, auch komplexe Datenbankkomponenten.

Die physische Migration hat die folgenden Einschränkungen:

- Der Parameter `innodb_page_size` muss auf seinen Standardwert (16KB) gesetzt sein.
- Der `innodb_data_file_path`-Parameter darf nur mit einer Datendatei konfiguriert werden, die den Standarddateinamen `"ibdata1:12M:autoextend"` verwendet. Datenbanken mit zwei Datendateien oder nur einer Datendatei eines anderen Namens können mit dieser Methode nicht migriert werden.

  Nachfolgend finden Sie Beispiele für unzulässige Dateinamen: `"innodb_data_file_path=ibdata1:50M; ibdata2:50M:autoextend"` und `"innodb_data_file_path=ibdata01:50M:autoextend"`.
- Der Parameter `innodb_log_files_in_group` muss auf seinen Standardwert (2) gesetzt sein.

Die logische Migration hat die folgenden Vorteile:

- Sie können Untermengen der Datenbank migrieren, beispielsweise bestimmte Tabellen oder Teile einer Tabelle.

- Die Daten können unabhängig von der physischen Speicherstruktur migriert werden.

Die logische Migration hat die folgenden Einschränkungen:

- Die logische Migration ist normalerweise langsamer als die physische Migration.
- Komplexe Datenbankkomponenten können den logischen Migrationsprozess verlangsamen. In einigen Fällen können komplexe Datenbankkomponenten den logischen Migrationsprozess sogar blockieren.

In der folgenden Tabelle sind Ihre Optionen und die Migrationstypen für jede Option aufgelistet.

Migration von	Migrationstyp	Lösung
Eine RDS für MySQL-DB-Instance	Physisch	Sie können Daten aus einer RDS für MySQL-DB-Instance migrieren, indem Sie zunächst eine Aurora MySQL-Read Replica einer MySQL-DB-Instance erstellen. Wenn die Replica-Verzögerung zwischen der MySQL-DB-Instance und der Aurora MySQL-Read Replica 0 beträgt, können Sie Ihre Client-Anwendungen anweisen, aus der Aurora Read Replica zu lesen und dann die Replikation stoppen, um die Aurora MySQL Read Replica in ein eigenständiges Aurora MySQL-DB-Cluster für das Lesen und Schreiben zu transformieren. Details hierzu finden Sie unter Migrieren von Daten aus einer RDS-für-MySQL-DB-Instance zu einem Amazon-Aurora-MySQL-DB-Cluster mittels einer Aurora Read Replica (Lesereplikat).
Ein RDS für MySQL-DB-Snapshot	Physisch	Sie können Daten direkt aus einem RDS für MySQL-DB-Snapshot in einen Amazon Aurora MySQL-DB-Cluster migrieren. Details hierzu finden Sie unter Migrieren eines RDS für MySQL-Snapshots zu Aurora.
einer MySQL-Datenbank außerhalb von Amazon RDS	Logisch	Sie können mithilfe des Dienstprogramms `mysqldump` eine Dump-Datei mit den Daten erstellen und diese dann in einen bestehenden Amazon Aurora MySQL-DB-Cluster importieren. Details hierzu finden Sie unter Logische

Migration von	Migrationstyp	Lösung
		Migration von MySQL zu Amazon Aurora MySQL mithilfe von mysqldump. Um Metadaten für Datenbankbenutzer während der Migration aus einer externen MySQL-Datenbank zu exportieren, können Sie stattdessen auch einen MySQL-Shell-Befehl verwenden `mysqldump` . Weitere Informationen finden Sie unter Instance Dump Utility, Schema Dump Utility und Table Dump Utility. **Note** Das Hilfsprogramm mysqlpump ist seit MySQL 8.0.34 veraltet.
einer MySQL-Datenbank außerhalb von Amazon RDS	Physisch	Sie können die Sicherungsdateien aus Ihrer Datenbank in einen Amazon Simple Storage Service (Amazon S3)-Bucket kopieren und dann einen Amazon Aurora MySQL-DB-Cluster aus diesen Dateien wiederherstellen. Dieser Weg ist bedeutend schneller als eine Datenmigration mit `mysqldump` . Details hierzu finden Sie unter Physische Migration von MySQL mithilfe von Percona XtraBackup und Amazon S3.

Migration von	Migrationstyp	Lösung
einer MySQL-Datenbank außerhalb von Amazon RDS	Logisch	Sie können die Daten in der Datenbank als Textdateien speichern und diese in einen Amazon S3-Bucket kopieren. Anschließend können die Daten in einen vorhandenen Aurora MySQL-DB-Cluster laden, indem Sie den MySQL-Befehl `LOAD DATA FROM S3` verwenden. Weitere Informationen finden Sie unter Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket.
Eine Datenbank, die nicht MySQL-kompatibel ist	Logisch	Sie können AWS Database Migration Service (AWS DMS) verwenden, um Daten aus einer Datenbank zu migrieren , die nicht MySQL-kompatibel ist. Weitere Informationen dazu finden Sie unter Was ist ein AWS Datenbank migrationsdienst? AWS DMS

Note

Wenn Sie eine MySQL-Datenbank extern zu Amazon RDS migrieren, werden die in der Tabelle beschriebenen Migrationsoptionen nur unterstützt, wenn Ihre Datenbank die InnoDB- oder MyISAM-Tabellenbereiche unterstützt.
Wenn die MySQL-Datenbank, die Sie zu Aurora MySQL migrieren, `memcached` verwendet, müssen Sie `memcached` vor der Migration entfernen.
Sie können von einigen älteren Versionen von MySQL 8.0, einschließlich 8.0.11, 8.0.13 und 8.0.15, nicht zu Aurora MySQL Version 3.05 und höher migrieren. Wir empfehlen, vor der Migration auf MySQL Version 8.0.28 zu aktualisieren.

Migrieren von Daten aus einer externen MySQL-Datenbank zu einem Amazon-Aurora-MySQL-DB-Cluster

Wenn Ihre Datenbank die InnoDB- oder MyISAM-Tabellenräume unterstützt, können Sie die Daten wie folgt in einen Amazon Aurora MySQL-DB-Cluster migrieren:

- Sie können mithilfe des Dienstprogramms `mysqldump` eine Dump-Datei mit den Daten erstellen und diese dann in einen bestehenden Amazon Aurora MySQL-DB-Cluster importieren. Weitere Informationen finden Sie unter Logische Migration von MySQL zu Amazon Aurora MySQL mithilfe von mysqldump.
- Sie können die Dateien der vollständigen und inkrementellen Datenbanksicherungen in einen Amazon S3-Bucket kopieren und sie dann in einen Amazon Aurora MySQL-DB-Cluster wiederherstellen. Dieser Weg ist bedeutend schneller als eine Datenmigration mit `mysqldump`. Weitere Informationen finden Sie unter Physische Migration von MySQL mithilfe von Percona XtraBackup und Amazon S3.

Themen

Physische Migration von MySQL mithilfe von Percona XtraBackup und Amazon S3

Sie können die Dateien der vollständigen und inkrementellen Sicherung aus Ihrer MySQL-Quelldatenbank (Version 5.7 oder 8.0) in einen Amazon S3-Bucket kopieren. Anschließend können Sie die Wiederherstellung zu einem Amazon Aurora MySQL-DB-Cluster mit derselben Hauptversion wie der dieser Dateien durchführen.

Diese Option kann erheblich schneller sein als das Migrieren der Daten mithilfe von `mysqldump`, da durch die Verwendung von `mysqldump` alle Befehle für die erneute Erstellung des Schemas und der Daten aus Ihrer Quelldatenbank im neuen Aurora MySQL-DB-Cluster erneut ausgeführt werden. Da die MySQL-Quelldatendateien kopiert werden, können sie von Aurora MySQL sofort als Daten für einen Aurora MySQL-DB-Cluster verwendet werden.

Dazu können Sie mithilfe der Binärprotokollreplikation während des Migrationsprozesses die Ausfallzeit minimieren. Wenn Sie die Binärprotokollreplikation verwenden, bleibt die externe MySQL-Datenbank für Transaktionen geöffnet, während die Daten in das Aurora MySQL-DB-Cluster migriert werden. Nachdem das Aurora MySQL-DB-Cluster erstellt wurde, können Sie das Aurora MySQL-

DB-Cluster mithilfe der Binärprotokollreplikation mit den Transaktionen synchronisieren, die nach der Sicherung ausgeführt wurden. Sobald das Aurora MySQL-DB-Cluster den Stand der MySQL-Datenbank erreicht hat, können Sie die Migration beenden, indem Sie bei neuen Transaktionen vollständig zum Aurora MySQL-DB-Cluster wechseln. Weitere Informationen finden Sie unter Synchronisieren des Amazon Aurora MySQL-DB-Clusters mit der MySQL-Datenbank mittels Replikation.

Inhalt

Einschränkungen und Überlegungen

Die folgenden Einschränkungen und Überlegungen gelten für die Wiederherstellung zu einem Amazon Aurora MySQL DB-Cluster von einem Amazon S3-Bucket:

- Sie können Ihre Daten nur zu einem neuen und nicht zu einem bereits vorhandenen DB-Cluster migrieren.
- Sie müssen Percona verwenden XtraBackup , um Ihre Daten auf S3 zu sichern. Weitere Informationen finden Sie unter Percona installieren XtraBackup.
- Der Amazon S3 S3-Bucket und der Aurora MySQL-DB-Cluster müssen sich in derselben AWS Region befinden.
- Sie können nicht von folgenden Quellen aus wiederherstellen:
  - DB-Cluster-Snapshot-Export zu Amazon S3. Sie können auch keine Daten von einem DB-Cluster-Snapshot-Export in Ihren Amazon-S3-Bucket migrieren.
  - Verschlüsselte Quelldatenbank; Sie können jedoch die migrierten Daten verschlüsseln. Sie können die Daten während des Migrationsprozesses auch unverschlüsselt lassen.
  - MySQL 5.5- oder 5.6-Datenbank
- Percona Server for MySQL wird nicht als Quelldatenbank unterstützt, da sie `compression_dictionary*` Tabellen im `mysql` Schema enthalten kann.
- Eine Wiederherstellung auf einen Aurora Serverless-DB-Cluster ist nicht möglich.
- Für Haupt- und Nebenversionen wird keine abwärtskompatible Migration unterstützt. Das heißt, Sie können nicht von MySQL Version 8.0 zu Aurora MySQL Version 2 (kompatibel mit MySQL 5.7) und auch nicht von MySQL Version 8.0.32 zu Aurora MySQL Version 3.03 migrieren, das mit der MySQL-Community-Version 8.0.26 kompatibel ist.
- Sie können von einigen älteren Versionen von MySQL 8.0, einschließlich 8.0.11, 8.0.13 und 8.0.15, nicht zu Aurora MySQL Version 3.05 und höher migrieren. Wir empfehlen, vor der Migration auf MySQL Version 8.0.28 zu aktualisieren.
- Das Importieren von Amazon S3 wird von der DB-Instance-Klasse db.t2.micro nicht unterstützt. Sie können jedoch eine Wiederherstellung zu einer anderen DB-Instance-Klasse ausführen und die DB-Instance-Klasse später ändern. Weitere Informationen zu DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.
- Amazon S3 begrenzt die Größe einer Datei, die in einen S3-Bucket hochgeladen werden kann, auf 5 TB. Wenn eine Sicherungsdatei größer als 5 TB ist, müssen Sie die Sicherungsdatei in kleinere Dateien aufteilen.
- Amazon RDS begrenzt die Anzahl der Dateien, die in einen S3-Bucket hochgeladen werden können, auf 1 Million. Wenn es mehr als 1 Million Sicherungsdateien für Ihre Datenbank gibt (einschließlich aller vollständigen und inkrementellen Sicherungen), speichern Sie diese mittels Gzip (.gz), tar (.tar.gz) oder Percona xbstream (.xbstream) in dem S3-Bucket. Percona XtraBackup 8.0 unterstützt nur Percona xbstream für die Komprimierung.

- Um Verwaltungsdienste für jedes DB-Cluster bereitzustellen, wird der `rdsadmin`-Benutzer erstellt, wenn das DB-Cluster erstellt wird. Da dies ein reservierter Benutzer in RDS ist, gelten die folgenden Einschränkungen:
  - Funktionen, Prozeduren, Ansichten, Ereignisse und Trigger mit `'rdsadmin'@'localhost'`-Definierer werden nicht importiert. Weitere Informationen finden Sie unter Gespeicherte Objekte mit 'rdsadmin'@'localhost' als Definierer und Berechtigungen von Masterbenutzerkonten mit Amazon Aurora MySQL..
  - Wenn der Aurora MySQL-DB-Cluster erstellt wird, wird ein Master-Benutzer mit den maximal unterstützten Rechten erstellt. Bei der Wiederherstellung aus der Sicherung werden alle nicht unterstützten Rechte, die den importierten Benutzern zugewiesen wurden, beim Import automatisch entfernt.

    Informationen zu Benutzern, die davon betroffen sein könnten, finden Sie unter Benutzerkonten mit nicht unterstützten Rechten. Weitere Informationen zu den in Aurora MySQL unterstützten Rechten finden Sie unter Rollenbasiertes Berechtigungsmodell.
- Für Aurora MySQL Version 3 werden keine dynamischen Rechte importiert. Von Aurora unterstützte dynamische Rechte können nach der Migration importiert werden. Weitere Informationen finden Sie unter Dynamische Rechte in Aurora MySQL Version 3.
- Vom Benutzer erstellte Tabellen im `mysql`-Schema werden nicht migriert.
- Der `innodb_data_file_path`-Parameter darf nur mit einer Datendatei konfiguriert werden, die den Standarddateinamen `ibdata1:12M:autoextend` verwendet. Datenbanken mit zwei Datendateien oder nur einer Datendatei eines anderen Namens können mit dieser Methode nicht migriert werden.

  Nachfolgend finden Sie Beispiele für unzulässige Dateinamen: `innodb_data_file_path=ibdata1:50M`, `ibdata2:50M:autoextend` und `innodb_data_file_path=ibdata01:50M:autoextend`.
- Sie können nicht von einer Quelldatenbank migrieren, deren Tabellen außerhalb des standardmäßigen MySQL-Datenverzeichnisses definiert sind.
- Die maximal unterstützte Größe für unkomprimierte Sicherungen mit dieser Methode ist derzeit auf 64 TiB begrenzt. Bei komprimierten Sicherungen wird dieser Grenzwert gesenkt, um den Speicheranforderungen bei der Dekomprimierung Rechnung zu tragen. In solchen Fällen wäre die maximal unterstützte Backup-Größe (`64 TiB – compressed backup size`).
- Aurora MySQL unterstützt den Import von MySQL und anderen externen Komponenten und Plugins nicht.

- Aurora MySQL stellt nicht die gesamte Datenbank wieder her. Sie sollten das Datenbankschema und die Werte der folgenden Elemente der MySQL-Quelldatenbank speichern und dem Aurora MySQL-DB-Cluster nach der Wiederherstellung hinzufügen:
  - Benutzerkonten
  - Funktionen
  - Gespeicherte Prozeduren
  - Zeitzoneninformation. Die Zeitzoneninformation wird vom lokalen Betriebssystem des Amazon Aurora MySQL-DB-Clusters übernommen. Weitere Informationen finden Sie unter Lokale Zeitzone für Amazon Aurora-DB-Cluster.

Bevor Sie beginnen

Bevor Sie Ihre Daten in einen Amazon S3-Bucket kopieren und daraus einen DB-Cluster wiederherstellen können, müssen Sie folgende Schritte durchführen:

- Installieren Sie Percona XtraBackup auf Ihrem lokalen Server.
- Autorisieren Sie Aurora MySQL für den Zugriff auf den Amazon S3-Bucket in Ihrem Namen.

Percona installieren XtraBackup

Amazon Aurora kann einen DB-Cluster aus Dateien wiederherstellen, die mit Percona XtraBackup erstellt wurden. Sie können Percona XtraBackup über Software-Downloads — Percona installieren.

Verwenden Sie für die MySQL 5.7-Migration Percona XtraBackup 2.4.

Verwenden Sie für die MySQL 8.0-Migration Percona XtraBackup 8.0. Stellen Sie sicher, dass die XtraBackup Percona-Version mit der Engine-Version Ihrer Quelldatenbank kompatibel ist.

Erforderliche Berechtigungen

Für die Migration von MySQL-Daten in einen Amazon Aurora MySQL-DB-Cluster sind mehrere Berechtigungen erforderlich:

- Der Benutzer, der Aurora auffordert, einen neuen Cluster aus einem Amazon S3 S3-Bucket zu erstellen, muss über die Berechtigung verfügen, die Buckets für Ihr AWS Konto aufzulisten. Sie gewähren dem Benutzer diese Berechtigung mithilfe einer AWS Identity and Access Management (IAM-) Richtlinie.

- Aurora benötigt die Berechtigung, in Ihrem Namen auf den Amazon S3-Bucket mit den Dateien zum Erstellen des Amazon Aurora MySQL-DB-Clusters zuzugreifen. Sie erteilen Aurora die erforderlichen Berechtigungen, indem Sie eine IAM-Servicerolle verwenden.
- Der anfordernde Benutzer muss zudem über die Berechtigung zum Auflisten der IAM-Rollen Ihres AWS -Kontos verfügen.
- Wenn der anfordernde Benutzer die IAM-Servicerolle erstellen oder anfordern möchte, dass die IAM-Servicerolle von Aurora erstellt wird (über die Konsole), muss er über die Berechtigung zum Erstellen einer IAM-Rolle für Ihr AWS -Konto verfügen.
- Wenn Sie beabsichtigen, die Daten während des Migrationsprozesses zu verschlüsseln, aktualisieren Sie die IAM-Richtlinie des Benutzers, der die Migration durchführen wird, um RDS-Zugriff auf die für die Verschlüsselung der Backups AWS KMS keys verwendeten Daten zu gewähren. Anweisungen finden Sie unter Erstellen einer IAM-Zugriffsrichtlinie für AWS KMS-Ressourcen.

Die folgende IAM-Richtlinie gewährt einem Benutzer beispielsweise die erforderlichen Mindestberechtigungen zur Verwendung der Konsole, um IAM-Rollen aufzulisten, eine IAM-Rolle zu erstellen, die Amazon S3-Buckets für Ihr Konto aufzulisten und die KMS-Schlüssel aufzulisten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:AttachRolePolicy",
                "s3:ListBucket",
                "kms:ListKeys"
            ],
            "Resource": "*"
        }
    ]
}
```

Damit ein IAM-Benutzer eine IAM-Rolle mit einem Amazon S3-Bucket verknüpfen kann, muss der IAM-Benutzer die Berechtigung `iam:PassRole` für diese IAM-Rolle besitzen. Mit dieser

Berechtigung kann ein Administrator einschränken, welche IAM-Rollen ein Benutzer mit Amazon S3-Buckets verknüpfen kann.

So ermöglicht die folgende IAM-Richtlinie einem Benutzer, die Rolle namens `S3Access` mit einem Amazon S3-Bucket zu verknüpfen.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AllowS3AccessRole",
            "Effect":"Allow",
            "Action":"iam:PassRole",
            "Resource":"arn:aws:iam::123456789012:role/S3Access"
        }
    ]
}
```

Weitere Informationen zu IAM-Benutzerberechtigungen finden Sie unter Verwalten des Zugriffs mit Richtlinien.

Erstellen der IAM-Servicerolle

Sie können eine Rolle für sich selbst AWS Management Console erstellen lassen, indem Sie die Option Neue Rolle erstellen wählen (siehe weiter unten in diesem Thema). Wenn Sie diese Option auswählen und einen Namen für die neue Rolle angeben, erstellt Aurora die benötigte IAM-Servicerolle, damit Aurora mit dem von Ihnen angegebenen Namen auf Ihren Amazon S3-Bucket zugreifen kann.

Alternativ können Sie die Rolle auf folgende Weise manuell erstellen.

So erstellen Sie eine IAM-Rolle für Aurora zum Zugriff auf Amazon S3

1. Führen Sie die Schritte unter au Erstellen einer IAM-Zugriffsrichtlinie für Amazon S3-Ressourcen.
2. Führen Sie die Schritte unter au Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.
3. Führen Sie die Schritte unter au Zuweisen einer IAM-Rolle zu einem Amazon-Aurora-MySQL-DB-Cluster.

Sichern der wiederherzustellenden Dateien als Amazon Aurora MySQL-DB-Cluster

Sie können mit Percona eine vollständige Sicherung Ihrer MySQL-Datenbankdateien erstellen XtraBackup und die Sicherungsdateien in einen Amazon S3 S3-Bucket hochladen. Wenn Sie Percona bereits XtraBackup zum Sichern Ihrer MySQL-Datenbankdateien verwenden, können Sie alternativ Ihre vorhandenen vollständigen und inkrementellen Backup-Verzeichnisse und -Dateien in einen Amazon S3 S3-Bucket hochladen.

Themen

- Erstellen Sie ein vollständiges Backup mit Percona XtraBackup
- Verwenden von inkrementellen Backups mit Percona XtraBackup
- Überlegungen zu Sicherungen

Erstellen Sie ein vollständiges Backup mit Percona XtraBackup

Um eine vollständige Sicherung Ihrer MySQL-Datenbankdateien zu erstellen, die aus Amazon S3 wiederhergestellt werden kann, um einen Aurora MySQL-DB-Cluster zu erstellen, verwenden Sie das XtraBackup Percona-Hilfsprogramm (`xtrabackup`), um Ihre Datenbank zu sichern.

Mit dem folgenden Befehl können Sie beispielsweise eine Sicherung einer MySQL-Datenbank erstellen und die Dateien im Ordner `/on-premises/s3-restore/backup` speichern.

```
xtrabackup --backup --user=<myuser> --password=<password> --target-dir=</on-premises/
s3-restore/backup>
```

Wenn Sie die Sicherung in einer Archivdatei komprimieren möchten (die bei Bedarf aufgeteilt werden kann), können Sie mit der Option `--stream` eines der folgenden Formate festlegen:

- Gzip (.gz)
- tar (.tar)
- Percona xbstream (.xbstream)

Mit dem folgenden Befehl wird eine Sicherung einer MySQL-Datenbank erstellt und in mehreren Gzip-Dateien gespeichert.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=tar \
   --target-dir=</on-premises/s3-restore/backup> | gzip - | split -d --bytes=500MB \
```

```
   - </on-premises/s3-restore/backup/backup>.tar.gz
```

Mit dem folgenden Befehl wird ein Backup einer MySQL-Datenbank erstellt und in mehreren tar-Dateien gespeichert.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=tar \
   --target-dir=</on-premises/s3-restore/backup> | split -d --bytes=500MB \
   - </on-premises/s3-restore/backup/backup>.tar
```

Mit dem folgenden Befehl wird ein Backup einer MySQL-Datenbank erstellt und in mehreren xbstream-Dateien gespeichert.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=xbstream \
   --target-dir=</on-premises/s3-restore/backup> | split -d --bytes=500MB \
   - </on-premises/s3-restore/backup/backup>.xbstream
```

> **Note**
>
> Falls der folgende Fehler angezeigt wird, haben Sie möglicherweise unterschiedliche Dateiformate in Ihrem Befehl verwendet:
>
> ```
> ERROR:/bin/tar: This does not look like a tar archive
> ```

Sobald Sie Ihre MySQL-Datenbank mit dem XtraBackup Percona-Hilfsprogramm gesichert haben, können Sie Ihre Backup-Verzeichnisse und -Dateien in einen Amazon S3 S3-Bucket kopieren.

Weitere Informationen zum Erstellen und Hochladen einer Datei in einen Amazon S3-Bucket finden Sie unter Erste Schritte mit Amazon Simple Storage Service im Amazon S3-Handbuch "Erste Schritte".

Verwenden von inkrementellen Backups mit Percona XtraBackup

Amazon Aurora MySQL unterstützt sowohl vollständige als auch inkrementelle Backups, die mit XtraBackup Percona erstellt wurden. Wenn Sie Percona bereits verwenden XtraBackup , um vollständige und inkrementelle Backups Ihrer MySQL-Datenbankdateien durchzuführen, müssen Sie kein vollständiges Backup erstellen und die Sicherungsdateien auf Amazon S3 hochladen. Sie können stattdessen viel Zeit sparen, indem Sie die vorhandenen Sicherungsverzeichnisse und -

dateien der vollständigen und inkrementelle Sicherungen in einen Amazon S3-Bucket hochladen. Weitere Informationen finden Sie unter Ein inkrementelles Backup erstellen auf der Percona-Website.

Wenn Sie die Dateien der vollständigen und inkrementellen Backups in einen Amazon S3-Bucket hochladen, müssen Sie den Inhalt des Basisverzeichnisses rekursiv kopieren. Es müssen sämtliche Verzeichnisse und Dateien der vollständigen und inkrementellen Backups enthalten sein. Diese Kopie muss die Verzeichnisstruktur im Amazon-S3-Bucket beibehalten. Aurora durchläuft alle Dateien und Verzeichnisse. Aurora verwendet die in jedem inkrementellen Backup enthaltene `xtrabackup-checkpoints`-Datei, um das Basisverzeichnis zu identifizieren und inkrementelle Backups nach dem Bereich der Protokollsequenznummer (Log Sequence Number, LSN) zu ordnen.

Weitere Informationen zum Erstellen und Hochladen einer Datei in einen Amazon S3-Bucket finden Sie unter Erste Schritte mit Amazon Simple Storage Service im Amazon S3-Handbuch "Erste Schritte".

Überlegungen zu Sicherungen

Aurora unterstützt keine Teil-Backups, die mit Percona XtraBackup erstellt wurden. Sie können beim Sichern der Quelldateien Ihrer Datenbank nicht die folgenden Optionen verwenden, um eine Teilsicherung zu erstellen: `--tables`, `--tables-exclude`, `--tables-file`, `--databases`, `--databases-exclude` oder `--databases-file`.

Weitere Informationen zum Sichern Ihrer Datenbank mit Percona finden Sie unter Percona XtraBackup XtraBackup — Dokumentation und Arbeiten mit Binärprotokollen auf der Percona-Website.

Aurora unterstützt inkrementelle Backups, die mit XtraBackup Percona erstellt wurden. Weitere Informationen finden Sie unter Ein inkrementelles Backup erstellen auf der Percona-Website.

Aurora verarbeitet Sicherungsdateien auf Basis des Dateinamens. Achten Sie daher unbedingt darauf, dass die Namenserweiterungen der Sicherungsdateien dem Dateiformat entsprechen — z. B. `.xbstream` für Dateien, die im xbstream-Format von Percona gespeichert wurden.

Aurora verarbeitet Sicherungsdateien in alphanumerischer Reihenfolge. Verwenden Sie immer die Option `split` für den Befehl `xtrabackup`, um sicherzustellen, dass die Sicherungsdateien in der richtigen Reihenfolge geschrieben und benannt werden.

Amazon S3 begrenzt die Größe einer Datei, die in einen Amazon S3-Bucket hochgeladen werden kann, auf 5 TB. Wenn die Sicherungsdaten Ihrer Datenbank 5 TB überschreiten, müssen Sie die Sicherungsdateien mit dem Befehl `split` in mehrere Dateien aufteilen, die jeweils kleiner als 5 TB sind.

Aurora begrenzt die Anzahl der Quelldateien, die in einen Amazon S3-Bucket hochgeladen werden können, auf 1 Million Dateien. In manchen Situationen können die Sicherungsdaten Ihrer Datenbank einschließlich aller vollständigen und inkrementellen Sicherungen aus sehr vielen Dateien bestehen. Verwenden Sie in diesen Fällen ein tar-Archiv (.tar.gz), um die Dateien der vollständigen und inkrementellen Sicherungen im Amazon S3-Bucket zu speichern.

Sie können Dateien beim Hochladen in einen Amazon S3-Bucket serverseitig verschlüsseln lassen. Anschließend können Sie aus diesen verschlüsselten Dateien ein Amazon-Aurora-MySQL-DB-Cluster wiederherstellen. Amazon Aurora MySQL kann DB-Cluster mit Dateien wiederherstellen, die mittels der folgenden Arten der serverseitigen Verschlüsselung verschlüsselt wurden:

- Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3): Jedes Objekt wird mit einem eindeutigen Schlüssel mit starker Multifaktor-Verschlüsselung verschlüsselt.
- Serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln (SSE-KMS) — Ähnlich wie SSE-S3, aber Sie haben die Möglichkeit, Verschlüsselungsschlüssel selbst zu erstellen und zu verwalten, und es gibt auch andere Unterschiede.

Informationen zur serverseitigen Verschlüsselung beim Hochladen von Dateien in einen Amazon S3-Bucket finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung im Amazon S3-Entwicklerhandbuch.

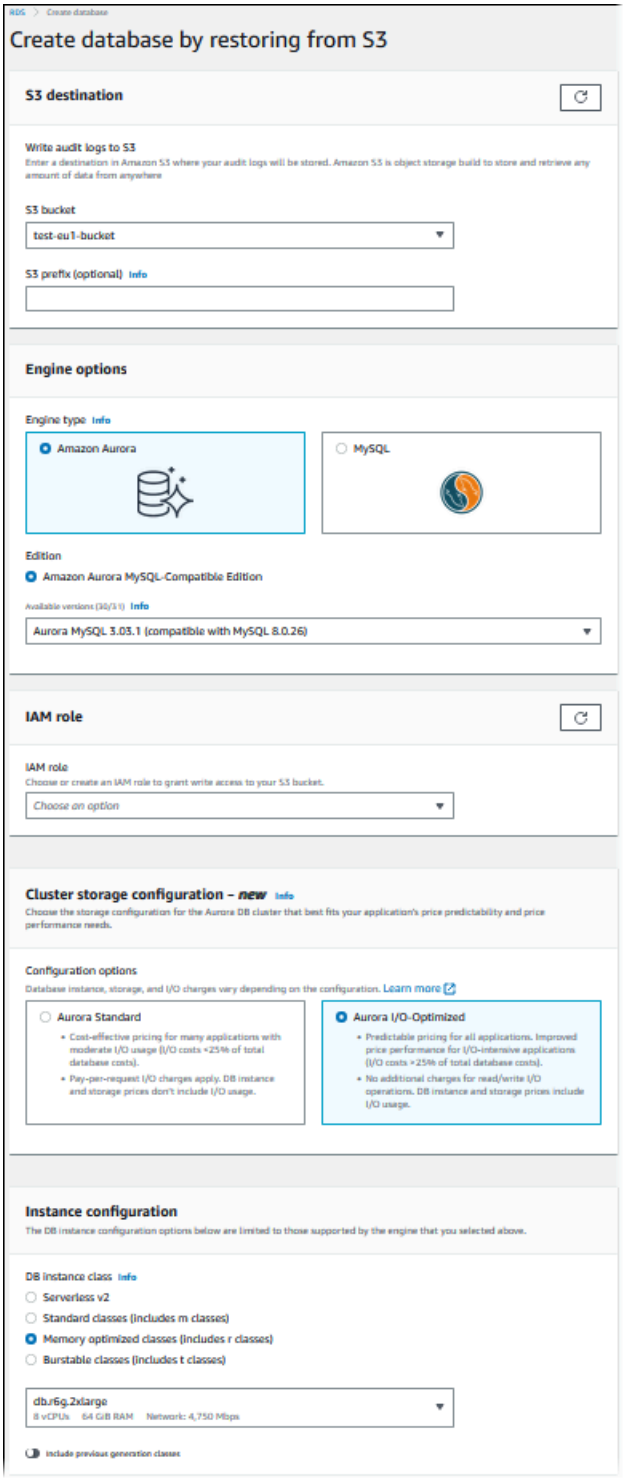
Wiederherstellen eines Amazon Aurora-MySQL-DB-Clusters aus einem Amazon S3-Bucket

Sie können Ihre Sicherungsdateien aus Ihrem Amazon-S3-Bucket wiederherstellen, um einen neuen Amazon-Aurora-MySQL-DB-Cluster zu erstellen, indem Sie die Amazon-RDS-Konsole verwenden.

So stellen Sie ein Amazon Aurora MySQL-DB-Cluster aus Dateien in einem Amazon S3-Bucket wieder her

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der oberen rechten Ecke der Amazon RDS-Konsole die AWS Region aus, in der Sie Ihren DB-Cluster erstellen möchten. Wählen Sie dieselbe AWS Region wie der Amazon S3 S3-Bucket, der Ihr Datenbank-Backup enthält.
3. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann die Option Restore from S3 (Aus S3 wiederherstellen) aus.
4. Wählen Sie Von S3 wiederherstellen.

Die Seite Datenbank durch Wiederherstellen von S3 erstellen wird angezeigt.



5. Unter S3-Ziel:

   a. Wählen Sie den S3-Bucket aus, in dem sich die Sicherungsdateien befinden.

b. (Optional) Geben Sie für S3 folder path prefix (S3-Ordnerpfadpräfix) ein Dateipfadpräfix für die Dateien ein, die in Ihrem Amazon S3-Bucket gespeichert sind.

   Wenn Sie kein Präfix angeben, dann erstellt RDS Ihre DB-Instance unter Verwendung aller Dateien und Ordner im Stammordner des S3-Bucket. Wenn Sie ein Präfix angeben, erstellt RDS Ihre DB-Instance mit den Ordnern und Dateien im S3-Bucket, deren vollständiger Pfadname mit dem angegebenen Präfix beginnt.

   Beispiel: Sie speichern Sicherungsdateien auf S3 in einem Unterordner namens 'backups' und haben mehrere Sätze von Sicherungsdateien, die sich jeweils in einem eigenen Verzeichnis befinden (gzip_backup1, gzip_backup2 usw.). Sie müssen nun das Präfix backups/gzip_backup1 angeben, um die Wiederherstellung mit den Dateien im Ordner gzip_backup1 durchzuführen.

6. Unter Engine-Optionen:

   a. Wählen Sie in Engine type (Engine-Typ) die Option Amazon Aurora aus.

   b. Wählen Sie für Version die Aurora MySQL-Engine-Version für Ihre wiederhergestellte DB-Instance aus.

7. Für die IAM-Rolle können Sie eine vorhandene IAM-Rolle auswählen.

8. (Optional) Sie können auch eine neue IAM-Rolle erstellen lassen, indem Sie Neue Rolle erstellen wählen. Wenn ja:

   a. Geben Sie den IAM-Rollennamen ein.

   b. Wählen Sie aus, ob Sie den Zugriff auf den KMS-Schlüssel zulassen möchten:

      - Wenn Sie die Sicherungsdateien nicht verschlüsselt haben, wählen Sie No (Nein) aus.
      - Wenn Sie die Sicherungsdateien mit AES-256 (SSE-S3) verschlüsselt haben, als Sie diese zu Amazon S3 hochgeladen haben, wählen Sie Nein aus. In diesem Fall werden die Daten automatisch entschlüsselt.
      - Wenn Sie die Sicherungsdateien beim Hochladen auf Amazon S3 mit serverseitiger Verschlüsselung AWS KMS (SSE-KMS) verschlüsselt haben, wählen Sie Ja. Wählen Sie dann den richtigen KMS-Schlüssel für AWS KMS key.

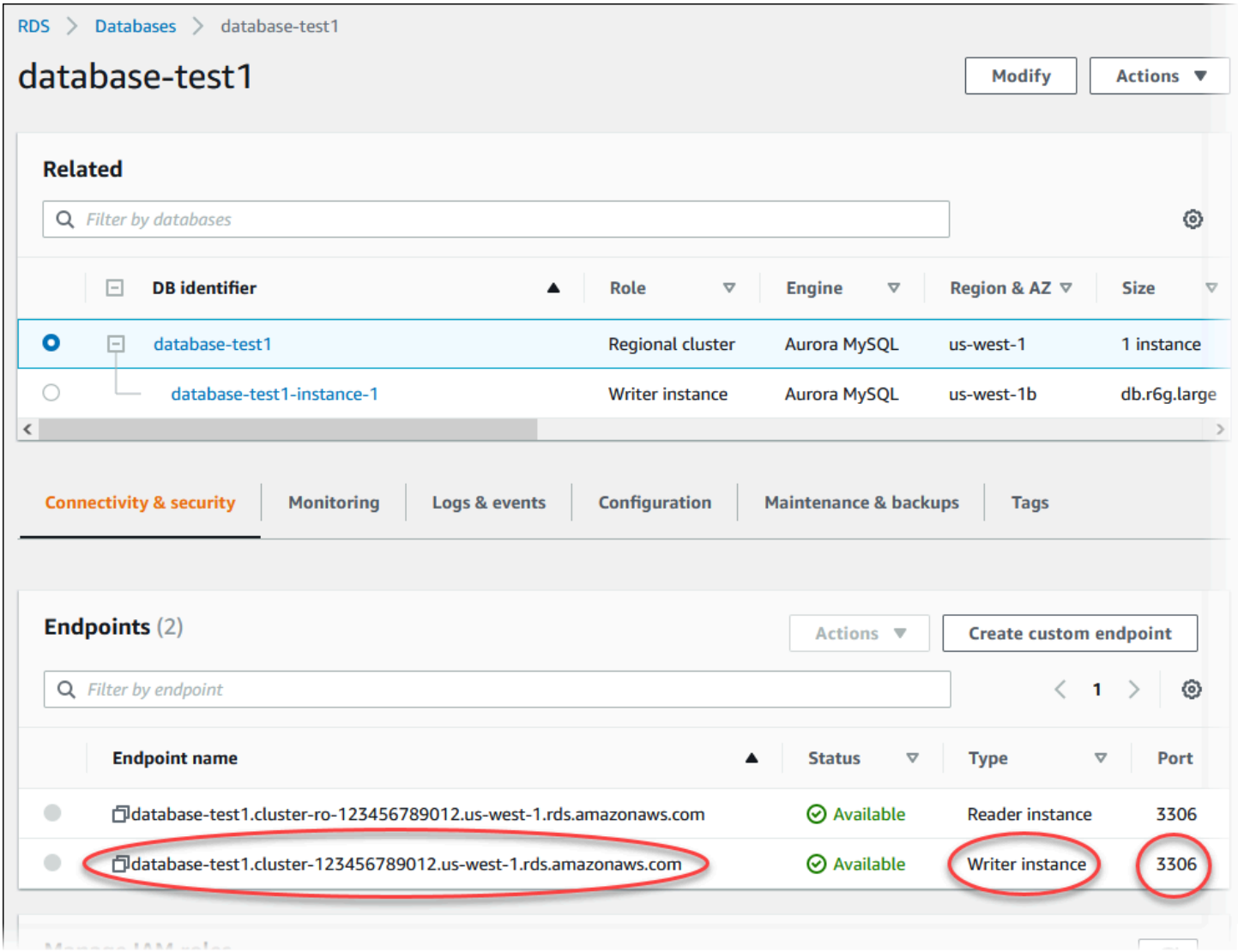
        Das AWS Management Console erstellt eine IAM-Richtlinie, die es Aurora ermöglicht, die Daten zu entschlüsseln.

Weitere Informationen finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung im Amazon S3-Entwicklerhandbuch.

9. Wählen Sie Einstellungen für Ihren DB-Cluster aus, z. B. die DB-Cluster-Speicherkonfiguration, die DB-Instance-Klasse, die DB-Cluster-ID und die Anmeldeinformationen. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.
10. Passen Sie zusätzliche Einstellungen für Ihren Aurora MySQL-DB-Cluster nach Bedarf an.
11. Wählen Sie Create database (Datenbank erstellen) , um Ihre Aurora-DB-Instance zu starten.

In der Amazon RDS-Konsole wird die neue DB-Instance in der Liste der DB-Instances angezeigt. Die DB-Instance wird mit dem Status creating (Wird erstellt) angezeigt, bis sie erstellt wurde und einsatzbereit ist. Wenn sich der Status in available (Verfügbar) ändert, können Sie die Verbindung mit der primären Instance des DB-Clusters herstellen. Je nach Klasse und Speicherort der DB-Instance kann es einige Minuten dauern, bis sie verfügbar ist.

Um das neu erstellte Cluster anzuzeigen, wählen Sie die Ansicht Database (Datenbank) in der Amazon RDS-Konsole und anschließend das DB-Cluster aus. Weitere Informationen finden Sie unter Anzeigen eines Amazon Aurora-DB-Clusters.



Notieren Sie den Port und den Writer-Endpunkt des DB-Clusters. Verwenden Sie den Writer-Endpunkt und den Port des DB-Clusters in den JDBC- und ODBC-Verbindungszeichenfolgen aller Anwendungen, die Lese- oder Schreibvorgänge ausführen.

Synchronisieren des Amazon Aurora MySQL-DB-Clusters mit der MySQL-Datenbank mittels Replikation

Damit es zu einer möglichst kurzen bzw. überhaupt keiner Unterbrechung während der Migration kommt, können Sie die in der MySQL-Datenbank durchgeführten Transaktionen mittels Replikation in das Aurora MySQL-DB-Cluster übernehmen. Durch die Replikation können die in der MySQL-Datenbank während der Migration durchgeführten Transaktionen in das DB-Cluster übernommen werden. Sobald das DB-Cluster auf dem Stand des MySQL-Masters ist, können Sie die Replikation anhalten und die Migration nach Aurora MySQL beenden.

Themen

Konfigurieren der externen MySQL-Datenbank und des Aurora MySQL-DB-Clusters für die verschlüsselte Replikation

Wenn Sie Daten sicher replizieren möchten, können Sie eine verschlüsselte Replikation verwenden.

> **Note**
>
> Wenn Sie keine verschlüsselte Replikation benötigen, können Sie diese Schritte überspringen und mit der Anleitung unter fortfahre Synchronisieren des Amazon Aurora MySQL-DB-Clusters mit der externen MySQL-Datenbank.

Folgende Voraussetzungen gelten für die Verwendung einer verschlüsselten Replikation:

- Secure Sockets Layer (SSL) muss in der externen MySQL-Primärdatenbank aktiviert sein.
- Ein Clientschlüssel und ein Clientzertifikat müssen für das Aurora MySQL-DB-Cluster vorbereitet werden.

Während der verschlüsselten Replikation dient das Aurora MySQL-DB-Cluster als Client für den MySQL-Datenbankserver. Die Zertifikate und Schlüssel für den Aurora MySQL-Client befinden sich in Dateien im PEM-Format.

So konfigurieren Sie die externe MySQL-Datenbank und das Aurora MySQL-DB-Cluster für die verschlüsselte Replikation

1. Stellen Sie sicher, dass alle Vorbereitungen für die verschlüsselte Replikation getroffen wurden:
   - Wenn SSL auf dem externen Server mit der MySQL-Primärdatenbank nicht aktiviert ist und Sie keinen Clientschlüssel und kein Clientzertifikat vorbereitet haben, aktivieren Sie SSL auf dem MySQL-Datenbankserver und generieren Sie den Clientschlüssel und das Clientzertifikat.
   - Wenn SSL auf die externen Primäre aktiviert ist, geben Sie einen Clientschlüssel und ein Clientzertifikat für das Aurora MySQL-DB-Cluster an. Wenn Sie diese Werte nicht haben,

erstellen Sie ein einen neuen Schlüssel und ein neues Zertifikat für das Aurora MySQL-DB-Cluster. Sie benötigen zur Signierung des Clientzertifikats den Zertifizierungsstellenschlüssel, den Sie zum Konfigurieren von SSL auf der externen MySQL-Primärdatenbank verwendet haben.

Weitere Informationen finden Sie unter Creating SSL Certificates and Keys Using openssl in der MySQL-Dokumentation.

Sie benötigen das Zertifizierungsstellenzertifikat, den Clientschlüssel und das Clientzertifikat.

2. Stellen Sie als Primärbenutzer über SSL eine Verbindung zum Aurora MySQL-DB-Cluster her.

   Informationen zum Herstellen einer Verbindung mit einem Aurora MySQL-DB-Cluster über SSL finden Sie unter Verwenden von TLS mit DB-Clustern von Aurora MySQL.

3. Führen Sie die gespeicherte Prozedur mysql.rds_import_binlog_ssl_material aus, um die SSL-Informationen in das Aurora MySQL-DB-Cluster zu importieren.

   Fügen Sie die Informationen aus den PEM-Dateien für das Aurora MySQL-DB-Cluster in die korrekte JSON-Nutzlast für den Parameter `ssl_material_value` ein.

   Im folgenden Beispiel werden SSL-Informationen in ein Aurora MySQL-DB-Cluster importiert. Der Code in den PEM-Dateien ist in der Regel länger als in diesem Beispiel.

```
call mysql.rds_import_binlog_ssl_material(
'{"ssl_ca":"-----BEGIN CERTIFICATE-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END CERTIFICATE-----\n","ssl_cert":"-----BEGIN CERTIFICATE-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END CERTIFICATE-----\n","ssl_key":"-----BEGIN RSA PRIVATE KEY-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
```

```
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END RSA PRIVATE KEY-----\n"}');
```

Weitere Informationen finden Sie unter mysql.rds_import_binlog_ssl_material und Verwenden von TLS mit DB-Clustern von Aurora MySQL.

> **Note**
>
> Nach dem Ausführen der Prozedur werden die SSL-Informationen in Dateien gespeichert. Um die Dateien später zu löschen, können Sie die mysql.rds_remove_binlog_ssl_material gespeicherte Prozedur ausführen.

Synchronisieren des Amazon Aurora MySQL-DB-Clusters mit der externen MySQL-Datenbank

Sie können das Amazon Aurora MySQL-DB-Cluster mittels Replikation mit der MySQL-Datenbank synchronisieren.

So synchronisieren Sie das Aurora MySQL-DB-Cluster mittels Replikation mit der MySQL-Datenbank

1. Stellen Sie sicher, dass die Datei "/etc/my.cnf" für die externe MySQL-Datenbank die relevanten Einträge enthält.

   Wenn keine verschlüsselte Replikation erforderlich ist, muss die externe MySQL-Datenbank mit aktivierten Binärprotokollen (binlogs) und deaktiviertem SSL gestartet werden. Dies sind die relevanten Einträge für unverschlüsselte Daten in der Datei "/etc/my.cnf".

   ```
   log-bin=mysql-bin
   server-id=2133421
   innodb_flush_log_at_trx_commit=1
   sync_binlog=1
   ```

   Wenn die verschlüsselte Replikation erforderlich ist, muss die externe MySQL-Datenbank mit aktivierten Binärprotokollen und aktiviertem SSL gestartet werden. Die Einträge in der Datei "/etc/my.cnf" müssen dann die Speicherorte der PEM-Dateien für den MySQL-Datenbankserver enthalten.

```
log-bin=mysql-bin
server-id=2133421
innodb_flush_log_at_trx_commit=1
sync_binlog=1

# Setup SSL.
ssl-ca=/home/sslcerts/ca.pem
ssl-cert=/home/sslcerts/server-cert.pem
ssl-key=/home/sslcerts/server-key.pem
```

Mit dem folgenden Befehl können Sie prüfen, ob SSL aktiviert ist.

```
mysql> show variables like 'have_ssl';
```

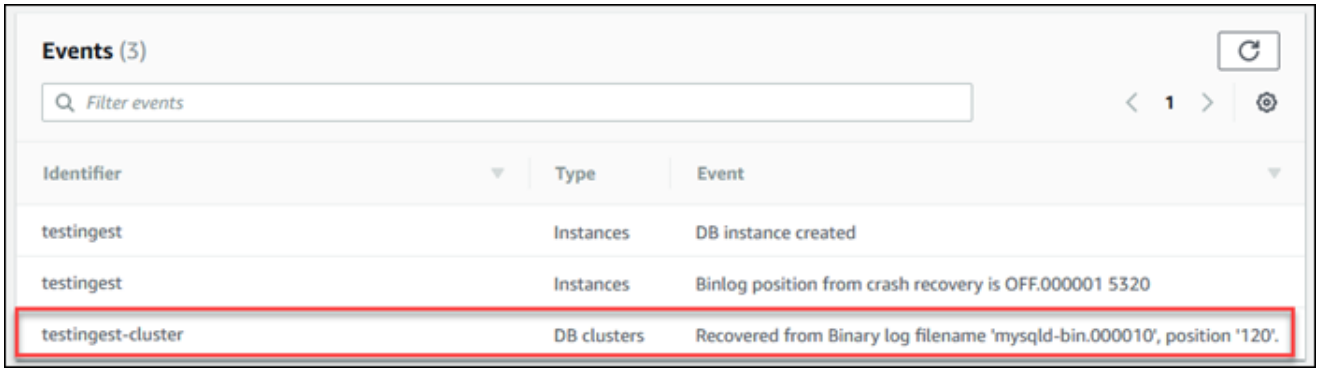
Die Ausgabe sollte in etwa wie folgt aussehen.

```
+~-~-~-~-~-~-~-~-~-~-~-~-~-~-~--+~-~-~-~-~-~--+
| Variable_name | Value |
+~-~-~-~-~-~-~-~-~-~-~-~-~-~-~--+~-~-~-~-~-~--+
| have_ssl      | YES   |
+~-~-~-~-~-~-~-~-~-~-~-~-~-~-~--+~-~-~-~-~-~--+
1 row in set (0.00 sec)
```

2. Bestimmen Sie die Startposition für die Replikation im Binärprotokoll. Sie legen die Startposition für die Replikation in einem späteren Schritt fest.

   Mit dem AWS Management Console

   a. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
   b. Wählen Sie im Navigationsbereich die Option Events.
   c. Notieren Sie in der Liste Events (Ereignisse) die Position im Ereignis Recovered from Binary log filename (Wiederhergestellt aus Binärprotokoll-Dateiname).



Verwenden Sie den AWS CLI

Sie können den Namen und die Position der Binlog-Datei auch mit dem Befehl AWS CLI describe-events abrufen. Im Folgenden wird ein `describe-events` Beispielbefehl gezeigt.

```
PROMPT> aws rds describe-events
```

Identifizieren Sie in der Ausgabe das Ereignis, das die Binärprotokoll-Position anzeigt.

3. Erstellen Sie bei bestehender Verbindung mit der externen MySQL-Datenbank einen Benutzer für die Replikation. Dieses Konto wird ausschließlich für die Replikation verwendet und muss auf Ihre Domäne beschränkt sein, um die Sicherheit zu erhöhen. Im Folgenden wird ein Beispiel gezeigt.

```
mysql> CREATE USER '<user_name>'@'<domain_name>' IDENTIFIED BY '<password>';
```

Der Benutzer benötigt die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE`. Gewähren Sie dem Benutzer diese Berechtigungen.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO
 '<user_name>'@'<domain_name>';
```

Wenn die Replikation verschlüsselt durchgeführt werden muss, fordern Sie für den Replikationsbenutzer eine SSL-Verbindung an. Sie können beispielsweise das folgende Statement verwenden, damit für das Benutzerkonto "encrypted_user" eine SSL-Verbindung *<user_name>*.

```
GRANT USAGE ON *.* TO '<user_name>'@'<domain_name>' REQUIRE SSL;
```

> **Note**
>
> Wenn `REQUIRE SSL` nicht angegeben wird, kann die Replikationsverbindung ohne entsprechende Meldung auf eine unverschlüsselte Verbindung zurückgesetzt werden.

4. Fügen Sie in der Amazon RDS-Console die IP-Adresse des Servers, der die externe MySQL-Datenbank hostet, zur VPC-Sicherheitsgruppe für den Aurora MySQL-DB-Cluster hinzu. Weitere Informationen zum Ändern einer VPC-Sicherheitsgruppe finden Sie unter Sicherheitsgruppen für Ihre VPC im Amazon Virtual Private Cloud-Benutzerhandbuch.

   Sie müssen möglicherweise noch das lokale Netzwerk so konfigurieren, dass es Verbindungen von der IP-Adresse des Aurora MySQL-DB-Clusters zulässt, damit Sie mit der externen MySQL-Datenbank kommunizieren können. Verwenden Sie den Befehl `host`, um die IP-Adresse des Aurora MySQL-DB-Clusters herauszufinden.

   ```
   host <db_cluster_endpoint>
   ```

   Der Hostname ist der DNS-Name aus dem Aurora MySQL-DB-Cluster-Endpunkt.

5. Aktivieren Sie die Binärprotokollreplikation, indem Sie die gespeicherte Prozedur mysql.rds_reset_external_master (Aurora-MySQL-Version 2) oder mysql.rds_reset_external_source (Aurora MySQL Version 3) ausführen. Diese gespeicherte Prozedur hat die folgende Syntax.

   ```
   CALL mysql.rds_set_external_master (
     host_name
     , host_port
     , replication_user_name
     , replication_user_password
     , mysql_binary_log_file_name
     , mysql_binary_log_file_location
     , ssl_encryption
   );

   CALL mysql.rds_set_external_source (
   ```

```
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
);
```

Informationen zu den Parametern finden Sie unter mysql.rds_reset_external_master (Aurora-MySQL-Version 2) und mysql.rds_reset_external_source (Aurora MySQL Version 3).

Verwenden Sie für `mysql_binary_log_file_name` und `mysql_binary_log_file_location` die Position im Ereignis Recovered from Binary log filename (Wiederhergestellt aus Binärprotokoll-Dateiname), die Sie zuvor notiert haben.

Wenn die Daten im Aurora MySQL-DB-Cluster nicht verschlüsselt sind, muss der Parameter `ssl_encryption` auf `0` festgelegt werden. Sind die Daten verschlüsselt, muss der Parameter `ssl_encryption` auf 1 gesetzt werden.

Im folgenden Beispiel wird die Prozedur für ein Aurora MySQL-DB-Cluster mit verschlüsselten Daten ausgeführt.

```
CALL mysql.rds_set_external_master(
  'Externaldb.some.com',
  3306,
  'repl_user'@'mydomain.com',
  'password',
  'mysql-bin.000010',
  120,
  1);

CALL mysql.rds_set_external_source(
  'Externaldb.some.com',
  3306,
  'repl_user'@'mydomain.com',
  'password',
  'mysql-bin.000010',
  120,
  1);
```

Diese gespeicherte Prozedur weist die Parameter zu, die das Aurora MySQL-DB-Cluster zum Herstellen einer Verbindung mit der externen MySQL-Datenbank und zum Lesen seines Binärprotokolls verwendet. Wenn die Daten verschlüsselt sind, werden auch das SSL-Zertifizierungsstellenzertifikat, das Clientzertifikat und der Clientschlüssel auf die lokale Festplatte heruntergeladen.

6. Starten Sie die Binärprotokollreplikation, indem Sie die gespeicherte Prozedur mysql.rds_start_replication ausführen.

```
CALL mysql.rds_start_replication;
```

7. Überwachen Sie den Rückstand des Aurora MySQL-DB-Clusters gegenüber der MySQL-Replikationsprimärdatenbank. Stellen Sie dazu eine Verbindung zum Aurora MySQL-DB-Cluster her und führen Sie den folgenden Befehl aus.

```
Aurora MySQL version 2:
SHOW SLAVE STATUS;

Aurora MySQL version 3:
SHOW REPLICA STATUS;
```

In der Befehlsausgabe wird im Feld `Seconds Behind Master` angezeigt, wie weit das Aurora MySQL-DB-Cluster hinter der MySQL-Primären zurückliegt. Wenn dieser Wert `0` (null) lautet, hat das Aurora MySQL-DB-Cluster den Stand der Primären erreicht und Sie können im nächsten Schritt die Replikation anhalten.

8. Stellen Sie eine Verbindung zur MySQL-Replikationsprimärdatenbank her und halten Sie die Replikation an. Rufen Sie dazu die gespeicherte Prozedur mysql.rds_stop_replication auf.

```
CALL mysql.rds_stop_replication;
```

Verkürzung der Zeit für die physische Migration zu Amazon Aurora MySQL

Mit den folgenden Datenbankänderungen können Sie den Vorgang der Migration einer Datenbank zu Amazon Aurora MySQL beschleunigen.

> **Important**
>
> Stellen Sie sicher, dass Sie diese Updates auf einer Kopie der Produktionsdatenbank und nicht auf der Produktionsdatenbank selbst durchführen. Anschließend können Sie die Kopie sichern und zu Ihrem Aurora MySQL DB-Cluster wiederherstellen, um Service-Unterbrechungen in der Produktionsdatenbank vermeiden.

Nicht unterstützte Tabellentypen

Aurora MySQL unterstützt nur die InnoDB-Engine für Datenbanktabellen. Wenn die Datenbank MyISAM-Tabellen enthält, müssen diese vor der Migration nach Aurora MySQL konvertiert werden. Während der Migration wird für die Konvertierung von MyISAM nach InnoDB zusätzlicher Speicherplatz benötigt.

Um das Risiko zu senken, dass der Speicherplatz nicht ausreicht, oder um den Migrationsvorgang zu beschleunigen, wandeln Sie alle MyISAM-Tabellen vor der Migration in InnoDB-Tabellen um. Die Größe der resultierenden InnoDB-Tabelle entspricht den Größenanforderungen von Aurora MySQL für diese Tabelle. Führen Sie zum Umwandeln einer MyISAM-Tabelle in eine InnoDB-Tabelle den folgenden Befehl aus:

```
ALTER TABLE schema.table_name engine=innodb, algorithm=copy;
```

Aurora MySQL unterstützt keine komprimierten Tabellen oder Seiten, d. h. Tabellen, die mit `ROW_FORMAT=COMPRESSED` oder erstellt wurden`COMPRESSION = {"zlib"|"lz4"}`.

Um das Risiko zu senken, dass der Speicherplatz nicht ausreicht, oder um den Migrationsvorgang zu beschleunigen, erweitern Sie komprimierte Tabellen, indem Sie `ROW_FORMAT` auf `DEFAULT`, `COMPACT`, `DYNAMIC` oder `REDUNDANT` einstellen. Legen Sie für komprimierte Seiten fest`COMPRESSION="none"`.

Weitere Informationen finden Sie unter InnoDB-Zeilenformate und InnoDB-Tabellen- und Seitenkomprimierung in der MySQL-Dokumentation.

Sie können mit dem folgenden SQL-Skript alle Datenbanktabellen der MySQL-DB-Instance auflisten, die MyISAM-Tabellen oder komprimierte Tabellen sind.

```
-- This script examines a MySQL database for conditions that block
-- migrating the database into Aurora MySQL.
-- It must be run from an account that has read permission for the
```

```
-- INFORMATION_SCHEMA database.

-- Verify that this is a supported version of MySQL.

select msg as `==> Checking current version of MySQL.`
from
  (
  select
    'This script should be run on MySQL version 5.6 or higher. ' +
    'Earlier versions are not supported.' as msg,
    cast(substring_index(version(), '.', 1) as unsigned) * 100 +
      cast(substring_index(substring_index(version(), '.', 2), '.', -1)
      as unsigned)
    as major_minor
  ) as T
where major_minor <> 506;


-- List MyISAM and compressed tables. Include the table size.

select concat(TABLE_SCHEMA, '.', TABLE_NAME) as `==> MyISAM or Compressed Tables`,
round(((data_length + index_length) / 1024 / 1024), 2) "Approx size (MB)"
from INFORMATION_SCHEMA.TABLES
where
  ENGINE <> 'InnoDB'
  and
  (
    -- User tables
    TABLE_SCHEMA not in ('mysql', 'performance_schema',
                         'information_schema')
    or
    -- Non-standard system tables
    (
      TABLE_SCHEMA = 'mysql' and TABLE_NAME not in
        (
          'columns_priv', 'db', 'event', 'func', 'general_log',
          'help_category', 'help_keyword', 'help_relation',
          'help_topic', 'host', 'ndb_binlog_index', 'plugin',
          'proc', 'procs_priv', 'proxies_priv', 'servers', 'slow_log',
          'tables_priv', 'time_zone', 'time_zone_leap_second',
          'time_zone_name', 'time_zone_transition',
          'time_zone_transition_type', 'user'
        )
    )
```

```
  )
  or
  (
    -- Compressed tables
       ROW_FORMAT = 'Compressed'
  );
```

Benutzerkonten mit nicht unterstützten Rechten

Benutzerkonten mit Rechten, die von Aurora MySQL nicht unterstützt werden, werden ohne die nicht unterstützten Rechte importiert. Die Liste der unterstützten Rechte finden Sie unter Rollenbasiertes Berechtigungsmodell.

Sie können die folgende SQL-Abfrage in Ihrer Quelldatenbank ausführen, um die Benutzerkonten aufzulisten, die nicht unterstützte Rechte haben.

```
SELECT
    user,
    host
FROM
    mysql.user
WHERE
    Shutdown_priv = 'y'
    OR File_priv = 'y'
    OR Super_priv = 'y'
    OR Create_tablespace_priv = 'y';
```

Dynamische Rechte in Aurora MySQL Version 3

Dynamische Rechte werden nicht importiert. Aurora MySQL Version 3 unterstützt die folgenden dynamischen Rechte.

```
'APPLICATION_PASSWORD_ADMIN',
'CONNECTION_ADMIN',
'REPLICATION_APPLIER',
'ROLE_ADMIN',
'SESSION_VARIABLES_ADMIN',
'SET_USER_ID',
'XA_RECOVER_ADMIN'
```

Das folgende Beispielskript gewährt den Benutzerkonten im Aurora MySQL-DB-Cluster die unterstützten dynamischen Rechte.

```
-- This script finds the user accounts that have Aurora MySQL supported dynamic
 privileges
-- and grants them to corresponding user accounts in the Aurora MySQL DB cluster.

/home/ec2-user/opt/mysql/8.0.26/bin/mysql -uusername -pxxxxx -P8026 -h127.0.0.1 -BNe
 "SELECT
  CONCAT('GRANT ', GRANTS, ' ON *.* TO ', GRANTEE ,';') AS grant_statement
  FROM (select GRANTEE, group_concat(privilege_type) AS GRANTS FROM
 information_schema.user_privileges
      WHERE privilege_type IN (
        'APPLICATION_PASSWORD_ADMIN',
        'CONNECTION_ADMIN',
        'REPLICATION_APPLIER',
        'ROLE_ADMIN',
        'SESSION_VARIABLES_ADMIN',
        'SET_USER_ID',
        'XA_RECOVER_ADMIN')
      AND GRANTEE NOT IN (\"'mysql.session'@'localhost'\",
\"'mysql.infoschema'@'localhost'\",\"'mysql.sys'@'localhost'\") GROUP BY GRANTEE)
      AS PRIVGRANTS; " | /home/ec2-user/opt/mysql/8.0.26/bin/mysql -u master_username -
p master_password -h DB_cluster_endpoint
```

Gespeicherte Objekte mit 'rdsadmin'@'localhost' als Definierer

Funktionen, Prozeduren, Ansichten, Ereignisse und Trigger mit `'rdsadmin'@'localhost'` als Definierer werden nicht importiert.

Mit dem folgenden SQL-Skript können die in Ihrer MySQL-Datenbank gespeicherten Objekte mit nicht unterstützten Definierern auflisten.

```
-- This SQL query lists routines with `rdsadmin`@`localhost` as the definer.

SELECT
    ROUTINE_SCHEMA,
    ROUTINE_NAME
FROM
    information_schema.routines
WHERE
    definer = 'rdsadmin@localhost';

-- This SQL query lists triggers with `rdsadmin`@`localhost` as the definer.

SELECT
```

```
    TRIGGER_SCHEMA,
    TRIGGER_NAME,
    DEFINER
FROM
    information_schema.triggers
WHERE
    DEFINER = 'rdsadmin@localhost';

-- This SQL query lists events with `rdsadmin`@`localhost` as the definer.

SELECT
    EVENT_SCHEMA,
    EVENT_NAME
FROM
    information_schema.events
WHERE
    DEFINER = 'rdsadmin@localhost';

-- This SQL query lists views with `rdsadmin`@`localhost` as the definer.
SELECT
    TABLE_SCHEMA,
    TABLE_NAME
FROM
    information_schema.views
WHERE
    DEFINER = 'rdsadmin@localhost';
```

Logische Migration von MySQL zu Amazon Aurora MySQL mithilfe von mysqldump

Da Amazon Aurora MySQL eine MySQL-kompatible Datenbank ist, können Sie mit dem Dienstprogramm `mysqldump` Daten aus einer MySQL- oder MariaDB-Datenbank in einen vorhandenen Aurora MySQL-DB-Cluster kopieren.

Informationen, wie Sie dies für sehr große MySQL-Datenbanken durchführen, finden Sie unter Importieren von Daten in eine MySQL- oder MariaDB-DB-Instance mit reduzierter Ausfallzeit. Informationen zu MySQL-Datenbanken mit kleineren Datenmengen finden Sie unter Importieren von Daten aus einer MySQL- oder MariaDB-DB in eine MySQL- oder MariaDB-DB-Instance.

Migrieren von Daten aus einer DB-Instance von RDS für MySQL in einen DB-Cluster von Amazon Aurora MySQL

Sie können Daten aus einer DB-Instance von RDS für MySQL in einen DB-Cluster von Amazon Aurora MySQL migrieren (kopieren).

Themen

- Migrieren eines RDS für MySQL-Snapshots zu Aurora
- Migrieren von Daten aus einer RDS-für-MySQL-DB-Instance zu einem Amazon-Aurora-MySQL-DB-Cluster mittels einer Aurora Read Replica (Lesereplikat)

> **Note**
>
> Da Amazon Aurora MySQL mit MySQL kompatibel ist, können Sie Daten aus einer MySQL-Datenbank migrieren, indem Sie eine Replikation zwischen Ihrer MySQL-Datenbank und einem Amazon Aurora MySQL-DB-Cluster einrichten. Weitere Informationen finden Sie unter Replikation mit Amazon Aurora.

Migrieren eines RDS für MySQL-Snapshots zu Aurora

Sie können einen DB-Snapshot einer RDS-MySQL-DB-Instance migrieren, um einen Aurora-MySQL-DB-Cluster zu erstellen. Der neue Aurora-MySQL-DB-Cluster wird mit den Daten der ursprünglichen RDS für MySQL-DB-Instance gefüllt. Der DB-Snapshot muss von einer DB-Instance von Amazon RDS erstellt worden sein, die eine mit Aurora MySQL kompatible MySQL-Version ausführt.

Sie können einen manuell oder automatisch erstellten DB-Snapshot migrieren. Nachdem der DB-Cluster erstellt wurde, können Sie optional Aurora-Replikate erstellen.

> **Note**
>
> Sie können eine MySQL-DB-Instance zu einem Aurora MySQL-DB-Cluster auch migrieren, indem Sie zunächst eine Aurora Read Replica der MySQL-Quell-DB-Instance erstellen. Weitere Informationen finden Sie unter Migrieren von Daten aus einer RDS-für-MySQL-DB-Instance zu einem Amazon-Aurora-MySQL-DB-Cluster mittels einer Aurora Read Replica (Lesereplikat).

Sie können von einigen älteren Versionen von MySQL 8.0, einschließlich 8.0.11, 8.0.13 und 8.0.15, nicht zu Aurora MySQL Version 3.05 und höher migrieren. Wir empfehlen, vor der Migration auf MySQL Version 8.0.28 zu aktualisieren.

Gehen Sie wie folgt vor:

1. Bestimmen Sie die Menge an Speicher, die für den Aurora MySQL-DB-Cluster bereitgestellt werden soll. Weitere Informationen finden Sie unter Wie viel Speicherplatz benötige ich?
2. Verwenden Sie die Konsole zum Erstellen des Snapshots in der AWS-Region, in der sich die Amazon-RDS-MySQL-Instance befindet. Informationen zum Erstellen von DB-Snapshots finden Sie unter Erstellen eines DB-Snapshots.
3. Wenn sich der DB-Snapshot nicht in derselben AWS-Region wie der DB-Cluster befindet, kopieren Sie ihn mit der Amazon-RDS-Konsole in diese AWS-Region. Informationen zum Kopieren von DB-Snapshots finden Sie unter Kopieren eines DB-Snapshots.
4. Verwenden Sie die Konsole, um den DB-Snapshot zu migrieren und einen Aurora MySQL-DB-Cluster mit denselben Datenbanken wie die ursprüngliche MySQL-DB-Instance zu erstellen.

⚠ Warning

Amazon RDS beschränkt jedes AWS-Konto auf jeweils eine Snapshot-Kopie in jede AWS-Region.

Wie viel Speicherplatz benötige ich?

Wenn Sie den Snapshot einer MySQL-DB-Instance zu einem Aurora MySQL-DB-Cluster migrieren, verwendet Aurora ein Amazon Elastic Block Store (Amazon EBS)-Volume, um die Daten aus dem Snapshot vor der Migration zu formatieren. In manchen Fällen ist zusätzlicher Speicherplatz erforderlich, um die Daten für die Migration zu formatieren.

Tabellen, die keine MyISAM-Tabellen und nicht komprimiert sind, können bis zu 16 TB groß sein. Wenn Sie MyISAM-Tabellen besitzen, muss Aurora zusätzlichen Speicherplatz im Volume verwenden, um die Tabellen so zu konvertieren, dass sie mit Aurora MySQL kompatibel sind. Wenn Sie komprimierte Tabellen besitzen, muss Aurora zusätzlichen Speicherplatz im Volume verwenden, um diese Tabellen zu erweitern, bevor sie im Aurora-Cluster-Volume gespeichert werden. Aufgrund dieses zusätzlichen Platzbedarfs sollten Sie sicherstellen, dass keine der MyISAM-Tabellen und

der komprimierten Tabellen, die von Ihrer MySQL-DB-Instance migriert werden, die Größe von 8 TB übersteigt.

Reduzieren des erforderlichen Speicherplatzes für die Migration von Daten zu Amazon Aurora MySQL

Sie können bei Bedarf das Datenbankschema vor dem Migrieren nach Amazon Aurora ändern. Eine solche Änderung kann in den folgenden Fällen hilfreich sein:

- Sie möchten die Migration beschleunigen.
- Sie wissen nicht genau, wie viel Speicherplatz bereitgestellt werden muss.
- Ein Migrationsversuch ist fehlgeschlagen, weil nicht genügend Speicherplatz verfügbar war.

Sie können die folgenden Änderungen vornehmen, um das Migrieren einer Datenbank zu Amazon Aurora zu optimieren.

> **Important**
>
> Führen Sie diese Aktualisierungen für die neue DB-Instance durch, die aus einem Snapshot einer Produktionsdatenbank wiederhergestellt wurde, statt eine Produktions-Instance zu verwenden. Anschließend können Sie die Daten aus dem Snapshot der neuen DB-Instance in den Aurora-DB-Cluster migrieren, um Service-Unterbrechungen bei der Produktionsdatenbank zu vermeiden.

Tabellentyp	Einschränkung oder Richtlinie
MyISAM-Tabellen	Aurora MySQL unterstützt ausschließlich InnoDB-Tabellen. Wenn die Datenbank MyISAM-Tabellen enthält, müssen diese vor der Migration nach Aurora MySQL konvertiert werden. Während der Migration wird für die Konvertierung von MyISAM nach InnoDB zusätzlicher Speicherplatz benötigt. Um das Risiko zu senken, dass der Speicherplatz nicht ausreicht , oder um den Migrationsvorgang zu beschleunigen, wandeln Sie alle MyISAM-Tabellen vor der Migration in InnoDB-Tabellen um. Die Größe der resultierenden InnoDB-Tabelle entspricht

Tabellentyp	Einschränkung oder Richtlinie
	den Größenanforderungen von Aurora MySQL für diese Tabelle. Führen Sie zum Umwandeln einer MyISAM-Tabelle in eine InnoDB-Tabelle den folgenden Befehl aus: `alter table <schema>.<table_name> engine=innodb, algorithm=copy;`
Komprimierte Tabellen	Aurora MySQL unterstützt keine komprimierten Tabellen (d. h. mit erstellte Tabelle `ROW_FORMAT=COMPRESSED`). Um das Risiko zu senken, dass der Speicherplatz nicht ausreicht , oder um den Migrationsvorgang zu beschleunigen, erweitern Sie komprimierte Tabellen, indem Sie `ROW_FORMAT` auf `DEFAULT`, `COMPACT`, `DYNAMIC` oder `REDUNDANT` einstellen. Weitere Informationen finden Sie unter InnoDB row formats in der MySQL-Dokumentation.

Sie können mit dem folgenden SQL-Skript alle Datenbanktabellen der MySQL-DB-Instance auflisten, die MyISAM-Tabellen oder komprimierte Tabellen sind.

```
-- This script examines a MySQL database for conditions that block
-- migrating the database into Amazon Aurora.
-- It needs to be run from an account that has read permission for the
-- INFORMATION_SCHEMA database.

-- Verify that this is a supported version of MySQL.

select msg as `==> Checking current version of MySQL.`
from
  (
  select
    'This script should be run on MySQL version 5.6 or higher. ' +
    'Earlier versions are not supported.' as msg,
    cast(substring_index(version(), '.', 1) as unsigned) * 100 +
      cast(substring_index(substring_index(version(), '.', 2), '.', -1)
      as unsigned)
    as major_minor
  ) as T
```

```
where major_minor <> 506;


-- List MyISAM and compressed tables. Include the table size.

select concat(TABLE_SCHEMA, '.', TABLE_NAME) as `==> MyISAM or Compressed Tables`,
round(((data_length + index_length) / 1024 / 1024), 2) "Approx size (MB)"
from INFORMATION_SCHEMA.TABLES
where
  ENGINE <> 'InnoDB'
  and
  (
    -- User tables
    TABLE_SCHEMA not in ('mysql', 'performance_schema',
                         'information_schema')
    or
    -- Non-standard system tables
    (
      TABLE_SCHEMA = 'mysql' and TABLE_NAME not in
        (
          'columns_priv', 'db', 'event', 'func', 'general_log',
          'help_category', 'help_keyword', 'help_relation',
          'help_topic', 'host', 'ndb_binlog_index', 'plugin',
          'proc', 'procs_priv', 'proxies_priv', 'servers', 'slow_log',
          'tables_priv', 'time_zone', 'time_zone_leap_second',
          'time_zone_name', 'time_zone_transition',
          'time_zone_transition_type', 'user'
        )
    )
  )
  or
  (
    -- Compressed tables
       ROW_FORMAT = 'Compressed'
  );
```

Das Skript produziert eine Ausgabe wie im folgenden Beispiel. Das Beispiel zeigt zwei Tabellen, die vom MyISAM- in das InnoDB-Format umgewandelt werden müssen. Außerdem wird die ungefähre Größe jeder Tabelle in Megabyte (MB) angezeigt.

```
+---------------------------------+------------------+
| ==> MyISAM or Compressed Tables | Approx size (MB) |
+---------------------------------+------------------+
```

```
| test.name_table                  |          2102.25 |
| test.my_table                    |            65.25 |
+----------------------------------+------------------+
2 rows in set (0.01 sec)
```

Migrieren eines DB-Snapshots von RDS for MySQL zu einem Aurora-MySQL-DB-Cluster

Sie können einen DB-Snapshot einer DB-Instance von RDS for MySQL mit der AWS Management Console oder der AWS CLI migrieren, um einen Aurora-MySQL-DB-Cluster zu erstellen. Der neue Aurora-MySQL-DB-Cluster wird mit den Daten der ursprünglichen RDS für MySQL-DB-Instance gefüllt. Informationen zum Erstellen von DB-Snapshots finden Sie unter Erstellen eines DB-Snapshots.

Wenn sich der DB-Snapshot nicht in der AWS-Region befindet, in der Sie die Daten speichern möchten, kopieren Sie den DB-Snapshot in die betreffende AWS-Region. Informationen zum Kopieren von DB-Snapshots finden Sie unter Kopieren eines DB-Snapshots.

Konsole

Wenn Sie den DB-Snapshot mithilfe der AWS Management Console migrieren, nimmt die Konsole die erforderlichen Aktionen vor, um den DB-Cluster und die primäre Instance zu erstellen.

Sie können sich auch dafür entscheiden, dass Ihr neuer Aurora MySQL DB-Cluster im Ruhezustand verschlüsselt wird, indem Sie eine AWS KMS key.

So migrieren Sie einen MySQL -DB-Snapshot mithilfe der AWS Management Console:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Starten Sie die Migration entweder von der MySQL DB-Instance oder vom Snapshot aus:

   Um die Migration von der DB-Instance aus zu starten:

   1. Wählen Sie im Navigationsbereich Databases (Datenbanken) und anschließend die MySQL-DB-Instance aus.
   2. Wählen Sie unter Actions (Aktionen) die Option Migrate latest snapshot (Aktuellen Snapshot migrieren) aus.

   Um die Migration vom Snapshot aus zu starten:

1. Klicken Sie auf Snapshots (Snapshots).
2. Wählen Sie auf der Seite Snapshots (Snapshots) den Snapshot aus, den Sie zu einem Aurora MySQL-DB-Cluster migrieren möchten.
3. Wählen Sie die Option Snapshot-Aktionen und anschließend Snapshot migrieren.

Die Seite Datenbank migrieren wird angezeigt.

3. Legen Sie auf der Seite Migrate Database (Datenbank migrieren) Folgendes fest:

   - Migrate to DB Engine (Zu DB-Engine migrieren): Wählen Sie `aurora` aus.
   - DB Engine Version (DB-Engine-Version): Wählen Sie die DB-Engine-Version für das Aurora MySQL-DB-Cluster aus.
   - DB-Instance-Klasse: Wählen Sie eine DB-Instance-Klasse, die über ausreichend Speicher und Kapazität für Ihre Datenbank verfügt, z. B. `db.r3.large`. Aurora-Cluster-Volumes nehmen automatisch an Größe zu, wenn die Datenmenge in Ihrer Datenbank zunimmt. Ein Aurora-Cluster-Volume kann auf eine maximale Größe von 128 tebibytes (TiB) anwachsen. Sie müssen daher nur eine DB-Instance-Klasse auswählen, die den aktuellen Speicheranforderungen entspricht. Weitere Informationen finden Sie unter Übersicht über Amazon-Aurora-Speicher.
   - DB Instance Identifier (DB-Instance-Kennung): Geben Sie einen Namen für den DB-Cluster ein. Dieser muss im Konto für die ausgewählte AWS-Region eindeutig sein. Dieser Bezeichner wird in den Endpunktadressen für die Instances im DB-Cluster verwendet. Sie können den Namen aussagekräftiger machen, indem Sie Angaben wie AWS-Region und DB-Engine hinzufügen, z. B. **`aurora-cluster1`**.

     Für den DB-Instance-Bezeichner gelten folgende Einschränkungen:

     - Sie darf 1 bis 63 alphanumerische Zeichen oder Bindestriche enthalten.
     - Das erste Zeichen muss ein Buchstabe sein.
     - Er darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
     - Es muss für alle DB-Instances pro AWS-Konto und AWS-Region eindeutig sein.
   - Virtual Private Cloud (VPC): Wenn bereits eine VPC vorhanden ist, können Sie diese VPC mit dem Aurora MySQL-DB-Cluster verwenden, indem Sie die VPC-ID auswählen, beispielsweise `vpc-a464d1c1`. Weitere Informationen zum Erstellen einer VPC finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4).

Andernfalls können Sie von Aurora eine neue VPC erstellen lassen, indem Sie auf Neue VPC erstellen klicken.

- DB-Subnetzgruppe: Wenn bereits eine Subnetzgruppe vorhanden ist, können Sie diese Subnetzgruppe mit dem Aurora-MySQL-DB-Cluster verwenden, indem Sie die Subnetzgruppen-ID auswählen, beispielsweise `gs-subnet-group1`.

  Andernfalls können Sie von Aurora eine neue Subnetzgruppe erstellen lassen, indem Sie auf Neue Subnetzgruppe erstellen klicken.

- Öffentliche Zugänglichkeit: Wählen Sie Nein aus, um anzugeben, dass nur Ressourcen innerhalb Ihrer VPC auf Instances im DB-Cluster zugreifen dürfen. Wählen Sie Ja aus, um anzugeben, dass Ressourcen im öffentlichen Netzwerk auf Instances im DB-Cluster zugreifen dürfen. Die Standardeinstellung lautet Ja.

  > **Note**
  >
  > Der Produktions-DB-Cluster muss sich nicht unbedingt in einem öffentlichen Subnetz befinden, da nur die Anwendungsserver Zugriff auf ihren DB-Cluster benötigen. Wenn sich das DB-Cluster nicht in einem öffentlichen Subnetz befinden muss, legen Sie Publicly Accessible (Öffentlich zugänglich) auf No (Nein) fest.

- Availability Zone (Availability Zone): Wählen Sie die Availability Zone aus, in der die primäre Instance für Ihr Aurora-MySQL-DB-Cluster gehostet werden soll. Wenn die Availability Zone durch Aurora ausgewählt werden soll, wählen Sie No Preference (Keine Präferenz) aus.
- Database Port (Datenbankport): Geben Sie den Standardport ein, der beim Verbinden der Instances im Aurora MySQL-DB-Cluster verwendet werden soll. Der Standardwert ist `3306`.

  > **Note**
  >
  > Möglicherweise lässt die Firewall eines Unternehmens den Zugriff auf Standardports, wie z. B. den MySQL-Standardport 3306, nicht zu. Geben Sie in diesem Fall einen Port ein, der von der Firewall Ihres Unternehmens zugelassen wird. Sie benötigen diesen Port-Wert später, wenn Sie eine Verbindung mit dem Aurora MySQL-DB-Cluster herstellen.

- Verschlüsselung: Wählen Sie Verschlüsselung aktivieren aus, um Ihren neuen Aurora MySQL-DB-Cluster im Ruhezustand zu verschlüsseln. Wenn Sie Verschlüsselung aktivieren wählen, müssen Sie einen KMS-Schlüssel als Wert AWS KMS key wählen.

  Wenn Ihr DB-Snapshot nicht verschlüsselt ist, geben Sie einen Verschlüsselungsschlüssel an, damit Ihr DB-Cluster in Ruhe verschlüsselt wird.

  Wenn Ihr DB-Snapshot verschlüsselt ist, geben Sie einen Verschlüsselungsschlüssel an, damit Ihr DB-Cluster in Ruhe mit dem angegebenen Verschlüsselungsschlüssel verschlüsselt wird. Sie können den vom DB-Snapshot verwendeten Verschlüsselungsschlüssel oder einen anderen Schlüssel angeben. Aus einem verschlüsselten DB-Snapshot kann kein unverschlüsselter DB-Cluster erstellt werden.
- Auto Minor Version Upgrade (Automatisches Unterversions-Upgrade): Diese Einstellung ist für Aurora MySQL-DB-Cluster nicht relevant.

  Weitere Informationen über Engine-Updates für Aurora MySQL finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.

4. Wählen Sie Migrate (Migrieren) aus, um den DB-Snapshot zu migrieren.
5. Klicken Sie auf Instances und danach auf das Pfeilsymbol, um die DB-Cluster-Details anzuzeigen und den Fortschritt der Migration zu überwachen. Auf der Detailseite wird der Cluster-Endpunkt zum Herstellen einer Verbindung mit der primären Instance des DB-Clusters angezeigt. Weitere Informationen zum Herstellen einer Verbindung mit einem Aurora-MySQL-DB-Cluster finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

AWS CLI

Sie können einen Aurora-DB-Cluster aus einem DB-Snapshot einer RDS für MySQL-DB-Instance erstellen, indem Sie den `restore-db-cluster-from-snapshot`-Befehl mit folgenden Parametern verwenden:

- `--db-cluster-identifier` – Der Name des zu erstellenden DB-Clusters.
- `--engine aurora-mysql` – Für einen mit MySQL 5.7 oder 8.0 kompatiblen DB-Cluster
- `--kms-key-id` – DerAWS KMS key zur optionalen Verschlüsselung des DB-Clusters, je nachdem, ob Ihr DB-Snapshot verschlüsselt ist.
  - Wenn Ihr DB-Snapshot nicht verschlüsselt ist, geben Sie einen Verschlüsselungsschlüssel an, damit Ihr DB-Cluster in Ruhe verschlüsselt wird. Andernfalls wird Ihr DB-Cluster nicht verschlüsselt.

- Wenn Ihr DB-Snapshot verschlüsselt ist, geben Sie einen Verschlüsselungsschlüssel an, damit Ihr DB-Cluster in Ruhe mit dem angegebenen Verschlüsselungsschlüssel verschlüsselt wird. Ansonsten wird Ihr DB-Cluster im Ruhezustand mit dem Verschlüsselungsschlüssel für den DB-Snapshot verschlüsselt.

  > **Note**
  >
  > Aus einem verschlüsselten DB-Snapshot kann kein unverschlüsselter DB-Cluster erstellt werden.

- `--snapshot-identifier` – Der Amazon-Ressourcenname (ARN) des zu migrierenden DB-Snapshots. Weitere Informationen zu Amazon RDS-ARNs finden Sie unter Amazon Relational Database Service (Amazon RDS).

Wenn Sie den DB-Snapshot mit dem Befehl `RestoreDBClusterFromSnapshot` migrieren, erstellt der Befehl sowohl den DB-Cluster als auch die primäre Instance.

In diesem Beispiel erstellen Sie ein mit MySQL 5.7 kompatibles DB-Cluster mit dem Namen *`mydbcluster`* aus einem DB-Snapshot, dessen ARN auf *`mydbsnapshotARN`* festgelegt wurde.

Für Linux, macOSoder Unix:

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier mydbcluster \
    --snapshot-identifier mydbsnapshotARN \
    --engine aurora-mysql
```

Windows:

```
aws rds restore-db-cluster-from-snapshot ^
    --db-cluster-identifier mydbcluster ^
    --snapshot-identifier mydbsnapshotARN ^
    --engine aurora-mysql
```

In diesem Beispiel erstellen Sie einen mit MySQL 5.7 kompatiblen DB-Cluster mit dem Namen *`mydbcluster`* aus einem DB-Snapshot, dessen ARN auf *`mydbsnapshotARN`* festgelegt wurde.

Für Linux, macOSoder Unix:

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier mydbcluster \
    --snapshot-identifier mydbsnapshotARN \
    --engine aurora-mysql
```

Windows:

```
aws rds restore-db-cluster-from-snapshot ^
    --db-cluster-identifier mydbcluster ^
    --snapshot-identifier mydbsnapshotARN ^
    --engine aurora-mysql
```

Migrieren von Daten aus einer RDS-für-MySQL-DB-Instance zu einem Amazon-Aurora-MySQL-DB-Cluster mittels einer Aurora Read Replica (Lesereplikat)

Aurora verwendet die binäre Protokoll-Replizierungsfunktionalität der MySQL-DB-Engine, um für eine MySQL-Quell-DB-Instance einen speziellen Typ von DB-Cluster zu erstellen, der als „Aurora Read Replica“ bezeichnet wird. Aktualisierungen, die an der RDS-für-MySQL-DB-Quell-Instance vorgenommen werden, werden asynchron in diese Aurora Read Replica repliziert.

Es wird empfohlen, diese Funktionalität zu verwenden, um eine Migration aus einer RDS-für-MySQL-DB-Instance zu einem Aurora-MySQL-DB-Cluster durchzuführen, indem Sie eine Aurora Read Replica Ihrer MySQL-DB-Quell-Instance erstellen. Wenn die Replikationsverzögerung zwischen der RDS-für-MySQL-DB-Instance und der Aurora Read Replica 0 beträgt, können Sie die Clientanwendungen für den Zugriff auf die Aurora Read Replica konfigurieren und dann die Replikation stoppen, damit die Aurora Read Replica als eigenständiger Aurora MySQL-DB-Cluster verwendet wird. Beachten Sie, dass die Migration sehr lange dauern kann. Pro Tebibyte (TiB) Daten werden mehrere Stunden benötigt.

Eine Liste der Regionen, in denen Aurora erhältlich ist, finden Sie unter Amazon Aurora in der Allgemeine AWS-Referenz.

Wenn Sie eine Aurora Read Replica einer RDS-für-MySQL-DB-Instance erstellen, wird von Amazon RDS automatisch ein DB-Snapshot der RDS for MySQL-DB-Quell-Instance erstellt (privat für Amazon RDS und kostenlos). Anschließend migriert Amazon RDS die Daten vom DB-Snapshot zum Aurora-Lesereplikat. Nach dem Migrieren der Daten des DB-Snapshots zum neuen Aurora-MySQL-DB-Cluster startet Amazon RDS die Replikation zwischen Ihrer RDS-für-MySQL-DB-Instance und dem Aurora MySQL-DB-Cluster. Wenn die RDS-für-MySQL-DB-Instance Tabellen enthält, die andere Speicher-Engines als InnoDB oder ein komprimiertes Zeilenformat verwenden, können Sie die Erstellung einer Aurora Read Replica beschleunigen, indem Sie diese Tabellen für die Verwendung der InnoDB-Speicher-Engine und des dynamischen Zeilenformats konfigurieren, bevor Sie die Aurora Read Replica erstellen. Weitere Informationen zum Kopieren eines MySQL-DB-Snapshots zu einem Aurora MySQL-DB-Cluster finden Sie unter Migrieren von Daten aus einer DB-Instance von RDS für MySQL in einen DB-Cluster von Amazon Aurora MySQL.

Sie können nur eine Aurora-Read Replica für eine RDS-für-MySQL-DB-Instance erstellen.

> **Note**
>
> Aufgrund von Funktionsunterschieden zwischen Aurora-MySQL und der MySQL-Datenbank-Engine-Version der als Replikationsprimäre dienenden RDS-für-MySQL-DB-Instance kann es

bei der Replikation zu Problemen kommen. Bei Problemen können Sie Fragen im Amazon-RDS-Community-Forum stellen oder sich an AWS Support wenden.
Sie können keine Aurora Read Replica erstellen, wenn Ihre RDS-für-MySQL-DB-Instance bereits die Quelle für eine regionsübergreifende Read Replica enthält.
Sie können von einigen älteren Versionen von RDS für MySQL 8.0, einschließlich 8.0.11, 8.0.13 und 8.0.15, nicht zu Aurora MySQL Version 3.05 und höher migrieren. Wir empfehlen, vor der Migration auf RDS für MySQL Version 8.0.28 zu aktualisieren.

Weitere Informationen zu MySQL-Lesereplikaten finden Sie unter Arbeiten mit Read Replicas von MariaDB-, MySQL- und PostgreSQL-DB-Instances.

Erstellen einer Aurora Read Replica

Sie können eine Aurora Read Replica für eine RDS-für-MySQL-DB-Instance über die Konsole, die AWS CLI oder die RDS-API erstellen.

Konsole

So erstellen Sie eine Aurora Read Replica einer RDS-für-MySQL-DB-Instance

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie die MySQL DB-Instance aus, die Sie als Quelle für Ihr Aurora Read Replica verwenden möchten.
4. Wählen Sie für Actions (Aktionen) Create Aurora read replica (Aurora Read Replica erstellen) aus.
5. Legen Sie die in der folgenden Tabelle beschriebenen DB-Cluster-Einstellungen für die Aurora-Read Replica fest.

Option	Beschreibung
DB-Instance-Klasse	Wählen Sie eine DB-Instance-Klasse aus, die die Verarbeitungs- und Speicheranforderungen der primären Instance im DB-Cluster definiert. Weitere

Option	Beschreibung
	Informationen zu den Optionen für DB-Instance-Klasse n finden Sie unter Aurora DB-Instance-Klassen.
Multi-AZ-Bereitstellung	Wählen Sie Replika in einer anderen Zone erstellen aus, um eine Standby Replica des neuen DB-Cluste rs in einer anderen Availability Zone für eine Failover-Unterstützung in der AWS-Zielregion zu erstellen. Weitere Informationen über die Multi-AZ-Bereitstellung finden Sie unter Regionen und Availability Zones.
DB-Instance-Kennung	Geben Sie einen Namen für die primäre Instance des DB-Clusters der Aurora-Read Replica ein. Dieser Bezeichner wird in der Endpunktadresse für die primäre Instance des neuen DB-Clusters verwendet. Für den DB-Instance-Bezeichner gelten folgende Einschränkungen: • Sie darf 1 bis 63 alphanumerische Zeichen oder Bindestriche enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Er darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten. • Sie muss bei allen DB-Instances für jedes AWS-Konto und jede AWS-Region eindeutig sein. Da das Aurora Read Replica-DB-Cluster aus einem Snapshot der DB-Quell-Instance erstellt wird, sind der Master-Benutzername und das Master-Passwort für die Aurora Read Replica mit dem Master-Benutzernam en und Master-Passwort für die DB-Quell-Instance identisch.

Option	Beschreibung
Virtual Private Cloud (VPC)	Wählen Sie die VPC aus, die als Host für das DB-Cluster dienen soll. Wählen Sie Create a new VPC (Neue VPC erstellen) aus, wenn Aurora eine VPC für Sie erstellen soll. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.
DB-Subnetzgruppe	Wählen Sie die DB-Subnetzgruppe aus, die für den DB-Cluster verwendet werden soll. Wählen Sie Create a new DB subnet group (Neue DB-Subnetzgruppe erstellen), wenn Aurora eine DB-Subnetzgruppe für Sie erstellen soll. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.
Öffentliche Zugänglichkeit	Wählen Sie `Yes` aus, um dem DB-Cluster eine öffentliche IP-Adresse zu geben. Wählen Sie andernfalls `No` aus. Die Instances in Ihrem DB-Cluster können eine Mischung aus öffentlichen und privaten DB-Instances sein. Weitere Informationen darüber, wie Sie den öffentlichen Zugriff für Instances deaktivieren, finden Sie unter Ausblenden einer DB-Clusters in einer VPC vor dem Internet.
Availability Zone	Legen Sie fest, ob Sie eine bestimmte Availability Zone angeben möchten. Weitere Informationen über Availability Zones finden Sie unter Regionen und Availability Zones.
VPC-Sicherheitsgruppe (Firewall)	Wählen Sie Neue VPC-Sicherheitsgruppe erstellen aus, damit Aurora eine VPC-Sicherheitsgruppe für Sie erstellt. Wählen Sie Vorhandene VPC-Sicherheitsgruppen auswählen aus, um eine oder mehrere VPC-Sicherheitsgruppen auszuwählen und den Netzwerkzugriff auf das DB-Cluster zu schützen. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.

Option	Beschreibung
Datenbankport	Geben Sie den Port an, über den Anwendungen und Dienstprogramme auf die Datenbank zugreifen können. Aurora-MySQL;-DB-Cluster verwenden standardmäßig den MySQL-Standardport 3306. Die Firewalls einiger Unternehmen blockieren Verbindungen mit diesem Port. Wenn die Firewall Ihres Unternehmens den Standardport blockiert, wählen Sie einen anderen Port für den neuen DB-Cluster aus.
DB-Parametergruppe	Wählen Sie eine DB-Parametergruppe für den Aurora MySQL DB-Cluster aus. Aurora verfügt über eine DB-Standardparametergruppe, die Sie verwenden können, oder Sie können Ihre eigene DB-Parametergruppe erstellen. Weitere Informationen zu DB-Parame tergruppen finden Sie unter Arbeiten mit Parameter gruppen.
DB-Cluster-Parametergruppe	Wählen Sie eine DB-Cluster-Parametergruppe für den Aurora-MySQL-DB-Cluster aus. Aurora verfügt über eine DB-Cluster-Standardparametergruppe, die Sie verwenden können, oder Sie können Ihre eigene DB-Cluster-Parametergruppe erstellen. Weitere Informati onen zu DB-Cluster-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Option	Beschreibung
Verschlüsselung	Wählen Sie Verschlüsselung deaktivieren aus, wenn das neue Aurora-DB-Cluster nicht verschlüsselt werden soll. Wählen Sie Verschlüsselung aktivieren aus, wenn das neue Aurora-DB-Cluster im Ruhezustand verschlüsselt werden soll. Wenn Sie Verschlüsselung aktivieren wählen, müssen Sie einen KMS-Schlüssel als Wert AWS KMS key wählen. Wenn Ihre MySQL-DB-Instance nicht verschlüsselt ist, geben Sie einen Verschlüsselungsschlüssel an, damit Ihr DB-Cluster im Ruhezustand verschlüsselt wird. Wenn Ihre MySQL-DB-Instance verschlüsselt ist, geben Sie einen Verschlüsselungsschlüssel an, damit Ihr DB-Cluster in Ruhe mit dem angegebenen Verschlüsselungsschlüssel verschlüsselt wird. Sie können den von der MySQL DB-Instance verwendeten Verschlüsselungsschlüssel oder einen anderen Schlüssel angeben. Aus einer verschlüsselten MySQL-DB-Instance kann kein unverschlüsselter DB-Cluster erstellt werden.
Priorität	Wählen Sie eine Failover-Priorität für den DB-Cluster aus. Wenn Sie keinen Wert auswählen, wird als Standard tier-1 eingestellt. Diese Priorität bestimmt die Reihenfolge, in der Aurora-Replikate bei der Wiederherstellung nach einem Ausfall der primären Instance hochgestuft werden. Weitere Informationen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.
Aufbewahrungszeitraum für Backups	Wählen Sie den Aufbewahrungszeitraum (1 bis 35 Tage) für Sicherungskopien der Datenbank in Aurora aus. Backup-Kopien können für point-in-time Wiederherstellungen (PITR) Ihrer Datenbank bis zur zweiten verwendet werden.

Option	Beschreibung
Verbesserte Überwachung	Wählen Sie Erweiterte Überwachung aktivieren aus, um die Erfassung von Metriken in Echtzeit für das Betriebssystem zu aktivieren, in dem Ihr DB-Cluster ausgeführt wird. Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).
Überwachungsrolle	Nur verfügbar, wenn Verbesserte Überwachung auf Erweiterte Überwachung aktivieren gesetzt ist. Wählen Sie die IAM-Rolle aus, die Sie erstellt haben, um Aurora die Kommunikation mit Amazon CloudWatch Logs für Sie zu ermöglichen, oder wählen Sie Standard aus, damit Aurora eine Rolle mit dem Namen für Sie erstellt`rds-monitoring-role` . Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).
Granularität	Nur verfügbar, wenn Verbesserte Überwachung auf Erweiterte Überwachung aktivieren gesetzt ist. Mit ihr können Sie die Zeitspanne zwischen den Erfassungen der Kennzahlen des DB-Clusters in Sekunden festlegen.
Kleinere Versions-Updates automatisch aktivieren	Diese Einstellung wird für Aurora MySQL-DB-Cluster nicht verwendet. Weitere Informationen über Engine-Updates für Aurora MySQL finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.
Wartungsfenster	Wählen Sie Fenster auswählen aus und geben Sie den wöchentlichen Zeitraum an, in dem Systemwartungen durchgeführt werden können. Sie können auch Keine Präferenz auswählen, damit Aurora einen Zeitraum nach dem Zufallsprinzip auswählt.

6. Wählen Sie Read Replica erstellen aus.

AWS CLI

Um eine Aurora Read Replica aus einer RDS-für-MySQL-Quell-DB-Instance zu erstellen, verwenden Sie die AWS CLI-Befehle `create-db-cluster` und `create-db-instance`, um einen neuen Aurora-MySQL-DB-Cluster zu erstellen. Geben Sie beim Aufrufen des Befehls `create-db-cluster` mit dem Parameter `--replication-source-identifier` den Amazon-Ressourcennamen (ARN) der gewünschten MySQL-DB-Instance an. Weitere Informationen zu Amazon RDS-ARNs finden Sie unter Amazon Relational Database Service (Amazon RDS).

Geben Sie nicht den Masterbenutzernamen, das Masterpasswort oder den Datenbanknamen an, da die Aurora-Read Replica diese Werte aus der MySQL-DB-Instance übernimmt.

Für Linux, macOSoder Unix:

```
aws rds create-db-cluster --db-cluster-identifier sample-replica-cluster --engine
 aurora \
    --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2 \
    --replication-source-identifier arn:aws:rds:us-west-2:123456789012:db:primary-
mysql-instance
```

Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-replica-cluster --engine
 aurora ^
    --db-subnet-group-name mysubnetgroup --vpc-security-group-ids sg-c7e5b0d2 ^
    --replication-source-identifier arn:aws:rds:us-west-2:123456789012:db:primary-
mysql-instance
```

Wenn Sie die Konsole verwenden, um eine Aurora Read Replica zu erstellen, erstellt Aurora automatisch die primäre Instance für die Aurora Read Replica Ihres DB-Clusters. Wenn Sie die AWS CLI zum Erstellen einer Aurora-Read Replica verwenden, müssen Sie die primäre Instance explizit für Ihren DB-Cluster anlegen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance.

Sie können eine primäre Instance für Ihr DB-Cluster erstellen, indem Sie den `create-db-instance`-Befehl AWS CLI mit folgenden Parametern verwenden.

- `--db-cluster-identifier`

Der Name Ihres DB-Clusters.

- `--db-instance-class`

  Der Name der DB-Instance-Klasse, die für Ihre primäre Instance verwendet werden soll.

- `--db-instance-identifier`

  Der Name Ihrer primären Instance.

- `--engine aurora`

In diesem Beispiel erstellen Sie eine primäre Instance mit dem Namen *myreadreplicainstance* für den DB-Cluster mit dem Namen *myreadreplicacluster* unter Verwendung der DB-Instance-Klasse, die in *myinstanceclass* angegeben ist.

Example

Für Linux, macOSoder Unix:

```
aws rds create-db-instance \
    --db-cluster-identifier myreadreplicacluster \
    --db-instance-class myinstanceclass \
    --db-instance-identifier myreadreplicainstance \
    --engine aurora
```

Windows:

```
aws rds create-db-instance ^
    --db-cluster-identifier myreadreplicacluster ^
    --db-instance-class myinstanceclass ^
    --db-instance-identifier myreadreplicainstance ^
    --engine aurora
```

RDS-API

Um eine Aurora-Read Replica aus einer RDS-für-MySQL-DB-Quell-Instance zu erstellen, verwenden Sie die Amazon RDS-API-Befehle `CreateDBCluster` und `CreateDBInstance`, um einen neuen Aurora-DB-Cluster und eine neue primäre Instance zu erstellen. Geben Sie nicht den Masterbenutzernamen, das Masterpasswort oder den Datenbanknamen an, da die Aurora Read Replica diese Werte aus der RDS-für-MySQL-DB-Instance übernimmt.

Sie können einen neuen Aurora-DB-Cluster für eine Aurora Read Replica aus einer RDS-für-MySQL-DB-Quell-Instance erstellen, indem Sie den Amazon RDS-API-Befehl `CreateDBCluster` mit folgenden Parametern verwenden:

- `DBClusterIdentifier`

  Name des zu erstellenden DB-Clusters.

- `DBSubnetGroupName`

  Der Name der DB-Subnetzgruppe, die mit diesem DB-Cluster verknüpft werden soll.

- `Engine=aurora`

- `KmsKeyId`

  Die AWS KMS key, mit der der DB-Cluster optional verschlüsselt wird, je nachdem, ob Ihre MySQL-DB-Instance verschlüsselt ist.

  - Wenn Ihre MySQL-DB-Instance nicht verschlüsselt ist, geben Sie einen Verschlüsselungsschlüssel an, damit Ihr DB-Cluster im Ruhezustand verschlüsselt wird. Ansonsten wird Ihr DB-Cluster im Ruhezustand mit dem Standard-Verschlüsselungsschlüssel für Ihr Konto verschlüsselt.
  - Wenn Ihre MySQL-DB-Instance verschlüsselt ist, geben Sie einen Verschlüsselungsschlüssel an, damit Ihr DB-Cluster in Ruhe mit dem angegebenen Verschlüsselungsschlüssel verschlüsselt wird. Ansonsten wird Ihr DB-Cluster im Ruhezustand mit dem Verschlüsselungsschlüssel für die MySQL-DB-Instance verschlüsselt.

  > **Note**
  >
  > Aus einer verschlüsselten MySQL-DB-Instance kann kein unverschlüsselter DB-Cluster erstellt werden.

- `ReplicationSourceIdentifier`

  Der Amazon Resource Name (ARN) für die Quell-MySQL DB-Instance. Weitere Informationen zu Amazon RDS-ARNs finden Sie unter Amazon Relational Database Service (Amazon RDS).

- `VpcSecurityGroupIds`

  Die Liste der EC2-VPC-Sicherheitsgruppen, die mit diesem DB-Cluster verknüpft werden sollen.

In diesem Beispiel erstellen Sie ein DB-Cluster namens *myreadreplicacluster* aus einer MySQL-DB-Quell-Instance mit einem auf *mysqlmasterARN* festgelegten ARN, verbunden mit einer DB-Subnetzgruppe namens *mysubnetgroup* und einer VPC-Sicherheitsgruppe namens *mysecuritygroup*.

Example

```
https://rds.us-east-1.amazonaws.com/
    ?Action=CreateDBCluster
    &DBClusterIdentifier=myreadreplicacluster
    &DBSubnetGroupName=mysubnetgroup
    &Engine=aurora
    &ReplicationSourceIdentifier=mysqlprimaryARN
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &Version=2014-10-31
    &VpcSecurityGroupIds=mysecuritygroup
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20150927/us-east-1/rds/aws4_request
    &X-Amz-Date=20150927T164851Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=6a8f4bd6a98f649c75ea04a6b3929ecc75ac09739588391cd7250f5280e716db
```

Wenn Sie die Konsole verwenden, um eine Aurora Read Replica zu erstellen, erstellt Aurora automatisch die primäre Instance für die Aurora Read Replica Ihres DB-Clusters. Wenn Sie die AWS CLI zum Erstellen einer Aurora-Read Replica verwenden, müssen Sie die primäre Instance explizit für Ihren DB-Cluster anlegen. Die primäre Instance ist die erste in einem DB-Cluster erstellte Instance.

Sie können eine primäre Instance für Ihr DB-Cluster erstellen, indem Sie den Amazon RDS-API-Befehl `CreateDBInstance` mit folgenden Parametern verwenden:

- `DBClusterIdentifier`

  Der Name Ihres DB-Clusters.
- `DBInstanceClass`

  Der Name der DB-Instance-Klasse, die für Ihre primäre Instance verwendet werden soll.
- `DBInstanceIdentifier`

  Der Name Ihrer primären Instance.

- `Engine=aurora`

In diesem Beispiel erstellen Sie eine primäre Instance mit dem Namen *`myreadreplicainstance`* für den DB-Cluster mit dem Namen *`myreadreplicacluster`* unter Verwendung der DB-Instance-Klasse, die in *`myinstanceclass`* angegeben ist.

Example

```
https://rds.us-east-1.amazonaws.com/
    ?Action=CreateDBInstance
    &DBClusterIdentifier=myreadreplicacluster
    &DBInstanceClass=myinstanceclass
    &DBInstanceIdentifier=myreadreplicainstance
    &Engine=aurora
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &Version=2014-09-01
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20140424/us-east-1/rds/aws4_request
    &X-Amz-Date=20140424T194844Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=bee4aabc750bf7dad0cd9e22b952bd6089d91e2a16592c2293e532eeaab8bc77
```

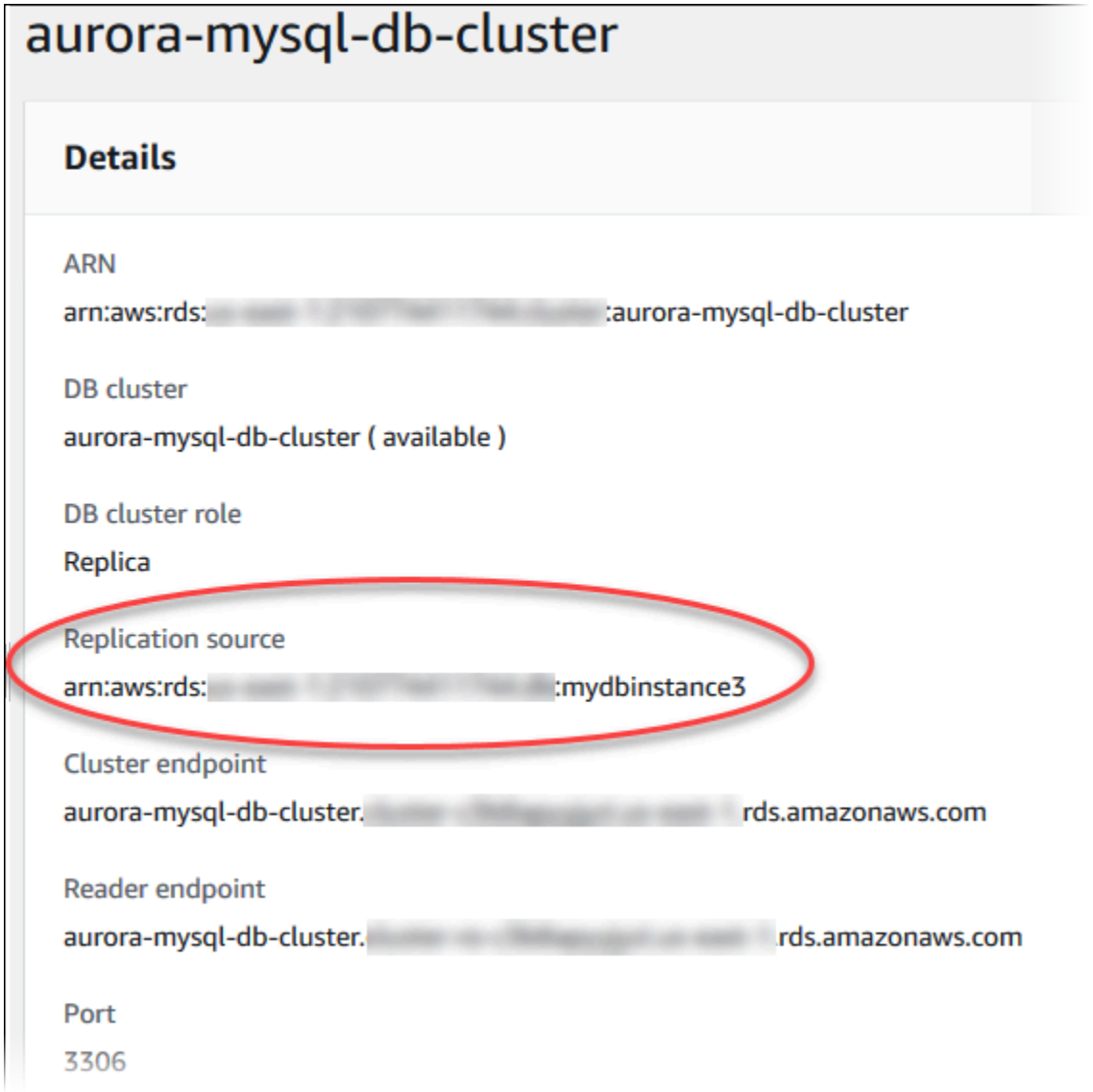
Anzeigen einer Aurora-Read Replica

Sie können die MySQL-Aurora MySQL-Replikationsbeziehungen für Ihre Aurora-MySQL-DB-Cluster über die AWS Management Console oder die AWS CLI anzeigen.

Konsole

So zeigen Sie die MySQL-DB-Primär-Instance für eine Aurora-Read Replica an:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie das DB-Cluster für die Aurora Read Replica aus, um Details anzuzeigen. Die Informationen zur MySQL-DB-Primäre-Instance werden im Feld Replication source (Replikationsquelle) angezeigt.



AWS CLI

Um die MySQL-Aurora MySQL-Replikationsbeziehungen für Ihre Aurora-MySQL-DB-Cluster über die AWS CLI anzuzeigen, verwenden Sie die Befehle `describe-db-clusters` und `describe-db-instances`.

Um zu ermitteln, welche MySQL-DB-Instance die Primär-Instance ist, verwenden Sie `describe-db-clusters` und geben die Cluster-ID der Aurora Read Replica für die Option `--db-cluster-identifier` an. Der ARN der als primäre Replikation verwendeten DB-Instance wird in der Befehlsausgabe mit dem Element `ReplicationSourceIdentifier` angezeigt.

Um zu ermitteln, welches DB-Cluster die Aurora Read Replica ist, verwenden Sie `describe-db-instances` und geben die Instance-ID der MySQL-DB-Instance für die Option `--db-instance-identifier` an. Informationen zur DB-Cluster-ID für die Aurora Read Replica finden Sie im Element `ReadReplicaDBClusterIdentifiers` in der Ausgabe.

Example

Für Linux, macOSoder Unix:

```
aws rds describe-db-clusters \
    --db-cluster-identifier myreadreplicacluster
```

```
aws rds describe-db-instances \
    --db-instance-identifier mysqlprimary
```

Windows:

```
aws rds describe-db-clusters ^
    --db-cluster-identifier myreadreplicacluster
```

```
aws rds describe-db-instances ^
    --db-instance-identifier mysqlprimary
```

Hochstufen einer Aurora Read Replica

Nach Abschluss der Migration können Sie die Aurora Read Replica über die AWS Management Console oder die AWS CLI zu einem eigenständigen DB-Cluster hochstufen.

Anschließend können Sie Ihre Clientanwendungen für den Zugriff auf den Endpunkt der Aurora Read Replica konfigurieren. Weitere Informationen zu den Aurora-Endpunkten finden Sie unter Amazon Aurora-Verbindungsverwaltung. Die Hochstufung sollte ziemlich schnell erfolgen. Während des Vorgangs sind Lese- und Schreibzugriffe auf die Aurora-Read Replica möglich. Sie können allerdings in dieser Zeit weder die MySQL-DB-Primär-Instance löschen noch die Verknüpfung zwischen der DB-Instance und der Aurora-Read Replica aufheben.

Halten Sie vor der Hochstufung der Aurora Read Replica alle Schreibtransaktionen zur MySQL-DB-Quell-Instance an und warten Sie anschließend, bis die Replikationsverzögerung der Aurora Read Replica 0 erreicht. Sie können die Replikatverzögerung für eine Aurora-Read Replica anzeigen,

indem Sie den Befehl `SHOW SLAVE STATUS` (Aurora-MySQL-Version 2) oder `SHOW REPLICA STATUS` (Aurora-MySQL-Version 3) auf Ihrem Aurora-Lesereplikat aufrufen. Überprüfen Sie den Wert Sekunden hinter Master.

Schreibzugriffe auf die Aurora-Read Replica sollten erst durchgeführt werden, nachdem die Schreibtransaktionen zur Primären angehalten wurden und die Replikationsverzögerung 0 beträgt. Wenn Sie zur Aurora Read Replica schreiben, bevor die Replikationsverzögerung null erreicht, und Tabellen geändert werden, die auch im primären MySQL geändert werden, könnte die Replikation zu Aurora unterbrochen werden. Falls dies geschieht, müssen Sie die Aurora-Read Replica löschen und erneut erstellen.

Konsole

So stufen Sie eine Aurora-Read Replica zu einem Aurora-DB-Cluster hoch:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den DB-Cluster für das Aurora Read Replica aus.
4. Wählen Sie für Actions (Aktionen) Promote (Hochstufen) aus.
5. Klicken Sie auf Promote Read Replica) Read Replica hochstufen.

Bestätigen Sie nach der Werbung, dass das Hochstufen abgeschlossen wurde, indem Sie das folgende Verfahren anwenden.

Um zu bestätigen, dass das Aurora Read Replica hochgestuft wurde

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Stellen Sie auf der Seite Ereignisse sicher, dass für den Cluster, den Sie hochgestuft haben, ein `Promoted Read Replica cluster to a stand-alone database cluster` Ereignis vorliegt.

Nach Abschluss der Hochstufung wird die Verknüpfung zwischen der MySQL-DB-Primär-Instance und der Aurora-Read Replica aufgehoben. Sie können dann die DB-Instance bei Bedarf löschen.

AWS CLI

Um ein Aurora-Lesereplikat zu einem eigenständigen DB-Cluster hochzustufen, verwenden Sie den `promote-read-replica-db-cluster` AWS CLI-Befehl .

Example

Für Linux, macOSoder Unix:

```
aws rds promote-read-replica-db-cluster \
    --db-cluster-identifier myreadreplicacluster
```

Windows:

```
aws rds promote-read-replica-db-cluster ^
    --db-cluster-identifier myreadreplicacluster
```

Verwalten von Amazon Aurora MySQL

In den folgenden Abschnitten wird das Verwalten eines Amazon-Aurora-MySQL-DB-Clusters erläutert.

Themen

Verwalten von Performance und Skalierung für Amazon Aurora MySQL

Skalierung von Aurora MySQL-DB-Instances

Sie können Aurora MySQL-DB-Instances auf zwei Arten skalieren, durch Skalierung der Instance oder durch Skalierung der Lesevorgänge. Weitere Informationen zur Lese-Skalierung finden Sie unter Skalierung von Lesevorgängen.

Sie können Ihr Aurora-MySQL-DB-Cluster skalieren, indem Sie die DB-Instance-Klasse für jede DB-Instance im DB-Cluster ändern. Aurora MySQL unterstützt mehrere DB-Instance-Klassen, die für Aurora optimiert sind. Verwenden Sie keine db.t2- oder db.t3-Instance-Klassen für größere Aurora-Cluster mit einer Größe von mehr als 40 TB. Die Spezifikationen der von Aurora MySQL unterstützten DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.

> **Note**
>
> Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter Verwendung von T-Instance-Klassen für Entwicklung und Tests.

Maximale Verbindungen zu einer Aurora MySQL-DB-Instance

Die maximale Anzahl der zulässigen Verbindungen mit einer Aurora MySQL-DB-Instance wird durch den Parameter `max_connections` in der Instance-Ebenen-Parametergruppe für die DB-Instance festgelegt.

Die folgende Tabelle listet den Standardwert von `max_connections` für jede DB-Instance auf, die für Aurora MySQL verfügbar ist. Sie können die maximal zulässige Anzahl von Verbindungen mit Ihrer Aurora MySQL-DB-Instance erhöhen, indem Sie die Instance auf eine DB-Instance-Klasse mit mehr Arbeitsspeicher skalieren oder einen größeren Wert für den Parameter `max_connections` in der DB-Parametergruppe für Ihre Instance festlegen, wobei ein Wert von bis zu 16.000 möglich ist.

> **Tip**
>
> Wenn Ihre Anwendungen häufig Verbindungen öffnen und schließen oder langlebige Verbindungen in großer Zahl offen lassen, empfehlen wir Ihnen, Amazon-RDS-Proxy zu verwenden. RDS-Proxy ist ein vollständig verwalteter, hochverfügbarer Datenbank-Proxy, der Datenbankverbindungen sicher und effizient per Verbindungspooling freigibt. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

Weitere Informationen dazu, wie Aurora Serverless v2-Instances diesen Parameter behandeln, finden Sie unter Maximale Anzahl der Verbindungen für Aurora Serverless v2.

Instance class	Vorgabewert max_connections		
db.t2.small	45		
db.t2.Medium	90		
db.t3.small	45		
db.t3.medium	90		
db.t3.large	135		
db.t4g.medium	90		

Instance class	Vorgabewert max_connections		
db.t4g.large	135		
db.r3.large	1000		
db.r3.xlarge	2000		
db.r3.2xlarge	3000		
db.r3.4xlarge	4000		
db.r3.8xlarge	5000		
db.r4.large	1000		
db.r4.xlarge	2000		
db.r4.2xlarge	3000		
db.r4.4xlarge	4000		
db.r4.8xlarge	5000		
db.r4.16xlarge	6 000		
db.r5.large	1000		
db.r5.xlarge	2000		
db.r5.2xlarge	3 000		
db.r5.4xlarge	4000		
db.r5.8xlarge	5000		
db.r5.12xlarge	6 000		
db.r5.16xlarge	6 000		

Instance class	Vorgabewert max_connections		
db.r5.24xlarge	7000		
db.r6g.large	1000		
db.r6g.xlarge	2000		
db.r6g.2xlarge	3 000		
db.r6g.4xlarge	4000		
db.r6g.8xlarge	5000		
db.r6g.12xlarge	6 000		
db.r6g.16xlarge	6 000		
db.r6i.large	1000		
db.r6i.xlarge	2000		
db.r6i.2xlarge	3000		
db.r6i.4xlarge	4000		
db.r6i.8xlarge	5000		
db.r6i.12xlarge	6 000		
db.r6i.16xlarge	6 000		
db.r6i.24xlarge	7000		
db.r6i.32xlarge	7000		
db.r7g.large	1000		
db.r7g.xlarge	2000		

Instance class	Vorgabewert max_connections
db.r7g.2xlarge	3000
db.r7g.4xlarge	4000
db.r7g.8xlarge	5000
db.r7g.12xlarge	6 000
db.r7g.16xlarge	6 000
db.x2g.large	2000
db.x2g.xlarge	3000
db.x2g.2xlarge	4000
db.x2g.4xlarge	5000
db.x2g.8xlarge	6 000
db.x2g.12xlarge	7000
db.x2g.16xlarge	7000

Wenn Sie eine neue Parametergruppe erstellen, um einen eigenen Standardwert für den Verbindungsgrenzwert zu erstellen, werden Sie feststellen, dass der Standard-Verbindungsgrenzwert mithilfe einer auf dem Wert `DBInstanceClassMemory` basierenden Formel abgeleitet wird. Wie in der vorhergehenden Tabelle dargestellt, erzeugt die Formel Verbindungsbegrenzungen, die bei einer Verdoppelung des Speichers über die progressiv größeren R3-, R4- und R5-Instances um jeweils 1000 und bei unterschiedlichen Speichergrößen von T2- und T3-Instances um 45 erhöht werden.

Weitere Informationen darüber, wie `DBInstanceClassMemory` berechnet wird, finden Sie unter Festlegen von DB-Parametern.

Aurora MySQL- und RDS for MySQL-DB-Instances weisen unterschiedliche Speicher-Overhead-Mengen auf. Daher kann der `max_connections`-Wert für Aurora MySQL- und RDS for MySQL-DB-Instances, die dieselbe Instance-Klasse verwenden, unterschiedlich sein. Die Werte in der Tabelle gelten nur für Aurora MySQL-DB-Instances.

> **Note**
>
> Die deutlich niedrigeren Verbindungsgrenzwerte für T2- und T3-Instances basieren darauf, dass diese Instances-Klassen bei Aurora nur für Entwicklungs- und Testszenarien und nicht für Produktionsworkloads vorgesehen sind.

Für Systeme, die Standardwerte für andere größere Arbeitsspeicherverbraucher verwenden, beispielsweise Pufferpool und Abfragezwischenspeicher, werden die Standard-Verbindungsgrenzwerte angepasst. Wenn Sie diese anderen Einstellungen für Ihr Cluster ändern, sollten Sie auch den Verbindungsgrenzwert ändern, um die Zu- oder Abnahme des verfügbaren Arbeitsspeichers in den DB-Instances zu berücksichtigen.

Temporäre Speicherlimits für Aurora MySQL

Aurora MySQL speichert Tabellen und Indizes im Aurora Speichersubsystem. Aurora MySQL verwendet separaten temporären oder lokalen Speicher für nicht persistente temporäre Dateien und temporäre Nicht-InnoDB-Tabellen. Zum lokalen Speicher gehören auch Dateien, die für Zwecke wie das Sortieren großer Datensätze während der Abfrageverarbeitung oder für Indexerstellungsvorgänge verwendet werden. Es enthält keine temporären InnoDB-Tabellen.

Weitere Informationen zu temporären Tabellen in Aurora MySQL Version 3 finden Sie unter Neues temporäres Tabellenverhalten in Aurora-MySQL-Version 3. Weitere Informationen zu temporären Tabellen in Version 2 finden Sie unter Temporäres Tabellenverhalten in Aurora-MySQL-Version 2.

Die Daten und temporären Dateien auf diesen Volumes gehen verloren, wenn die DB-Instance gestartet und gestoppt wird und wenn der Host ausgetauscht wird.

Diese lokalen Speichervolumes werden von Amazon Elastic Block Store (EBS) unterstützt und können durch die Verwendung einer größeren DB-Instance-Klasse erweitert werden. Weitere Informationen über Speicher finden Sie unter Amazon Aurora-Speicher und -Zuverlässigkeit.

Lokaler Speicher wird auch für den Import von Daten aus Amazon S3 mit `LOAD DATA FROM S3` oder `LOAD XML FROM S3` und für den Export von Daten nach S3 mit SELECT INTO OUTFILE

S3 verwendet. Weitere Informationen zum Importieren von und Exportieren nach S3 finden Sie im Folgenden:

- Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket
- Speichern von Daten aus einem Amazon Aurora MySQL-DB-Cluster in Textdateien in einem Amazon S3-Bucket

Aurora MySQL verwendet separaten permanenten Speicher für Fehlerprotokolle, allgemeine Protokolle, langsame Query-Logs und Audit-Logs für die meisten Aurora MySQL-DB-Instance-Klassen (ausgenommen Instance-Klassentypen mit hoher Leistung wie db.t2, db.t3 und db.t4g). Die Daten auf diesem Volume werden beim Starten und Stoppen der DB-Instance sowie beim Host-Austausch beibehalten.

Dieses permanente Speichervolumen wird ebenfalls von Amazon EBS unterstützt und hat eine feste Größe entsprechend der DB-Instance-Klasse. Es kann nicht durch die Verwendung einer größeren DB-Instance-Klasse erweitert werden.

Die folgende Tabelle zeigt die maximale Menge an temporärem und permanentem Speicher, die für jede Aurora MySQL-DB-Instance-Klasse verfügbar ist. Informationen zur Unterstützung der DB-Instance-Klasse für Aurora finden Sie unter Aurora DB-Instance-Klassen.

DB-Instance-Klasse	Maximal verfügbarer temporäre/lokaler Speicher (GiB)	Zusätzlicher maximaler verfügbarer Speicherplatz für Protokolldateien (GiB)
db.x2g.16xlarge	1280	500
db.x2g.12xlarge	960	500
db.x2g.8xlarge	640	500
db.x2g.4xlarge	320	500
db.x2g.2xlarge	160	60
db.x2g.xlarge	80	60
db.x2g.large	40	60

DB-Instance-Klasse	Maximal verfügbarer temporäre/lokaler Speicher (GiB)	Zusätzlicher maximaler verfügbarer Speicherplatz für Protokolldateien (GiB)
db.r7g.16xlarge	1280	500
db.r7g.12xlarge	960	500
db.r7g.8xlarge	640	500
db.r7g.4xlarge	320	500
db.r7g.2xlarge	160	60
db.r7g.xlarge	80	60
db.r7g.large	32	60
db.r6i.32xlarge	2560	500
db.r6i.24xlarge	1920	500
db.r6i.16xlarge	1280	500
db.r6i.12xlarge	960	500
db.r6i.8xlarge	640	500
db.r6i.4xlarge	320	500
db.r6i.2xlarge	160	60
db.r6i.xlarge	80	60
db.r6i.large	32	60
db.r6g.16xlarge	1280	500
db.r6g.12xlarge	960	500
db.r6g.8xlarge	640	500

DB-Instance-Klasse	Maximal verfügbarer temporäre/lokaler Speicher (GiB)	Zusätzlicher maximaler verfügbarer Speicherplatz für Protokolldateien (GiB)
db.r6g.4xlarge	320	500
db.r6g.2xlarge	160	60
db.r6g.xlarge	80	60
db.r6g.large	32	60
db.r5.24xlarge	1920	500
db.r5.16xlarge	1280	500
db.r5.12xlarge	960	500
db.r5.8xlarge	640	500
db.r5.4xlarge	320	500
db.r5.2xlarge	160	60
db.r5.xlarge	80	60
db.r5.large	32	60
db.r4.16xlarge	1280	500
db.r4.8xlarge	640	500
db.r4.4xlarge	320	500
db.r4.2xlarge	160	60
db.r4.xlarge	80	60
db.r4.large	32	60
db.t4g.large	32	–

DB-Instance-Klasse	Maximal verfügbarer temporäre/lokaler Speicher (GiB)	Zusätzlicher maximaler verfügbarer Speicherplatz für Protokolldateien (GiB)
db.t4g.medium	32	–
db.t3.large	32	–
db.t3.medium	32	–
db.t3.small	32	–
db.t2.medium	32	–
db.t2.small	32	–

Important

Diese Werte stellen die theoretische maximale Menge an freiem Speicher auf jeder DB-Instance dar. Der tatsächliche lokale Speicher, der Ihnen zur Verfügung steht, ist möglicherweise niedriger. Aurora verwendet einen lokalen Speicher für seine Verwaltungsprozesse und die DB-Instance verwendet einen lokalen Speicher, noch bevor Sie Daten laden. Sie können den für eine bestimmte DB-Instance verfügbaren temporären Speicher anhand der unter beschriebenen `FreeLocalStorage` CloudWatch Metrik überwachen CloudWatch Amazon-Metriken für Amazon Aurora. Sie können die Menge des freien Speichers zur Zeit überprüfen. Sie können auch die Menge des freien Speichers im Laufe der Zeit abzeichnen. Die Überwachung des freien Speichers im Laufe der Zeit hilft Ihnen festzustellen, ob der Wert steigt oder sinkt, oder um die Mindest-, Maximal- oder Durchschnittswerte zu ermitteln.
(Dies gilt nicht für Aurora Serverless v2.)

Rückverfolgen eines Aurora-DB-Clusters

Mit Amazon Aurora MySQL-kompatible Edition können Sie einen DB-Cluster auf einen bestimmten Zeitpunkt zurückverfolgen, ohne die Daten aus einer Sicherung wiederherstellen zu müssen.

Inhalt

Übersicht zur Rückverfolgung

Durch die Rückverfolgung wird der DB-Cluster auf den angegebenen Zeitpunkt "zurückgespult". Die Rückverfolgung ersetzt nicht das Sichern des DB-Clusters, damit dieser mit dem Stand eines bestimmten Zeitpunkts wiederhergestellt werden kann. Gegenüber herkömmlichen Sicherungen und Wiederherstellungen bietet die Rückverfolgung jedoch einige Vorteile:

- Sie können Fehler einfach rückgängig machen. Wenn Sie versehentlich eine destruktive Aktion ausführen – beispielsweise eine DELETE-Anweisung ohne WHERE-Klausel –, können Sie den DB-Cluster bei minimaler Unterbrechung der Service-Bereitstellung auf den Zeitpunkt vor der destruktiven Aktion rückverfolgen.
- Sie können einen DB-Cluster schnell rückverfolgen. Das Wiederherstellen eines DB-Clusters auf den Status eines bestimmten Zeitpunkts startet einen neuen DB-Cluster und stellt diesen aus den Sicherungsdaten oder einem DB-Cluster-Snapshot wieder her. Dies kann einige Stunden dauern. Die Rückverfolgung eines DB-Clusters macht keinen neuen DB-Cluster erforderlich. Zudem erfolgt das "Zurückspulen" innerhalb weniger Minuten.
- Sie können frühere Datenänderungen untersuchen. Sie können einen DB-Cluster mehrfach in der Zeit zurück- und vorspulen, um zu ermitteln, wann eine bestimmte Datenänderung vorgenommen wurde. Sie können beispielsweise einen DB-Cluster drei Stunden zurück und anschließend eine Stunde vorspulen. In diesem Fall liegt der Rückverfolgungszeitpunkt zwei Stunden vor der Originalzeit.

> **Note**
>
> Weitere Informationen zum Wiederherstellen eines DB-Cluster für einen bestimmten Zeitpunkt finden Sie unter Übersicht über das Sichern und Wiederherstellen eines Aurora-DB-Clusters.

Rückverfolgungsfenster

Für die Rückverfolgung gilt ein Zielfenster für die Rückverfolgung und ein Ist-Rückverfolgungsfenster:

- Das Zielfenster für die Rückverfolgung gibt den Zeitraum an, über den die Rückverfolgung des DB-Clusters möglich sein soll. Wenn Sie die Rückverfolgung aktivieren, geben Sie ein Zielfenster für die Rückverfolgung an. Sie können beispielsweise ein Zielfenster von 24 Stunden für die Rückverfolgung angeben, wenn die Rückverfolgung des DB-Clusters über einen Tag möglich sein soll.
- Das tatsächliche Rückverfolgungsfenster bezeichnet den tatsächlichen Zeitraum, über den die Rückverfolgung des DB-Clusters möglich ist. Diese Dauer kann kürzer als die des Zielfensters für die Rückverfolgung sein. Das tatsächliche Rückverfolgungsfenster basiert auf dem Workload und dem für Informationen zu Datenbankänderungen (die sogenannten Änderungsdatensätze) verfügbaren Arbeitsspeicher.

Wenn Sie ein Aurora-DB-Cluster mit aktivierter Rückverfolgung aktualisieren, generieren Sie Änderungsdatensätze. Aurora bewahrt Änderungsdatensätze für das Zielfenster für die Rückverfolgung auf und Sie zahlen für die Speicherung einen Stundensatz. Die Anzahl gespeicherter Änderungsdatensätze hängt vom Zielfenster für die Rückverfolgung und von der Workload auf dem DB-Cluster ab. Die Workload bezeichnet die Anzahl der Änderungen, die Sie in einem gegebenen Zeitraum am DB-Cluster vornehmen. Bei starker Workload werden mehr Änderungsdatensätze im Zielfenster für die Rückverfolgung gespeichert als bei geringerer Workload.

Das Zielfenster für die Rückverfolgung bezeichnet also die maximale Dauer, über die eine Rückverfolgung des DB-Clusters möglich sein soll. In den meisten Fällen ist eine Rückverfolgung über die von Ihnen angegebene Maximaldauer möglich. In einigen Fällen kann der DB-Cluster aber nicht genug Änderungsdatensätze speichern, um eine Rückverfolgung über diese Maximaldauer zu ermöglichen, das Ist-Rückverfolgungsfenster ist in einer solchen Situation kleiner als das Zielfenster. Normalerweise ist das Ist-Rückverfolgungsfenster kleiner als das Zielfenster, wenn die Workload auf

dem DB-Cluster extrem hoch ist. Wenn das Ist-Rückverfolgungsfenster kleiner als das Zielfenster ist, senden wir eine Benachrichtigung.

Wenn die Rückverfolgung für einen DB-Cluster aktiviert ist und Sie eine im DB-Cluster gespeicherte Tabelle löschen, bewahrt Aurora die betreffende Tabelle in den Änderungsdatensätzen für die Rückverfolgung auf. Dies ermöglicht Ihnen die Rückkehr zu einem Zeitpunkt vor dem Löschen der Tabelle. Wenn das Zielfenster für die Rückverfolgung nicht genug Platz zum Speichern der Tabelle bietet, wird die Tabelle schließlich aus den Änderungsdatensätzen für die Rückverfolgung entfernt.

Rückverfolgungszeit

Die Rückverfolgung durch Aurora erfolgt immer auf einen Zeitpunkt, der für den DB-Cluster konsistent ist. Dadurch wird das Auftreten noch nicht eingetragener Transaktionen nach Abschluss der Rückverfolgung verhindert. Wenn Sie eine Zeit für eine Rückverfolgung angeben, wählt Aurora automatisch den nächstgelegenen konsistenten Zeitpunkt. Dieser Ansatz bedeutet, dass der abgeschlossene Backtrack möglicherweise nicht genau der von Ihnen angegebenen Zeit entspricht, aber Sie können die genaue Zeit für einen Backtrack mithilfe des describe-db-cluster-backtracks AWS CLI-Befehls ermitteln. Weitere Informationen finden Sie unter Abrufen vorhandener Rückverfolgungen.

Einschränkungen der Rückverfolgung

Die folgenden Einschränkungen gelten für die Rückverfolgung:

- Die Rückverfolgung ist nur für DB-Cluster verfügbar, die mit aktivierter Rückverfolgungsfunktion erstellt wurden. Sie können einen DB-Cluster nicht ändern, um die Backtrack-Funktion zu aktivieren. Sie können die Rückverfolgungsfunktion aktivieren, wenn Sie einen neuen DB-Cluster erstellen oder einen Snapshot eines DB-Clusters wiederherstellen.
- Die Obergrenze für das Zielfenster für die Rückverfolgung beträgt 72 Stunden.
- Die Rückverfolgung betrifft den gesamten DB-Cluster. Sie können also beispielsweise nicht eine einzelne Tabelle oder eine einzelne Datenaktualisierung verfolgen.
- Sie können keine regionsübergreifenden Read Replicas aus einem Backtrack-fähigen Cluster erstellen, aber Sie können trotzdem die Binärprotokollreplikation (Binlog) auf dem Cluster aktivieren. Wenn Sie versuchen, einen DB-Cluster zurückzuverfolgen, für den die Binärprotokollierung aktiviert ist, tritt normalerweise ein Fehler auf, es sei denn, Sie erzwingen die Rückverfolgung. Jeder Versuch, einen Backtrack zu erzwingen, macht die nachgeschalteten Read Replicas kaputt und beeinträchtigt andere Operationen wie Blue/Green-Bereitstellungen.

- Sie können einen Datenbankklon nicht auf einen Zeitpunkt zurückverfolgen, der vor der Erstellung des Datenbankklons liegt. Sie können aber die ursprüngliche Datenbank auf einen Zeitpunkt vor der Erstellung des Klons zurückverfolgen. Weitere Informationen zum Klonen von Datenbanken erhalten Sie unter Klonen eines Volumes für einen Amazon-Aurora-DB-Cluster.
- Bei der Rückverfolgung kommt es zu einer kurzen Betriebsunterbrechung der DB-Instance. Sie müssen Anwendungen vor dem Starten einer Rückverfolgung stoppen oder anhalten, um sicherzustellen, dass keine neuen Lese- oder Schreibanforderungen ergehen. Während der Rückverfolgung hält Aurora die Datenbank an, schließt alle offenen Verbindungen und verwirft noch nicht durchgeführte Lese- und Schreibvorgänge. Dann wird der Abschluss der Rückverfolgung abgewartet.
- Sie können keinen regionsübergreifenden Snapshot eines Clusters mit Backtrack-Aktivierung in einer Region wiederherstellen, die Backtracking nicht unterstützt. AWS
- Wenn Sie ein direktes Upgrade für einen Cluster mit Rückverfolgungsmöglichkeit von Aurora MySQL Version 2 auf Version 3 durchführen, können Sie nicht auf einen Zeitpunkt vor der Durchführung des Upgrades zurückgehen.

Verfügbarkeit von Regionen und Versionen

Die Rückverfolgung ist für Aurora PostgreSQL nicht verfügbar.

Im Folgenden sind die unterstützten Engines und die Regionsverfügbarkeit für die Rückverfolgung mit Aurora MySQL aufgeführt.

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
USA Ost (Ohio)	Alle Versionen	Alle Versionen
USA Ost (Nord-Virginia)	Alle Versionen	Alle Versionen
USA West (Nordkalifornien)	Alle Versionen	Alle Versionen
USA West (Oregon)	Alle Versionen	Alle Versionen
Afrika (Kapstadt)	–	–

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Asia Pacific (Hongkong)	–	–
Asien-Pazifik (Jakarta)	–	–
Asien-Pazifik (Melbourne)	–	–
Asien-Pazifik (Mumbai)	Alle Versionen	Alle Versionen
Asien-Pazifik (Osaka)	Alle Versionen	Version 2.07.3 und höher
Asien-Pazifik (Seoul)	Alle Versionen	Alle Versionen
Asien-Pazifik (Singapur)	Alle Versionen	Alle Versionen
Asien-Pazifik (Sydney)	Alle Versionen	Alle Versionen
Asien-Pazifik (Tokio)	Alle Versionen	Alle Versionen
Kanada (Zentral)	Alle Versionen	Alle Versionen
Kanada West (Calgary)	–	–
China (Peking)	–	–
China (Ningxia)	–	–
Europa (Frankfurt)	Alle Versionen	Alle Versionen

Region	Aurora-MySQL-Version 3	Aurora-MySQL-Version 2
Europa (Irland)	Alle Versionen	Alle Versionen
Europa (London)	Alle Versionen	Alle Versionen
Europa (Milan)	–	–
Europa (Paris)	Alle Versionen	Alle Versionen
Europa (Spain)	–	–
Europa (Stockholm)	–	–
Europa (Zürich)	–	–
Israel (Tel Aviv)	–	–
Naher Osten (Bahrain)	–	–
Naher Osten (VAE)	–	–
Südamerika (São Paulo)	–	–
AWS GovCloud (USA Ost)	–	–
AWS GovCloud (US-West)	–	–

Überlegungen zum Upgrade für rückverfolgungsfähige Cluster

Sie können ein Upgrade für einen DB-Cluster mit Rückverfolgungsmöglichkeit von Aurora MySQL Version 2 auf Version 3 durchführen, da alle Nebenversionen von Aurora MySQL Version 3 für die Rückverfolgung unterstützt werden.

Konfigurieren der Rückverfolgung

Um die Rückverfolgungsfunktion zu verwenden, müssen Sie die Rückverfolgung aktivieren und ein Zielfenster für die Rückverfolgung angeben. Andernfalls wird die Rückverfolgung deaktiviert.

Geben Sie für das Zielfenster für die Rückverfolgung an, für wie lange Sie Ihre Datenbank mit dieser Funktion zurückverfolgen können möchten. Aurora versucht, genügend Änderungsaufzeichnungen aufzubewahren, um dieses Zeitfenster zu unterstützen.

Konsole

Sie können die Konsole verwenden, um die Rückverfolgung beim Erstellen eines DB-Clusters zu konfigurieren. Sie können auch einen DB-Cluster ändern, um das Rückverfolgungsfenster für einen rückverfolgungsfähigen Cluster zu ändern. Wenn Sie die Rückverfolgung für einen Cluster vollständig deaktivieren, indem Sie das Rückverfolgungsfenster auf 0 setzen, können Sie die Rückverfolgung für diesen Cluster nicht erneut aktivieren.

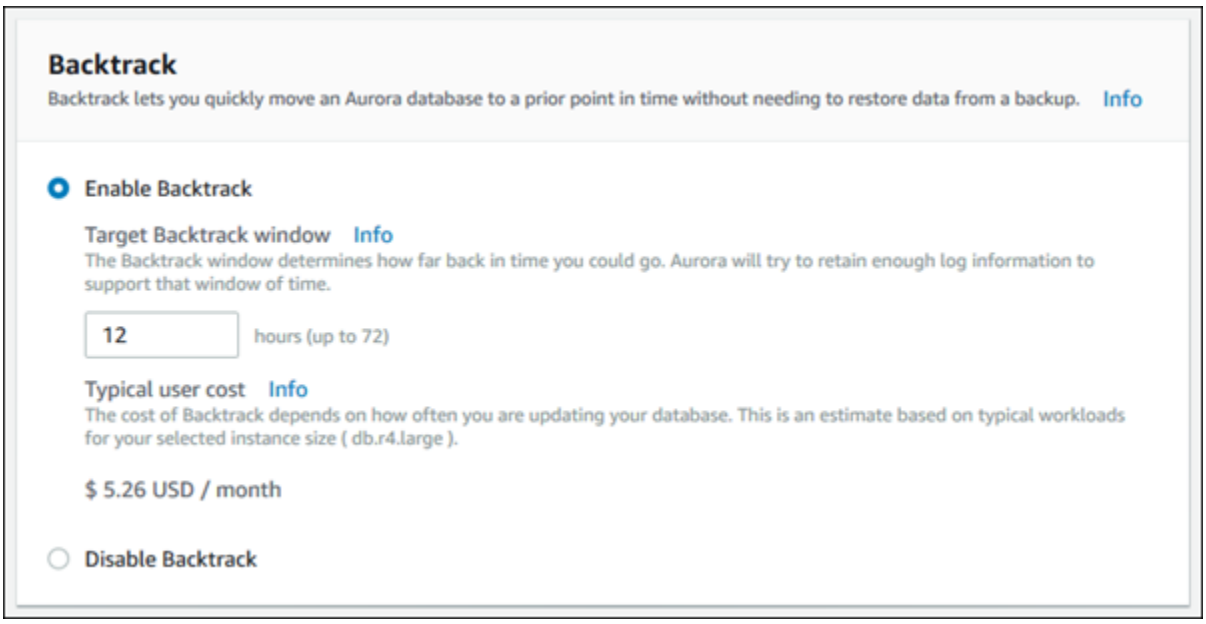
Themen

- Konfigurieren der Rückverfolgung mit der Konsole beim Erstellen eines DB-Clusters
- Konfigurieren der Rückverfolgung mit der Konsole beim Ändern eines DB-Clusters

Konfigurieren der Rückverfolgung mit der Konsole beim Erstellen eines DB-Clusters

Wenn Sie ein neues Aurora MySQL-DB-Cluster erstellen, wird die Rückverfolgung konfiguriert, indem Sie Enable Backtrack (Rückverfolgung aktivieren) wählen und für Target Backtrack window (Zielfenster für die Rückverfolgung) im Bereich Backtrack (Rückverfolgung) einen Wert größer als 0 eingeben.

Befolgen Sie die Anweisungen unter , um einen DB-Cluster zu erstelle Erstellen eines Amazon Aurora-DB Clusters. Die folgende Abbildung zeigt den Bereich Backtrack (Rückverfolgung).



Wenn Sie einen DB-Cluster erstellen, verfügt Aurora über keinerlei Daten zur Workload des DB-Clusters. Deshalb können die Kosten für den neuen DB-Cluster nicht geschätzt werden. Stattdessen stellt die Konsole einen typischen Wert für die Benutzerkosten für das angegebene Zielfenster für die Rückverfolgung basierend auf einer typischen Workload dar. Diese typischen Kosten dienen also nur als Hinweis auf die möglichen Kosten, die durch die Verwendung der Rückverfolgungsfunktion entstehen können.

> **Important**
>
> Ihre tatsächlichen Kosten können niedriger sein, weil sie von der Workload des DB-Clusters abhängig sind.

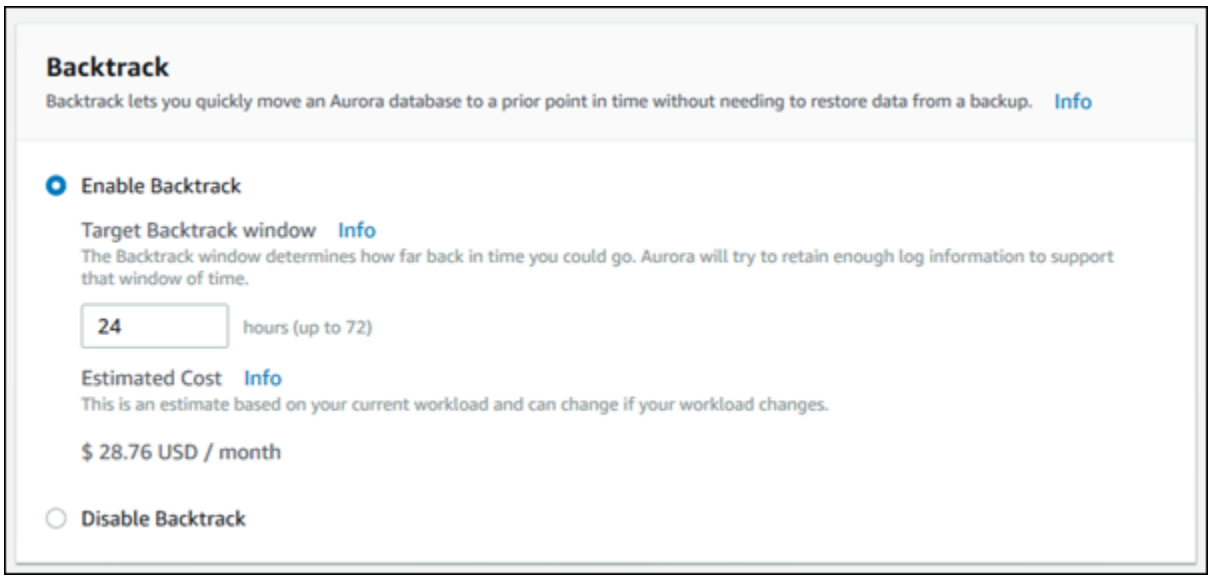
Konfigurieren der Rückverfolgung mit der Konsole beim Ändern eines DB-Clusters

Sie können die Rückverfolgung für einen DB-Cluster mit der Konsole ändern.

> **Note**
>
> Derzeit können Sie die Rückverfolgungsfunktion nur für einen DB-Cluster ändern, für den die Funktion „Backtrack“ aktiviert ist. Der Abschnitt Backtrack wird nicht für einen DB-Cluster angezeigt, der mit deaktivierter Backtrack-Funktion erstellt wurde oder wenn die Backtrack-Funktion für den DB-Cluster deaktiviert wurde.

Ändern Sie die Rückverfolgung für einen DB-Cluster mit der Konsole wie folgt:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Databases (Datenbanken) aus.
3. Wählen Sie den zu ändernden Cluster und dann die Option Modify (Ändern) aus.
4. Ändern Sie für das Target Backtrack window (Zielfenster für die Rückverfolgung) den Zeitraum, über den die Rückverfolgung möglich sein soll. Die Obergrenze ist 72 Stunden.



   Die Konsole zeigt die geschätzten Kosten für die von Ihnen angegebene Größe des Zeitfensters basierend auf der Workload des DB-Clusters in der Vergangenheit an:

   - Wenn Backtracking auf dem DB-Cluster deaktiviert war, basiert die Kostenschätzung auf der `VolumeWriteIOPS` Metrik für den DB-Cluster in Amazon CloudWatch.
   - Wenn Backtracking zuvor auf dem DB-Cluster aktiviert war, basiert die Kostenschätzung auf der `BacktrackChangeRecordsCreationRate` Metrik für den DB-Cluster in Amazon CloudWatch.
5. Klicken Sie auf Weiter.
6. Wählen Sie für Einplanung von Änderungen eine der folgenden Optionen:

   - Apply during the next scheduled maintenance window (Im nächsten geplanten Wartungszeitfenster anwenden): Die Änderung für Target Backtrack window (Zielfenster für die Rückverfolgung) soll erst im nächsten Wartungszeitfenster angewendet werden.

- Apply immediately (Sofort anwenden): Die Änderung für Target Backtrack window (Zielfenster für die Rückverfolgung) soll so bald wie möglich angewendet werden.

7. Wählen Sie Modify Cluster (Cluster ändern) aus.

AWS CLI

Wenn Sie mit dem create-db-cluster AWS CLI-Befehl einen neuen Aurora MySQL-DB-Cluster erstellen, wird Backtracking konfiguriert, wenn Sie einen `--backtrack-window` Wert angeben, der größer als Null ist. Der Wert `--backtrack-window` gibt das Zielfenster für die Rückverfolgung an. Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Sie können den `--backtrack-window` Wert auch mit den folgenden AWS CLI-Befehlen angeben:

- modify-db-cluster
- restore-db-cluster-from-s3
- restore-db-cluster-from-Schnappschuss
- restore-db-cluster-to-point-in-time

Das folgende Verfahren beschreibt, wie Sie das Zielfenster für die Rückverfolgung für einen DB-Cluster mit der änder AWS CLI.

Um das Ziel-Backtrack-Fenster für einen DB-Cluster zu ändern, verwenden Sie AWS CLI

- Rufen Sie den modify-db-cluster AWS CLI-Befehl auf und geben Sie die folgenden Werte an:
  - `--db-cluster-identifier`: Name des DB-Clusters.
  - `--backtrack-window`: maximaler Zeitraum in Sekunden für die Rückverfolgung des DB-Clusters.

  Im folgenden Beispiel wird für das Zielfenster für die Rückverfolgung von `sample-cluster` ein Wert von einem Tag (86 400 Sekunden) festgelegt.

  Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier sample-cluster \
```

```
    --backtrack-window 86400
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --backtrack-window 86400
```

> **Note**
>
> Derzeit kann die Rückverfolgung nur für einen DB-Cluster aktiviert werden, der mit aktivierter Rückverfolgungsfunktion erstellt wurde.

RDS-API

Wenn Sie einen neuen Aurora MySQL-DB-Cluster über die Amazon RDS-API-Operation CreateDBCluster erstellen, wird die Rückverfolgung konfiguriert, wenn Sie für `BacktrackWindow` einen Wert größer als 0 angeben. Der Wert `BacktrackWindow` gibt das Zielfenster für die Rückverfolgung für den mit dem Wert `DBClusterIdentifier` angegebenen DB-Cluster an. Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Sie können den Wert für `BacktrackWindow` auch mittels der folgenden API-Operationen angeben:

- ModifyDBCluster
- DB S3 wiederhergestellt ClusterFrom
- DB wurde wiederhergestellt ClusterFromSnapshot
- DB wurde wiederhergestellt ClusterToPointInTime

> **Note**
>
> Derzeit kann die Rückverfolgung nur für einen DB-Cluster aktiviert werden, der mit aktivierter Rückverfolgungsfunktion erstellt wurde.

Ausführen einer Rückverfolgung

Sie können einen DB-Cluster auf einen bestimmten Zeitpunkt im Zielfenster für die Rückverfolgung rückverfolgen. Wenn der Zeitstempel für die Rückverfolgung nicht vor dem frühestmöglichen Rückverfolgungszeitpunkt und auch nicht in der Zukunft liegt, wird der DB-Cluster auf den betreffenden Zeitpunkt rückverfolgt.

Andernfalls tritt üblicherweise ein Fehler auf. Wenn Sie versuchen, einen DB-Cluster mit aktivierter Binärprotokollierung rückzuverfolgen, tritt üblicherweise ein Fehler auf, sofern Sie nicht das Erzwingen der Rückverfolgung veranlasst haben. Das Erzwingen einer Rückverfolgung kann zu Problemen mit anderen Operationen führen, die Binärprotokollierung verwenden.

> **Important**
>
> Die Rückverfolgung erzeugt keine binlog-Einträge für die von der Funktion vorgenommenen Änderungen. Wenn Sie die Binärprotokollierung für den DB-Cluster aktiviert haben, ist die Rückverfolgung möglicherweise nicht mit der binlog-Implementierung kompatibel.

> **Note**
>
> Bei Datenbankklonen können Sie den DB-Cluster auf einen Zeitpunkt rückverfolgen, der vor dem Zeitpunkt der Erstellung des Klons liegt. Weitere Informationen zum Klonen von Datenbanken erhalten Sie unter Klonen eines Volumes für einen Amazon-Aurora-DB-Cluster.

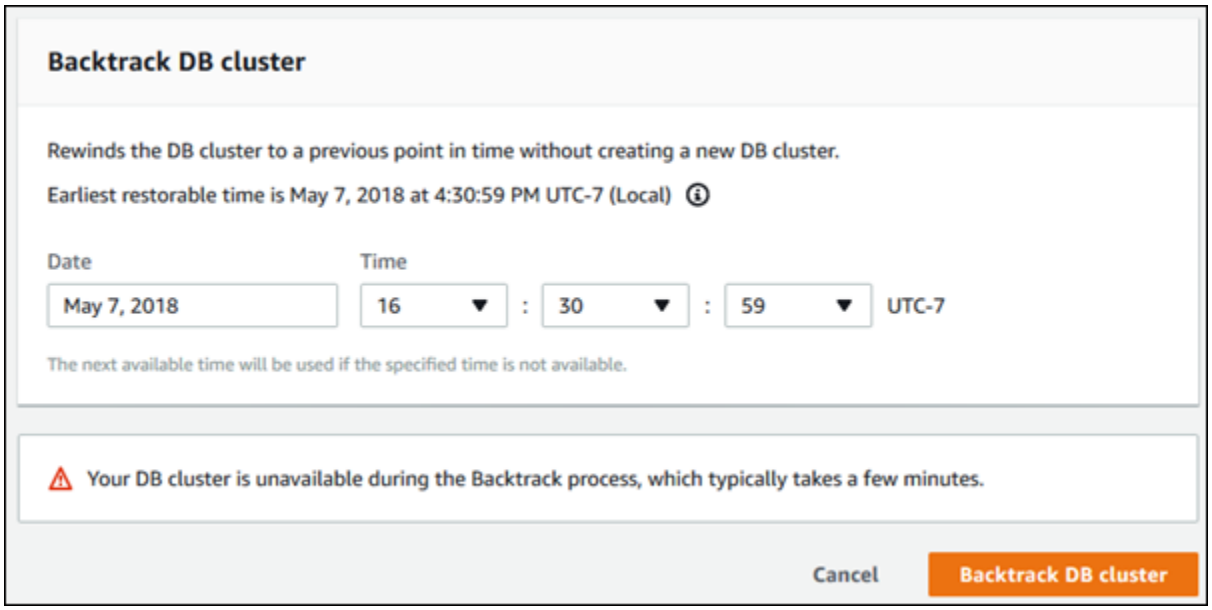
Konsole

Das folgende Verfahren beschreibt, wie Sie eine Rückverfolgung für einen DB-Cluster mit der Konsole durchführen.

Führen Sie eine Rückverfolgung mit der Konsole wie folgt durch:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die primäre Instance für den DB-Cluster aus, den Sie rückverfolgen möchten.
4. Wählen Sie unter Actions (Aktionen) die Option Backtrack DB cluster (DB-Cluster rückverfolgen) aus.

5. Geben Sie auf der Seite Backtrack DB cluster (DB-Cluster rückverfolgen) den Zeitstempel ein, zu dem der DB-Cluster rückverfolgt werden soll.



6. Wählen Sie Backtrack DB cluster (DB-Cluster rückverfolgen) aus.

AWS CLI

Im folgenden Verfahren wird beschrieben, wie ein DB-Cluster mit der rückverfolgt wir AWS CLI.

Um einen DB-Cluster zurückzuverfolgen, verwenden Sie AWS CLI

- Rufen Sie den backtrack-db-cluster AWS CLI-Befehl auf und geben Sie die folgenden Werte an:
  - `--db-cluster-identifier`: Name des DB-Clusters.
  - `--backtrack-to` – Der Zeitstempel im ISO 8601-Format, zu dem das DB-Cluster zurückverfolgt werden soll.

  Das folgende Beispiel führt eine Rückverfolgung des DB-Clusters `sample-cluster` auf den 19. März 2018 um 10:00 Uhr durch.

  Für LinuxmacOS, oderUnix:

```
aws rds backtrack-db-cluster \
    --db-cluster-identifier sample-cluster \
```

```
    --backtrack-to 2018-03-19T10:00:00+00:00
```

Windows:

```
aws rds backtrack-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --backtrack-to 2018-03-19T10:00:00+00:00
```

RDS-API

Um ein DB-Cluster über die Amazon RDS-API zurückzuverfolgen, verwenden Sie die Operation BacktrackDBCluster. Diese Operation nimmt die Rückverfolgung des mit `DBClusterIdentifier` angegebenen DB-Clusters auf den angegebenen Zeitpunkt vor.

Überwachung der Rückverfolgung

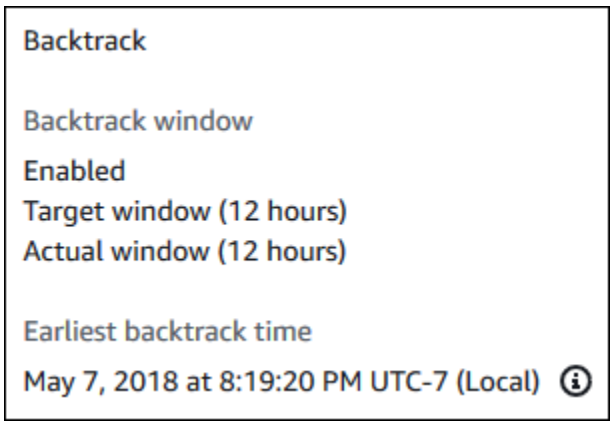
Sie können Rückverfolgungsinformationen für einen DB-Cluster anzeigen sowie Rückverfolgungskennzahlen überwachen.

Konsole

Zeigen Sie mit der Konsole Rückverfolgungsinformationen für einen DB-Cluster an und überwachen Sie die Rückverfolgungskennzahlen wie folgt:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Databases (Datenbanken) aus.
3. Wählen Sie den Namen des DB-Clusters, um die zugehörigen Informationen anzuzeigen.

   Die Rückverfolgungsinformationen befinden sich im Bereich Backtrack (Rückverfolgung).



Wenn die Rückverfolgung aktiviert ist, sind folgende Informationen verfügbar:

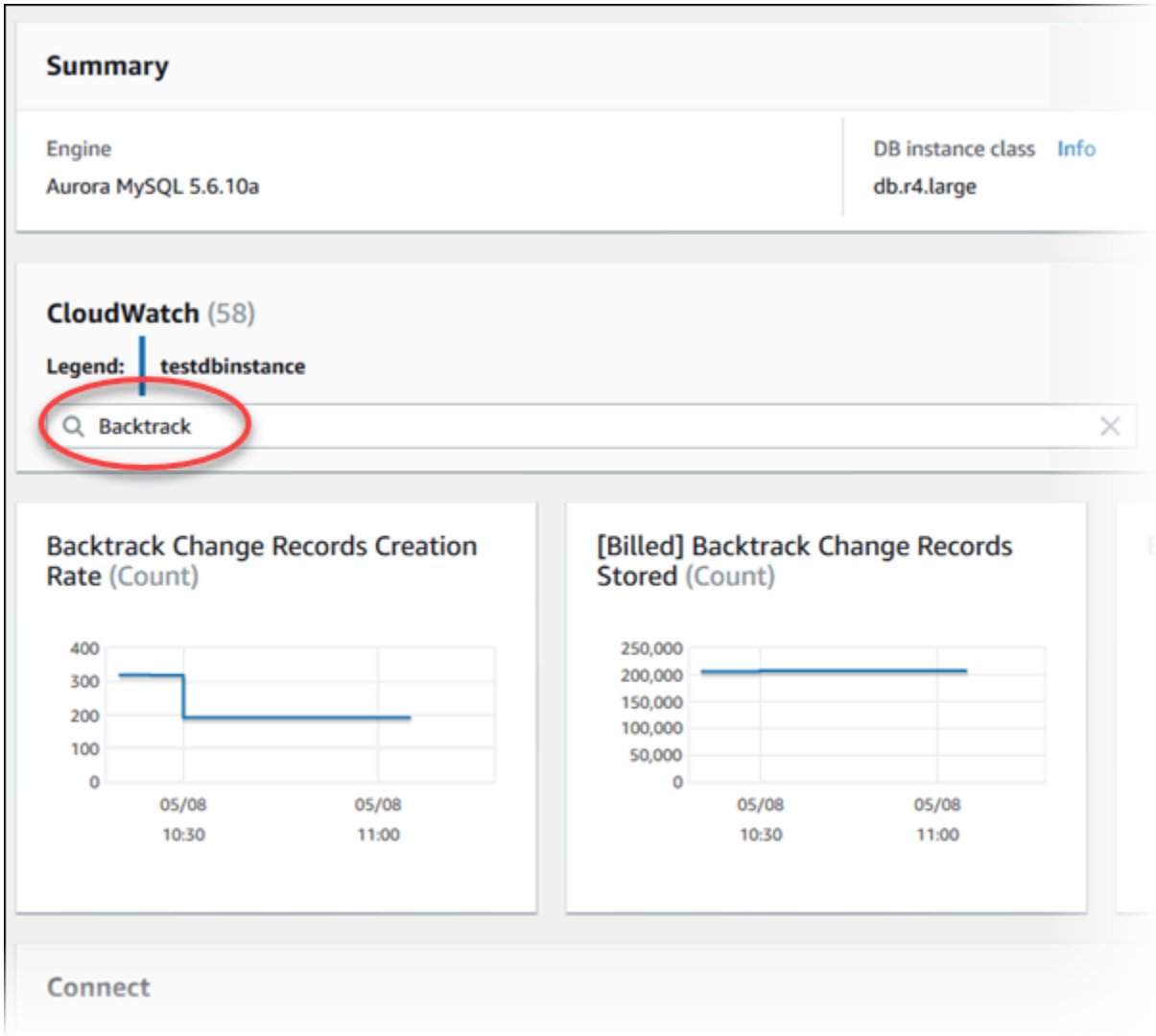
- Target window (Zielfenster): der zurzeit für das Zielfenster für die Rückverfolgung angegebene Zeitraum. Das Zielfenster bezeichnet die maximale Dauer, für die eine Rückverfolgung durchgeführt werden kann, sofern genug Speicher verfügbar ist.
- Actual window (Tatsächliches Fenster): der tatsächliche Zeitraum, über den Sie die Rückverfolgung ausführen können; dieser kann kleiner als das Zielfenster für die Rückverfolgung sein. Das Ist-Rückverfolgungsfenster basiert auf der Workload und dem für die Aufnahme von Änderungsdatensätzen für die Rückverfolgung verfügbaren Speicher.
- Earliest backtrack time (Früheste Rückverfolgungszeit): der früheste Rückverfolgungszeitpunkt, der für das DB-Cluster möglich ist. Sie können einen DB-Cluster nicht auf eine vor dem angezeigten Zeitpunkt liegende Zeit rückverfolgen.

4. Zeigen Sie die Rückverfolgungskennzahlen für den DB-Cluster wie folgt an:

   a. Wählen Sie im Navigationsbereich Instances aus.

   b. Wählen Sie den Namen der primären Instance des DB-Clusters, um die Details anzuzeigen.

   c. Geben Sie im CloudWatchAbschnitt etwas **`Backtrack`** in das CloudWatchFeld ein, um nur die Backtrack-Metriken anzuzeigen.



Die folgenden Kennzahlen werden angezeigt:

- Backtrack Change Records Creation Rate (Count) (Erstellungsrate (Anzahl) der Änderungsdatensätze für die Rückverfolgung): Diese Metrik gibt die Anzahl der Änderungsdatensätze für die Rückverfolgung an, die im Verlauf von fünf Minuten für das DB-Cluster erstellt wurden. Sie können diese Kennzahl heranziehen, um die Rückverfolgungskosten für das Zielfenster für die Rückverfolgung zu schätzen.
- [Billed] Backtrack Change Records Stored (Count) ([Berechnete] für die Rückverfolgung gespeicherte Änderungsdatensätze (Anzahl)): Diese Metrik gibt die tatsächliche Anzahl der Änderungsdatensätze für die Rückverfolgung an, die vom DB-Cluster verwendet werden.
- Backtrack Window Actual (Minutes) (Tatsächliches Rückverfolgungsfenster (Minuten)): Diese Metrik gibt an, ob es eine Differenz zwischen dem Zielfenster für die

Rückverfolgung und dem tatsächlichen Rückverfolgungsfenster gibt. Wenn das Zielfenster für die Rückverfolgung beispielsweise 2 Stunden (120 Minuten) lang ist und diese Kennzahl angibt, dass das Ist-Rückverfolgungsfenster nur 100 Minuten lang ist, ist das Ist-Rückverfolgungsfenster kleiner als das Zielfenster.

- Backtrack Window Alert (Count) (Rückverfolgungsfenster-Alarm (Anzahl)): Diese Metrik gibt an, wie oft das tatsächliche Rückverfolgungsfenster über einen bestimmten Zeitraum kleiner als das Zielfenster für die Rückverfolgung ist.

> **Note**
>
> Die folgenden Kennzahlen können hinter der aktuellen Zeit zurückliegen:
>
> - Erstellungsrate (Anzahl) der Änderungsdatensätze für die Rückverfolgung
> - [Billed] Backtrack Change Records Stored (Count) ([Berechnete] für die Rückverfolgung gespeicherte Änderungsdatensätze (Anzahl))

AWS CLI

Das folgende Verfahren beschreibt, wie Sie Rückverfolgungsinformationen für einen DB-Cluster mit anzeige AWS CLI.

Um Backtrack-Informationen für einen DB-Cluster anzuzeigen, verwenden Sie AWS CLI

- Rufen Sie den describe-db-clusters AWS CLI-Befehl auf und geben Sie die folgenden Werte an:
  - `--db-cluster-identifier`: Name des DB-Clusters.

  Das folgende Beispiel listet Rückverfolgungsinformationen für au `sample-cluster`.

  Für LinuxmacOS, oderUnix:

```
aws rds describe-db-clusters \
    --db-cluster-identifier sample-cluster
```

  Windows:

```
aws rds describe-db-clusters ^
    --db-cluster-identifier sample-cluster
```

RDS-API

Um die Rückverfolgungsinformationen für einen DB-Cluster über die Amazon RDS-API anzuzeigen, verwenden Sie die Aktion DescribeDBClusters. Diese Operation gibt Rückverfolgungsinformationen für den mit dem Wert `DBClusterIdentifier` angegebenen DB-Cluster zurück.

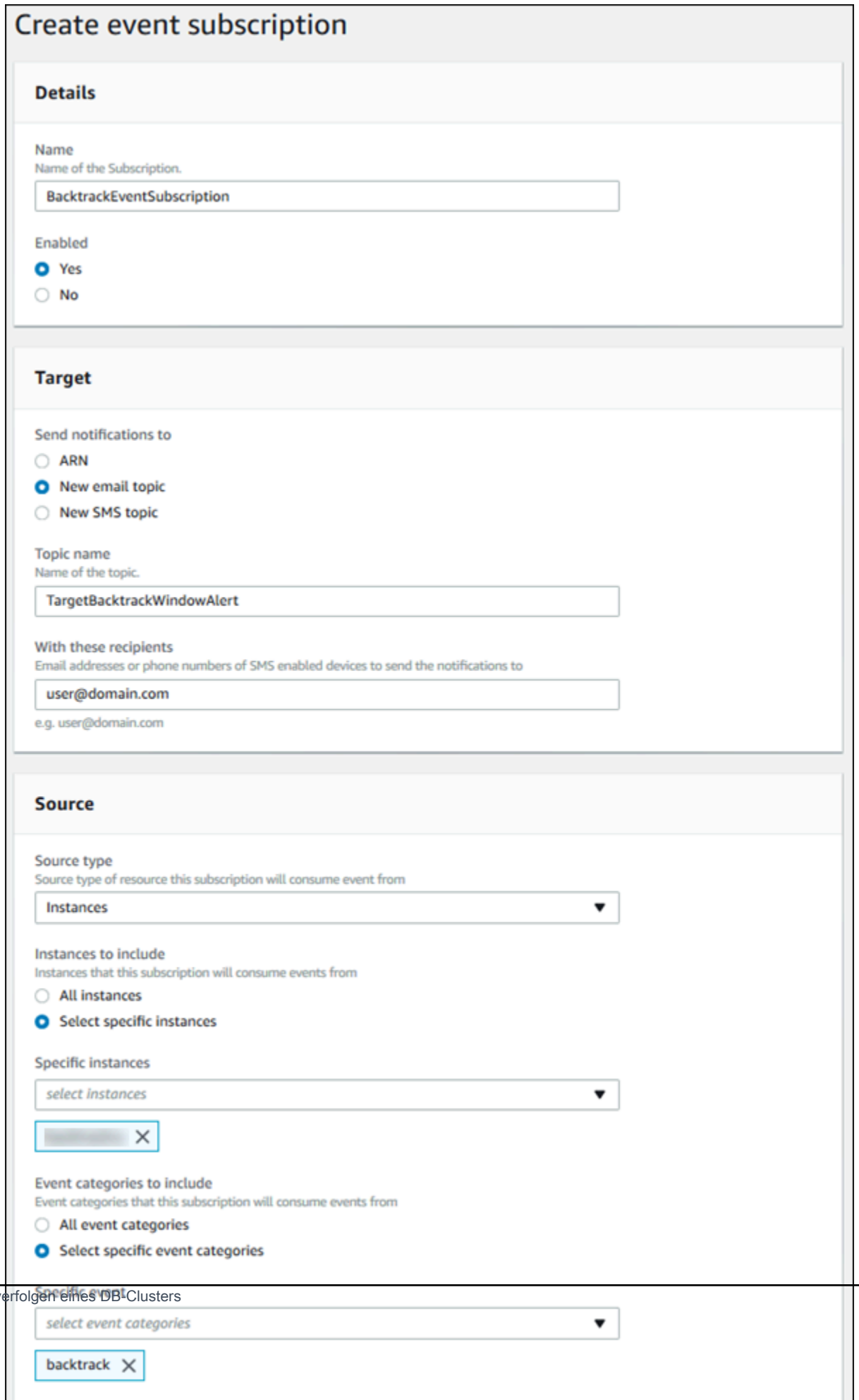
Abonnieren eines Rückverfolgungsereignisses mit der Konsole

Das folgende Verfahren beschreibt, wie Sie ein Rückverfolgungsereignis mit der Konsole abonnieren. Das Ereignis sendet eine E-Mail oder SMS, wenn das Ist-Rückverfolgungsfenster kürzer als das Zielfenster für die Rückverfolgung ist.

Zeigen Sie Rückverfolgungsinformationen mit der Konsole wie folgt an:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Event subscriptions (Ereignisabonnements) aus.
3. Wählen Sie Create event subscription (Ereignisabonnement erstellen) aus.
4. Geben Sie in das Feld Name (Name) einen Namen für das Ereignisabonnement ein und stellen Sie sicher, dass für Enabled (Aktiviert) der Wert Yes (Ja) ausgewählt ist.
5. Wählen Sie im Bereich Target (Ziel) die Option New email topic (Neues E-Mail-Thema) aus.
6. Geben Sie unter Topic name (Themenname) einen Namen für das Thema und unter With these recipients (Mit diesen Empfängern) die E-Mail-Adressen oder Telefonnummern der Benachrichtigungsempfänger ein.
7. Wählen Sie im Bereich Source (Quelle) für Source type (Quellentyp) den Wert Instances (Instances) aus.
8. Wählen Sie für Instances to include (Einzuschließende Instances) den Wert Select specific instances (Bestimmte Instances auswählen) und dann die DB-Instance aus.
9. Wählen Sie für Event categories to include (Einzuschließende Ereigniskategorien) den Wert Select specific event categories (Bestimmte Ereigniskategorien auswählen) und dann Backtrack (Rückverfolgen) aus.

Die Seite sollte der folgenden Seite ähneln.


Create event subscription
Details
Name
Name of the Subscription.
BacktrackEventSubscription
Enabled
Yes
No
Target
Send notifications to
ARN
New email topic
New SMS topic
Topic name
Name of the topic.
TargetBacktrackWindowAlert
With these recipients
Email addresses or phone numbers of SMS enabled devices to send the notifications to
user@domain.com
e.g. user@domain.com
Source
Source type
Source type of resource this subscription will consume event from
Instances
Instances to include
Instances that this subscription will consume events from
All instances
Select specific instances
Specific instances
select instances
Event categories to include
Event categories that this subscription will consume events from
All event categories
Select specific event categories
select event categories
backtrack

10. Wählen Sie Create aus.

Abrufen vorhandener Rückverfolgungen

Sie können Informationen über existierende Rückverfolgungen für einen DB-Cluster abrufen. Zu diesen Informationen gehören die eindeutige ID der Rückverfolgung, Ausgangs- und Zielzeitpunkt der Rückverfolgung, Datum und Zeitpunkt der Anforderung der Rückverfolgung und der aktuelle Status der Rückverfolgung.

> **Note**
>
> Derzeit können vorhandene Rückverfolgungen nicht mit der Konsole abgerufen werden.

AWS CLI

Das folgende Verfahren beschreibt, wie Sie vorhandene Rückverfolgungen für einen DB-Cluster mit der abrufe AWS CLI.

Um vorhandene Backtracks mit dem abzurufen AWS CLI

- Rufen Sie den describe-db-cluster-backtracks AWS CLI-Befehl auf und geben Sie die folgenden Werte an:
  - `--db-cluster-identifier`: Name des DB-Clusters.

  Im folgenden Beispiel werden die für vorhandenen Rückverfolgungen abgerufe `sample-cluster`.

  Für LinuxmacOS, oderUnix:

```
aws rds describe-db-cluster-backtracks \
    --db-cluster-identifier sample-cluster
```

  Windows:

```
aws rds describe-db-cluster-backtracks ^
```

```
    --db-cluster-identifier sample-cluster
```

RDS-API

Verwenden Sie den Vorgang DescribeDB, um Informationen über die Backtracks für einen DB-Cluster mithilfe der Amazon RDS-API abzurufen. ClusterBacktracks Diese Operation gibt Informationen über Rückverfolgungen für den mit dem Wert `DBClusterIdentifier` angegebenen DB-Cluster zurück.

Deaktivieren der Rückverfolgung für einen DB-Cluster

Sie können die Rückverfolgungsfunktion für einen DB-Cluster deaktivieren.

Konsole

Sie können die Rückverfolgung für einen DB-Cluster mit der Konsole deaktivieren. Nachdem Sie die Rückverfolgung für einen Cluster vollständig deaktiviert haben, können Sie sie für diesen Cluster nicht erneut aktivieren.

Deaktivieren Sie die Rückverfolgungsfunktion für einen DB-Cluster mit der Konsole wie folgt:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Databases (Datenbanken) aus.
3. Wählen Sie den zu ändernden Cluster und dann die Option Modify (Ändern) aus.
4. Wählen Sie im Bereich Backtrack (Rückverfolgung) die Option Disable Backtrack (Rückverfolgung deaktivieren) aus.
5. Klicken Sie auf Weiter.
6. Wählen Sie für Einplanung von Änderungen eine der folgenden Optionen:
   - Apply during the next scheduled maintenance window (Während des nächsten geplanten Wartungszeitfensters anwenden): Die Änderung soll erst während des nächsten Wartungsfensters ausgeführt werden.
   - Apply immediately (Sofort anwenden): Die Änderung soll sobald wie möglich angewendet werden.
7. Wählen Sie Modify Cluster (Cluster ändern) aus.

AWS CLI

Sie können die Backtrack-Funktion für einen DB-Cluster mithilfe von deaktivieren, AWS CLI indem Sie das Backtrack-Zielfenster auf `0` (Null) setzen. Nachdem Sie die Rückverfolgung für einen Cluster vollständig deaktiviert haben, können Sie sie für diesen Cluster nicht erneut aktivieren.

Um das Ziel-Backtrack-Fenster für einen DB-Cluster zu ändern, verwenden Sie AWS CLI

- Rufen Sie den modify-db-cluster AWS CLI-Befehl auf und geben Sie die folgenden Werte an:
  - `--db-cluster-identifier`: Name des DB-Clusters.
  - `--backtrack-window` – Geben Sie `0` an, um die Rückverfolgung zu deaktivieren.

  Im folgenden Beispiel wird die Rückverfolgungsfunktion für `sample-cluster` deaktiviert, indem `--backtrack-window` der Wert `0` zugewiesen wird.

  Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --backtrack-window 0
```

  Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --backtrack-window 0
```

RDS-API

Um die Rückverfolgungsfunktion für einen DB-Cluster über die Amazon RDS-API zu deaktivieren, verwenden Sie die Aktion ModifyDBCluster. Weisen Sie `BacktrackWindow` den Wert `0` (Null) zu und geben Sie den DB-Cluster im Wert `DBClusterIdentifier` an. Nachdem Sie die Rückverfolgung für einen Cluster vollständig deaktiviert haben, können Sie sie für diesen Cluster nicht erneut aktivieren.

Testen von Amazon Aurora MySQL unter Verwendung von Fehlersimulationsabfragen

Sie können die Fehlertoleranz Ihres DB-Clusters von Aurora MySQL testen, indem Sie Fehlersimulationsabfragen verwenden. Fehlersimulationsabfragen werden als SQL-Befehle an eine Amazon Aurora-Instance ausgegeben. Sie ermöglichen Ihnen, eines der folgenden Fehlerereignisse geplant zu simulieren:

- Einen Ausfall einer Writer- oder Reader-DB-Instance
- Ein Ausfall eines Aurora-Replikats
- Einen Festplattenfehler
- Festplattenüberlastung

Wenn eine Fehlersimulationsabfrage einen Absturz angibt, erzwingt sie einen Absturz der DB-Instance von Aurora MySQL. Die anderen Fehler-Injection-Abfragen erzeugen Simulationen von Ausfallereignissen, lösen aber keine Ereignisse aus. Wenn Sie eine Fehlersimulationsabfrage senden, geben Sie auch einen Zeitraum vor, in dem die Simulation ablaufen soll.

Sie können eine Fehlersimulationsabfrage an eine Ihrer Aurora Replica-Instances senden, indem Sie eine Verbindung mit dem Endpunkt der Aurora Replica herstellen. Weitere Informationen finden Sie unter Amazon Aurora-Verbindungsverwaltung.

Zum Ausführen von Fehlersimulationsabfragen sind alle Master-Benutzerrechte erforderlich. Weitere Informationen finden Sie unter Berechtigungen von Hauptbenutzerkonten.

Testen eines Instance-Ausfalls

Sie können den Absturz einer Amazon-Aurora-Instance erzwingen, indem Sie die Fehlersimulationsabfrage `ALTER SYSTEM CRASH` verwenden.

Für diese Fehlersimulationsabfrage tritt kein Failover auf. Wenn Sie einen Failover testen möchten, können Sie die Instance-Operation Failover für Ihren DB-Cluster in der RDS-Konsole ausführen oder den AWS CLI-Befehl failover-db-cluster bzw. die RDS-API-Operation FailoverDBCluster verwenden.

Syntax

```
ALTER SYSTEM CRASH [ INSTANCE | DISPATCHER | NODE ];
```

Optionen

Diese Fehlersimulationsabfrage löst einen der folgenden Ausfalltypen aus:

- **`INSTANCE`** – Es wird ein Absturz der PostgreSQL-kompatiblen Datenbank für die Amazon-Aurora-Instance simuliert.
- **`DISPATCHER`** – Es wird ein Absturz des Dispatchers auf Schreiber-Instance für das Aurora-DB-Cluster simuliert. Der Dispatcher schreibt Updates zum Cluster-Volume für ein Amazon Aurora-DB-Cluster.
- **`NODE`** – Es wird ein Absturz sowohl der MySQL-kompatiblen Datenbank als auch des Dispatchers für die Amazon-Aurora-Instance simuliert. Für diese Fehlersimulationsabfrage wird auch der Cache gelöscht.

Der Standard-Ausfalltyp ist `INSTANCE`.

Testen eines Aurora-Replikatausfalls

Sie können den Ausfall eines Aurora-Replikats mittels der Fehlersimulationsabfrage `ALTER SYSTEM SIMULATE READ REPLICA FAILURE` simulieren.

Der Ausfall eines Aurora Replica blockiert alle Anfragen an einen Aurora Replica oder alle Aurora Replicas im DB-Cluster für einen bestimmten Zeitabschnitt. Wenn dieser abgelaufen ist, werden die betroffenen Aurora-Replikate automatisch mit der Haupt-Instance synchronisiert.

Syntax

```
ALTER SYSTEM SIMULATE percentage_of_failure PERCENT READ REPLICA FAILURE
    [ TO ALL | TO "replica name" ]
    FOR INTERVAL quantity { YEAR | QUARTER | MONTH | WEEK | DAY | HOUR | MINUTE |
 SECOND };
```

Optionen

Diese Fehlersimulationsabfrage verwendet die folgenden Parameter:

- **`percentage_of_failure`** – Der Prozentsatz der Anfragen, die während des Ausfallereignisses blockiert werden sollen. Dieser Wert kann ein Duplikat zwischen 0 und 100 sein. Wenn Sie 0 festlegen, werden keine Anfragen blockiert. Wenn 100 festgelegt wird, werden alle Anfragen blockiert.

- Ausfalltyp – Der zu simulierende Ausfalltyp. Legen Sie `TO ALL` fest, um Ausfälle für alle Aurora-Replikate im DB-Cluster zu simulieren. Geben Sie `TO` und den Namen eines Aurora-Replikats an, um einen Ausfall des einzelnen Aurora-Replikats zu simulieren. Der Standard-Ausfalltyp ist `TO ALL`.
- **`quantity`** – Der Zeitraum, über den der Ausfall des Aurora-Replikats simuliert werden soll. Das Intervall wird als eine Menge gefolgt von einer Zeiteinheit angegeben. Die Simulation wird für die Dauer der angegebenen Einheit auftreten. Beispielsweise ergibt `20 MINUTE` eine Simulation, die 20 Minuten lang ausgeführt wird.

> **Note**
>
> Seien Sie vorsichtig bei der Angabe des Zeitintervalls für das Ausfallereignis in Ihrem Aurora-Replikat. Wenn Sie ein zu langes Zeitintervall festlegen und Ihre Schreiber-Instance eine große Datenmenge während des Ausfallereignisses schreibt, könnte Ihr Aurora-DB-Cluster annehmen, dass Ihr Aurora-Replikat ausgefallen ist und es ersetzen.

Testen eines Festplattenausfalls

Sie können einen Datenträgerausfall für ein Aurora-DB-Cluster mittels der Fehlersimulationsabfrage `ALTER SYSTEM SIMULATE DISK FAILURE` simulieren.

Während einer Simulation eines Festplattenausfalls markiert der Aurora-DB-Cluster zufällige Festplattensegmente als fehlerhaft. Anfragen an diese Segmente werden für die Dauer der Simulation blockiert.

Syntax

```
ALTER SYSTEM SIMULATE percentage_of_failure PERCENT DISK FAILURE
    [ IN DISK index | NODE index ]
    FOR INTERVAL quantity { YEAR | QUARTER | MONTH | WEEK | DAY | HOUR | MINUTE |
 SECOND };
```

Optionen

Diese Fehlersimulationsabfrage verwendet die folgenden Parameter:

- **`percentage_of_failure`** – Der Prozentsatz des Datenträgers, der während des Ausfallereignisses als ausgefallen markiert werden soll. Dieser Wert kann ein Duplikat zwischen 0

und 100 sein. Wenn Sie 0 festlegen, wird kein Segment der Festplatte als fehlerhaft markiert. Wenn Sie 100 festlegen, wird die gesamte Festplatte als fehlerhaft markiert.

- **`DISK index`** – Ein spezifischer logischer Datenblock, für den das Ausfallereignis simuliert werden soll. Wenn Sie den verfügbaren Bereich an logischen Datenblocks überschreiten, erhalten Sie eine Fehlermeldung, in der Ihnen der maximal festlegbare Indexwert mitgeteilt wird. Weitere Informationen finden Sie unter Anzeigen des Volume-Status für einen Aurora MySQL-DB-Cluster.
- **`NODE index`** – Ein spezifischer Speicherknoten, für den das Ausfallereignis simuliert werden soll. Wenn Sie den verfügbaren Bereich an Speicherknoten überschreiten, erhalten Sie eine Fehlermeldung, in der Ihnen der maximal festlegbare Indexwert mitgeteilt wird. Weitere Informationen finden Sie unter Anzeigen des Volume-Status für einen Aurora MySQL-DB-Cluster.
- **`quantity`** – Der Zeitraum, über den der Datenträgerausfall simuliert werden soll. Das Intervall wird als eine Menge gefolgt von einer Zeiteinheit angegeben. Die Simulation wird für die Dauer der angegebenen Einheit auftreten. Beispielsweise ergibt `20 MINUTE` eine Simulation, die 20 Minuten lang ausgeführt wird.

Testen einer Festplattenüberlastung

Sie können einen Datenträgerausfall für ein Aurora-DB-Cluster mittels der Fehlersimulationsabfrage `ALTER SYSTEM SIMULATE DISK CONGESTION` simulieren.

Während einer Simulation einer Festplattenüberlastung markiert der Aurora-DB-Cluster zufällige Festplattensegmente als überlastet. Anfragen an diese Segmente werden für die Dauer der angegebenen minimalen und maximalen Verzögerungszeit während der Simulation verzögert.

Syntax

```
ALTER SYSTEM SIMULATE percentage_of_failure PERCENT DISK CONGESTION
    BETWEEN minimum AND maximum MILLISECONDS
    [ IN DISK index | NODE index ]
    FOR INTERVAL quantity { YEAR | QUARTER | MONTH | WEEK | DAY | HOUR | MINUTE |
 SECOND };
```

Optionen

Diese Fehlersimulationsabfrage verwendet die folgenden Parameter:

- **`percentage_of_failure`** – Der Prozentsatz des Datenträgers, der während des Ausfallereignisses als überlastet markiert werden soll. Dieser Wert kann ein Duplikat zwischen

0 und 100 sein. Wenn Sie 0 festlegen, wird kein Segment der Festplatte als überlastet markiert. Wenn Sie 100 festlegen, wird die gesamte Festplatte als überlastet markiert.

- **`DISK index`** oder **`NODE index`** – Ein spezifischer Datenträger oder Knoten, für den das Ausfallereignis simuliert werden soll. Wenn Sie den verfügbaren Bereich der Indizes für die Festplatten oder den Knoten überschreiten, erhalten Sie eine Fehlermeldung, in der Ihnen der maximal festlegbare Indexwert mitgeteilt wird.
- **`minimum`** und **`maximum`** – Der Mindest- und Höchstwert in Millisekunden für die Überlastungsverzögerung. Festplattensegmente, die als überlastet markiert sind, werden innerhalb des Bereichs zwischen der minimalen und maximalen Anzahl an Millisekunden während der Simulation verzögert.
- **`quantity`** – Der Zeitraum, über den die Datenträgerüberlastung simuliert werden soll. Das Intervall wird als eine Menge gefolgt von einer Zeiteinheit angegeben. Die Simulation wird für die Dauer der angegebenen Zeiteinheit ausgeführt. Beispielsweise ergibt `20 MINUTE` eine Simulation, die 20 Minuten lang ausgeführt wird.

Ändern von Tabellen in Amazon Aurora mithilfe von Fast DDL

Amazon Aurora umfasst Optimierungen, um einen `ALTER TABLE`-Vorgang nahezu sofort auszuführen. Der Vorgang schließt ab, ohne dass ein Kopieren der Tabelle erforderlich ist und ohne eine materielle Auswirkung auf andere DML-Statements zu haben. Da kein temporärer Speicher für eine Tabellenkopie benötigt wird, haben DDL-Statements praktische Vorteile, sogar für große Tabellen auf kleinen Instance-Klassen.

Aurora MySQL Version 3 ist mit der MySQL 8.0-Funktion namens Instant DDL kompatibel. Aurora MySQL Version 2 verwendet eine andere Implementierung namens Fast DDL.

Themen

Sofortige DDL (Aurora MySQL Version 3)

Die von Aurora MySQL Version 3 durchgeführte Optimierung zur Verbesserung der Effizienz einiger DDL-Vorgänge wird als Instant DDL bezeichnet.

Aurora MySQL Version 3 ist mit der Instant DDL von Community MySQL 8.0 kompatibel. Sie führen einen sofortigen DDL-Vorgang durch, indem Sie die Klausel `ALGORITHM=INSTANT` mit der `ALTER TABLE`-Anweisung verwenden. Weitere Informationen zu Syntax und Verwendung von Instant DDL finden Sie unter ALTER TABLE und Online DDL Operations in der MySQL-Dokumentation.

Die folgenden Beispiele veranschaulichen die Instant-DDL-Funktion. Die `ALTER TABLE`-Anweisungen fügen Spalten hinzu und ändern die Standardspaltenwerte. Die Beispiele umfassen sowohl reguläre als auch virtuelle Spalten sowie reguläre und partitionierte Tabellen. Bei jedem Schritt können Sie die Ergebnisse durch die Ausgabe von `SHOW CREATE TABLE`- und `DESCRIBE`-Anweisungen anzeigen.

```
mysql> CREATE TABLE t1 (a INT, b INT, KEY(b)) PARTITION BY KEY(b) PARTITIONS 6;
Query OK, 0 rows affected (0.02 sec)

mysql> ALTER TABLE t1 RENAME TO t2, ALGORITHM = INSTANT;
Query OK, 0 rows affected (0.01 sec)

mysql> ALTER TABLE t2 ALTER COLUMN b SET DEFAULT 100, ALGORITHM = INSTANT;
Query OK, 0 rows affected (0.00 sec)

mysql> ALTER TABLE t2 ALTER COLUMN b DROP DEFAULT, ALGORITHM = INSTANT;
Query OK, 0 rows affected (0.01 sec)

mysql> ALTER TABLE t2 ADD COLUMN c ENUM('a', 'b', 'c'), ALGORITHM = INSTANT;
Query OK, 0 rows affected (0.01 sec)

mysql> ALTER TABLE t2 MODIFY COLUMN c ENUM('a', 'b', 'c', 'd', 'e'), ALGORITHM =
 INSTANT;
Query OK, 0 rows affected (0.01 sec)

mysql> ALTER TABLE t2 ADD COLUMN (d INT GENERATED ALWAYS AS (a + 1) VIRTUAL), ALGORITHM
 = INSTANT;
Query OK, 0 rows affected (0.02 sec)

mysql> ALTER TABLE t2 ALTER COLUMN a SET DEFAULT 20,
    ->   ALTER COLUMN b SET DEFAULT 200, ALGORITHM = INSTANT;
Query OK, 0 rows affected (0.01 sec)

mysql> CREATE TABLE t3 (a INT, b INT) PARTITION BY LIST(a)(
    ->   PARTITION mypart1 VALUES IN (1,3,5),
    ->   PARTITION MyPart2 VALUES IN (2,4,6)
    -> );
```

```
Query OK, 0 rows affected (0.03 sec)

mysql> ALTER TABLE t3 ALTER COLUMN a SET DEFAULT 20, ALTER COLUMN b SET DEFAULT 200,
 ALGORITHM = INSTANT;
Query OK, 0 rows affected (0.01 sec)

mysql> CREATE TABLE t4 (a INT, b INT) PARTITION BY RANGE(a)
    ->   (PARTITION p0 VALUES LESS THAN(100), PARTITION p1 VALUES LESS THAN(1000),
    ->   PARTITION p2 VALUES LESS THAN MAXVALUE);
Query OK, 0 rows affected (0.05 sec)

mysql> ALTER TABLE t4 ALTER COLUMN a SET DEFAULT 20,
    ->   ALTER COLUMN b SET DEFAULT 200, ALGORITHM = INSTANT;
Query OK, 0 rows affected (0.01 sec)

/* Sub-partitioning example */
mysql> CREATE TABLE ts (id INT, purchased DATE, a INT, b INT)
    ->   PARTITION BY RANGE( YEAR(purchased) )
    ->     SUBPARTITION BY HASH( TO_DAYS(purchased) )
    ->     SUBPARTITIONS 2 (
    ->       PARTITION p0 VALUES LESS THAN (1990),
    ->       PARTITION p1 VALUES LESS THAN (2000),
    ->       PARTITION p2 VALUES LESS THAN MAXVALUE
    ->    );
Query OK, 0 rows affected (0.10 sec)

mysql> ALTER TABLE ts ALTER COLUMN a SET DEFAULT 20,
    ->   ALTER COLUMN b SET DEFAULT 200, ALGORITHM = INSTANT;
Query OK, 0 rows affected (0.01 sec)
```

Fast DDL (Aurora MySQL Version 2)

In MySQL wirken sich viele Data Definition Language (DDL)-Vorgänge signifikant auf die Leistungsfähigkeit aus.

Nehmen wir beispielsweise an, dass Sie eine `ALTER TABLE`-Operation verwenden, um eine Spalte zu einer Tabelle hinzuzufügen. Abhängig vom angegebenen Algorithmus für den Vorgang kann der Vorgang Folgendes beinhalten:

- Erstellen einer vollen Kopie für die Tabelle
- Erstellen einer temporären Tabelle für die Verarbeitung simultaner Data Manipulation Language (DML)-Vorgänge

- Erneutes Aufbauen aller Indizes für die Tabelle
- Anwenden von Tabellensperren beim Vornehmen von simultanen DML-Änderungen
- Verlangsamen des simultanen DML-Durchsatzes

Die von Aurora MySQL Version 2 durchgeführte Optimierung zur Verbesserung der Effizienz einiger DDL-Vorgänge wird als Fast DDL bezeichnet.

In Aurora MySQL Version 3 verwendet Aurora die MySQL 8.0-Funktion namens Instant DDL. Aurora MySQL Version 2 verwendet eine andere Implementierung namens Fast DDL.

> **Important**
>
> Zurzeit muss der Aurora-Labormodus aktiviert werden, um Fast DDL für Aurora MySQL verwenden zu können. Die Verwendung von Fast DDL für Produktions-DB-Cluster wird nicht empfohlen. Weitere Informationen zum Aktivieren des Aurora-Labormodus finden Sie unter Amazon Aurora MySQL-Labor-Modus.

Schnelle DDL-Beschränkungen

Aktuell hat Fast DDL folgende Einschränkungen:

- Sie unterstützt nur das Hinzufügen von löschbaren Spalten, ohne Standardwerte, bis zum Ende einer bestehenden Tabelle.
- Schnelle DDL funktioniert nicht für partitionierte Tabellen.
- Schnelle DDL funktioniert nicht für InnoDB-Tabellen, die das Zeilenformat REDUNDANT verwenden.
- Schnelle DDL funktioniert nicht für Tabellen mit Volltextsuchindizes.
- Wenn die maximal mögliche Datensatzgröße für die DDL-Operation zu groß ist, wird Fast DDL nicht verwendet. Eine Datensatzgröße ist zu groß, wenn sie größer als die Hälfte der Seitengröße ist. Die maximale Größe eines Datensatzes wird berechnet, indem die maximale Größe aller Spalten addiert wird. Bei Spalten variabler Größe werden nach InnoDB-Standards externe Bytes für die Berechnung nicht berücksichtigt.

Schnelle DDL-Syntax

```
ALTER TABLE tbl_name ADD COLUMN col_name column_definition
```

Dieses Statement verwendet die folgenden Optionen:

- **`tbl_name`** — Der Name der Tabelle, die geändert werden soll.
- **`col_name`** — Der Name der Spalte, die hinzugefügt werden soll.
- **`col_definition`** — Die Definition der Spalte, die hinzugefügt werden soll.

> **Note**
>
> Sie müssen eine löschbare Spaltendefinition ohne einen Standardwert festlegen. Andernfalls kann Fast DDL nicht verwendet werden.

Fast DDL-Beispiele

Die folgenden Beispiele veranschaulichen die Beschleunigung von Fast-DDL-Operationen. Im ersten SQL-Beispiel werden `ALTER TABLE`-Anweisungen für eine große Tabelle ausgeführt, ohne Fast DDL zu verwenden. Diese Operation benötigt beträchtliche Zeit. Ein CLI-Beispiel zeigt, wie Fast DDL für den Cluster aktiviert wird. Dann führt ein anderes SQL-Beispiel dieselben `ALTER TABLE` Anweisungen für eine identische Tabelle aus. Mit aktiviertem Fast DDL ist der Betrieb sehr schnell.

In diesem Beispiel wird die `ORDERS` Tabelle aus dem TPC-H-Benchmark verwendet, die 150 Millionen Zeilen enthält. Dieser Cluster verwendet absichtlich eine relativ kleine Instance-Klasse, um zu demonstrieren, wie lange `ALTER TABLE`-Anweisungen dauern können, wenn Sie Fast DDL nicht verwenden können. Im Beispiel wird ein Klon der Originaltabelle erstellt, der identische Daten enthält. Eine Überprüfung der Einstellung für `aurora_lab_mode` bestätigt, dass der Cluster Fast DDL nicht verwenden kann, da der Labormodus nicht aktiviert ist. Dann brauchen `ALTER TABLE ADD COLUMN` Anweisungen beträchtliche Zeit, um am Ende der Tabelle neue Spalten hinzuzufügen.

```
mysql> create table orders_regular_ddl like orders;
Query OK, 0 rows affected (0.06 sec)

mysql> insert into orders_regular_ddl select * from orders;
Query OK, 150000000 rows affected (1 hour 1 min 25.46 sec)

mysql> select @@aurora_lab_mode;
```

```
+-------------------+
| @@aurora_lab_mode |
+-------------------+
|                 0 |
+-------------------+

mysql> ALTER TABLE orders_regular_ddl ADD COLUMN o_refunded boolean;
Query OK, 0 rows affected (40 min 31.41 sec)

mysql> ALTER TABLE orders_regular_ddl ADD COLUMN o_coverletter varchar(512);
Query OK, 0 rows affected (40 min 44.45 sec)
```

In diesem Beispiel wird die gleiche Vorbereitung einer großen Tabelle wie im vorherigen Beispiel durchgeführt. Sie können den Labor-Modus jedoch nicht einfach innerhalb einer interaktiven SQL-Sitzung aktivieren. Diese Einstellung muss in einer benutzerdefinierten Parametergruppe aktiviert sein. Dazu müssen Sie die `mysql` Sitzung verlassen und einige AWS CLI-Befehle ausführen oder die AWS Management Console verwenden.

```
mysql> create table orders_fast_ddl like orders;
Query OK, 0 rows affected (0.02 sec)

mysql> insert into orders_fast_ddl select * from orders;
Query OK, 150000000 rows affected (58 min 3.25 sec)

mysql> set aurora_lab_mode=1;
ERROR 1238 (HY000): Variable 'aurora_lab_mode' is a read only variable
```

Das Aktivieren des Labor-Modus für den Cluster erfordert einige Arbeiten an einer Parametergruppe. In diesem Beispiel für eine AWS CLI wird eine Clusterparametergruppe verwendet, um sicherzustellen, dass alle DB-Instances im Cluster den gleichen Wert für die Einstellung des Labor-Modus verwenden.

```
$ aws rds create-db-cluster-parameter-group \
  --db-parameter-group-family aurora5.7 \
    --db-cluster-parameter-group-name lab-mode-enabled-57 --description 'TBD'
$ aws rds describe-db-cluster-parameters \
  --db-cluster-parameter-group-name lab-mode-enabled-57 \
    --query '*[*].[ParameterName,ParameterValue]' \
      --output text | grep aurora_lab_mode
aurora_lab_mode 0
$ aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name lab-mode-enabled-57 \
```

```
    --parameters ParameterName=aurora_lab_mode,ParameterValue=1,ApplyMethod=pending-
reboot
{
    "DBClusterParameterGroupName": "lab-mode-enabled-57"
}

# Assign the custom parameter group to the cluster that's going to use Fast DDL.
$ aws rds modify-db-cluster --db-cluster-identifier tpch100g \
  --db-cluster-parameter-group-name lab-mode-enabled-57
{
  "DBClusterIdentifier": "tpch100g",
  "DBClusterParameterGroup": "lab-mode-enabled-57",
  "Engine": "aurora-mysql",
  "EngineVersion": "5.7.mysql_aurora.2.10.2",
  "Status": "available"
}

# Reboot the primary instance for the cluster tpch100g:
$ aws rds reboot-db-instance --db-instance-identifier instance-2020-12-22-5208
{
  "DBInstanceIdentifier": "instance-2020-12-22-5208",
  "DBInstanceStatus": "rebooting"
}

$ aws rds describe-db-clusters --db-cluster-identifier tpch100g \
  --query '*[].[DBClusterParameterGroup]' --output text
lab-mode-enabled-57

$ aws rds describe-db-cluster-parameters \
  --db-cluster-parameter-group-name lab-mode-enabled-57 \
    --query '*[*].{ParameterName:ParameterName,ParameterValue:ParameterValue}' \
      --output text | grep aurora_lab_mode
aurora_lab_mode 1
```

Das folgende Beispiel zeigt die verbleibenden Schritte, nachdem die Änderung der Parametergruppe wirksam wird. Es testet die Einstellung für `aurora_lab_mode`, um sicherzustellen, dass der Cluster Fast DDL verwenden kann. Dann führt es `ALTER TABLE` Anweisungen aus, um Spalten am Ende einer anderen großen Tabelle hinzuzufügen. Dieses Mal werden die Anweisungen sehr schnell beendet.

```
mysql> select @@aurora_lab_mode;
+------------------+
| @@aurora_lab_mode |
```

```
+-------------------+
|                 1 |
+-------------------+

mysql> ALTER TABLE orders_fast_ddl ADD COLUMN o_refunded boolean;
Query OK, 0 rows affected (1.51 sec)

mysql> ALTER TABLE orders_fast_ddl ADD COLUMN o_coverletter varchar(512);
Query OK, 0 rows affected (0.40 sec)
```

Anzeigen des Volume-Status für einen Aurora MySQL-DB-Cluster

In Amazon Aurora besteht ein DB-Cluster-Volume aus einer Sammlung von logischen Blöcken. Jeder von ihnen stellt 10 Gigabyte des zugeteilten Arbeitsspeichers bereit. Diese Blöcke werden als Schutzgruppen bezeichnet.

Die Daten in den einzelnen Schutzgruppen werden über sechs physische Speichereinheiten, so genannte Speicherknoten, repliziert. Diese Speicherknoten werden in drei Availability Zones (AZs) in der AWS-Region zugeteilt, in der sich das DB-Cluster befindet. Jeder Speicherknoten wiederum besteht aus einem oder mehreren logischen Datenblöcken für das DB-Cluster-Volume. Weitere Informationen zu Schutzgruppen und Speicherknoten finden Sie unter Introducing the Aurora Storage Engine im AWS Database Blog.

Sie können den Ausfall eines gesamten Speicherknotens oder den eines einzelnen Datenblocks innerhalb eines Speicherknotens simulieren. Verwenden Sie hierfür die Fehlersimulationsanweisung `ALTER SYSTEM SIMULATE DISK FAILURE`. Sie geben für die Anweisung den Indexwert eines spezifischen logischen Datenblocks oder Speicherknotens an. Wenn Sie jedoch einen Indexwert angeben, der größer als die Anzahl der vom DB-Cluster-Volume verwendeten logischen Datenblöcke oder Speicherknoten ist, gibt die Anweisung einen Fehler zurück. Weitere Informationen über Fehlersimulationsabfragen finden Sie unter Testen von Amazon Aurora MySQL unter Verwendung von Fehlersimulationsabfragen.

Sie können diesen Fehler vermeiden, indem Sie die Anweisung `SHOW VOLUME STATUS` verwenden. Die Anweisung gibt zwei Serverstatusvariablen zurück, `Disks` und `Nodes`. Diese Variablen stellen jeweils die gesamte Anzahl an logischen Datenblocks und Speicherknoten für das DB-Cluster-Volume dar.

Syntax

```
SHOW VOLUME STATUS
```

Beispiel

Das folgende Beispiel zeigt ein typisches Ergebnis von SHOW VOLUME STATUS.

```
mysql> SHOW VOLUME STATUS;
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| Disks         | 96    |
| Nodes         | 74    |
+---------------+-------+
```

Optimieren von Aurora MySQL

Warteereignisse und Thread-Zustände sind wichtige Optimierungs-Tools für Aurora MySQL. Wenn Sie herausfinden, warum Sitzungen auf Ressourcen warten und was sie tun, können Sie Engpässe besser reduzieren. Anhand der Informationen in diesem Abschnitt können Sie mögliche Ursachen und Abhilfemaßnahmen ermitteln.

Amazon DevOps Guru für RDS kann proaktiv feststellen, ob in Ihren Aurora-MySQL-Datenbanken problematische Bedingungen vorliegen, die später zu größeren Problemen führen könnten. Amazon DevOps Guru für RDS veröffentlicht eine Erklärung und Empfehlungen für Korrekturmaßnahmen in einem proaktiven Einblick. Dieser Abschnitt enthält Einblicke in Bezug auf häufig auftretende Probleme.

> **Important**
>
> Die Warteereignisse und Thread-Zustände in diesem Abschnitt sind spezifisch für Aurora MySQL. Verwenden Sie die Informationen in diesem Abschnitt, um nur Amazon Aurora zu optimieren, nicht Amazon RDS for MySQL.
> Einige Warteereignisse in diesem Abschnitt haben keine Entsprechungen in den Open-Source-Versionen dieser Datenbank-Engines. Andere Warteereignisse haben dieselben Namen wie Ereignisse in Open-Source-Engines, verhalten sich jedoch anders. Beispielsweise funktioniert Amazon-Aurora-Speicher anders als Open-Source-Speicher, sodass speicherbezogene Warteereignisse auf unterschiedliche Ressourcenbedingungen hinweisen.

Themen

Grundlegende Konzepte für Aurora-MySQL-Optimierung

Bevor Sie Ihre Aurora-MySQL-Datenbank optimieren, stellen Sie sicher, dass Sie wissen, was Warteereignisse und Thread-Zustände sind und warum sie auftreten. Überprüfen Sie

auch die grundlegende Speicher- und Festplattenarchitektur von Aurora MySQL, wenn Sie die InnoDB-Speicher-Engine verwenden. Ein hilfreiches Architekturdiagramm finden Sie im MySQL-Referenzhandbuch.

Themen

- Aurora-MySQL-Warteereignisse
- Aurora-MySQL-Thread-Zustände
- Aurora-MySQL-Speicher
- Aurora-MySQL-Prozesse

Aurora-MySQL-Warteereignisse

Ein Warteereignis zeigt eine Ressource an, auf die eine Sitzung wartet. Das Warteereignis `io/socket/sql/client_connection` zeigt beispielsweise an, dass ein Thread gerade eine neue Verbindung verarbeitet. Zu den typischen Ressourcen, auf die eine Sitzung wartet, gehören die folgenden:

- Singlethread-Zugriff auf einen Puffer, beispielsweise wenn eine Sitzung versucht, einen Puffer zu ändern
- Eine Zeile, die derzeit von einer anderen Sitzung gesperrt ist
- Eine gelesene Datendatei
- Eine geschriebene Protokolldatei

Um beispielsweise eine Abfrage zu erfüllen, kann die Sitzung einen vollständigen Tabellenscan durchführen. Wenn sich die Daten noch nicht im Arbeitsspeicher befinden, wartet die Sitzung, bis die Datenträger-I/O abgeschlossen ist. Wenn die Puffer in den Speicher gelesen werden, muss die Sitzung möglicherweise warten, da andere Sitzungen auf dieselben Puffer zugreifen. Die Datenbank zeichnet die Wartezeiten unter Verwendung eines vordefinierten Warteereignisses auf. Diese Ereignisse sind in Kategorien eingeteilt.

Ein Wait-Ereignis allein zeigt kein Leistungsproblem an. Wenn sich beispielsweise die angeforderten Daten nicht im Speicher befinden, müssen die Daten von der Festplatte gelesen werden. Wenn eine Sitzung eine Zeile für eine Aktualisierung sperrt, wartet eine andere Sitzung darauf, dass die Zeile entsperrt wird, damit sie sie aktualisieren kann. Bei einem Commit muss gewartet werden, bis der Schreibvorgang in eine Protokolldatei abgeschlossen ist. Wartezeiten sind ein wesentlicher Bestandteil des normalen Funktionierens einer Datenbank.

Eine große Anzahl von Warteereignissen weist normalerweise auf ein Leistungsproblem hin. In solchen Fällen können Sie Warteereignisdaten verwenden, um zu bestimmen, wo die Sitzungen Zeit verbringen. Wenn beispielsweise ein Bericht, der normalerweise in Minuten ausgeführt wird, jetzt stundenlang ausgeführt wird, können Sie die Warteereignisse identifizieren, die am meisten zur Gesamtwartezeit beitragen. Wenn Sie die Ursachen für die häufigsten Warteereignisse ermitteln können, können Sie manchmal Änderungen vornehmen, die die Leistung verbessern. Wenn Ihre Sitzung beispielsweise auf eine Zeile wartet, die von einer anderen Sitzung gesperrt wurde, können Sie die Sperrsitzung beenden.

Aurora-MySQL-Thread-Zustände

Ein allgemeiner Thread-Zustand ist ein `State`-Wert, der der allgemeinen Abfrageverarbeitung zugeordnet ist. Der Thread-Zustand `sending data` gibt beispielsweise an, dass ein Thread Zeilen für eine Abfrage liest und filtert, um die richtige Ergebnismenge zu ermitteln.

Sie können Thread-Zustände verwenden, um Aurora MySQL auf ähnliche Weise zu optimieren, wie Sie Warteereignisse verwenden. Häufiges Vorkommen von `sending data` weist beispielsweise normalerweise darauf hin, dass eine Abfrage keinen Index verwendet. Weitere Informationen zu Thread-Zuständen finden Sie unter Allgemeine Thread-Zustände im MySQL-Referenzhandbuch.

Wenn Sie Performance Insights verwenden, gilt eine der folgenden Bedingungen:

- Performance Schema ist aktiviert – Aurora MySQL zeigt Warteereignisse anstelle des Thread-Zustands an.
- Performance-Schema ist nicht aktiviert – Aurora MySQL zeigt den Thread-Zustand an.

Es wird empfohlen, Performance Schema für die automatische Verwaltung zu konfigurieren. Das Leistungsschema bietet zusätzliche Einblicke und bessere Tools zur Untersuchung potenzieller Leistungsprobleme. Weitere Informationen finden Sie unter Aktivieren des Leistungsschemas für Performance Insights in Aurora MySQL.

Aurora-MySQL-Speicher

In Aurora MySQL sind die wichtigsten Speicherbereiche der Pufferpool und der Protokollpuffer.

Themen

- Puffer Pool

Puffer Pool

Der Pufferpool ist der gemeinsam genutzte Speicherbereich, in dem Aurora MySQL Tabellen- und Indexdaten zwischenspeichert. Abfragen können direkt aus dem Speicher auf häufig verwendete Daten zugreifen, ohne von der Festplatte zu lesen.

Der Pufferpool ist als verknüpfte Seitenliste strukturiert. Eine Seite kann mehrere Zeilen enthalten. Aurora MySQL verwendet einen LRU-Algorithmus (Least Latest Used), um Seiten aus dem Pool zu altern.

Weitere Informationen finden Sie unter Pufferpool im MySQL-Referenzhandbuch.

Aurora-MySQL-Prozesse

Aurora MySQL verwendet ein Prozessmodell, das sich stark von Aurora PostgreSQL unterscheidet.

Themen

- MySQL-Server (mysqld)
- Threads
- Thread-Pool

MySQL-Server (mysqld)

Der MySQL-Server ist ein einziger Betriebssystemprozess namens mysqld. Der MySQL-Server erzeugt keine zusätzlichen Prozesse. Daher verwendet eine Aurora-MySQL-Datenbank mysqld, um den größten Teil ihrer Arbeit zu erledigen.

Wenn der MySQL-Server startet, lauscht er auf Netzwerkverbindungen von MySQL-Clients. Wenn ein Client eine Verbindung zur Datenbank herstellt, öffnet mysqld einen Thread.

Threads

Verbindungsmanager-Threads verknüpfen jede Clientverbindung mit einem dedizierten Thread. Dieser Thread verwaltet die Authentifizierung, führt Anweisungen aus und gibt Ergebnisse an den Client zurück. Der Verbindungsmanager erstellt bei Bedarf neue Threads.

Der Thread-Cache ist die Menge der verfügbaren Threads. Wenn eine Verbindung endet, gibt MySQL den Thread an den Thread-Cache zurück, wenn der Cache nicht voll ist. Die `thread_cache_size`-Systemvariable bestimmt die Thread-Cache-Größe.

Thread-Pool

Der Thread-Pool besteht aus einer Reihe von Thread-Gruppen. Jede Gruppe verwaltet eine Reihe von Clientverbindungen. Wenn ein Client eine Verbindung mit der Datenbank herstellt, weist der Thread-Pool die Verbindungen Thread-Gruppen auf Round-Robin-Art zu. Der Thread-Pool trennt Verbindungen und Threads. Es gibt keine feste Beziehung zwischen Verbindungen und den Threads, die Anweisungen ausführen, die von diesen Verbindungen empfangen wurden.

Optimieren von Aurora MySQL mit Warteereignissen

Die folgende Tabelle fasst die Aurora-MySQL-Warteereignisse zusammen, die am häufigsten auf Leistungsprobleme hinweisen. Die folgenden Warteereignisse sind eine Teilmenge der Liste in Aurora-MySQL-Warteereignisse.

Warteereignis	Beschreibung
cpu	Dieses Ereignis tritt auf, wenn ein Thread in der CPU aktiv ist oder auf die CPU wartet.
io/aurora_redo_log_flush	Dieses Ereignis tritt ein, wenn eine Sitzung persistente Daten in den Aurora-Speicher schreibt.
io/aurora_respond_to_client	Das Ereignis tritt auf, wenn ein Thread darauf wartet, eine Ergebnismenge an einen Client zurückzugeben.
io/redo_log_flush	Dieses Ereignis tritt ein, wenn eine Sitzung persistente Daten in den Aurora-Speicher schreibt.
io/socket/sql/client_connection	Dieses Ereignis tritt auf, wenn ein Thread gerade eine neue Verbindung verarbeitet.
io/table/sql/handler	Dieses Ereignis tritt ein, wenn Arbeit an eine Speicher-Engine delegiert wurde.
synch/cond/innodb/row_lock_wait	Dieses Ereignis tritt auf, wenn eine Sitzung eine Zeile für eine Aktualisierung gesperrt hat

Warteereignis	Beschreibung
	und eine andere Sitzung versucht, dieselbe Zeile zu aktualisieren.
synch/cond/innodb/row_lock_wait_cond	Dieses Ereignis tritt auf, wenn eine Sitzung eine Zeile für eine Aktualisierung gesperrt hat und eine andere Sitzung versucht, dieselbe Zeile zu aktualisieren.
synch/cond/sql/MDL_context::COND_wait_status	Dieses Ereignis tritt ein, wenn Threads auf eine Tabellenmetadatensperre warten.
synch/mutex/innodb/aurora_lock_thread_slot_futex	Dieses Ereignis tritt auf, wenn eine Sitzung eine Zeile für eine Aktualisierung gesperrt hat und eine andere Sitzung versucht, dieselbe Zeile zu aktualisieren.
synch/mutex/innodb/buf_pool_mutex	Dieses Ereignis tritt ein, wenn ein Thread eine Sperre des InnoDB-Puffer-Pools für den Zugriff auf eine Seite im Speicher erworben hat.
synch/mutex/innodb/fil_system_mutex	Dieses Ereignis tritt auf, wenn eine Sitzung darauf wartet, auf den Tablespace-Speicherache zuzugreifen.
synch/mutex/innodb/trx_sys_mutex	Dieses Ereignis tritt auf, wenn eine hohe Datenbankaktivität mit einer großen Anzahl von Transaktionen besteht.
synch/sxlock/innodb/hash_table_locks	Dieses Ereignis tritt ein, wenn Seiten, die nicht im Pufferpool gefunden wurden, aus einer Datei gelesen werden müssen.

cpu

Das cpu-Warteereignis tritt auf, wenn ein Thread in der CPU aktiv ist oder auf die CPU wartet.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Versionen 2 und 3

Kontext

Für jede vCPU kann eine Verbindung an dieser CPU arbeiten. In einigen Situationen ist die Anzahl der aktiven Verbindungen, die zum Ausführen bereit sind, höher als die Anzahl der vCPUs. Dieses Ungleichgewicht führt dazu, dass Verbindungen auf CPU-Ressourcen warten. Wenn die Anzahl der aktiven Verbindungen konstant höher bleibt als die Anzahl der vCPUs, erfährt Ihre Instance CPU-Konflikte. Der Konflikt bewirkt, dass das `cpu`-Warteereignis auftritt.

> **Note**
>
> Die Performance-Insights-Metrik für CPU ist `DBLoadCPU`. Der Wert für `DBLoadCPU` kann vom Wert für die CloudWatch Metrik abweichen`CPUUtilization`. Die letztere Metrik wird aus der HyperVisor für eine Datenbank-Instance erfasst.

Performance-Insights-OS-Metriken liefern detaillierte Informationen zur CPU-Auslastung. Sie können beispielsweise die folgenden Metriken anzeigen:

- `os.cpuUtilization.nice.avg`
- `os.cpuUtilization.total.avg`
- `os.cpuUtilization.wait.avg`
- `os.cpuUtilization.idle.avg`

Performance Insights meldet die CPU-Auslastung durch die Datenbank-Engine als `os.cpuUtilization.nice.avg`.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die folgenden typischen Ursachen:

- Analytische Abfragen
- Hochgradig gleichzeitige Transaktionen
- Langlebige Transaktionen
- Ein plötzlicher Anstieg der Anzahl von Verbindungen, bekannt als Login-Sturm
- Eine Zunahme des Kontextwechsels

Aktionen

Wenn das `cpu`-Wait-Ereignis die Datenbankaktivität dominiert, weist dies nicht unbedingt auf ein Leistungsproblem hin. Reagieren Sie auf dieses Ereignis nur, wenn sich die Leistung verschlechtert.

Berücksichtigen Sie je nach Ursache des Anstiegs der CPU-Auslastung die folgenden Strategien:

- Erhöht die CPU-Kapazität des Hosts. Dieser Ansatz bietet normalerweise nur vorübergehende Erleichterung.
- Identifizieren Sie Top-Abfragen zur möglichen Optimierung.
- Leiten Sie ggf. einen schreibgeschützten Workload auf Reader-Knoten um.

Themen

Identifizieren Sie die Sitzungen oder Abfragen, die das Problem verursachen

Um die Sitzungen und Abfragen zu finden, suchen Sie in der Top-SQL-Tabelle in Performance Insights nach den SQL-Anweisungen mit der höchsten CPU-Auslastung. Weitere Informationen finden Sie unter Analyse der Metriken mit dem Performance Insights-Dashboard.

In der Regel verbrauchen ein oder zwei SQL-Anweisungen den Großteil der CPU-Zyklen. Konzentrieren Sie sich auf diese Anweisungen. Angenommen, Ihre DB-Instance verfügt über 2 vCPUs mit einer DB-Last von 3,1 durchschnittlichen aktiven Sitzungen (AAS), alle im CPU-Status. In diesem Fall ist Ihre Instance CPU-gebunden. Berücksichtigen Sie dabei die folgenden Strategien:

- Aktualisieren Sie auf eine größere Instance-Klasse mit mehr vCPUs.
- Stimmen Sie Ihre Abfragen auf eine geringere CPU-Last ein.

In diesem Beispiel haben die obersten SQL-Abfragen eine DB-Last von 1,5 AAS, alle im CPU-Status. Eine andere SQL-Anweisung hat eine Last von 0,1 im CPU-Status. Wenn Sie in diesem Beispiel die SQL-Anweisung mit der niedrigsten Last gestoppt haben, reduzieren Sie die Datenbanklast nicht wesentlich. Optimieren Sie jedoch die beiden Abfragen mit hoher Last, um doppelt so effizient zu sein, beseitigen Sie den CPU-Engpass. Wenn Sie die CPU-Last von 1,5 AAS um 50 Prozent reduzieren, verringert sich der AAS für jede Anweisung auf 0,75. Die gesamte für die CPU aufgewendete DB-Last beträgt jetzt 1,6 AAS. Dieser Wert liegt unter der maximalen vCPU-Linie von 2,0.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im Blogbeitrag Analysieren Sie Amazon Aurora MySQL Workloads mit Performance Insights. Siehe auch den AWS-Support-Artikel Wie kann ich eine hohe CPU-Auslastung auf meinen Amazon RDS for MySQL-Instances beheben und beheben?.

Analysieren und optimieren Sie die hohe CPU-Workload

Nachdem Sie die Abfrage oder Abfragen identifiziert haben, die die CPU-Auslastung erhöhen, können Sie sie entweder optimieren oder die Verbindung beenden. Das folgende Beispiel zeigt, wie Sie eine Verbindung beenden.

```
CALL mysql.rds_kill(processID);
```

Weitere Informationen finden Sie unter mysql.rds_kill.

Wenn Sie eine Sitzung beenden, löst die Aktion möglicherweise einen langen Rollback aus.

Befolgen Sie die Richtlinien für die Optimierung von Abfragen

Beachten Sie die folgenden Richtlinien, um Abfragen zu optimieren:

- Ausführen der `EXPLAIN`-Anweisung.

  Dieser Befehl zeigt die einzelnen Schritte an, die beim Ausführen einer Abfrage beteiligt sind. Weitere Informationen finden Sie unter Optimierung von Abfragen mit EXPLAIN in der MySQL-Dokumentation.
- Ausführen der `SHOW PROFILE`-Anweisung.

Verwenden Sie diese Anweisung, um Profildetails zu überprüfen, die die Ressourcennutzung für Anweisungen angeben können, die während der aktuellen Sitzung ausgeführt werden. Weitere Informationen finden Sie unter SHOW PROFILE-Anweisung in der MySQL-Dokumentation.

- Ausführen der `ANALYZE TABLE`-Anweisung.

  Verwenden Sie diese Anweisung, um die Indexstatistiken für die Tabellen zu aktualisieren, auf die die Abfrage mit hohem CPU-Verbrauch zugegriffen wird. Durch die Analyse der Anweisung können Sie dem Optimierer bei der Auswahl eines geeigneten Ausführungsplans helfen. Weitere Informationen finden Sie unter ANALYZE TABLE in der MySQL-Dokumentation.

Befolgen Sie die Richtlinien zur Verbesserung der CPU-Auslastung

Um die CPU-Auslastung in einer Datenbank-Instance zu verbessern, befolgen Sie die folgenden Richtlinien:

- Stellen Sie sicher, dass alle Abfragen die richtigen Indizes verwenden.
- Finden Sie heraus, ob Sie parallele Aurora-Abfragen verwenden können. Sie können diese Technik verwenden, um die CPU-Auslastung auf dem Hauptknoten zu reduzieren, indem Sie die Funktionsverarbeitung, die Zeilenfilterung und die Spaltenprojektion für die `WHERE`-Klausel herabstufen.
- Finden Sie heraus, ob die Anzahl der SQL-Ausführungen pro Sekunde die erwarteten Schwellenwerte erfüllt.
- Finden Sie heraus, ob Indexwartung oder neue Indexerstellung CPU-Zyklen in Anspruch nehmen, die von Ihrer Produktions-Workload benötigt werden Planen Sie Wartungsaktivitäten außerhalb der Spitzenzeiten.
- Finden Sie heraus, ob Sie die Partitionierung verwenden können, um den Abfragedatensatz zu reduzieren. Weitere Informationen finden Sie im Blogbeitrag So planen und optimieren Sie Amazon Aurora mit MySQL-Kompatibilität für konsolidierte Workloads.

Auf Verbindungsströme überprüfen

Ist die `DBLoadCPU`-Metrik nicht sehr hoch, aber die `CPUUtilization`-Metrik hoch, liegt die Ursache für die hohe CPU-Auslastung außerhalb der Datenbank-Engine. Ein klassisches Beispiel ist ein Verbindungssturm.

Prüfen Sie, ob die folgenden Bedingungen zutreffen:

- Sowohl die Performance-Insights-`CPUUtilization`Metrik als auch die Amazon CloudWatch-`DatabaseConnections`Metrik nehmen zu.
- Die Anzahl der Threads in der CPU ist größer als die Anzahl der vCPUs.

Wenn die vorhergehenden Bedingungen zutreffen, sollten Sie erwägen, die Anzahl der Datenbankverbindungen zu verringern. Sie können beispielsweise einen Verbindungspool wie RDS-Proxy verwenden. Informationen zu den bewährten Methoden für eine effektive Verbindungsverwaltung und -skalierung finden Sie im Whitepaper Handbuch von Amazon Aurora MySQL DBA für Verbindungsverwaltung.

io/aurora_redo_log_flush

Dieses `io/aurora_redo_log_flush`-Ereignis tritt ein, wenn eine Sitzung persistente Daten in den Amazon-Aurora-Speicher schreibt.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Version 2

Kontext

Das `io/aurora_redo_log_flush`-Ereignis ist für eine Schreiboperation mit Ein-/Ausgabe (I/O) in Aurora MySQL vorgesehen.

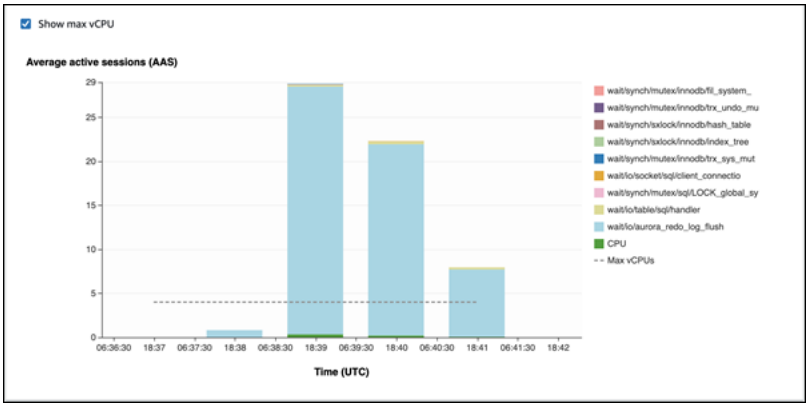
> **Note**
>
> In Aurora MySQL Version 3 heißt dieses Warteereignis io/redo_log_flush .

Wahrscheinliche Ursachen für erhöhte Wartezeiten

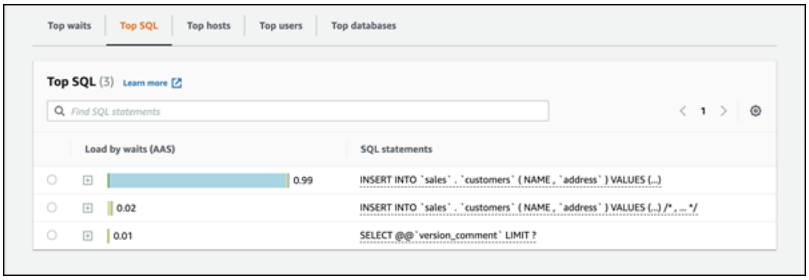
Aus Gründen der Datenpersistenz erfordern Commits ein dauerhaftes Schreiben in einen stabilen Speicher. Wenn die Datenbank zu viele Commits ausführt, gibt es ein Warteereignis für die I/O-Schreiboperation, das `io/aurora_redo_log_flush`-Warteereignis.

In den folgenden Beispielen werden 50.000 Datensätze mithilfe der db.r5.xlarge DB-Instance-Klasse in einen Aurora-MySQL-DB-Cluster eingefügt:

- Im ersten Beispiel fügt jede Sitzung zeilenweise 10.000 Datensätze ein. Wenn sich ein DML-Befehl (Data Manipulation Language) nicht innerhalb einer Transaktion befindet, verwendet Aurora MySQL standardmäßig implizite Commits. Autocommit ist aktiviert. Dies bedeutet, dass für jede Zeileneinfügung ein Commit vorhanden ist. Performance Insights zeigt, dass die Verbindungen die meiste Zeit damit verbringen, auf das `io/aurora_redo_log_flush`-Warteereignis zu warten.

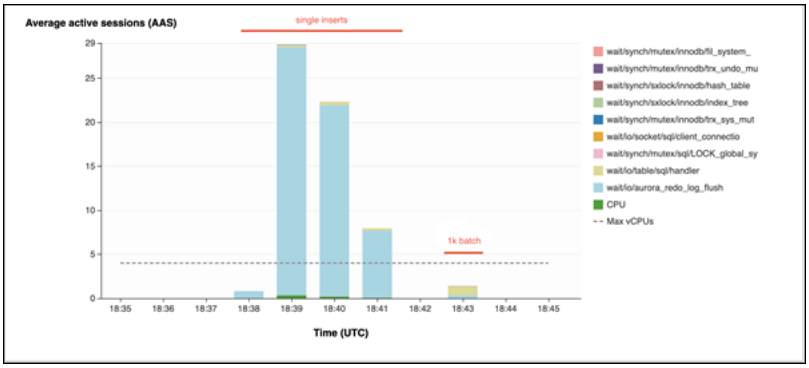
  

  Dies wird durch die verwendeten einfachen Einfügungsanweisungen verursacht.

  Die 50.000 Datensätze benötigen 3,5 Minuten, um eingefügt zu werden.

- Im zweiten Beispiel werden Einfügungen in 1.000 Batches vorgenommen, d.h. jede Verbindung führt 10 Commits statt 10.000 aus. Performance Insights zeigt, dass die Verbindungen nicht die meiste Zeit mit dem `io/aurora_redo_log_flush`-Warteereignis verbringen.



Die 50.000 Datensätze benötigen 4 Sekunden, um eingefügt zu werden.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Identifizieren Sie die problematischen Sitzungen und Abfragen

Wenn Ihre DB-Instance einen Engpass hat, besteht Ihre erste Aufgabe darin, die Sitzungen und Abfragen zu finden, die ihn verursachen. Einen nützlichen AWS-Datenbank-Blogbeitrag finden Sie unter Analysieren von Amazon-Aurora-MySQL-Workloads mit Performance Insights.

So identifizieren Sie Sitzungen und Abfragen, die einen Engpass verursachen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie Ihre DB-Instance aus.
4. Wählen Sie unter Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unten auf der Seite Top-SQL aus.

   Die Abfragen oben in der Liste verursachen die höchste Belastung der Datenbank.

Gruppieren Sie Ihre Schreiboperationen

Die folgenden Beispiele lösen das `io/aurora_redo_log_flush`-Warteereignis aus. (Autocommit ist aktiviert.)

```
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
```

```
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
....
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');

UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE id=xx;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE id=xx;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE id=xx;
....
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE id=xx;

DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
....
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
```

Um die Wartezeit auf das `io/aurora_redo_log_flush`-Wartezeitereignis zu verkürzen, gruppieren Sie Ihre Schreibvorgänge logisch in einem einzigen Commit, um persistente Speicheraufrufe zu reduzieren.

Deaktivieren Sie Autocommit

Deaktivieren Sie Autocommit, bevor Sie große Änderungen vornehmen, die nicht in einer Transaktion enthalten sind, wie im folgenden Beispiel gezeigt.

```
SET SESSION AUTOCOMMIT=OFF;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1=xx;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1=xx;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1=xx;
....
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1=xx;
-- Other DML statements here
COMMIT;

SET SESSION AUTOCOMMIT=ON;
```

Transaktionen verwenden

Sie können Transaktionen verwenden, wie im folgenden Beispiel gezeigt.

```
BEGIN
```

```
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
....
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');

DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
....
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;

-- Other DML statements here
END
```

Verwenden von Batches

Sie können Änderungen in Batches vornehmen, wie im folgenden Beispiel gezeigt. Die Verwendung zu großer Stapel kann jedoch zu Leistungsproblemen führen, insbesondere bei Lesereplikaten oder bei der point-in-time Wiederherstellung (PITR).

```
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES
('xxxx','xxxxx'),('xxxx','xxxxx'),...,('xxxx','xxxxx'),('xxxx','xxxxx');

UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1 BETWEEN xx AND
 xxx;

DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1<xx;
```

io/aurora_respond_to_client

Das `io/aurora_respond_to_client`-Ereignis tritt auf, wenn ein Thread darauf wartet, eine Ergebnismenge an einen Client zurückzugeben.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Version 2

In Versionen vor Version 2.07.7, 2.09.3 und 2.10.2 enthält dieses Warteereignis fälschlicherweise die Leerlaufzeit.

Kontext

Das Ereignis `io/aurora_respond_to_client` zeigt an, dass ein Thread darauf wartet, eine Ergebnismenge an einen Client zurückzugeben.

Die Abfrageverarbeitung ist abgeschlossen und die Ergebnisse werden an den Anwendungsclient zurückgegeben. Da jedoch nicht genügend Netzwerkbandbreite im DB-Cluster vorhanden ist, wartet ein Thread darauf, die Ergebnismenge zurückzugeben.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `io/aurora_respond_to_client`-Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die folgenden typischen Ursachen:

DB-Instance-Klasse reicht für die Workload nicht aus

Die vom DB-Cluster verwendete DB-Instance-Klasse verfügt nicht über die erforderliche Netzwerkbandbreite, um die Workload effizient zu verarbeiten.

Große Ergebnismengen

Es gab eine Zunahme der Größe der zurückgegebenen Ergebnismenge, da die Abfrage eine höhere Anzahl von Zeilen zurückgibt. Die größere Ergebnismenge verbraucht mehr Netzwerkbandbreite.

Erhöhte Belastung des Clients

Auf dem Client kann es zu CPU-, Speicher- oder Netzwerksättigung kommen. Eine Erhöhung der Belastung des Clients verzögert den Empfang von Daten aus dem Aurora-MySQL-DB-Cluster.

Erhöhte Netzwerklatenz

Es kann zu einer erhöhten Netzwerklatenz zwischen dem Aurora-MySQL-DB-Cluster und dem Client kommen. Eine höhere Netzwerklatenz erhöht die Zeit, die der Client benötigt, um die Daten zu empfangen.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Themen

- Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen
- Skalieren Sie die DB-Instance-Klasse
- Überprüfen Sie die Workload auf unerwartete Ergebnisse
- Verteilen Sie die Workload mit Leser-Instances
- Verwenden Sie den Modifikator SQL_BUFFER_RESULT

Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen

Sie können Performance Insights verwenden, um Abfragen anzuzeigen, die durch das `io/aurora_respond_to_client`-Warteereignis gesperrt wurden Normalerweise weisen Datenbanken mit mäßiger bis erheblicher Last Warteereignisse auf. Die Warteereignisse sind möglicherweise akzeptabel, wenn die Leistung optimal ist. Wenn die Leistung nicht optimal ist, untersuchen Sie, wo die Datenbank die meiste Zeit verbringt. Schauen Sie sich die Warteereignisse an, die zur höchsten Belastung beitragen und finden Sie heraus, ob Sie die Datenbank und die Anwendung optimieren können, um diese Ereignisse zu reduzieren.

So suchen Sie SQL-Abfragen, die für hohe Last verantwortlich sind

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus. Das Performance-Insights-Dashboard wird für diese DB-Instance angezeigt.
4. Wählen Sie im Diagramm zur Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unten auf der Seite Top-SQL aus.

   Das Diagramm listet die SQL-Abfragen auf, die für die Belastung verantwortlich sind. Diejenigen, die an der Spitze der Liste stehen, sind am meisten verantwortlich. Konzentrieren Sie sich auf diese Aussagen, um einen Engpass zu beheben.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im AWS-Database Blog-Beitrag Analysieren von Amazon-Aurora-MySQL-Workloads mit Performance Insights.

Skalieren Sie die DB-Instance-Klasse

Prüfen Sie, ob sich der Wert der Amazon-CloudWatch-Metriken in Bezug auf den Netzwerkdurchsatz erhöht, z. B. `NetworkReceiveThroughput` und `NetworkTransmitThroughput`. Wenn die Netzwerkbandbreite der DB-Instance-Klasse erreicht wird, können Sie die vom DB-Cluster verwendete DB-Instance-Klasse skalieren, indem Sie den DB-Cluster ändern. Eine DB-Instance-Klasse mit größerer Netzwerkbandbreite gibt Daten effizienter an Clients zurück.

Weitere Informationen zum Überwachen von Amazon-CloudWatch-Metriken finden Sie unter Anzeigen von Metriken in der Amazon-RDS-Konsole. Weitere Informationen zu DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen. Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Überprüfen Sie die Workload auf unerwartete Ergebnisse

Überprüfen Sie die Workload im DB-Cluster und stellen Sie sicher, dass keine unerwarteten Ergebnisse erzielt werden. Beispielsweise kann es Abfragen geben, die eine höhere Anzahl von Zeilen als erwartet zurückgeben. In diesem Fall können Sie Performance-Insights-Zählermetriken wie `Innodb_rows_read` verwenden. Weitere Informationen finden Sie unter Performance-Insights-Zählermetriken.

Verteilen Sie die Workload mit Leser-Instances

Sie können schreibgeschützte Workloads mit Aurora-Replikaten verteilen. Sie können horizontal skalieren, indem Sie weitere Aurora-Replikate hinzufügen. Dies kann zu einer Erhöhung der Drosselgrenzen für die Netzwerkbandbreite führen. Weitere Informationen finden Sie unter Amazon-Aurora-DB-Cluster.

Verwenden Sie den Modifikator SQL_BUFFER_RESULT

Sie können `SELECT`-Anweisungen den Modifikator `SQL_BUFFER_RESULT` hinzufügen, um das Ergebnis in eine temporäre Tabelle zu zwingen, bevor es an den Client zurückgegeben wird. Dieser Modifikator kann bei Leistungsproblemen helfen, wenn InnoDB-Sperren nicht freigegeben werden, weil sich Abfragen im Wartezustand `io/aurora_respond_to_client` befinden. Weitere Informationen finden Sie unter SELECT-Anweisung in der MySQL-Dokumentation.

io/redo_log_flush

Dieses `io/redo_log_flush`-Ereignis tritt ein, wenn eine Sitzung persistente Daten in den Amazon-Aurora-Speicher schreibt.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Version 3

Kontext

Das `io/redo_log_flush`-Ereignis ist für eine Schreiboperation mit Ein-/Ausgabe (I/O) in Aurora MySQL vorgesehen.

> **Note**
>
> In Aurora MySQL Version 2 heißt dieses Warteereignis io/aurora_redo_log_flush .

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Aus Gründen der Datenpersistenz erfordern Commits ein dauerhaftes Schreiben in einen stabilen Speicher. Wenn die Datenbank zu viele Commits ausführt, gibt es ein Warteereignis für die I/O-Schreiboperation, das `io/redo_log_flush`-Warteereignis.

Beispiele für das Verhalten dieses Warteereignisses finden Sie unter io/aurora_redo_log_flush.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Identifizieren Sie die problematischen Sitzungen und Abfragen

Wenn Ihre DB-Instance einen Engpass hat, besteht Ihre erste Aufgabe darin, die Sitzungen und Abfragen zu finden, die ihn verursachen. Einen nützlichen AWS-Datenbank-Blogbeitrag finden Sie unter Analysieren von Amazon-Aurora-MySQL-Workloads mit Performance Insights.

So identifizieren Sie Sitzungen und Abfragen, die einen Engpass verursachen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie Ihre DB-Instance aus.
4. Wählen Sie unter Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unten auf der Seite Top-SQL aus.

   Die Abfragen oben in der Liste verursachen die höchste Belastung der Datenbank.

Gruppieren Sie Ihre Schreiboperationen

Die folgenden Beispiele lösen das `io/redo_log_flush`-Warteereignis aus. (Autocommit ist aktiviert.)

```
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
....
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');

UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE id=xx;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE id=xx;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE id=xx;
....
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE id=xx;

DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
....
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
```

Um die Wartezeit auf das `io/redo_log_flush`-Wartezeitereignis zu verkürzen, gruppieren Sie Ihre Schreibvorgänge logisch in einem einzigen Commit, um persistente Speicheraufrufe zu reduzieren.

Deaktivieren Sie Autocommit

Deaktivieren Sie Autocommit, bevor Sie große Änderungen vornehmen, die nicht in einer Transaktion enthalten sind, wie im folgenden Beispiel gezeigt.

```
SET SESSION AUTOCOMMIT=OFF;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1=xx;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1=xx;
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1=xx;
....
UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1=xx;
-- Other DML statements here
COMMIT;

SET SESSION AUTOCOMMIT=ON;
```

Transaktionen verwenden

Sie können Transaktionen verwenden, wie im folgenden Beispiel gezeigt.

```
BEGIN
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');
....
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES ('xxxx','xxxxx');

DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;
....
DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1=xx;

-- Other DML statements here
END
```

Verwenden von Batches

Sie können Änderungen in Batches vornehmen, wie im folgenden Beispiel gezeigt. Die Verwendung zu großer Stapel kann jedoch zu Leistungsproblemen führen, insbesondere bei Lesereplikaten oder bei der point-in-time Wiederherstellung (PITR).

```
INSERT INTO `sampleDB`.`sampleTable` (sampleCol2, sampleCol3) VALUES
('xxxx','xxxxx'),('xxxx','xxxxx'),...,('xxxx','xxxxx'),('xxxx','xxxxx');

UPDATE `sampleDB`.`sampleTable` SET sampleCol3='xxxxx' WHERE sampleCol1 BETWEEN xx AND
 xxx;

DELETE FROM `sampleDB`.`sampleTable` WHERE sampleCol1<xx;
```

io/socket/sql/client_connection

Dieses `io/socket/sql/client_connection`-Ereignis tritt auf, wenn ein Thread gerade eine neue Verbindung verarbeitet.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Versionen 2 und 3

Kontext

Das `io/socket/sql/client_connection`-Ereignis zeigt an, dass mysqld damit beschäftigt ist, Threads zu erstellen, um eingehende neue Clientverbindungen zu verarbeiten. In diesem Szenario verlangsamt sich die Verarbeitung neuer Clientverbindungsanfragen, während Verbindungen warten, bis der Thread zugewiesen wird. Weitere Informationen finden Sie unter MySQL-Server (mysqld).

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die folgenden typischen Ursachen:

- Es gibt einen plötzlichen Anstieg neuer Benutzerverbindungen von der Anwendung zu Ihrer Amazon-RDS-Instance.
- Ihre DB-Instance kann keine neuen Verbindungen verarbeiten, da das Netzwerk, die CPU oder der Speicher gedrosselt werden.

Aktionen

Wenn `io/socket/sql/client_connection` die Datenbankaktivität dominiert, weist dies nicht unbedingt auf ein Leistungsproblem hin. In einer Datenbank, die nicht im Leerlauf ist, ist ein Warteereignis immer im Vordergrund. Handeln Sie nur, wenn die Leistung nachlässt. Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir unterschiedliche Maßnahmen.

Themen

- Identifizieren Sie die problematischen Sitzungen und Abfragen
- Befolgen Sie die bewährten Methoden für die Verbindungsverwaltung
- Vergrößern Sie Ihre Instance, wenn Ressourcen gedrosselt werden
- Prüfen Sie die Top-Hosts und Top-Benutzer
- Fragen Sie die performance_schema-Tabellen ab
- Prüfen Sie die Thread-Zustand Ihrer Abfragen
- Prüfen Sie Ihre Anfragen und Abfragen
- Kombinieren Sie Ihre Datenbankverbindungen

Identifizieren Sie die problematischen Sitzungen und Abfragen

Wenn Ihre DB-Instance einen Engpass hat, besteht Ihre erste Aufgabe darin, die Sitzungen und Abfragen zu finden, die ihn verursachen. Einen nützlichen Blogbeitrag finden Sie unter Analysieren von Amazon-Aurora-MySQL-Workloads mit Performance Insights.

So identifizieren Sie Sitzungen und Abfragen, die einen Engpass verursachen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie Ihre DB-Instance aus.
4. Wählen Sie unter Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unten auf der Seite Top-SQL aus.

   Die Abfragen oben in der Liste verursachen die höchste Belastung der Datenbank.

Befolgen Sie die bewährten Methoden für die Verbindungsverwaltung

Berücksichtigen Sie die folgenden Strategien, um Ihre Verbindungen zu verwalten:

- Verwenden Sie Verbindungspooling.

  Sie können die Anzahl der Verbindungen nach Bedarf schrittweise erhöhen. Weitere Informationen finden Sie im Whitepaper Amazon-Aurora-MySQL-Datenbankadministratorhandbuch.
- Verwenden Sie einen Reader-Knoten, um schreibgeschützten Datenverkehr umzuverteilen.

  Weitere Informationen finden Sie unter Aurora-Replikate und Amazon Aurora-Verbindungsverwaltung.

Vergrößern Sie Ihre Instance, wenn Ressourcen gedrosselt werden

Suchen Sie nach Beispielen für die Drosselung in den folgenden Ressourcen:

- CPU

  Überprüfen Sie Ihre Amazon- CloudWatch Metriken auf hohe CPU-Auslastung.
- Network (Netzwerk)

  Überprüfen Sie, ob der Wert der CloudWatch Metriken `network receive throughput` und steigt`network transmit throughput`. Wenn Ihre Instance das Netzwerkbandbreitenlimit für Ihre Instance-Klasse erreicht hat, sollten Sie Ihre RDS-Instance auf einen höheren Instance-Klassentyp skalieren. Weitere Informationen finden Sie unter Aurora DB-Instance-Klassen.
- Freisetzbarer Speicher

  Überprüfen Sie, ob die CloudWatch Metrik gelöscht wurde`FreeableMemory`. Ziehen Sie auch in Erwägung, die erweiterte Überwachung zu aktivieren. Weitere Informationen

finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).

Prüfen Sie die Top-Hosts und Top-Benutzer

Verwenden Sie Performance Insights, um die Top-Hosts und Top-Benutzer zu überprüfen. Weitere Informationen finden Sie unter Analyse der Metriken mit dem Performance Insights-Dashboard.

Fragen Sie die performance_schema-Tabellen ab

Um eine genaue Anzahl der aktuellen und gesamten Verbindungen zu erhalten, fragen Sie die `performance_schema`-Tabellen ab. Mit dieser Technik identifizieren Sie den Quellbenutzer oder Host, der für das Erstellen einer hohen Anzahl von Verbindungen verantwortlich ist. Fragen Sie die `performance_schema`-Tabellen beispielsweise wie folgt ab.

```
SELECT * FROM performance_schema.accounts;
SELECT * FROM performance_schema.users;
SELECT * FROM performance_schema.hosts;
```

Prüfen Sie die Thread-Zustand Ihrer Abfragen

Wenn Ihr Leistungsproblem andauert, überprüfen Sie die Thread-Zustand Ihrer Abfragen. Geben Sie im `mysql`-Client den folgenden Befehl aus.

```
show processlist;
```

Prüfen Sie Ihre Anfragen und Abfragen

Verwenden Sie AuroraAurora MySQL Advanced Auditing, um die Art der Anforderungen und Abfragen von Benutzerkonten zu überprüfen. Weitere Informationen zum Aktivieren der Prüfung finden Sie unter Verwenden von Advanced Auditing in einem Amazon Aurora MySQL DB-Cluster.

Kombinieren Sie Ihre Datenbankverbindungen

Erwägen Sie, Amazon RDS Proxy für die Verbindungsverwaltung zu verwenden. Durch die Verwendung von RDS Proxy können Sie Ihren Anwendungen erlauben, Datenbankverbindungen zu bündeln und gemeinsam zu nutzen, um ihre Skalierbarkeit zu verbessern. RDS Proxy macht Anwendungen widerstandsfähiger gegenüber Datenbankfehlern, indem er automatisch eine

Verbindung zu einer Standby-DB-Instance herstellt, während Anwendungsverbindungen erhalten bleiben. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

io/table/sql/handler

Dieses `io/table/sql/handler`-Ereignis tritt ein, wenn Arbeit an eine Speicher-Engine delegiert wurde.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora MySQL Version 3: 3.01.0 und 3.01.1
- Aurora-MySQL-Version 2

Kontext

Das `io/table`-Ereignis zeigt ein Warten auf den Zugriff auf eine Tabelle an. Dieses Ereignis tritt unabhängig davon auf, ob die Daten im Pufferpool zwischengespeichert werden oder über die Festplatte darauf zugegriffen wird. Das `io/table/sql/handler`-Ereignis weist auf eine Zunahme der Workload-Aktivität hin.

Ein Handler ist eine Routine, die auf eine bestimmte Art von Daten spezialisiert ist oder sich auf bestimmte spezielle Aufgaben konzentriert. Beispielsweise empfängt und verdaut ein Ereignis-Handler Ereignisse und Signale vom Betriebssystem oder von einer Benutzeroberfläche. Ein Speicherhandler führt Aufgaben im Zusammenhang mit dem Speicher aus. Ein Dateieingabe-Handler ist eine Funktion, die Dateieingaben empfängt und je nach Kontext spezielle Aufgaben für die Daten ausführt.

Ansichten wie `performance_schema.events_waits_current` zeigen oft `io/table/sql/handler` an, wenn das eigentliche Warten ein verschachteltes Warteereignis wie eine Sperre ist. Wenn das tatsächliche Warten nicht `io/table/sql/handler` ist, meldet Performance

Insights das verschachtelte Warteereignis. Wenn Performance Insights meldet`io/table/sql/handler`, stellt es die InnoDB-Verarbeitung der E/A-Anforderung dar und kein verstecktes verschachteltes Warteereignis. Weitere Informationen finden Sie unter Leistungsschema-Atom- und Molekülereignisse im MySQL-Referenzhandbuch.

> **Note**
>
> In den Aurora-MySQL-Versionen 3.01.0 und 3.01.1 wird synch/mutex/innodb/aurora_lock_thread_slot_futex jedoch als `io/table/sql/handler` gemeldet.

Das `io/table/sql/handler`-Ereignis erscheint oft in Top-Warteereignissen mit I/O-Wartezeiten wie `io/aurora_redo_log_flush` und `io/file/innodb/innodb_data_file`.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

In Performance Insights weisen plötzliche Spitzen im `io/table/sql/handler`-Ereignis auf eine Zunahme der Workload-Aktivität hin. Erhöhte Aktivität bedeutet eine erhöhte I/O.

Performance Insights filtert die Verschachtelungsereignis-IDs und meldet keine `io/table/sql/handler`-Wartezeit, wenn das zugrunde liegende verschachtelte Ereignis eine Sperrwartezeit ist. Wenn beispielsweise das Grundursachenereignis synch/mutex/innodb/aurora_lock_thread_slot_futex ist, zeigt Performance Insights diese Wartezeit in den Top-Warteereignissen an und nicht `io/table/sql/handler`.

In Ansichten wie `performance_schema.events_waits_current` werden Wartezeiten für `io/table/sql/handler` oft angezeigt, wenn das eigentliche Warten ein verschachteltes Warteereignis wie eine Sperre ist. Wenn die tatsächliche Wartezeit von `io/table/sql/handler` abweicht, schlägt Performance Insights die verschachtelte Wartezeit nach und meldet die tatsächliche Wartezeit anstelle von `io/table/sql/handler`. Wenn Performance Insights `io/table/sql/handler` meldet, ist die tatsächliche Wartezeit `io/table/sql/handler` und kein verstecktes verschachteltes Warteereignis. Weitere Informationen finden Sie unter Leistungsschema-Atom- und Molekülereignisse im MySQL-Referenzhandbuch 5.7.

> **Note**
>
> In den Aurora-MySQL-Versionen 3.01.0 und 3.01.1 wird synch/mutex/innodb/aurora_lock_thread_slot_futex jedoch als `io/table/sql/handler` gemeldet.

Aktionen

Wenn das Warteereignis die Datenbankaktivität dominiert, weist dies nicht unbedingt auf ein Leistungsproblem hin. Ein Warteereignis ist immer im Vordergrund, wenn die Datenbank aktiv ist. Sie müssen nur handeln, wenn sich die Leistung verschlechtert.

Abhängig von den anderen angezeigten Warteereignissen empfehlen wir unterschiedliche Aktionen.

Themen

- Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen
- Überprüfen Sie, ob eine Korrelation mit den Performance-Insights-Zählermetriken vorliegt
- Nach anderen korrelierten Warteereignissen suchen

Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen

Normalerweise weisen Datenbanken mit mäßiger bis erheblicher Last Warteereignisse auf. Die Warteereignisse sind möglicherweise akzeptabel, wenn die Leistung optimal ist. Wenn die Leistung nicht optimal ist, untersuchen Sie, wo die Datenbank die meiste Zeit verbringt. Schauen Sie sich die Warteereignisse an, die zur höchsten Belastung beitragen und finden Sie heraus, ob Sie die Datenbank und die Anwendung optimieren können, um diese Ereignisse zu reduzieren.

So suchen Sie SQL-Abfragen, die für hohe Last verantwortlich sind

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus. Das Performance-Insights-Dashboard wird für diese DB-Instance angezeigt.
4. Wählen Sie im Diagramm zur Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unten auf der Seite Top-SQL aus.

   Das Diagramm listet die SQL-Abfragen auf, die für die Belastung verantwortlich sind. Diejenigen, die an der Spitze der Liste stehen, sind am meisten verantwortlich. Konzentrieren Sie sich auf diese Aussagen, um einen Engpass zu beheben.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im Blogbeitrag Analysieren Sie Amazon Aurora MySQL Workloads mit Performance Insights.

Überprüfen Sie, ob eine Korrelation mit den Performance-Insights-Zählermetriken vorliegt

Suchen Sie nach Performance-Insights-Zählermetriken wie `Innodb_rows_changed`. Wenn Zählermetriken mit `io/table/sql/handler` korreliert sind, gehen Sie folgendermaßen vor:

1. Suchen Sie in Performance Insights nach den SQL-Anweisungen, die das `io/table/sql/handler`-Top-Warteereignis berücksichtigen. Optimieren Sie diese Anweisung, wenn möglich, damit sie weniger Zeilen zurückgibt.
2. Rufen Sie die obersten Tabellen aus den `schema_table_statistics`- und x `$schema_table_statistics`-Ansichten ab. Diese Ansichten zeigen den Zeitaufwand pro Tabelle an. Weitere Informationen finden Sie unter Die Ansichten schema_table_statistics und x $schema_table_statistics im MySQL-Referenzhandbuch.

   Standardmäßig werden Zeilen nach absteigender Gesamtwartezeit sortiert. Tabellen mit dem größten Streit erscheinen zuerst. Die Ausgabe gibt an, ob Zeit für Lese-, Schreibvorgänge, Abrufe, Einfügungen, Aktualisierungen oder Löschungen aufgewendet wird. Das folgende Beispiel wurde auf einer Instance von Aurora MySQL 2.09.1 ausgeführt.

```
mysql> select * from sys.schema_table_statistics limit 1\G

*************************** 1. row ***************************
     table_schema: read_only_db
       table_name: sbtest41
    total_latency: 54.11 m
     rows_fetched: 6001557
    fetch_latency: 39.14 m
    rows_inserted: 14833
   insert_latency: 5.78 m
     rows_updated: 30470
   update_latency: 5.39 m
     rows_deleted: 14833
   delete_latency: 3.81 m
 io_read_requests: NULL
          io_read: NULL
  io_read_latency: NULL
io_write_requests: NULL
         io_write: NULL
 io_write_latency: NULL
 io_misc_requests: NULL
  io_misc_latency: NULL
1 row in set (0.11 sec)
```

Nach anderen korrelierten Warteereignissen suchen

Wenn `synch/sxlock/innodb/btr_search_latch` und `io/table/sql/handler` zusammen am meisten zur DB-Ladeanomalie beitragen, prüfen Sie, ob die Variable `innodb_adaptive_hash_index` aktiviert ist. Wenn dies der Fall ist, sollten Sie den `innodb_adaptive_hash_index_parts`-Parameterwert erhöhen.

Wenn der Adaptive-Hash-Index ausgeschaltet, erwägen Sie, ihn einzuschalten. Weitere Informationen zum MySQL-Adaptive-Hash-Index finden Sie in den folgenden Ressourcen:

- Der Artikel Ist der Adaptive-Hash-Index in InnoDB für meinen Workload geeignet? auf der Percona-Website
- Adaptive-Hash-Index im MySQL-Referenzhandbuch
- Der Artikel Verbindung in MySQL InnoDB: Nützliche Informationen aus der Semaphores-Sektion auf der Percona-Website

> **Note**
>
> Der Adaptive-Hash-Index wird auf Aurora-Reader-DB-Instances nicht unterstützt. In einigen Fällen kann die Leistung auf einer Reader-Instance schwach sein, wenn `synch/sxlock/innodb/btr_search_latch` und `io/table/sql/handler` dominant sind. Wenn ja, erwägen Sie, die Workload vorübergehend auf die Writer-DB-Instance umzuleiten und den Adaptive-Hash-Index zu aktivieren.

synch/cond/innodb/row_lock_wait

Das `synch/cond/innodb/row_lock_wait`-Ereignis tritt auf, wenn eine Sitzung eine Zeile für ein Update gesperrt hat und eine andere Sitzung versucht, dieselbe Zeile zu aktualisieren. Weitere Informationen finden Sie unter InnoDB-Sperren in der MySQL-Referenz.

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora MySQL Version 3: 3.02.0, 3.02.1, 3.02.2

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Mehrere DML-Anweisungen (Data Manipulation Language) greifen gleichzeitig auf dieselbe Zeile oder dieselben Zeilen zu.

Aktionen

Abhängig von den anderen angezeigten Warteereignissen empfehlen wir unterschiedliche Aktionen.

Themen

- Finden und antworten Sie auf die SQL-Anweisungen, die für dieses Warteereignis verantwortlich sind
- Suchen und antworten Sie auf die Blockiersitzung

Finden und antworten Sie auf die SQL-Anweisungen, die für dieses Warteereignis verantwortlich sind

Verwenden Sie Performance Insights, um die SQL-Anweisungen zu identifizieren, die für dieses Warteereignis verantwortlich sind. Berücksichtigen Sie dabei die folgenden Strategien:

- Wenn Zeilensperren ein dauerhaftes Problem darstellen, erwägen Sie, die Anwendung neu zu schreiben, um eine optimistische Sperre zu verwenden.
- Verwenden Sie mehrzeilige Anweisungen.
- Verteilen Sie die Workload auf verschiedene Datenbankobjekte. Sie können dazu die Partitionierung verwenden.
- Prüfen Sie den Wert des `innodb_lock_wait_timeout`-Parameters. Es steuert, wie lange Transaktionen warten, bevor ein Timeout-Fehler generiert wird.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im Blogbeitrag Analysieren Sie Amazon Aurora MySQL Workloads mit Performance Insights.

Suchen und antworten Sie auf die Blockiersitzung

Stellen Sie fest, ob die Blockiersitzung im Leerlauf oder aktiv ist. Finden Sie außerdem heraus, ob die Sitzung von einer Anwendung oder einem aktiven Benutzer stammt.

Um die Sitzung zu identifizieren, die die Sperre hält, können Sie `SHOW ENGINE INNODB STATUS` ausführen. Das folgende Beispiel zeigt eine Beispielausgabe.

```
mysql> SHOW ENGINE INNODB STATUS;

---TRANSACTION 1688153, ACTIVE 82 sec starting index read
mysql tables in use 1, locked 1
LOCK WAIT 2 lock struct(s), heap size 1136, 2 row lock(s)
MySQL thread id 4244, OS thread handle 70369524330224, query id 4020834 172.31.14.179
 reinvent executing
select id1 from test.t1 where id1=1 for update
------- TRX HAS BEEN WAITING 24 SEC FOR THIS LOCK TO BE GRANTED:
RECORD LOCKS space id 11 page no 4 n bits 72 index GEN_CLUST_INDEX of table test.t1 trx
 id 1688153 lock_mode X waiting
Record lock, heap no 2 PHYSICAL RECORD: n_fields 5; compact format; info bits 0
```

Oder Sie können die folgende Abfrage verwenden, um Details zu aktuellen Sperren zu extrahieren.

```
mysql> SELECT p1.id waiting_thread,
    p1.user waiting_user,
    p1.host waiting_host,
    it1.trx_query waiting_query,
    ilw.requesting_engine_transaction_id waiting_transaction,
    ilw.blocking_engine_lock_id blocking_lock,
    il.lock_mode blocking_mode,
    il.lock_type blocking_type,
    ilw.blocking_engine_transaction_id blocking_transaction,
    CASE it.trx_state
        WHEN 'LOCK WAIT'
        THEN it.trx_state
        ELSE p.state end blocker_state,
    concat(il.object_schema,'.', il.object_name) as locked_table,
    it.trx_mysql_thread_id blocker_thread,
    p.user blocker_user,
    p.host blocker_host
FROM performance_schema.data_lock_waits ilw
JOIN performance_schema.data_locks il
ON ilw.blocking_engine_lock_id = il.engine_lock_id
AND ilw.blocking_engine_transaction_id = il.engine_transaction_id
JOIN information_schema.innodb_trx it
ON ilw.blocking_engine_transaction_id = it.trx_id join information_schema.processlist p
ON it.trx_mysql_thread_id = p.id join information_schema.innodb_trx it1
ON ilw.requesting_engine_transaction_id = it1.trx_id join
 information_schema.processlist p1
ON it1.trx_mysql_thread_id = p1.id\G
```

```
*************************** 1. row ***************************
waiting_thread: 4244
waiting_user: reinvent
waiting_host: 123.456.789.012:18158
waiting_query: select id1 from test.t1 where id1=1 for update
waiting_transaction: 1688153
blocking_lock: 70369562074216:11:4:2:70369549808672
blocking_mode: X
blocking_type: RECORD
blocking_transaction: 1688142
blocker_state: User sleep
locked_table: test.t1
blocker_thread: 4243
blocker_user: reinvent
blocker_host: 123.456.789.012:18156
1 row in set (0.00 sec)
```

Wenn Sie die Sitzung identifizieren, umfassen Ihre Optionen die Folgenden:

- Wenden Sie sich an den Besitzer der Anwendung oder den Benutzer.
- Wenn die Sperrsitzung im Leerlauf ist, erwägen Sie, die Sperrsitzung zu beenden. Diese Aktion könnte einen langen Rollback auslösen. Informationen zum Beenden einer Sitzung finden Sie unter Beenden einer Sitzung oder Abfrage.

Weitere Informationen zum Identifizieren blockierender Transaktionen finden Sie unter Verwenden von InnoDB-Transaktions- und Sperrinformationen im MySQL-Referenzhandbuch.

synch/cond/innodb/row_lock_wait_cond

Das `synch/cond/innodb/row_lock_wait_cond`-Ereignis tritt auf, wenn eine Sitzung eine Zeile für ein Update gesperrt hat und eine andere Sitzung versucht, dieselbe Zeile zu aktualisieren. Weitere Informationen finden Sie unter InnoDB-Sperren in der MySQL-Referenz.

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Version 2

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Mehrere DML-Anweisungen (Data Manipulation Language) greifen gleichzeitig auf dieselbe Zeile oder dieselben Zeilen zu.

Aktionen

Abhängig von den anderen angezeigten Warteereignissen empfehlen wir unterschiedliche Aktionen.

Themen

- Finden und antworten Sie auf die SQL-Anweisungen, die für dieses Warteereignis verantwortlich sind
- Suchen und antworten Sie auf die Blockiersitzung

Finden und antworten Sie auf die SQL-Anweisungen, die für dieses Warteereignis verantwortlich sind

Verwenden Sie Performance Insights, um die SQL-Anweisungen zu identifizieren, die für dieses Warteereignis verantwortlich sind. Berücksichtigen Sie dabei die folgenden Strategien:

- Wenn Zeilensperren ein dauerhaftes Problem darstellen, erwägen Sie, die Anwendung neu zu schreiben, um eine optimistische Sperre zu verwenden.
- Verwenden Sie mehrzeilige Anweisungen.
- Verteilen Sie die Workload auf verschiedene Datenbankobjekte. Sie können dazu die Partitionierung verwenden.
- Prüfen Sie den Wert des `innodb_lock_wait_timeout`-Parameters. Es steuert, wie lange Transaktionen warten, bevor ein Timeout-Fehler generiert wird.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im Blogbeitrag Analysieren Sie Amazon Aurora MySQL Workloads mit Performance Insights.

Suchen und antworten Sie auf die Blockiersitzung

Stellen Sie fest, ob die Blockiersitzung im Leerlauf oder aktiv ist. Finden Sie außerdem heraus, ob die Sitzung von einer Anwendung oder einem aktiven Benutzer stammt.

Um die Sitzung zu identifizieren, die die Sperre hält, können Sie `SHOW ENGINE INNODB STATUS` ausführen. Das folgende Beispiel zeigt eine Beispielausgabe.

```
mysql> SHOW ENGINE INNODB STATUS;

---TRANSACTION 2771110, ACTIVE 112 sec starting index read
mysql tables in use 1, locked 1
LOCK WAIT 2 lock struct(s), heap size 1136, 1 row lock(s)
MySQL thread id 24, OS thread handle 70369573642160, query id 13271336 172.31.14.179
 reinvent Sending data
select id1 from test.t1 where id1=1 for update
------- TRX HAS BEEN WAITING 43 SEC FOR THIS LOCK TO BE GRANTED:
RECORD LOCKS space id 11 page no 3 n bits 0 index GEN_CLUST_INDEX of table test.t1 trx
 id 2771110 lock_mode X waiting
Record lock, heap no 2 PHYSICAL RECORD: n_fields 5; compact format; info bits 0
```

Oder Sie können die folgende Abfrage verwenden, um Details zu aktuellen Sperren zu extrahieren.

```
mysql> SELECT p1.id waiting_thread,
              p1.user waiting_user,
              p1.host waiting_host,
              it1.trx_query waiting_query,
              ilw.requesting_trx_id waiting_transaction,
              ilw.blocking_lock_id blocking_lock,
              il.lock_mode blocking_mode,
              il.lock_type blocking_type,
              ilw.blocking_trx_id blocking_transaction,
              CASE it.trx_state
                WHEN 'LOCK WAIT'
                THEN it.trx_state
                ELSE p.state
              END blocker_state,
              il.lock_table locked_table,
              it.trx_mysql_thread_id blocker_thread,
              p.user blocker_user,
              p.host blocker_host
       FROM information_schema.innodb_lock_waits ilw
       JOIN information_schema.innodb_locks il
         ON ilw.blocking_lock_id = il.lock_id
        AND ilw.blocking_trx_id = il.lock_trx_id
       JOIN information_schema.innodb_trx it
         ON ilw.blocking_trx_id = it.trx_id
       JOIN information_schema.processlist p
         ON it.trx_mysql_thread_id = p.id
       JOIN information_schema.innodb_trx it1
         ON ilw.requesting_trx_id = it1.trx_id
```

```
       JOIN information_schema.processlist p1
         ON it1.trx_mysql_thread_id = p1.id\G

*************************** 1. row ***************************
      waiting_thread: 3561959471
        waiting_user: reinvent
        waiting_host: 123.456.789.012:20485
       waiting_query: select id1 from test.t1 where id1=1 for update
 waiting_transaction: 312337314
       blocking_lock: 312337287:261:3:2
       blocking_mode: X
       blocking_type: RECORD
blocking_transaction: 312337287
       blocker_state: User sleep
        locked_table: `test`.`t1`
      blocker_thread: 3561223876
        blocker_user: reinvent
        blocker_host: 123.456.789.012:17746
1 row in set (0.04 sec)
```

Wenn Sie die Sitzung identifizieren, umfassen Ihre Optionen die Folgenden:

- Wenden Sie sich an den Besitzer der Anwendung oder den Benutzer.
- Wenn die Sperrsitzung im Leerlauf ist, erwägen Sie, die Sperrsitzung zu beenden. Diese Aktion könnte einen langen Rollback auslösen. Informationen zum Beenden einer Sitzung finden Sie unter Beenden einer Sitzung oder Abfrage.

Weitere Informationen zum Identifizieren blockierender Transaktionen finden Sie unter Verwenden von InnoDB-Transaktions- und Sperrinformationen im MySQL-Referenzhandbuch.

synch/cond/sql/MDL_context::COND_wait_status

Dieses `synch/cond/sql/MDL_context::COND_wait_status`-Ereignis tritt ein, wenn Threads auf eine Tabellenmetadatensperre warten.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Versionen 2 und 3

Kontext

Das `synch/cond/sql/MDL_context::COND_wait_status`-Ereignis zeigt an, dass Threads auf eine Tabellenmetadatensperre warten. In einigen Fällen hält eine Sitzung eine Metadatensperre für eine Tabelle und eine andere Sitzung versucht, dieselbe Sperre für dieselbe Tabelle zu erhalten. In einem solchen Fall wartet die zweite Sitzung auf das `synch/cond/sql/MDL_context::COND_wait_status`-Warteereignis.

MySQL verwendet die Sperre von Metadaten, um den gleichzeitigen Zugriff auf Datenbankobjekte zu verwalten und die Datenkonsistenz sicherzustellen. Das Sperren von Metadaten gilt für Tabellen, Schemata, geplante Ereignisse, Tablespaces und Benutzersperren, die mit der `get_lock`-Funktion erworben wurden, und gespeicherte Programme. Gespeicherte Programme umfassen Prozeduren, Funktionen und Auslöser. Weitere Informationen finden Sie unter Metadata Locking in der MySQL-Dokumentation.

Die MySQL-Prozessliste zeigt diese Sitzung im Zustand `waiting for metadata lock`. Wenn in Performance Insights `Performance_schema` aktiviert ist, wird das Ereignis `synch/cond/sql/MDL_context::COND_wait_status` angezeigt.

Das Standardtimeout für eine Abfrage, die auf eine Metadatensperre wartet, basiert auf dem Wert des `lock_wait_timeout`-Parameters, der standardmäßig 31.536.000 Sekunden (365 Tage) beträgt.

Weitere Informationen zu verschiedenen InnoDB-Sperren und den Arten von Sperren, die Konflikte verursachen können, finden Sie unter InnoDB-Sperren in der MySQL-Dokumentation.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `synch/cond/sql/MDL_context::COND_wait_status`-Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die folgenden typischen Ursachen:

Langlebige Transaktionen

Eine oder mehrere Transaktionen ändern eine große Datenmenge und halten Tabellen für eine sehr lange Zeit gesperrt.

Leerlauf-Transaktionen

Eine oder mehrere Transaktionen bleiben lange offen, ohne festgeschrieben oder rückgängig gemacht zu werden.

DDL-Anweisungen zu großen Tabellen

Für sehr große Tabellen wurden eine oder mehrere DDL-Anweisungen (Data Definition Statements) ausgeführt, z. B. `ALTER TABLE`-Befehle.

Explizite Tabellensperren

Es gibt explizite Sperren für Tabellen, die nicht zeitnah freigegeben werden. Beispielsweise kann eine Anwendung `LOCK TABLE`-Anweisungen nicht ordnungsgemäß ausführen.

Aktionen

Wir empfehlen verschiedene Aktionen, abhängig von den Ursachen Ihres Warteereignisses und von der Version des Aurora-MySQL-DB-Clusters.

Themen

- Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen
- Nach vergangenen Ereignissen suchen
- Führen Sie Anfragen für Aurora MySQL Version 2 aus
- Antworten Sie auf die Blockiersitzung

Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen

Sie können Performance Insights verwenden, um Abfragen anzuzeigen, die durch das `synch/cond/sql/MDL_context::COND_wait_status`-Warteereignis gesperrt wurden Um jedoch die blockierende Sitzung zu identifizieren, fragen Sie Metadatentabellen von `performance_schema` und `information_schema` im DB-Cluster ab.

Normalerweise weisen Datenbanken mit mäßiger bis erheblicher Last Warteereignisse auf. Die Warteereignisse sind möglicherweise akzeptabel, wenn die Leistung optimal ist. Wenn die Leistung

nicht optimal ist, untersuchen Sie, wo die Datenbank die meiste Zeit verbringt. Schauen Sie sich die Warteereignisse an, die zur höchsten Belastung beitragen und finden Sie heraus, ob Sie die Datenbank und die Anwendung optimieren können, um diese Ereignisse zu reduzieren.

So suchen Sie SQL-Abfragen, die für hohe Last verantwortlich sind

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus. Das Performance-Insights-Dashboard wird für diese DB-Instance angezeigt.
4. Wählen Sie im Diagramm zur Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unten auf der Seite Top-SQL aus.

   Das Diagramm listet die SQL-Abfragen auf, die für die Belastung verantwortlich sind. Diejenigen, die an der Spitze der Liste stehen, sind am meisten verantwortlich. Konzentrieren Sie sich auf diese Aussagen, um einen Engpass zu beheben.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im AWS-Database Blog-Beitrag Analysieren von Amazon-Aurora-MySQL-Workloads mit Performance Insights.

Nach vergangenen Ereignissen suchen

Sie können einen Einblick in dieses Warteereignis erhalten, um nach früheren Vorkommen zu suchen. Führen Sie dazu die folgenden Aktionen aus:

- Überprüfen Sie die Datenmanipulationssprache (DML) und den DDL-Durchsatz und die Latenz, um festzustellen, ob sich die Workload geändert hat.

  Sie können Performance Insights verwenden, um Abfragen zu finden, die zum Zeitpunkt des Problems auf dieses Ereignis warten. Sie können auch den Digest der Abfragen anzeigen, die nahe dem Zeitpunkt des Problems ausgeführt werden.
- Wenn Überwachungsprotokolle oder allgemeine Protokolle für den DB-Cluster aktiviert sind, können Sie nach allen Abfragen suchen, die für die Objekte (schema.table) ausgeführt werden, die an der Wartetransaktion beteiligt sind. Sie können auch nach den Abfragen suchen, die vor der Transaktion ausgeführt wurden.

Die Informationen, die zur Fehlerbehebung vergangener Ereignisse zur Verfügung stehen, sind begrenzt. Durch das Ausführen dieser Prüfungen wird nicht angezeigt, welches Objekt auf Informationen wartet. Sie können jedoch Tabellen mit hoher Last zum Zeitpunkt des Ereignisses und die Menge häufig operierter Zeilen identifizieren, die zum Zeitpunkt des Problems Konflikte verursachen. Sie können diese Informationen dann verwenden, um das Problem in einer Testumgebung zu reproduzieren und Einblicke in seine Ursache zu geben.

Führen Sie Anfragen für Aurora MySQL Version 2 aus

In Aurora MySQL Version 2 können Sie die blockierte Sitzung direkt identifizieren, indem Sie `performance_schema`-Tabellen oder `sys`-Schemaansichten abfragen. Ein Beispiel kann veranschaulichen, wie Tabellen abfragen, um blockierende Abfragen und Sitzungen zu identifizieren.

In der folgenden Prozesslistenausgabe wartet die Verbindungs-ID 89 auf eine Metadatensperre und führt einen `TRUNCATE TABLE`-Befehl aus. In einer Abfrage der `performance_schema`-Tabellen oder `sys`-Schemaansichten zeigt die Ausgabe, dass die blockierende Sitzung 76 ist.

```
MySQL [(none)]> select @@version, @@aurora_version;
+-----------+------------------+
| @@version | @@aurora_version |
+-----------+------------------+
| 5.7.12    | 2.09.0           |
+-----------+------------------+
1 row in set (0.01 sec)

MySQL [(none)]> show processlist;
+----+-----------------+--------------------+-----------+---------+------
+---------------------------------+------------------------------+
| Id | User            | Host               | db        | Command | Time | State
                    | Info                           |
+----+-----------------+--------------------+-----------+---------+------
+---------------------------------+------------------------------+
|  2 | rdsadmin        | localhost          | NULL      | Sleep   |    0 | NULL
                    | NULL                           |
|  4 | rdsadmin        | localhost          | NULL      | Sleep   |    2 | NULL
                    | NULL                           |
|  5 | rdsadmin        | localhost          | NULL      | Sleep   |    1 | NULL
                    | NULL                           |
| 20 | rdsadmin        | localhost          | NULL      | Sleep   |    0 | NULL
                    | NULL                           |
| 21 | rdsadmin        | localhost          | NULL      | Sleep   |  261 | NULL
                    | NULL                           |
```

```
| 66 | auroramysql5712 | 172.31.21.51:52154 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 67 | auroramysql5712 | 172.31.21.51:52158 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 68 | auroramysql5712 | 172.31.21.51:52150 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 69 | auroramysql5712 | 172.31.21.51:52162 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 70 | auroramysql5712 | 172.31.21.51:52160 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 71 | auroramysql5712 | 172.31.21.51:52152 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 72 | auroramysql5712 | 172.31.21.51:52156 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 73 | auroramysql5712 | 172.31.21.51:52164 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 74 | auroramysql5712 | 172.31.21.51:52166 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 75 | auroramysql5712 | 172.31.21.51:52168 | sbtest123 | Sleep   |    0 | NULL
                    | NULL                          |
| 76 | auroramysql5712 | 172.31.21.51:52170 | NULL      | Query   |    0 | starting
                    | show processlist              |
| 88 | auroramysql5712 | 172.31.21.51:52194 | NULL      | Query   |   22 | User sleep
                    | select sleep(10000)           |
| 89 | auroramysql5712 | 172.31.21.51:52196 | NULL      | Query   |    5 | Waiting for
 table metadata lock | truncate table sbtest.sbtest1 |
+----+-----------------+--------------------+-----------+---------+------
+---------------------------------+-------------------------------+
18 rows in set (0.00 sec)
```

Als Nächstes zeigt eine Abfrage der `performance_schema`-Tabellen oder `sys`-Schemaansichten, dass die blockierende Sitzung 76 ist.

```
MySQL [(none)]> select * from sys.schema_table_lock_waits;

+---------------+-------------+-------------------+-------------
+-------------------------------+-------------------+-----------------------
+-------------------------------+--------------------+-----------------------------
+-------------------------------+--------------------+--------------
+-------------------------------+--------------------+-----------------------
+--------------------------+------------------------------+
| object_schema | object_name | waiting_thread_id | waiting_pid | waiting_account
           | waiting_lock_type | waiting_lock_duration | waiting_query
```

```
   | waiting_query_secs | waiting_query_rows_affected | waiting_query_rows_examined |
 blocking_thread_id | blocking_pid | blocking_account             | blocking_lock_type
 | blocking_lock_duration | sql_kill_blocking_query | sql_kill_blocking_connection |
+--------------+-------------+-------------------+-------------
+------------------------------+-------------------+----------------------
+------------------------------+-------------------+----------------------------
+------------------------------+-------------------+-------------
+------------------------------+-------------------+----------------------
+-------------------------+-----------------------------+
| sbtest        | sbtest1     |               121 |          89 |
 auroramysql5712@192.0.2.0    | EXCLUSIVE         | TRANSACTION           | truncate
 table sbtest.sbtest1 |                 10 |                           0 |
               0 |                108 |           76 | auroramysql5712@192.0.2.0    |
 SHARED_READ        | TRANSACTION            | KILL QUERY 76           | KILL 76
              |
+--------------+-------------+-------------------+-------------
+------------------------------+-------------------+----------------------
+------------------------------+-------------------+----------------------------
+------------------------------+-------------------+-------------
+------------------------------+-------------------+----------------------
+-------------------------+-----------------------------+
1 row in set (0.00 sec)
```

Antworten Sie auf die Blockiersitzung

Wenn Sie die Sitzung identifizieren, umfassen Ihre Optionen die Folgenden:

- Wenden Sie sich an den Besitzer der Anwendung oder den Benutzer.
- Wenn die Sperrsitzung im Leerlauf ist, erwägen Sie, die Sperrsitzung zu beenden. Diese Aktion könnte einen langen Rollback auslösen. Informationen zum Beenden einer Sitzung finden Sie unter Beenden einer Sitzung oder Abfrage.

Weitere Informationen zum Identifizieren blockierender Transaktionen finden Sie unter Verwenden von InnoDB-Transaktions- und Sperrinformationen in der MySQL-Dokumentation.

synch/mutex/innodb/aurora_lock_thread_slot_futex

Das `synch/mutex/innodb/aurora_lock_thread_slot_futex`-Ereignis tritt auf, wenn eine Sitzung eine Zeile für ein Update gesperrt hat und eine andere Sitzung versucht, dieselbe Zeile zu aktualisieren. Weitere Informationen finden Sie unter InnoDB-Sperren in der MySQL-Referenz.

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Version 2

> **Note**
>
> In den Aurora-MySQL-Versionen 3.01.0 und 3.01.1 wird dieses Warteereignis jedoch als io/table/sql/handler gemeldet.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Mehrere DML-Anweisungen (Data Manipulation Language) greifen gleichzeitig auf dieselbe Zeile oder dieselben Zeilen zu.

Aktionen

Abhängig von den anderen angezeigten Warteereignissen empfehlen wir unterschiedliche Aktionen.

Themen

- Finden und antworten Sie auf die SQL-Anweisungen, die für dieses Warteereignis verantwortlich sind
- Suchen und antworten Sie auf die Blockiersitzung

Finden und antworten Sie auf die SQL-Anweisungen, die für dieses Warteereignis verantwortlich sind

Verwenden Sie Performance Insights, um die SQL-Anweisungen zu identifizieren, die für dieses Warteereignis verantwortlich sind. Berücksichtigen Sie dabei die folgenden Strategien:

- Wenn Zeilensperren ein dauerhaftes Problem darstellen, erwägen Sie, die Anwendung neu zu schreiben, um eine optimistische Sperre zu verwenden.
- Verwenden Sie mehrzeilige Anweisungen.
- Verteilen Sie die Workload auf verschiedene Datenbankobjekte. Sie können dazu die Partitionierung verwenden.
- Prüfen Sie den Wert des `innodb_lock_wait_timeout`-Parameters. Es steuert, wie lange Transaktionen warten, bevor ein Timeout-Fehler generiert wird.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im Blogbeitrag Analysieren Sie Amazon Aurora MySQL Workloads mit Performance Insights.

Suchen und antworten Sie auf die Blockiersitzung

Stellen Sie fest, ob die Blockiersitzung im Leerlauf oder aktiv ist. Finden Sie außerdem heraus, ob die Sitzung von einer Anwendung oder einem aktiven Benutzer stammt.

Um die Sitzung zu identifizieren, die die Sperre hält, können Sie `SHOW ENGINE INNODB STATUS` ausführen. Das folgende Beispiel zeigt eine Beispielausgabe.

```
mysql> SHOW ENGINE INNODB STATUS;

----------------------TRANSACTION 302631452, ACTIVE 2 sec starting index read
mysql tables in use 1, locked 1
LOCK WAIT 2 lock struct(s), heap size 376, 1 row lock(s)
MySQL thread id 80109, OS thread handle 0x2ae915060700, query id 938819 10.0.4.12
 reinvent updating
UPDATE sbtest1 SET k=k+1 WHERE id=503
------- TRX HAS BEEN WAITING 2 SEC FOR THIS LOCK TO BE GRANTED:
RECORD LOCKS space id 148 page no 11 n bits 30 index `PRIMARY` of table
 `sysbench2`.`sbtest1` trx id 302631452 lock_mode X locks rec but not gap waiting
Record lock, heap no 30 PHYSICAL RECORD: n_fields 6; compact format; info bits 0
```

Oder Sie können die folgende Abfrage verwenden, um Details zu aktuellen Sperren zu extrahieren.

```
mysql> SELECT p1.id waiting_thread,
              p1.user waiting_user,
              p1.host waiting_host,
              it1.trx_query waiting_query,
              ilw.requesting_trx_id waiting_transaction,
              ilw.blocking_lock_id blocking_lock,
              il.lock_mode blocking_mode,
              il.lock_type blocking_type,
              ilw.blocking_trx_id blocking_transaction,
              CASE it.trx_state
                WHEN 'LOCK WAIT'
                THEN it.trx_state
                ELSE p.state
              END blocker_state,
              il.lock_table locked_table,
              it.trx_mysql_thread_id blocker_thread,
```

```
               p.user blocker_user,
               p.host blocker_host
        FROM information_schema.innodb_lock_waits ilw
        JOIN information_schema.innodb_locks il
          ON ilw.blocking_lock_id = il.lock_id
         AND ilw.blocking_trx_id = il.lock_trx_id
        JOIN information_schema.innodb_trx it
          ON ilw.blocking_trx_id = it.trx_id
        JOIN information_schema.processlist p
          ON it.trx_mysql_thread_id = p.id
        JOIN information_schema.innodb_trx it1
          ON ilw.requesting_trx_id = it1.trx_id
        JOIN information_schema.processlist p1
          ON it1.trx_mysql_thread_id = p1.id\G

*************************** 1. row ***************************
      waiting_thread: 3561959471
        waiting_user: reinvent
        waiting_host: 123.456.789.012:20485
       waiting_query: select id1 from test.t1 where id1=1 for update
 waiting_transaction: 312337314
       blocking_lock: 312337287:261:3:2
       blocking_mode: X
       blocking_type: RECORD
blocking_transaction: 312337287
       blocker_state: User sleep
        locked_table: `test`.`t1`
      blocker_thread: 3561223876
        blocker_user: reinvent
        blocker_host: 123.456.789.012:17746
1 row in set (0.04 sec)
```

Wenn Sie die Sitzung identifizieren, umfassen Ihre Optionen die Folgenden:

- Wenden Sie sich an den Besitzer der Anwendung oder den Benutzer.
- Wenn die Sperrsitzung im Leerlauf ist, erwägen Sie, die Sperrsitzung zu beenden. Diese Aktion könnte einen langen Rollback auslösen. Informationen zum Beenden einer Sitzung finden Sie unter Beenden einer Sitzung oder Abfrage.

Weitere Informationen zum Identifizieren blockierender Transaktionen finden Sie unter Verwenden von InnoDB-Transaktions- und Sperrinformationen im MySQL-Referenzhandbuch.

synch/mutex/innodb/buf_pool_mutex

Dieses `synch/mutex/innodb/buf_pool_mutex`-Ereignis tritt ein, wenn ein Thread eine Sperre des InnoDB-Puffer-Pools für den Zugriff auf eine Seite im Speicher erworben hat.

Themen

Relevante Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Version 2

Kontext

Der `buf_pool`-Mutex ist ein einzelner Mutex, der die Kontrolldatenstrukturen des Pufferpools schützt.

Weitere Informationen finden Sie unter Überwachen von InnoDB-Mutex-Wartezeiten mithilfe des Leistungsschemas in der MySQL-Dokumentation.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Dies ist ein Workload-spezifisches Warteereignis. Zu den häufigsten Ursachen für das Auftreten von `synch/mutex/innodb/buf_pool_mutex` unter den häufigsten Warteereignissen gehören die folgenden:

- Die Pufferpoolgröße ist nicht groß genug, um den Arbeitsdatensatz zu speichern.
- Die Workload ist für bestimmte Seiten einer bestimmten Tabelle in der Datenbank spezifischer, was zu Konflikten im Pufferpool führt.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen

Normalerweise weisen Datenbanken mit mäßiger bis erheblicher Last Warteereignisse auf. Die Warteereignisse sind möglicherweise akzeptabel, wenn die Leistung optimal ist. Wenn die Leistung nicht optimal ist, untersuchen Sie, wo die Datenbank die meiste Zeit verbringt. Schauen Sie sich die Warteereignisse an, die zur höchsten Belastung beitragen und finden Sie heraus, ob Sie die Datenbank und die Anwendung optimieren können, um diese Ereignisse zu reduzieren.

So zeigen Sie das Top-SQL-Diagramm in der AWS-Managementkonsole an

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus. Das Performance-Insights-Dashboard wird für diese DB-Instance angezeigt.
4. Wählen Sie im Diagramm zur Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unter dem Datenbankauslastungsdiagramm die Option Top-SQL aus.

   Das Diagramm listet die SQL-Abfragen auf, die für die Belastung verantwortlich sind. Diejenigen, die an der Spitze der Liste stehen, sind am meisten verantwortlich. Konzentrieren Sie sich auf diese Aussagen, um einen Engpass zu beheben.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im Blogbeitrag Analysieren Sie Amazon Aurora MySQL Workloads mit Performance Insights.

Performance Insights verwenden

Dieses Ereignis hängt mit der Workload zusammen. Mit Performance Insights können Sie Folgendes tun:

- Identifizieren Sie, wann Warteereignisse beginnen und ob sich die Workload zu dieser Zeit aus den Anwendungsprotokollen oder verwandten Quellen ändert.
- Identifizieren Sie die SQL-Anweisungen, die für dieses Warteereignis verantwortlich sind. Untersuchen Sie den Ausführungsplan der Abfragen, um sicherzustellen, dass diese Abfragen optimiert sind und geeignete Indizes verwenden.

  Wenn die obersten Abfragen, die für das Warteereignis verantwortlich sind, sich auf dasselbe Datenbankobjekt oder dieselbe Tabelle beziehen, sollten Sie erwägen, dieses Objekt oder die Tabelle zu partitionieren.

Erstellen eines Aurora-Replikats

Sie können Aurora-Replikationen erstellen, um schreibgeschützten Datenverkehr bereitzustellen. Sie können Aurora Auto Scaling auch verwenden, um Überspannungen im Leseverkehr zu behandeln. Stellen Sie sicher, dass geplante schreibgeschützte Aufgaben und logische Backups auf Aurora-Replikaten ausgeführt werden.

Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Auto Scaling mit Aurora Replicas.

Überprüfen Sie die Größe des Pufferpools

Prüfen Sie anhand der Metrik `innodb_buffer_pool_wait_free`, ob die Pufferpoolgröße für die Workload ausreicht. Wenn der Wert dieser Metrik hoch ist und kontinuierlich zunimmt, deutet dies darauf hin, dass die Größe des Pufferpools nicht ausreicht, um die Workload zu bewältigen. Wenn `innodb_buffer_pool_size` richtig eingestellt wurde, sollte der Wert von `innodb_buffer_pool_wait_free` klein sein. Weitere Informationen finden Sie unter Innodb_buffer_pool_wait_free in der MySQL-Dokumentation.

Erhöhen Sie die Pufferpool-Größe, wenn die DB-Instance über genügend Speicher für Sitzungspuffer und Betriebssystemaufgaben verfügt. Wenn dies nicht der Fall ist, ändern Sie die DB-Instance in eine größere DB-Instance-Klasse, um zusätzlichen Speicher zu erhalten, der dem Pufferpool zugewiesen werden kann.

> **Note**
>
> Aurora MySQL passt den Wert von `innodb_buffer_pool_instances` automatisch basierend auf der konfigurierten `innodb_buffer_pool_size` an.

Überwachen Sie den globalen Statusverlauf

Durch die Überwachung der Änderungsraten von Statusvariablen können Sie Sperr- oder Speicherprobleme auf Ihrer DB-Instance erkennen. Aktivieren Sie den globalen Statusverlauf (GoSH), wenn er noch nicht aktiviert ist. Weitere Informationen zu GoSH finden Sie unter Verwalten des globalen Statusverlaufs.

Sie können auch benutzerdefinierte Amazon-CloudWatch-Metriken erstellen, um Statusvariablen zu überwachen. Weitere Informationen finden Sie unter Veröffentlichen benutzerdefinierter Metriken.

synch/mutex/innodb/fil_system_mutex

Dieses `synch/mutex/innodb/fil_system_mutex`-Ereignis tritt auf, wenn eine Sitzung darauf wartet, auf den Tablespace-Speichercache zuzugreifen.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Versionen 2 und 3

Kontext

InnoDB verwendet Tablespaces, um den Speicherbereich für Tabellen und Protokolldateien zu verwalten. Der Tablespace-Speichercache ist eine globale Speicherstruktur, die Informationen über Tablespaces verwaltet. MySQL verwendet `synch/mutex/innodb/fil_system_mutex` Wartezeiten, um den gleichzeitigen Zugriff auf den Tablespace-Speichercache zu steuern.

Das Ereignis `synch/mutex/innodb/fil_system_mutex` zeigt an, dass derzeit mehr als eine Operation vorhanden ist, die Informationen im Tabellenbereichsspeichercache für denselben Tabellenbereich abrufen und bearbeiten muss.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `synch/mutex/innodb/fil_system_mutex`-Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, tritt dies normalerweise auf, wenn alle der folgenden Bedingungen vorliegen:

- Eine Zunahme der gleichzeitigen DML-Vorgänge (Data Manipulation Language), die Daten in derselben Tabelle aktualisieren oder löschen.
- Der Tablespace für diese Tabelle ist sehr groß und hat viele Datenseiten.
- Der Füllfaktor für diese Datenseiten ist niedrig.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Themen

- Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen
- Reorganisieren Sie große Tabellen außerhalb der Hauptverkehrszeiten

Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen

Normalerweise weisen Datenbanken mit mäßiger bis erheblicher Last Warteereignisse auf. Die Warteereignisse sind möglicherweise akzeptabel, wenn die Leistung optimal ist. Wenn die Leistung nicht optimal ist, untersuchen Sie, wo die Datenbank die meiste Zeit verbringt. Schauen Sie sich die Warteereignisse an, die zur höchsten Belastung beitragen und finden Sie heraus, ob Sie die Datenbank und die Anwendung optimieren können, um diese Ereignisse zu reduzieren.

So suchen Sie SQL-Abfragen, die für hohe Last verantwortlich sind

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus. Das Performance-Insights-Dashboard wird für diese DB-Instance angezeigt.
4. Wählen Sie im Diagramm zur Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unten auf der Seite Top-SQL aus.

   Das Diagramm listet die SQL-Abfragen auf, die für die Belastung verantwortlich sind. Diejenigen, die an der Spitze der Liste stehen, sind am meisten verantwortlich. Konzentrieren Sie sich auf diese Aussagen, um einen Engpass zu beheben.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im Blogbeitrag Analysieren Sie Amazon Aurora MySQL Workloads mit Performance Insights.

Eine andere Möglichkeit herauszufinden, welche Abfragen eine hohe Anzahl von `synch/mutex/innodb/fil_system_mutex`-Wartezeiten verursachen, besteht darin, `performance_schema` zu überprüfen, wie im folgenden Beispiel.

```
mysql> select * from performance_schema.events_waits_current where EVENT_NAME='wait/
synch/mutex/innodb/fil_system_mutex'\G
*************************** 1. row ***************************
            THREAD_ID: 19
             EVENT_ID: 195057
         END_EVENT_ID: 195057
           EVENT_NAME: wait/synch/mutex/innodb/fil_system_mutex
               SOURCE: fil0fil.cc:6700
          TIMER_START: 1010146190118400
            TIMER_END: 1010146196524000
           TIMER_WAIT: 6405600
                SPINS: NULL
        OBJECT_SCHEMA: NULL
          OBJECT_NAME: NULL
           INDEX_NAME: NULL
          OBJECT_TYPE: NULL
OBJECT_INSTANCE_BEGIN: 47285552262176
     NESTING_EVENT_ID: NULL
   NESTING_EVENT_TYPE: NULL
            OPERATION: lock
      NUMBER_OF_BYTES: NULL
                FLAGS: NULL
*************************** 2. row ***************************
            THREAD_ID: 23
             EVENT_ID: 5480
         END_EVENT_ID: 5480
           EVENT_NAME: wait/synch/mutex/innodb/fil_system_mutex
               SOURCE: fil0fil.cc:5906
          TIMER_START: 995269979908800
            TIMER_END: 995269980159200
           TIMER_WAIT: 250400
                SPINS: NULL
        OBJECT_SCHEMA: NULL
          OBJECT_NAME: NULL
           INDEX_NAME: NULL
          OBJECT_TYPE: NULL
OBJECT_INSTANCE_BEGIN: 47285552262176
     NESTING_EVENT_ID: NULL
   NESTING_EVENT_TYPE: NULL
            OPERATION: lock
      NUMBER_OF_BYTES: NULL
                FLAGS: NULL
*************************** 3. row ***************************
```

```
            THREAD_ID: 55
             EVENT_ID: 23233794
         END_EVENT_ID: NULL
           EVENT_NAME: wait/synch/mutex/innodb/fil_system_mutex
               SOURCE: fil0fil.cc:449
          TIMER_START: 1010492125341600
            TIMER_END: 1010494304900000
           TIMER_WAIT: 2179558400
                SPINS: NULL
        OBJECT_SCHEMA: NULL
          OBJECT_NAME: NULL
           INDEX_NAME: NULL
          OBJECT_TYPE: NULL
OBJECT_INSTANCE_BEGIN: 47285552262176
     NESTING_EVENT_ID: 23233786
   NESTING_EVENT_TYPE: WAIT
            OPERATION: lock
      NUMBER_OF_BYTES: NULL
                FLAGS: NULL
```

Reorganisieren Sie große Tabellen außerhalb der Hauptverkehrszeiten

Reorganisieren Sie große Tabellen, die Sie während eines Wartungsfensters außerhalb der Produktionszeiten als Quelle einer großen Anzahl von `synch/mutex/innodb/fil_system_mutex`-Warteereignissen identifizieren. Dadurch wird sichergestellt, dass die Bereinigung der internen Tablespaces-Zuordnung nicht erfolgt, wenn der schnelle Zugriff auf die Tabelle kritisch ist. Informationen zum Reorganisieren von Tabellen finden Sie unter OPTIMIZE TABLE-Anweisung in der MySQL-Referenz.

synch/mutex/innodb/trx_sys_mutex

Dieses `synch/mutex/innodb/trx_sys_mutex`-Ereignis tritt auf, wenn eine hohe Datenbankaktivität mit einer großen Anzahl von Transaktionen besteht.

Themen

- Relevante Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Relevante Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Engine-Versionen unterstützt:

- Aurora-MySQL-Versionen 2 und 3

Kontext

Intern verwendet das InnoDB-Datenbankmodul die wiederholbare Lese-Isolationsstufe mit Snapshots, um Lesekonsistenz zu gewährleisten. Dies gibt Ihnen eine zeitpunktbezogene Ansicht der Datenbank zum Zeitpunkt der Erstellung des Snapshots.

In InnoDB werden alle Änderungen auf die Datenbank angewendet, sobald sie eintreffen, unabhängig davon, ob sie festgeschrieben wurden. Dieser Ansatz bedeutet, dass ohne Multiversions-Parallelitätssteuerung (MVCC) alle mit der Datenbank verbundenen Benutzer alle Änderungen und die neuesten Zeilen sehen. Daher benötigt InnoDB eine Möglichkeit, die Änderungen zu verfolgen, um zu verstehen, was bei Bedarf zurückgesetzt werden soll.

Dazu verwendet InnoDB ein Transaktionssystem (`trx_sys`) zum Verfolgen von Snapshots. Das Transaktionssystem führt folgenden Aktionen:

- Verfolgt die Transaktions-ID für jede Zeile in den Rückgängig-Protokollen.
- Verwendet eine interne InnoDB-Struktur namens `ReadView`, die hilft zu identifizieren, welche Transaktions-IDs für einen Snapshot sichtbar sind.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Jede Datenbankoperation, die eine konsistente und kontrollierte Behandlung (Erstellen, Lesen, Aktualisieren und Löschen) von Transaktions-IDs erfordert, erzeugt einen Aufruf von `trx_sys` an den Mutex.

Diese Aufrufe erfolgen innerhalb von drei Funktionen:

- `trx_sys_mutex_enter` – Erzeugt den Mutex.
- `trx_sys_mutex_exit` – Gibt den Mutex frei.
- `trx_sys_mutex_own` – Testet, ob der Mutex im Besitz ist.

Die Instrumentierung des InnoDB-Leistungsschemas verfolgt alle `trx_sys`-Mutex-Aufrufe. Die Verfolgung umfasst unter anderem die Verwaltung von `trx_sys` beim Starten oder

Herunterfahren der Datenbank, Rollback-Vorgänge, das Rückgängigmachen von Bereinigungen, den Zeilenlesezugriff und das Laden von Pufferpools. Eine hohe Datenbankaktivität mit einer großen Anzahl von Transaktionen führt dazu, dass `synch/mutex/innodb/trx_sys_mutex` unter den Top-Warteereignissen erscheint.

Weitere Informationen finden Sie unter Überwachen von InnoDB-Mutex-Wartezeiten mithilfe des Leistungsschemas in der MySQL-Dokumentation.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Identifizieren der Sitzungen und Abfragen, die die Ereignisse verursachen

Normalerweise weisen Datenbanken mit mäßiger bis erheblicher Last Warteereignisse auf. Die Warteereignisse sind möglicherweise akzeptabel, wenn die Leistung optimal ist. Wenn die Leistung nicht optimal ist, untersuchen Sie, wo die Datenbank die meiste Zeit verbringt. Schauen Sie sich die Warteereignisse an, die zur höchsten Belastung beitragen. Finden Sie heraus, ob Sie die Datenbank und die Anwendung optimieren können, um diese Ereignisse zu reduzieren.

So zeigen Sie das Top-SQL-Diagramm in AWS Management Console an

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus. Das Performance-Insights-Dashboard wird für diese DB-Instance angezeigt.
4. Wählen Sie im Diagramm zur Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unter dem Datenbankauslastungsdiagramm die Option Top-SQL aus.

   Das Diagramm listet die SQL-Abfragen auf, die für die Belastung verantwortlich sind. Diejenigen, die an der Spitze der Liste stehen, sind am meisten verantwortlich. Konzentrieren Sie sich auf diese Aussagen, um einen Engpass zu beheben.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im Blogbeitrag Analysieren Sie Amazon Aurora MySQL Workloads mit Performance Insights.

Untersuchen Sie andere Warteereignisse

Untersuchen Sie die anderen Warteereignisse, die dem `synch/mutex/innodb/trx_sys_mutex`-Warteereignis zugeordnet sind. Auf diese Weise finden Sie weitere Informationen über die Art der

Workload. Eine große Anzahl von Transaktionen kann den Durchsatz verringern, die Workload kann dies jedoch auch erforderlich machen.

Weitere Informationen zum Optimieren von Transaktionen finden Sie unter Optimieren der InnoDB-Transaktionsverwaltung in der MySQL-Dokumentation.

synch/sxlock/innodb/hash_table_locks

Das -`synch/sxlock/innodb/hash_table_locks`Ereignis tritt auf, wenn Seiten, die nicht im Pufferpool gefunden werden, aus dem Speicher gelesen werden müssen.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für die folgenden Versionen unterstützt:

- Aurora-MySQL-Versionen 2 und 3

Kontext

Das Ereignis `synch/sxlock/innodb/hash_table_locks` zeigt an, dass eine Workload häufig auf Daten zugreift, die nicht im Pufferpool gespeichert sind. Dieses Warteereignis ist mit neuen Seitenhinzufügungen und alten Datenräumungen aus dem Pufferpool verbunden. Die im Pufferpool gespeicherten Daten und neuen Daten müssen zwischengespeichert werden, sodass die gealterten Seiten geräumt werden, um das Zwischenspeichern der neuen Seiten zu ermöglichen. MySQL verwendet einen am wenigsten verwendeten (LRU) -Algorithmus, um Seiten aus dem Puffer-Pool zu entfernen. Die Workload versucht, auf Daten zuzugreifen, die nicht in den Pufferpool geladen wurden, oder auf Daten, die aus dem Pufferpool vertrieben wurden.

Dieses Warteereignis tritt auf, wenn der Workload auf die Daten in Dateien auf der Festplatte zugreifen muss oder wenn Blöcke von der LRU-Liste des Pufferpools befreit oder zur LRU-Liste des Pufferpools hinzugefügt werden. Diese Vorgänge warten darauf, eine gemeinsame ausgeschlossene Sperre (SX-Lock) zu erhalten. Diese SX-Sperre wird für die Synchronisation über die Hash-

Tabelle verwendet, bei der es sich um eine Tabelle im Speicher handelt, die die Leistung des Pufferpoolzugriffs verbessern soll.

Weitere Informationen finden Sie unter Bufferpool in der MySQL-Dokumentation.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `synch/sxlock/innodb/hash_table_locks`-Warteereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die folgenden typischen Ursachen:

Ein unterdimensionierter Pufferpool

Die Größe des Pufferpools ist zu klein, um alle häufig aufgerufenen Seiten im Speicher zu behalten.

Starke Workload

Die Workload verursacht häufige Bereinigungen und das Neuladen von Datenseiten in den Puffercache.

Fehler beim Lesen der Seiten

Es gibt Fehler beim Lesen von Seiten im Pufferpool, die auf eine Beschädigung von Daten hinweisen können.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Themen

- Erhöhen Sie die Größe des Pufferpools
- Verbesserung der Datenzugriffsmuster
- Reduzieren oder vermeiden Sie vollständige Tabellen-Scans
- Überprüfen Sie die Fehlerprotokolle auf Seitenbeschädigung

Erhöhen Sie die Größe des Pufferpools

Stellen Sie sicher, dass diese Pufferpools für die Workload entsprechend dimensioniert sind. Sie können dazu die Trefferrate des Pufferpools überprüfen. Wenn der Wert unter 95 Prozent sinkt, sollten Sie in der Regel die Größe des Pufferpools erhöhen. Ein größerer Pufferpool kann häufig

aufgerufene Seiten länger im Speicher halten. Um die Größe des Pufferpools zu vergrößern, ändern Sie den Wert des `innodb_buffer_pool_size`-Parameters. Der Standardwert dieses Parameters basiert auf der DB-Instance-Klassengröße. Weitere Informationen finden Sie unter bewährte Methoden für die Amazon-Aurora-MySQL-Datenbankkonfiguration.

Verbesserung der Datenzugriffsmuster

Überprüfen Sie die von dieser Wartezeit betroffenen Abfragen und deren Ausführungspläne. Erwägen Sie, die Datenzugriffsmuster zu verbessern. Wenn Sie beispielsweise mysqli_result:: fetch_array verwenden können Sie versuchen, die Abrufgröße des Arrays zu erhöhen.

Sie können Performance Insights verwenden, um Abfragen und Sitzungen anzuzeigen, die möglicherweise ein `synch/sxlock/innodb/hash_table_locks`-Warteereignis verursachen.

So suchen Sie SQL-Abfragen, die für hohe Last verantwortlich sind

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Performance-Insights aus.
3. Wählen Sie eine DB-Instance aus. Das Performance-Insights-Dashboard wird für diese DB-Instance angezeigt.
4. Wählen Sie im Diagramm zur Datenbanklast die Option Nach Wartezeit aufteilen.
5. Wählen Sie unten auf der Seite Top-SQL aus.

   Das Diagramm listet die SQL-Abfragen auf, die für die Belastung verantwortlich sind. Diejenigen, die an der Spitze der Liste stehen, sind am meisten verantwortlich. Konzentrieren Sie sich auf diese Aussagen, um einen Engpass zu beheben.

Eine nützliche Übersicht über die Fehlerbehebung mit Performance Insights finden Sie im AWS-Database Blog-Beitrag Analysieren von Amazon-Aurora-MySQL-Workloads mit Performance Insights.

Reduzieren oder vermeiden Sie vollständige Tabellen-Scans

Überwachen Sie Ihre Workload, um zu sehen, ob vollständige Tabellen-Scans ausgeführt werden, und wenn dies der Fall ist, reduzieren oder vermeiden Sie sie. Sie können beispielsweise Statusvariablen wie `Handler_read_rnd_next` überwachen. Weitere Informationen finden Sie unter Server-Status-Variablen in der MySQL-Dokumentation.

Überprüfen Sie die Fehlerprotokolle auf Seitenbeschädigung

Sie können mysql-error.log auf korruptionsbezogene Nachrichten überprüfen, die zum Zeitpunkt des Problems erkannt wurden. Nachrichten, mit denen Sie arbeiten können, um das Problem zu beheben, befinden sich im Fehlerprotokoll. Möglicherweise müssen Sie Objekte neu erstellen, die als beschädigt gemeldet wurden.

Optimierung von Aurora MySQL mit Thread-Status

In der folgenden Tabelle werden die häufigsten allgemeinen Thread-Zustände für Aurora MySQL zusammengefasst.

Allgemeiner Thread-Zustand	Beschreibung
???	Dieser Thread-Zustand zeigt an, dass ein Thread eine `SELECT`-Anweisung verarbeitet, die die Verwendung einer internen temporären Tabelle zum Sortieren der Daten erfordert.
???	Dieser Thread-Zustand zeigt an, dass ein Thread Zeilen für eine Abfrage liest und filtert, um die richtige Ergebnismenge zu ermitteln.

Erstellen des Sortierindex

Dieser `creating sort index`-Thread-Zustand zeigt an, dass ein Thread eine `SELECT`-Anweisung verarbeitet, die die Verwendung einer internen temporären Tabelle zum Sortieren der Daten erfordert.

Themen

- Unterstützte Engine-Versionen
- Context
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Thread-Statusinformationen werden für die folgenden Versionen unterstützt:

- Aurora MySQL Version 2 bis 2.09.2

Context

Der Zustand `creating sort index` wird angezeigt, wenn eine Abfrage mit einer `ORDER BY`- oder `GROUP BY`-Klausel keinen vorhandenen Index verwenden kann, um die Operation auszuführen.

In diesem Fall muss MySQL eine teurere `filesort`-Operation ausführen. Dieser Vorgang wird normalerweise im Speicher ausgeführt, wenn die Ergebnismenge nicht zu groß ist. Andernfalls geht es darum, eine Datei auf der Festplatte zu erstellen.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Das Auftreten von `creating sort index` deutet nicht allein auf ein Problem hin. Wenn die Leistung schlecht ist und Sie häufig `creating sort index`-Instances sehen, sind die wahrscheinlichste Ursache langsame Abfragen mit `ORDER BY`- oder `GROUP BY`-Operatoren.

Aktionen

Die allgemeine Richtlinie besteht darin, Abfragen mit `ORDER BY`- oder `GROUP BY`-Klauseln zu finden, die mit den Erhöhungen des Zustands `creating sort index` verbunden sind. Prüfen Sie dann, ob das Hinzufügen eines Index oder das Vergrößern der Sortierpuffergröße das Problem löst.

Themen

- Schalten Sie das Leistungsschema ein, wenn es nicht aktiviert ist
- Identifizieren Sie die Problemanfragen
- Untersuchen Sie die Erklärungspläne für die Dateisortierungs-Nutzung
- Erhöhen Sie die Sortierpuffergröße

Schalten Sie das Leistungsschema ein, wenn es nicht aktiviert ist

Performance Insights meldet Thread-Status nur, wenn Leistungsschema-Instrumente nicht aktiviert sind. Wenn Leistungsschema-Instrumente aktiviert sind, meldet Performance Insights stattdessen Warteereignisse. Leistungsschema-Instrumente bieten zusätzliche Erkenntnisse und bessere Tools, wenn Sie potenzielle Leistungsprobleme untersuchen. Daher wird empfohlen, dass Sie das Leistungsschema aktivieren. Weitere Informationen finden Sie unter Aktivieren des Leistungsschemas für Performance Insights in Aurora MySQL.

Identifizieren Sie die Problemanfragen

KennUm aktuelle Abfragen zu identifizieren, die eine Erhöhung des `creating sort index`-Zustands verursachen, führen Sie `show processlist` aus und prüfen Sie, ob eine der Abfragen `ORDER BY` oder `GROUP BY` hat. Führen Sie optional `explain for connection N` aus, wobei `N` die Prozesslisten-ID der Abfrage mit `filesort` ist.

Um frühere Abfragen zu identifizieren, die diese Zunahmen verursachen, aktivieren Sie das Protokoll für langsame Abfragen und suchen Sie die Abfragen mit `ORDER BY`. Führen Sie `EXPLAIN` für die langsamen Abfragen aus und suchen Sie nach „using filesort“. Weitere Informationen finden Sie unter Untersuchen Sie die Erklärungspläne für die Dateisortierungs-Nutzung.

Untersuchen Sie die Erklärungspläne für die Dateisortierungs-Nutzung

Identifizieren Sie die Anweisungen mit `ORDER BY`- oder `GROUP BY`-Klauseln, die den `creating sort index`-Zustand ergeben.

Das folgende Beispiel zeigt, wie `explain` für eine Abfrage ausgeführt wird. Die Spalte `Extra` zeigt, dass diese Abfrage `filesort` verwendet.

```
mysql> explain select * from mytable order by c1 limit 10\G
*************************** 1. row ***************************
           id: 1
  select_type: SIMPLE
        table: mytable
   partitions: NULL
         type: ALL
possible_keys: NULL
          key: NULL
      key_len: NULL
          ref: NULL
         rows: 2064548
     filtered: 100.00
        Extra: Using filesort
1 row in set, 1 warning (0.01 sec)
```

Das folgende Beispiel zeigt das Ergebnis der Ausführung von `EXPLAIN` für dieselbe Abfrage, nachdem ein Index für Spalte `c1` erstellt wurde.

```
mysql> alter table mytable add index (c1);
```

```
mysql> explain select * from mytable order by c1 limit 10\G
*************************** 1. row ***************************
           id: 1
  select_type: SIMPLE
        table: mytable
   partitions: NULL
         type: index
possible_keys: NULL
```

```
          key: c1
      key_len: 1023
          ref: NULL
         rows: 10
     filtered: 100.00
        Extra: Using index
1 row in set, 1 warning (0.01 sec)
```

Informationen zur Verwendung von Indizes zur Optimierung der Sortierreihenfolge finden Sie unter ORDER BY-Optimierung in der MySQL-Dokumentation.

Erhöhen Sie die Sortierpuffergröße

Um festzustellen, ob für eine bestimmte Abfrage ein `filesort`-Prozess erforderlich ist, der eine Datei auf dem Datenträger erstellt hat, überprüfen Sie den `sort_merge_passes`-Variablenwert, nachdem Sie die Abfrage ausgeführt haben. Es folgt ein Beispiel.

```
mysql> show session status like 'sort_merge_passes';
+-------------------+-------+
| Variable_name     | Value |
+-------------------+-------+
| Sort_merge_passes | 0     |
+-------------------+-------+
1 row in set (0.01 sec)

--- run query
mysql> select * from mytable order by u limit 10;
--- run status again:

mysql> show session status like 'sort_merge_passes';
+-------------------+-------+
| Variable_name     | Value |
+-------------------+-------+
| Sort_merge_passes | 0     |
+-------------------+-------+
1 row in set (0.01 sec)
```

Wenn der Wert von `sort_merge_passes` hoch ist, sollten Sie die Größe des Sortierpuffers erhöhen. Wenden Sie den Anstieg auf Sitzungsebene an, da eine globale Erhöhung der RAM-MySQL-Nutzung erheblich erhöhen kann. Das folgende Beispiel zeigt, wie Sie die Größe des Sortierpuffers ändern, bevor Sie eine Abfrage ausführen.

```
mysql> set session sort_buffer_size=10*1024*1024;
Query OK, 0 rows affected (0.00 sec)
-- run query
```

Senden von Daten

Dieser `sending data`-Thread-Zustand zeigt an, dass ein Thread Zeilen für eine Abfrage liest und filtert, um die richtige Ergebnismenge zu ermitteln. Der Name ist irreführend, da er andeutet, dass der Zustand Daten überträgt, nicht sammelt und vorbereitet, um später gesendet zu werden.

Themen

Unterstützte Engine-Versionen

Diese Thread-Statusinformationen werden für die folgenden Versionen unterstützt:

- Aurora MySQL Version 2 bis 2.09.2

Context

Viele Thread-Zustände sind kurzlebig. Operationen, die während `sending data` auftreten, führen in der Regel eine große Anzahl von Platten- oder Cache-Lesevorgängen durch. Daher ist `sending data` häufig der am längsten ausgeführte Zustand während der Lebensdauer einer bestimmten Abfrage. Dieser Status wird angezeigt, wenn Aurora MySQL Folgendes tut:

- Lesen und Verarbeiten von Zeilen für eine `SELECT`-Anweisung
- Durchführen einer großen Anzahl von Lesevorgängen von der Festplatte oder vom Speicher
- Vollständiges Lesen aller Daten aus einer bestimmten Abfrage durchführen
- Lesen von Daten aus einer Tabelle, einem Index oder der Arbeit einer gespeicherten Prozedur
- Daten sortieren, gruppieren oder bestellen

Nachdem der `sending data`-Zustand die Vorbereitung der Daten abgeschlossen hat, zeigt der Thread-Zustand `writing to net` die Rückgabe der Daten an den Client an. Normalerweise wird `writing to net` nur erfasst, wenn die Ergebnismenge sehr groß ist oder eine starke Netzwerklatenz die Übertragung verlangsamt.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Das Auftreten von `sending data` deutet nicht allein auf ein Problem hin. Wenn die Leistung schlecht ist und Sie häufige Instances von `sending data` sehen, sind die wahrscheinlichsten Ursachen wie folgt.

Themen

- Ineffiziente Abfrage
- Suboptimale Serverkonfiguration

Ineffiziente Abfrage

In den meisten Fällen ist für diesen Status eine Abfrage verantwortlich, die keinen geeigneten Index verwendet, um die Ergebnismenge einer bestimmten Abfrage zu finden. Betrachten Sie beispielsweise eine Abfrage, die eine 10-Millionen-Datensatztabelle für alle Bestellungen in Kalifornien liest, wobei die Bundesstaatsspalte nicht indiziert oder schlecht indiziert ist. Im letzteren Fall könnte der Index existieren, aber der Optimierer ignoriert ihn aufgrund der geringen Kardinalität.

Suboptimale Serverkonfiguration

Wenn im Zustand `sending data` mehrere Abfragen erscheinen, ist der Datenbankserver möglicherweise schlecht konfiguriert. Insbesondere könnte der Server die folgenden Probleme haben:

- Der Datenbankserver verfügt nicht über genügend Rechenkapazität: Festplatten-I/O, Festplattentyp und Geschwindigkeit, CPU oder Anzahl der CPUs.
- Der Server sortiert nach allokierten Ressourcen, wie dem InnoDB-Pufferpool für InnoDB-Tabellen oder dem Schlüsselpuffer für MyIsam-Tabellen.
- Arbeitsspeichereinstellungen pro Thread wie `sort_buffer`, `read_buffer` und `join_buffer` verbrauchen mehr RAM als erforderlich, wodurch der physische Server an Speicherressourcen mangelt.

Aktionen

Die allgemeine Richtlinie besteht darin, Abfragen zu finden, die eine große Anzahl von Zeilen zurückgeben, indem Sie das Leistungsschema überprüfen. Wenn die Protokollierung von Abfragen aktiviert ist, die keine Indizes verwenden, können Sie auch die Ergebnisse der langsamen Protokolle untersuchen.

Themen

- Schalten Sie das Leistungsschema ein, wenn es nicht aktiviert ist
- Prüfen Sie die Speichereinstellungen
- Untersuchen Sie die Erklärungspläne zur Indexverwendung
- Überprüfen Sie das Volume der zurückgegebenen Daten
- Auf Parallelitätsprobleme prüfen
- Überprüfen der Struktur Ihrer Abfrage

Schalten Sie das Leistungsschema ein, wenn es nicht aktiviert ist

Performance Insights meldet Thread-Status nur, wenn Leistungsschema-Instrumente nicht aktiviert sind. Wenn Leistungsschema-Instrumente aktiviert sind, meldet Performance Insights stattdessen Warteereignisse. Leistungsschema-Instrumente bieten zusätzliche Erkenntnisse und bessere Tools, wenn Sie potenzielle Leistungsprobleme untersuchen. Daher wird empfohlen, dass Sie das Leistungsschema aktivieren. Weitere Informationen finden Sie unter Aktivieren des Leistungsschemas für Performance Insights in Aurora MySQL.

Prüfen Sie die Speichereinstellungen

Untersuchen Sie die Speichereinstellungen für die primären Pufferpools. Stellen Sie sicher, dass diese Pools für die Workload entsprechend dimensioniert sind. Wenn Ihre Datenbank mehrere Pufferpool-Instances verwendet, stellen Sie sicher, dass sie nicht in viele kleine Pufferpools unterteilt sind. Threads können jeweils nur einen Pufferpool verwenden.

Stellen Sie sicher, dass die folgenden Speichereinstellungen, die für jeden Thread verwendet werden, richtig dimensioniert sind:

- read_buffer
- read_rnd_buffer

- sort_buffer
- join_buffer
- binlog_cache

Wenn Sie keinen bestimmten Grund haben, die Einstellungen zu ändern, verwenden Sie die Standardwerte.

Untersuchen Sie die Erklärungspläne zur Indexverwendung

Überprüfen Sie bei Abfragen im `sending data`-Thread-Zustand den Plan, um festzustellen, ob geeignete Indizes verwendet werden. Wenn eine Abfrage keinen nützlichen Index verwendet, sollten Sie Hinweise wie `USE INDEX` oder `FORCE INDEX` hinzufügen. Hinweise können die Zeit zum Ausführen einer Abfrage erheblich verlängern oder verkürzen, seien Sie also vorsichtig, bevor Sie sie hinzufügen.

Überprüfen Sie das Volume der zurückgegebenen Daten

Überprüfen Sie die abgefragten Tabellen und die Menge der Daten, die sie enthalten. Kann irgendeine dieser Daten archiviert werden? In vielen Fällen ist die Ursache für schlechte Ausführungszeiten der Abfragen nicht das Ergebnis des Abfrageplans, sondern das Datenvolumen, das verarbeitet werden soll. Viele Entwickler fügen einer Datenbank sehr effizient Daten hinzu, berücksichtigen jedoch selten den Lebenszyklus von Datensätzen in den Entwurfs- und Entwicklungsphasen.

Suchen Sie nach Abfragen, die in Datenbanken mit geringem Volume gut funktionieren, aber in Ihrem aktuellen System schlecht funktionieren. Manchmal erkennen Entwickler, die bestimmte Abfragen entwerfen, möglicherweise nicht, dass diese Abfragen 350.000 Zeilen zurückgeben. Die Entwickler haben die Abfragen möglicherweise in einer Umgebung mit geringerem Volumen und kleineren Datensätzen entwickelt als in Produktionsumgebungen.

Auf Parallelitätsprobleme prüfen

Überprüfen Sie, ob mehrere Abfragen desselben Typs gleichzeitig ausgeführt werden. Einige Formen von Abfragen werden effizient ausgeführt, wenn sie alleine laufen. Wenn jedoch ähnliche Abfrageformen zusammen oder in hohem Volumen ausgeführt werden, können sie Parallelitätsprobleme verursachen. Oft werden diese Probleme verursacht, wenn die Datenbank temporäre Tabellen verwendet, um Ergebnisse zu rendern. Eine restriktive Transaktionsisolationsstufe kann auch Parallelitätsprobleme verursachen.

Wenn Tabellen gleichzeitig gelesen und geschrieben werden, verwendet die Datenbank möglicherweise Sperren. Um Perioden schlechter Leistung zu identifizieren, untersuchen Sie die Verwendung von Datenbanken durch umfangreiche Batch-Prozesse. Um die letzten Sperren und Rollbacks anzuzeigen, überprüfen Sie die Ausgabe des `SHOW ENGINE INNODB STATUS`-Befehls.

Überprüfen der Struktur Ihrer Abfrage

Prüfen Sie, ob erfasste Abfragen aus diesen Status Unterabfragen verwenden. Diese Art von Abfrage führt häufig zu einer schlechten Leistung, da die Datenbank die Ergebnisse intern kompiliert und sie dann wieder in die Abfrage einfügt, um Daten zu rendern. Dieser Prozess ist ein zusätzlicher Schritt für die Datenbank. In vielen Fällen kann dieser Schritt zu einer schlechten Leistung in einem stark gleichzeitigen Ladezustand führen.

Überprüfen Sie auch, ob Ihre Abfragen eine große Anzahl von `ORDER BY`- und `GROUP BY`-Klauseln verwenden. Bei solchen Operationen muss die Datenbank oft zuerst den gesamten Datensatz im Speicher bilden. Dann muss es auf eine bestimmte Weise bestellen oder gruppieren, bevor es an den Kunden zurückgegeben wird.

Optimierung von Aurora MySQL mit proaktiven Einblicken von Amazon DevOps Guru

Die proaktiven Einblicke von DevOps Guru erkennen bekannte problematische Bedingungen auf Ihren Aurora-MySQL-DB-Clustern, bevor sie auftreten. DevOps Guru kann Folgendes tun:

- Vermeiden vieler häufig auftretender Datenbankprobleme durch Abgleich der Datenbankkonfiguration mit den allgemein empfohlenen Einstellungen.
- Warnen vor kritischen Problemen in der Flotte, die, wenn sie nicht überprüft werden, später zu größeren Problemen führen können.
- Benachrichtigung bei neu erkannten Problemen.

Jeder proaktive Einblick beinhaltet eine Analyse der Problemursache und Empfehlungen für Korrekturmaßnahmen.

Themen

Die Länge der InnoDB-Verlaufsliste wurde deutlich erhöht

Ab dem *Datum* wurde Ihre Verlaufsliste für Zeilenänderungen erheblich erweitert, bis hin zur *Länge* auf der *DB-Instance*. Dieser Anstieg wirkt sich auf die Leistung beim Herunterfahren von Abfragen und Datenbanken aus.

Themen

Unterstützte Engine-Versionen

Diese Insight-Informationen werden für alle Versionen von unterstützt.

Kontext

Das InnoDB-Transaktionssystem behält die Multiversion Concurrency Control (MVCC) bei. Wenn eine Zeile geändert wird, wird die Version der geänderten Daten vor der Änderung als Undo-Datensatz in einem Undo-Protokoll gespeichert. Jeder Undo-Datensatz hat einen Verweis auf seinen vorherigen Redo-Datensatz, wodurch eine verknüpfte Liste entsteht.

Die InnoDB-Verlaufsliste ist eine globale Liste der Undo-Protokolle für übernommene Transaktionen. MySQL verwendet die Verlaufsliste, um Datensätze und Protokollseiten zu löschen, wenn Transaktionen den Verlauf nicht mehr benötigen. Die Länge der Verlaufsliste ist die Gesamtzahl der Undo-Protokolle, die Änderungen in der Verlaufsliste enthalten. Jedes Protokoll umfasst eine oder mehrere Änderungen. Wenn die Länge der InnoDB-Verlaufsliste zu groß wird, was auf eine große Anzahl alter Zeilenversionen hinweist, werden Abfragen und Datenbankabschaltungen langsamer.

Mögliche Ursachen für dieses Problem

Zu den typischen Ursachen einer langen Verlaufsliste gehören die folgenden:

- Transaktionen mit langer Laufzeit, entweder beim Lesen oder Schreiben
- Eine hohe Schreiblast

Aktionen

Abhängig von den Ursachen Ihres Einblicks empfehlen wir verschiedene Aktionen.

Themen

- Beginnen Sie keine Operation, die ein Herunterfahren der Datenbank beinhaltet, bis die InnoDB-Verlaufsliste kürzer wird
- Identifizieren und beenden Sie lang andauernde Transaktionen
- Verwenden Sie Performance Insights, um die Top-Hosts und Top-Benutzer zu identifizieren.

Beginnen Sie keine Operation, die ein Herunterfahren der Datenbank beinhaltet, bis die InnoDB-Verlaufsliste kürzer wird

Da eine lange InnoDB-Verlaufsliste das Herunterfahren von Datenbanken verlangsamt, sollten Sie die Listengröße reduzieren, bevor Sie Operationen einleiten, die ein Herunterfahren der Datenbank beinhalten. Zu diesen Vorgängen gehören Datenbank-Upgrades der Hauptversionen.

Identifizieren und beenden Sie lang andauernde Transaktionen

Sie können Transaktionen mit langer Laufzeit finden, indem Sie `information_schema.innodb_trx` abfragen.

> **Note**
>
> Achten Sie auch auf lang andauernde Transaktionen auf Lesereplikaten.

So identifizieren und beenden Sie lang andauernde Transaktionen

1. Führen Sie das folgende Skript in Ihrem SQL-Client aus:

```
SELECT a.trx_id,
      a.trx_state,
      a.trx_started,
      TIMESTAMPDIFF(SECOND,a.trx_started, now()) as "Seconds Transaction Has Been
 Open",
      a.trx_rows_modified,
      b.USER,
      b.host,
```

```
      b.db,
      b.command,
      b.time,
      b.state
FROM  information_schema.innodb_trx a,
      information_schema.processlist b
WHERE a.trx_mysql_thread_id=b.id
  AND TIMESTAMPDIFF(SECOND,a.trx_started, now()) > 10
ORDER BY trx_started
```

2. Beenden Sie jede lang laufende Transaktion mit einem `COMMIT`- oder `ROLLBACK`-Befehl.

Verwenden Sie Performance Insights, um die Top-Hosts und Top-Benutzer zu identifizieren.

Optimieren Sie Transaktionen, so dass eine große Anzahl geänderter Zeilen sofort bestätigt wird.

Relevante Metriken

Die folgenden Metriken beziehen sich auf diesen Einblick:

- trx_rseg_history_len

  Weitere Informationen finden Sie in der Metriktabelle InnoDB INFORMATION_SCHEMA im MySQL 5.7-Referenzhandbuch.

Die Datenbank erstellt temporäre Tabellen auf der Festplatte

Ihre aktuelle Nutzung temporärer Tabellen auf der Festplatte ist erheblich gestiegen, und zwar bis zu *`Prozentsatz`*. Die Datenbank erstellt ungefähr die *`Anzahl`* temporärer Tabellen pro Sekunde. Dies kann die Leistung beeinträchtigen und die Festplattenoperationen auf der *`DB-Instance`* erhöhen.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Mögliche Ursachen für dieses Problem
- Aktionen
- Relevante Metriken

Unterstützte Engine-Versionen

Diese Insight-Informationen werden für alle Versionen von unterstützt.

Kontext

Manchmal ist es notwendig, dass der MySQL-Server während der Verarbeitung einer Abfrage eine interne temporäre Tabelle erstellt. Aurora MySQL kann eine interne temporäre Tabelle im Speicher speichern, wo sie von der TempTable- oder MEMORY-Speicherengine verarbeitet oder von InnoDB auf der Festplatte gespeichert werden kann. Weitere Informationen finden Sie unter Interne Verwendung temporärer Tabellen in MySQL im MySQL-Referenzhandbuch.

Mögliche Ursachen für dieses Problem

Eine Zunahme temporärer Tabellen auf der Festplatte weist auf die Verwendung komplexer Abfragen hin. Wenn der konfigurierte Speicher nicht ausreicht, um temporäre Tabellen im Speicher zu speichern, erstellt Aurora MySQL die Tabellen auf der Festplatte. Dies kann die Leistung beeinträchtigen und den Festplattenbetrieb erhöhen.

Aktionen

Abhängig von den Ursachen Ihres Einblicks empfehlen wir verschiedene Aktionen.

- Für Aurora-MySQL-Version 3 empfehlen wir die Verwendung der TempTable-Speicher-Engine.
- Optimieren Sie Ihre Abfragen, um weniger Daten zurückzugeben, indem Sie nur die erforderlichen Spalten auswählen.

  Wenn Sie das Performance-Schema aktivieren und alle `statement`-Instrumente aktiviert und zeitgesteuert sind, können Sie `SYS.statements_with_temp_tables` abfragen, um die Liste der Abfragen abzurufen, die temporäre Tabellen verwenden. Weitere Informationen finden Sie unter Voraussetzungen für die Verwendung des sys–Schemas in der MySQL-Dokumentation.
- Erwägen Sie die Indizierung von Spalten, die an Sortier- und Gruppierungsoperationen beteiligt sind.
- Schreiben Sie Ihre Abfragen neu, um `BLOB`- und `TEXT`-Spalten zu vermeiden. Diese Spalten verwenden immer die Festplatte.
- Optimieren Sie die folgenden Datenbankparameter: `tmp_table_size` und `max_heap_table_size`.

  Der Standardwert für diese Parameter ist 16 MiB. Wenn Sie die MEMORY-Speicher-Engine für temporäre In-Memory-Tabellen verwenden, wird deren maximale Größe durch den

`tmp_table_size`- oder `max_heap_table_size`-Wert definiert, je nachdem, welcher Wert kleiner ist. Wenn diese maximale Größe erreicht ist, konvertiert MySQL die interne temporäre In-Memory-Tabelle automatisch in eine interne temporäre InnoDB-Tabelle auf der Festplatte. Weitere Informationen finden Sie unter Verwenden der TempTable-Speicher-Engine Amazon RDS für MySQL und Amazon Aurora MySQL.

> **Note**
>
> Beim expliziten Erstellen von MEMORY-Tabellen mit CREATE TABLE bestimmt nur die `max_heap_table_size`-Variable, wie groß eine Tabelle werden kann. Es erfolgt auch keine Konvertierung in ein Festplattenformat.

Relevante Metriken

Die folgenden Performance Insights-Metriken beziehen sich auf diesen Einblick:

- Created_tmp_disk_tables
- Created_tmp_tables

Weitere Informationen finden Sie unter Created_tmp_disk_tables in der MySQL-Dokumentation.

Arbeiten mit Parallel Query für Amazon Aurora MySQL

Dieses Thema beschreibt, wie Sie Amazon-Aurora-MySQL-kompatible Edition Parallel Query optimal nutzen. Diese Funktion verwendet für bestimmte datenintensive Abfragen einen speziellen Verarbeitungspfad. Dabei kommt zum Tragen, dass die Architektur von Aurora verschiedene Speicherquellen nutzt. Parallel Query ist am wirkungsvollsten in Verbindung mit Aurora MySQL DB-Clustern, deren Tabellen Millionen Zeilen und analytische Abfragen unterstützen, deren Abarbeitung Minuten oder Stunden dauert.

Inhalt

Übersicht über Parallel Query für Aurora MySQL

Aurora MySQL Parallel Query ist eine Optimierung, die bei der Verarbeitung datenintensiver Abfragen einen Teil der I/O-Operationen und Berechnungen parallelisiert. Die parallelisierten Vorgänge beinhalten das Abrufen von Zeilen aus dem Speicher, das Extrahieren von Spaltenwerten und das Bestimmen der Zeilen, die den Bedingungen der `WHERE`-Klausel und der JOIN-Klauseln entsprechen. Diese datenintensive Arbeit wird auf der Ebene des verteilten Speichers von Aurora an mehrere Knoten in der verteilten Speicherschicht delegiert (aus Datenbanksicht herabgestuft). Ohne eine

Parallelabfrage leitet jede Abfrage die gescannten Daten zu einem einzigen Knoten innerhalb des Aurora MySQL-Clusters (Hauptknoten) und die Verarbeitung jeglicher Abfragen erfolgt dort.

> **Tip**
>
> Die PostgreSQL-Datenbank-Engine hat auch eine Funktion, die auch „parallel query bzw. Paralleabfragen“ genannt wird. Diese Funktion steht in keinem Zusammenhang mit der parallelen Abfrage von Aurora.

Wenn die Funktion für parallele Abfragen aktiviert ist, bestimmt die Aurora-MySQL-Engine automatisch, wann Abfragen von Nutzen sein können, ohne dass SQL-Änderungen wie Hinweise oder Tabellenattribute erforderlich sind. In den folgenden Abschnitten lesen Sie, in welchen Fällen Abfragen parallelisiert werden. Dabei erfahren Sie auch, wie Parallelabfragen nur dann eingesetzt werden, wenn sie den größten Nutzen bringen.

> **Note**
>
> Die Funktion für die Optimierung der parallelen Abfrageausführung ist besonders bei Abfragen sinnvoll, die mehrere Minuten oder Stunden in Anspruch nehmen. Aurora MySQL führt in der Regel keine parallele Abfrageoptimierung für kostengünstige Abfragen durch. Es führt auch im Allgemeinen keine parallele Abfrageoptimierung durch, wenn ein anderes Optimierungsverfahren geeigneter wäre (z. B. Abfrage-Caching, Caching im Bufferpool oder Index-Lookups). Wenn Sie der Meinung sind, dass die parallele Abfrageausführung anders als erwartet angewendet wird, lesen Sie den Abschnitt Überprüfen, welche Anweisungen Parallel Query verwenden.

Themen

Vorteile

Mit parallelen Abfragen können Sie datenintensive analytische Abfragen für Aurora MySQL-Tabellen ausführen. In vielen Fällen verbessert sich die Leistung im Vergleich mit herkömmlichen Verfahren, in denen Abfragen arbeitsteilig verarbeitet werden, um mehrere Größenordnungen.

Vorteile der parallelen Abfrageausführung:

- Höhere I/O-Leistung, weil physische Leseanforderungen auf mehrere Speicherknoten parallelisiert werden.
- Reduzierter Netzwerkverkehr. Aurora überträgt nicht komplette Datenseiten von den Speicherknoten zum Hauptknoten, um dort überflüssige Zeilen und Spalten herauszufiltern. Aurora überträgt stattdessen kompakte Tupel, die nur die Spaltenwerte enthalten, die für den Ergebnissatz erforderlich sind.
- Niedrigere CPU-Last im Hauptknoten, weil die Funktionsverarbeitung, Zeilenfilterung und Spaltenprojektion für die `WHERE`-Klausel herabgestuft werden.
- Weniger Speicherdruck im Bufferpool. Die von der parallelen Abfrage verarbeiteten Seiten werden dem Bufferpool nicht hinzugefügt. Dieser Ansatz reduziert die Wahrscheinlichkeit, dass ein datenintensiver Scan häufig verwendete Daten aus dem Bufferpool entfernt.
- Möglicherweise weniger Datenduplikate in der ETL-Pipeline (Extract, Transform, Load), weil langwierige analytische Abfragen auf Bestandsdaten ausgeführt werden können.

Architektur

Parallele Abfragen machen sich die maßgeblichen Architekturprinzipien von Aurora MySQL zunutze: Entkopplung zwischen Datenbank-Engine und Speichersubsystem und weniger Netzwerkdatenverkehr durch Optimierung von Kommunikationsprotokollen. Aurora MySQL verwendet diese Techniken, um schreibintensive Operationen wie Redo-Protokoll-Verarbeitung zu beschleunigen. Parallel Query wendet die gleichen Prinzipien auf Leseoperationen an.

> **Note**
>
> Die Architektur von Aurora MySQL Parallel Query ist anders als die ähnlich benannter Funktionen in anderen Datenbanksystemen. Aurora MySQL Parallel Query ist kein symmetrisches Multiprocessing (SMP) und ist daher nicht von der CPU-Kapazität des Datenbankservers abhängig. Die Parallelverarbeitung erfolgt auf der Speicherschicht, völlig losgelöst vom Aurora MySQL-Server, der als Abfragekoordinator fungiert.

Ohne eine Parallelabfrage beinhaltet die Verarbeitung einer Aurora-Abfrage standardmäßig die Übertragung von Rohdaten an einen Einzelknoten innerhalb des Aurora-Clusters (dem Hauptknoten). Aurora führt dann die gesamte weitere Verarbeitung für diese Abfrage in einem einzigen Thread auf diesem einzelnen Knoten durch. Parallel Query delegiert einen Großteil dieser I/O- und CPU-intensiven Arbeit an Knoten aus der Speicherschicht. Nur die kompakten Zeilen aus dem Ergebnissatz werden an den Hauptknoten zurück übertragen. Die Zeilen sind dann bereits gefiltert und die Spaltenwerte bereits extrahiert und umgewandelt. Der Leistungsvorteil ergibt sich aus dem reduzierten Netzwerkdatenverkehr, einer niedrigeren CPU-Last im Hauptknoten und der Parallelisierung der I/O-Vorgänge aller Speicherknoten. Wie viele E/A-Vorgänge, Filterungen und Projektionen parallel ablaufen, ist unabhängig von der Anzahl der DB-Instances im Aurora-Cluster, der die Abfrage ausführt.

Voraussetzungen

Um alle Funktionen der parallelen Abfrage verwenden zu können, wird ein Aurora MySQL-DB-Cluster benötigt, auf dem Version 2.09 und höher ausgeführt wird. Wenn Sie bereits einen Cluster haben, den Sie mit der parallelen Abfrage verwenden möchten, können Sie ihn auf eine kompatible Version aktualisieren und anschließend die parallele Abfrage einschalten. Stellen Sie in diesem Fall sicher, dass Sie das Upgrade-Verfahren unter Wichtige Punkte bei einem Upgrade für parallele Abfragen befolgen, da die Namen der Konfigurationseinstellungen und Standardwerte in diesen neueren Versionen unterschiedlich sind.

Die DB-Instances in Ihrem Cluster müssen die `db.r*`-Instance-Klassen verwenden.

Stellen Sie sicher, dass die Hash-Join-Optimierung für Ihren Cluster aktiviert ist. Um zu erfahren wie dies geht, vgl. Hash-Join für parallele Abfrage-Cluster aktivieren.

Zum Anpassen von Parametern wie `aurora_parallel_query` und `aurora_disable_hash_join` benötigen Sie eine benutzerdefinierte Parametergruppe, die Sie mit dem Cluster verwenden. Sie können diese Parameter für jede DB-Instance einzeln angeben, indem Sie eine DB-Parametergruppe verwenden. Es wird jedoch empfohlen, sie in einer DB-Cluster-Parametergruppe anzugeben. Auf diese Weise übernehmen alle DB-Instances in Ihrem Cluster die gleichen Einstellungen für diese Parameter.

Einschränkungen

Parallele Abfragen unterliegen folgenden Einschränkungen:

- Parallelabfragen werden mit der DB-Cluster-Speicherkonfiguration Aurora I/O-Optimized nicht unterstützt.

- Sie können eine parallele Abfrage nicht mit den Instance-Klassen db.t2 oder db.t3 verwenden. Diese Einschränkung gilt auch dann, wenn Sie eine Parallelabfrage mit dem SQL-Hinweis `aurora_pq_force` anfordern.
- Die parallele Abfrage gilt nicht für Tabellen, die das Zeilenformat `COMPRESSED` oder `REDUNDANT` verwenden. Verwenden Sie die Zeilenformate `COMPACT` oder `DYNAMIC` für Tabellen, die Sie mit der parallelen Abfrage verwenden möchten.
- Aurora verwendet einen kostenbasierten Algorithmus, um zu bestimmen, ob der parallele Abfragemechanismus für jede SQL-Anweisung verwendet werden soll. Die Verwendung bestimmter SQL-Konstrukte in einer Anweisung kann eine parallele Abfrage verhindern oder eine parallele Abfrage für diese Anweisung unwahrscheinlich machen. Hinweise zur Kompatibilität von SQL-Konstrukten mit parallelen Abfragen finden Sie unter Zusammenwirken von Parallel Query und SQL-Konstrukten.
- Jede Aurora-DB-Instance kann nur eine bestimmte Anzahl Parallelabfrage-Sitzungen gleichzeitig leisten. In Abfragen, die mehrere Komponenten mit paralleler Abfrageausführung enthalten (z. B. Unterabfragen, Join-Abfragen oder `UNION`-Operatoren), werden diese Phasen nacheinander ausgeführt. Die Anweisung zählt stets nur als einzelne Parallelabfrage-Sitzung. Wenn Sie überwachen möchten, wie viele Sitzungen derzeit geöffnet sind, verwenden Sie die Parallel-Query-Statusvariablen. Um herauszufinden, wie viele gleichzeitige Sitzungen eine DB-Instance maximal zulässt, fragen Sie die Statusvariable a `Aurora_pq_max_concurrent_requests`.
- Die parallele Abfrage ist in allen anderen AWS-Regionen verfügbar, die Aurora unterstützt. Für die meisten AWS-Regionen ist die mindestens erforderliche Aurora-MySQL-Version für die Verwendung der parallelen Abfrage 2.09.
- Parallelabfragen wurden entwickelt, um die Leistung datenintensiver Abfragen zu verbessern. Diese Funktion ist nicht für einfache Abfragen konzipiert.
- Wir empfehlen, Leserknoten für SELECT-Anweisungen zu verwenden, insbesondere für datenintensive Anweisungen.

I/O-Kosten bei Parallelabfragen

Wenn Ihr Aurora MySQL Cluster eine parallele Abfrage verwendet, erfolgt möglicherweise eine Zunahme der `VolumeReadIOPS`-Werte. Parallel Query verwendet den Bufferpool nicht. Obwohl die Abfragen schnell sind, kann diese optimierte Verarbeitung zu einem Anstieg der Lesevorgänge und der damit verbundenen Gebühren führen.

Die I/O-Kosten für parallele Abfragen werden für Ihre Abfrage auf der Speicherebene gemessen und sind gleich oder höher, wenn die parallele Abfrage aktiviert ist. Ihr Vorteil ist die Verbesserung der Abfrageleistung. Es gibt zwei Gründe für potenziell höhere I/O-Kosten bei parallelen Abfragen:

- Selbst wenn sich einige Daten in einer Tabelle im Pufferpool befinden, müssen bei der parallelen Abfrage alle Daten auf der Speicherebene gescannt werden, was I/O-Kosten verursacht.
- Das Ausführen einer parallelen Abfrage führt nicht zu einem Aufwärmvorgang des Pufferpools. Folglich fallen bei aufeinanderfolgenden Läufen derselben parallelen Abfrage die vollen I/O-Kosten an.

Planen eines Parallel Query-Clusters

Bei der Planung eines DB-Clusters mit aktivierter paralleler Abfrage müssen einige Entscheidungen getroffen werden. Dazu gehören das Ausführen von Einrichtungsschritten (das Erstellen oder Wiederherstellen eines vollständigen Aurora MySQL-Clusters) und die Entscheidung, wie weit in Ihrem DB-Cluster die parallele Abfrage eingeschaltet werden sollen.

Berücksichtigen Sie bei der Planung Folgendes:

- Wenn Sie Aurora MySQL verwenden, das mit MySQL 5.7 kompatibel ist, müssen Sie Aurora MySQL 2.09 oder höher auswählen. In diesem Fall erstellen Sie immer einen bereitgestellten Cluster. Anschließend aktivieren Sie die parallele Abfrage mit dem Parameter `aurora_parallel_query`.

  Wenn Sie einen vorhandenen Aurora MySQL-Cluster haben, auf dem Version 2.09 oder höher ausgeführt wird, müssen Sie keinen neuen Cluster erstellen, um die parallele Abfrage verwenden zu können. Sie können Ihren Cluster oder bestimmte DB-Instances im Cluster einer Parametergruppe zuordnen, bei der der Parameter `aurora_parallel_query` aktiviert ist. Dadurch können Sie die Zeit und den Aufwand für die Einrichtung der relevanten Daten für die parallele Abfrage reduzieren.
- Planen Sie alle großen Tabellen, die neu organisiert werden müssen, damit Sie die parallele Abfrage verwenden können, wenn Sie auf diese zugreifen. Möglicherweise müssen Sie neue Versionen einiger großer Tabellen erstellen, bei denen die parallele Abfrage nützlich ist. Beispielsweise müssen Sie möglicherweise Volltextsuchindizes entfernen. Details hierzu finden Sie unter Erstellen von Schema-Objekten, mit denen die Vorteile von Parallel Query genutzt werden können.

Überprüfen der Versionskompatibilität von Aurora MySQL für Parallel Query

Um zu überprüfen, welche Aurora-MySQL-Versionen mit parallelen Abfrage-Clustern kompatibel sind, verwenden Sie den AWS CLI-Befehl `describe-db-engine-versions` und überprüfen Sie den Wert des Feldes `SupportsParallelQuery`. Das folgende Codebeispiel zeigt, wie Sie überprüfen können, welche Kombinationen für Cluster für parallele Abfragen in einer bestimmten AWS-Region verfügbar sind. Stellen Sie sicher, dass Sie die vollständige `--query`-Parameterzeichenfolge in einer einzigen Zeile angeben.

```
aws rds describe-db-engine-versions --region us-east-1 --engine aurora-mysql \
--query '*[]|[?SupportsParallelQuery == `true`].[EngineVersion]' --output text
```

Die vorhergehenden Befehle erzeugen eine Ausgabe, die der folgenden ähnelt: Die Ausgabe hängt davon ab, welche Aurora-MySQL-Versionen in der angegebenen AWS-Region verfügbar sind.

```
5.7.mysql_aurora.2.11.1
8.0.mysql_aurora.3.01.0
8.0.mysql_aurora.3.01.1
8.0.mysql_aurora.3.02.0
8.0.mysql_aurora.3.02.1
8.0.mysql_aurora.3.02.2
8.0.mysql_aurora.3.03.0
```

Nachdem Sie angefangen haben, die parallele Abfrage mit einem Cluster zu verwenden, können Sie die Leistung überwachen und Hindernisse bei der Nutzung der parallelen Abfrage beseitigen. Diese Anweisungen finden Sie unter Optimierung der Abfrageleistung fürParallel Query.

Erstellen eines DB-Clusters für Parallel Query

Um einen für Parallel Query geeigneten Aurora MySQL-Cluster anzulegen, ihm neue Instances hinzuzufügen oder andere administrative Aufgaben zu erledigen, verwenden Sie die gleichen AWS Management Console- und AWS CLI-Techniken wie für andere Aurora-MySQL-Cluster. Sie können einen neuen Cluster erstellen, auf dem Sie parallele Abfragen ausführen können. Sie können auch einen für parallele Abfragen geeigneten DB-Cluster erstellen, indem Sie diesen aus einem Snapshot eines MySQL-kompatiblen Aurora-DB-Clusters wiederherstellen. Wenn Sie sich nicht sicher sind, wie ein neuer Aurora MySQL-Cluster erstellt wird, finden Sie unter diesem Link die erforderlichen Hintergrundinformationen und Anforderungen: Erstellen eines Amazon Aurora-DB Clusters.

Wenn Sie sich für eine Version einer Aurora MySQL-Engine entscheiden, empfehlen wir Ihnen, die neueste verfügbare Engine auszuwählen. Derzeit unterstützen die AuroraMySQL-Versionen 2.09 und

höher die parallele Abfrage. Wenn Sie Aurora MySQL 2.09 und höher verwenden, haben Sie mehr Flexibilität, die parallele Abfrage zu aktivieren und zu deaktivieren, oder die parallele Abfragen mit vorhandenen Clustern zu verwenden.

Unabhängig davon, ob Sie einen neuen Cluster erstellen oder aus einem Snapshot wiederherstellen, gilt: Sie fügen neue DB-Instances genauso hinzu wie bei anderen Aurora MySQL-Clustern.

Erstellen eines Parallel Query-Clusters über die Konsole

Sie können wie folgt über die Konsole einen neuen Parallelabfragecluster erstellen.

So erstellen Sie über die -Konsole einen Parallelabfragecluste AWS Management Console

1. Gehen Sie vor, wie im allgemeinen AWS Management Console-Verfahren auf der Seite Erstellen eines Amazon Aurora-DB Clusters beschrieben.
2. Wählen Sie auf dem Bildschirm Engine auswählen die Option Aurora MySQL.

   Wählen Sie für Engine-Version, die Option Aurora MySQL 2.09 oder höher aus. Bei diesen Versionen haben Sie die geringsten Einschränkungen für die Verwendung der parallelen Abfrage. Diese Versionen haben auch die größte Flexibilität, um die parallele Abfrage jederzeit ein- oder auszuschalten.

   Wenn es nicht praktikabel ist, eine aktuelle Aurora MySQL-Version für diesen Cluster zu verwenden, wählen Sie Show versions that support the parallel query Funktion (Versionen anzeigen, die die parallele Abfrage unterstützen). Dadurch wird das Menü Version so gefiltert, dass nur die spezifischen Aurora MySQL-Versionen angezeigt werden, die mit der parallelen Abfrage kompatibel sind.
3. Wählen Sie unter Zusätzliche Konfiguration eine Parametergruppe aus, die Sie für die DB-Cluster-Parametergruppe erstellt haben. Die Verwendung einer solchen benutzerdefinierten Parametergruppe ist für Aurora MySQL 2.09 und höher erforderlich. Geben Sie in Ihrer DB-Cluster-Parametergruppe die Parametereinstellungen `aurora_parallel_query=ON` und `aurora_disable_hash_join=OFF` an. Dadurch wird die parallele Abfrage für den Cluster und die Hash-Join-Optimierung aktiviert, die in Kombination mit der parallelen Abfrage funktioniert.

So kontrollieren Sie, ob ein neuer Cluster parallelabfragefähig ist:

1. Erstellen Sie einen Cluster, wie vorhergehend beschrieben.

2. (Für Aurora MySQL Version 2 oder 3): Prüfen Sie, ob auf die Konfigurationseinstellung `aurora_parallel_query` die Bedingung „true“ zutrifft.

```
mysql> select @@aurora_parallel_query;
+-------------------------+
| @@aurora_parallel_query |
+-------------------------+
|                       1 |
+-------------------------+
```

3. (Für Aurora-MySQL-Version 2) Überprüfen Sie, ob die `aurora_disable_hash_join`-Einstellung „false“ ist.

```
mysql> select @@aurora_disable_hash_join;
+----------------------------+
| @@aurora_disable_hash_join |
+----------------------------+
|                          0 |
+----------------------------+
```

4. Überprüfen Sie bei einigen großen Tabellen und datenintensiven Abfragen die Abfragepläne, um zu bestätigen, dass einige Ihrer Abfragen die Optimierung für die parallele Abfrage verwenden. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Überprüfen, welche Anweisungen Parallel Query verwenden.

Erstellen eines Parallel Query-Clusters mit der CLI

Sie können wie folgt mit der CLI einen neuen Parallelabfragecluster erstellen.

So erstellen Sie über die -Konsole einen Parallelabfragecluste AWS CLI

1. (Optional) Überprüfen Sie, welche Aurora MySQL-Versionen mit parallelen Abfrage-Clustern kompatibel sind. Verwenden Sie dazu den Befehl `describe-db-engine-versions` und überprüfen Sie den Wert des Feldes `SupportsParallelQuery`. Ein Beispiel finden Sie unter Überprüfen der Versionskompatibilität von Aurora MySQL für Parallel Query.
2. (Optional) Erstellen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe mit den Einstellungen `aurora_parallel_query=ON` und `aurora_disable_hash_join=OFF`. Verwenden Sie Befehle wie die folgenden.

```
aws rds create-db-cluster-parameter-group --db-parameter-group-family aurora-
mysql5.7 --db-cluster-parameter-group-name pq-enabled-57-compatible
aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-name pq-
enabled-57-compatible \
  --parameters
 ParameterName=aurora_parallel_query,ParameterValue=ON,ApplyMethod=pending-reboot
aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-name pq-
enabled-57-compatible \
  --parameters
 ParameterName=aurora_disable_hash_join,ParameterValue=OFF,ApplyMethod=pending-
reboot
```

Wenn Sie diesen Schritt ausführen, geben Sie die Option `--db-cluster-parameter-group-name` *`my_cluster_parameter_group`* in der nachfolgenden `create-db-cluster`-Anweisung an. Geben Sie den Namen Ihrer eigenen Parametergruppe an. Wenn Sie diesen Schritt auslassen, erstellen Sie die Parametergruppe und ordnen sie später dem Cluster zu, wie unter beschriebe Aktivieren und Deaktivieren der parallelen Abfragen.

3. Gehen Sie vor, wie im allgemeinen AWS CLI-Verfahren auf der Seite Erstellen eines Amazon Aurora-DB Clusters beschrieben.
4. Geben Sie die folgenden Optionen an:

   - Verwenden Sie für die Option `--engine` den Wert `aurora-mysql`. Diese Werte erzeugen parallele Abfrage-Cluster, die mit MySQL 5.7 oder 8.0 kompatibel sind.
   - Geben Sie für die Option `--db-cluster-parameter-group-name` den Namen einer DB-Cluster-Parametergruppe an, die Sie erstellt und für die Sie den Parameterwert `aurora_parallel_query=ON` zugewiesen haben. Wenn Sie diese Option auslassen, können Sie den Cluster mit einer Standardparametergruppe erstellen und ihn später so ändern, dass er eine solche benutzerdefinierte Parametergruppe verwendet.
   - Verwenden Sie für die Option `--engine-version` eine Aurora MySQL-Version, die mit der parallelen Abfrage kompatibel ist. Verwenden Sie das Verfahren aus Planen eines Parallel Query-Clusters, um bei Bedarf eine Liste der Versionen abzurufen. Verwenden Sie mindestens Version 2.09.0. Diese und alle höheren Versionen enthalten wesentliche Verbesserungen für parallelen Abfragen.

     Wie das aussehen kann, sehen Sie am nachfolgenden Beispielcode. Ersetzen Sie Ihren eigenen Wert für jede der Umgebungsvariablen wie *`$CLUSTER_ID`*. In diesem Beispiel wird auch die Option `--manage-master-user-password` zum Generieren

des Hauptbenutzerpassworts und zum Verwalten dieses Passworts in Secrets Manager angegeben. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager. Alternativ können Sie die Option `--master-password` verwenden, um das Passwort selbst festzulegen und zu verwalten.

```
aws rds create-db-cluster --db-cluster-identifier $CLUSTER_ID \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --master-username $MASTER_USER_ID --manage-master-user-password \
  --db-cluster-parameter-group-name $CUSTOM_CLUSTER_PARAM_GROUP

aws rds create-db-instance --db-instance-identifier ${INSTANCE_ID}-1 \
  --engine same_value_as_in_create_cluster_command \
  --db-cluster-identifier $CLUSTER_ID --db-instance-class $INSTANCE_CLASS
```

5. Überprüfen Sie, ob ein von Ihnen erstellter oder wiederhergestellter Cluster parallelabfragefähig ist.

   Prüfen Sie, ob auf die Konfigurationseinstellung `aurora_parallel_query` vorhanden ist. Wenn diese Einstellung den Wert „1“ hat, können Sie die parallele Abfrage verwenden. Wenn diese Einstellung den Wert „0“ hat, müssen Sie ihn auf „1“ festlegen, bevor Sie die parallele Abfrage verwenden können. In jedem Fall ist der Cluster in der Lage, die parallele Abfrage durchzuführen.

```
mysql> select @@aurora_parallel_query;
+------------------------+
| @@aurora_parallel_query|
+------------------------+
|                      1 |
+------------------------+
```

Stellen Sie einen Snapshot in einem parallelen Abfragecluster mit dem AWS CLI wie folgt wieder her:

1. Überprüfen Sie, welche Aurora MySQL-Versionen mit parallelen Abfrage-Clustern kompatibel sind. Verwenden Sie dazu den Befehl `describe-db-engine-versions` und überprüfen Sie den Wert des Feldes `SupportsParallelQuery`. Ein Beispiel finden Sie unter Überprüfen der Versionskompatibilität von Aurora MySQL für Parallel Query. Entscheiden Sie, welche Version für den wiederhergestellten Cluster verwendet werden soll. Wählen Sie Aurora MySQL 2.09.0 oder höher für einen mit MySQL 5.7 kompatiblen Cluster.
2. Suchen Sie einen Aurora MySQL-kompatiblen Cluster-Snapshot.

3. Gehen Sie vor, wie im allgemeinen AWS CLI-Verfahren auf der Seite Wiederherstellen aus einem DB-Cluster-Snapshot beschrieben.

```
aws rds restore-db-cluster-from-snapshot \
  --db-cluster-identifier mynewdbcluster \
  --snapshot-identifier mydbclustersnapshot \
  --engine aurora-mysql
```

4. Überprüfen Sie, ob ein von Ihnen erstellter oder wiederhergestellter Cluster parallelabfragefähig ist. Verwenden Sie das gleiche Verifizierungsverfahren wie in Erstellen eines Parallel Query-Clusters mit der CLI.

Aktivieren und Deaktivieren der parallelen Abfragen

Wenn die parallele Abfrage aktiviert ist, bestimmt Aurora MySQL, ob sie zur Laufzeit für jede Abfrage verwendet wird. Werden Join-Abfragen, Union-Abfragen, Unterabfragen usw. durchgeführt, entscheidet Aurora MySQL bei jedem Abfrageblock, ob zur Laufzeit parallel abgefragt werden soll. Details dazu finden Sie unter Überprüfen, welche Anweisungen Parallel Query verwenden und Zusammenwirken von Parallel Query und SQL-Konstrukten.

Sie können parallele Abfragen sowohl auf globaler als auch auf Sitzungsebene für eine DB-Instance dynamisch ein- und ausschalten, indem Sie die Option aurora_parallel_query verwenden. Sie können die Einstellung `aurora_parallel_query` in Ihrer DB-Clustergruppe so ändern, dass die parallele Abfrage standardmäßig aktiviert oder deaktiviert wird.

```
mysql> select @@aurora_parallel_query;
+------------------------+
| @@aurora_parallel_query|
+------------------------+
|                      1 |
+------------------------+
```

Um de Parameter `aurora_parallel_query` auf Sitzungsebene zu aktivieren und zu deaktivieren, verwenden Sie die Standardmethoden zum Anpassen von Client-Konfigurationseinstellungen. Sie können dies beispielsweise über die `mysql`-Befehlszeile oder in einer JDBC- oder ODBC-Anwendung tun. Der Befehl für den Standard-MySQL-Client lautet `set session aurora_parallel_query = {'ON'/'OFF'}`. Sie können den Parameter auf Sitzungsebene auch der JDBC-Konfiguration oder innerhalb Ihres Anwendungscodes hinzufügen, um parallele Abfragen dynamisch ein- oder auszuschalten.

Sie können die Einstellung für den Parameter `aurora_parallel_query` dauerhaft ändern, entweder für eine bestimmte DB-Instance oder für den gesamten Cluster. Wenn Sie den Parameterwert in einer DB-Parametergruppe angeben, gilt dieser Wert nur für bestimmte DB-Instances in Ihrem Cluster. Wenn Sie den Parameterwert in einer DB-Cluster-Parametergruppe angeben, erben alle DB-Instances im Cluster dieselbe Einstellung. Um den Parameter `aurora_parallel_query` umzuschalten, wenden Sie die Methoden an, die Sie auch für Parametergruppen verwenden, siehe Arbeiten mit Parametergruppen. Dazu gehen Sie wie folgt vor:

1. Erstellen Sie eine benutzerdefinierte Cluster-Parametergruppe (empfohlen) oder eine benutzerdefinierte DB-Parametergruppe.
2. Aktualisieren Sie in dieser Parametergruppe `parallel_query` auf den gewünschten Wert.
3. Abhängig davon, ob Sie eine DB-Cluster-Parametergruppe oder eine DB-Parametergruppe erstellt haben, hängen Sie die Parametergruppe Ihrem Aurora-Cluster oder den spezifischen DB-Instances an, in denen Sie die Parallelabfrage-Funktion verwenden möchten.

> **Tip**
>
> Da es sich bei `aurora_parallel_query` um einen dynamischen Parameter handelt, ist ein Neustart des Clusters nach dem Ändern dieser Einstellung nicht erforderlich. Alle Verbindungen, die vor dem Umschalten der Option eine parallele Abfrage verwendeten, setzen diesen Vorgang fort, bis die Verbindung geschlossen oder die Instance neu gestartet wird.

Sie können den Parallelabfrageparameter nachträglich anpassen. Verwenden Sie dazu die API-Operationen ModifyDBClusterParameterGroup oder ModifyDBParameterGroup oder die AWS Management Console.

Hash-Join für parallele Abfrage-Cluster aktivieren

Parallele Abfragen werden typischerweise für ressourcenintensive Abfragen verwendet, die von der Hash-Join-Optimierung profitieren. Daher ist es hilfreich sicherzustellen, dass Hash-Joins für Cluster aktiviert sind, in denen Sie parallele Abfragen verwenden möchten. Informationen zur effektiven Verwendung von Hash-Joins finden Sie unter Optimierung von großen Aurora-MySQL-Join-Abfragen mit Hash-Joins.

Ein- und Ausschalten der parallelen Abfrage mit der Konsole

Sie können die parallele Abfrage auf DB-Instance-Ebene oder DB-Cluster-Ebene aktivieren oder deaktivieren, indem Sie mit Parametergruppen arbeiten.

So aktivieren oder deaktivieren Sie die parallele Abfrage für einen DB-Cluster mit der AWS Management Console

1. Erstellen Sie eine benutzerdefinierte Parametergruppe, wie in Arbeiten mit Parametergruppen beschrieben.
2. Aktualisieren Sie aurora_parallel_query zu 1 (aktiviert) oder 0 (deaktiviert). Für Cluster, in denen die parallele Abfragefunktion verfügbar ist, ist aurora_parallel_query standardmäßig deaktiviert.
3. Wenn Sie eine benutzerdefinierte Cluster-Parametergruppe verwenden, fügen Sie sie dem Aurora-DB-Cluster zu, in dem Sie die parallele Abfrage verwenden möchten. Wenn Sie eine benutzerdefinierte DB-Parametergruppe verwenden, fügen Sie sie einer oder mehreren DB-Instances im Cluster zu. Wir empfehlen die Verwendung einer Cluster-Parametergruppe. Dadurch wird sichergestellt, dass alle DB-Instances im Cluster die gleichen Einstellungen für die parallele Abfrage und zugehörige Funktionen wie Hash-Join haben.

Ein- und Ausschalten der parallelen Abfrage mit der CLI

Sie können den Parallelabfrageparameter nachträglich anpassen. Verwenden Sie dazu den Befehl `modify-db-cluster-parameter-group` oder `modify-db-parameter-group`. Wählen Sie den entsprechenden Befehl, je nachdem, ob Sie den Wert von `aurora_parallel_query` über eine DB-Cluster-Parametergruppe oder eine DB-Parametergruppe angeben.

So aktivieren oder deaktivieren Sie die parallele Abfrage für einen DB-Cluster mit der CLI

- Passen Sie den Parallelabfrageparameter nachträglich an. Verwenden Sie dazu den Befehl `modify-db-cluster-parameter-group`. Verwenden Sie einen Befehl wie den folgenden. Ersetzen Sie den entsprechenden Namen mit Ihrer eigenen benutzerdefinierten Parametergruppe. Setzen Sie entweder `ON` oder `OFF` ein in den `ParameterValue`-Teil der Option `--parameters`.

```
$ aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-
name cluster_param_group_name \
```

```
  --parameters
 ParameterName=aurora_parallel_query,ParameterValue=ON,ApplyMethod=pending-reboot
{
    "DBClusterParameterGroupName": "cluster_param_group_name"
}

aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-
name cluster_param_group_name \
  --parameters ParameterName=aurora_pq,ParameterValue=ON,ApplyMethod=pending-reboot
```

Sie können parallele Abfragen auch auf Sitzungsebene aktivieren oder deaktivieren, beispielsweise über die Befehlszeile `mysql` oder in einer JDBC- oder ODBC-Anwendung. Verwenden Sie dafür die Standardmethoden zum Anpassen von Client-Konfigurationseinstellungen. Beispielsweise lautet der Befehl für den Standard-MySQL-Client `set session aurora_parallel_query = {'ON'/'OFF'}` für Aurora MySQL.

Sie können den Parameter auf Sitzungsebene auch der JDBC-Konfiguration oder innerhalb Ihres Anwendungscodes hinzufügen, um parallele Abfragen dynamisch ein- oder auszuschalten.

Überschreiben des Parallelabfrageoptimierers

Sie können die Sitzungsvariable `aurora_pq_force` verwenden, um den Parallelabfrageoptimierer zu überschreiben und für jede Abfrage eine Parallelabfrage anzufordern. Wir empfehlen diese Vorgehensweise nur zu Testzwecken. Das folgende Beispiel zeigt, wie Sie `aurora_pq_force` in einer Sitzung verwenden.

```
set SESSION aurora_parallel_query = ON;
set SESSION aurora_pq_force = ON;
```

Gehen Sie wie folgt vor, um die Überschreibung zu deaktivieren:

```
set SESSION aurora_pq_force = OFF;
```

Wichtige Punkte bei einem Upgrade für parallele Abfragen

Abhängig von der Original- und Zielversionen beim Upgrade eines parallelen Abfrage-Clusters finden Sie möglicherweise Verbesserungen bei den Abfragetypen, die parallele Abfragen optimieren können. Möglicherweise müssen Sie auch feststellen, dass Sie keinen speziellen Engine-

Modusparameter für parallele Abfragen angeben müssen. In den folgenden Abschnitten werden die Überlegungen beim Upgrade eines Clusters erläutert, bei dem die parallele Abfrage aktiviert ist.

Upgrade paralleler Abfrage-Cluster auf Aurora-MySQL-Version 3

Mehrere SQL-Anweisungen, Klauseln und Datentypen haben ab Aurora-MySQL-Version 3 neuen oder verbesserten Support für parallele Abfragen. Prüfen Sie beim Upgrade von einer Version, die vor Version 3 liegt, ob zusätzliche Abfragen von parallelen Abfrageoptimierungen profitieren können. Informationen zu diesen Erweiterungen für parallele Abfragen finden Sie unter Spaltendatentypen, Partitionierte Tabellen und Aggregationsfunktionen, GROUP BY-Klauseln und HAVING-Klauseln.

Wenn Sie einen Parallelabfragecluster von Aurora MySQL 2.08 oder niedriger aktualisieren, informieren Sie sich auch über Änderungen beim Einschalten der parallelen Abfrage. Lesen Sie dazu Upgrade auf Aurora MySQL 2.09 und höher.

In Aurora-MySQL-Version 3 ist die Hash-Join-Optimierung standardmäßig aktiviert. Die Konfigurationsoption `aurora_disable_hash_join` aus früheren Versionen wird nicht verwendet.

Upgrade auf Aurora MySQL 2.09 und höher

In Aurora MySQL 2.09 und höher funktioniert die parallele Abfrage für bereitgestellte Cluster und erfordert keinen `parallelquery`-Engine-Modus-Parameter. Daher müssen Sie keinen neuen Cluster erstellen oder aus einem vorhandenen Snapshot wiederherstellen, um die parallele Abfrage mit diesen Versionen verwenden zu können. Sie können die unter Upgrade der Nebenversion oder der Patch-Ebene eines Aurora MySQL-DB-Clusters beschriebenen Upgrade-Verfahren verwenden, um den Cluster auf eine solche Version zu aktualisieren. Sie können einen älteren Cluster aktualisieren, unabhängig davon, ob es sich um einen Parallelabfragecluster oder um einen bereitgestellten Cluster handelte. Um die Anzahl der Optionen im Menü Engine-Version zu reduzieren, können Sie Versionen anzeigen, die die parallele Abfrage unterstützen auswählen, um die Einträge in diesem Menü zu filtern. Wählen Sie dann Aurora MySQL 2.09 oder höher aus.

Nachdem Sie einen früheren Parallelabfragecluster auf Aurora MySQL 2.09 oder höher aktualisiert haben, aktivieren Sie die parallele Abfrage im aktualisierten Cluster. Die parallele Abfrage ist in diesen Versionen standardmäßig deaktiviert, und die Vorgehensweise zum Aktivieren ist anders. Die Hash-Join-Optimierung ist ebenfalls standardmäßig deaktiviert und muss separat aktiviert werden. Stellen Sie daher sicher, dass Sie diese Einstellungen nach dem Upgrade wieder aktivieren. Anweisungen dazu finden Sie unter Aktivieren und Deaktivieren der parallelen Abfragen und Hash-Join für parallele Abfrage-Cluster aktivieren.

Insbesondere schalten Sie die parallele Abfrage mithilfe der Konfigurationsparameter `aurora_parallel_query=ON` und `aurora_disable_hash_join=OFF` anstelle von `aurora_pq_supported` und `aurora_pq` ein. Die Parameter `aurora_pq_supported` und `aurora_pq` sind in den neueren Aurora MySQL-Versionen veraltet.

Im aktualisierten Cluster weist das Attribut `EngineMode` den Wert `provisioned` anstelle von `parallelquery` auf. Um zu prüfen, ob die parallele Abfrage für eine angegebene Engine-Version verfügbar ist, überprüfen Sie nun den Wert des Feldes `SupportsParallelQuery` in der Ausgabe des `describe-db-engine-versions`-Befehls AWS CLI. In früheren Aurora MySQL-Versionen haben Sie überprüft, ob `parallelquery` in der Liste `SupportedEngineModes` vorhanden ist.

Nach dem Upgrade auf Aurora MySQL 2.09 oder höher können Sie die folgenden Funktionen nutzen. Diese Funktionen sind nicht für Parallelabfragecluster verfügbar, auf denen ältere Aurora MySQL-Versionen ausgeführt werden.

- Performance-Insights. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .
- Rückverfolgung. Weitere Informationen finden Sie unter Rückverfolgen eines Aurora-DB-Clusters.
- Stoppen und Starten des Clusters. Weitere Informationen finden Sie unter Stoppen und Starten eines Amazon Aurora-DB-Clusters.

Optimierung der Abfrageleistung fürParallel Query

Um mit Parallel Query die Abarbeitung einer Workload beeinflussen zu können, müssen Sie überlegen, wie Sie Parallel Query für die Abfragen einsetzen, bei denen diese Optimierung den größten Effekt hat.

Gehen Sie dazu wie folgt vor:

- Stellen Sie sicher, dass Ihre größten Tabellen mit der parallelen Abfrage kompatibel sind. Sie können Tabelleneigenschaften ändern oder einige Tabellen neu erstellen, damit Abfragen für diese Tabellen die Optimierung für die parallele Abfrage nutzen können. Um zu erfahren wie, siehe Erstellen von Schema-Objekten, mit denen die Vorteile von Parallel Query genutzt werden können.
- Überwachen Sie, welche Abfragen mit Parallel Query ausgeführt werden. Um zu erfahren wie, siehe Überwachen von Parallel Query.

- Stellen Sie sicher, dass die parallele Abfrage für die datenintensivsten und am längsten laufenden Abfragen und mit der richtigen Parallelität für Ihren Workload verwendet wird. Um zu erfahren wie, siehe Überprüfen, welche Anweisungen Parallel Query verwenden.
- Optimieren Sie Ihren SQL-Code, um die parallele Abfrage zu aktivieren, um sie auf die erwarteten Abfragen anzuwenden. Um zu erfahren wie, siehe Zusammenwirken von Parallel Query und SQL-Konstrukten.

Erstellen von Schema-Objekten, mit denen die Vorteile von Parallel Query genutzt werden können

Bevor Sie Tabellen erstellen oder ändern, die Sie für die parallele Abfrage verwenden möchten, sollten Sie sich mit den unter Voraussetzungen und Einschränkungen beschriebenen Anforderungen vertraut machen.

Wenn Sie Parallelabfragen starten, müssen Tabellen die Einstellungen `ROW_FORMAT=Compact` oder `ROW_FORMAT=Dynamic` verwenden. Öffnen Sie deshalb die Konfigurationseinstellungen von Aurora und prüfen Sie, ob an der Konfigurationsoption `INNODB_FILE_FORMAT` Änderungen vorgenommen wurden. Geben Sie die Anweisung `SHOW TABLE STATUS` aus, um das Zeilenformat aller Tabellen einer Datenbank zu bestätigen.

Bevor Sie Ihr Schema ändern, um die parallele Abfrage zu aktivieren, um mit mehr Tabellen zu arbeiten, stellen Sie sicher, dass Sie es testen. Ihre Tests sollten bestätigen, ob die parallele Abfrage zu einer besseren Nettoleistung für diese Tabellen führt. Stellen Sie außerdem sicher, dass die Schema-Anforderungen an Parallel Query mit Ihren Zielen vereinbar sind.

Zum Beispiel: Prüfen Sie vor der Umstellung von `ROW_FORMAT=Compressed` auf `ROW_FORMAT=Compact` oder `ROW_FORMAT=Dynamic` die Leistung von Workloads anhand der ursprünglichen und der neuen Tabellen. Berücksichtigen Sie außerdem eventuelle sonstige Effekte (z. B. erhöhtes Datenvolumen).

Überprüfen, welche Anweisungen Parallel Query verwenden

Im normalen Betrieb müssen Sie nichts Besonderes unternehmen, um Parallel Query zu nutzen. Erfüllt eine Abfrage die grundlegenden Anforderungen einer Parallelabfrage, entscheidet der Abfrageoptimierer bei jeder Abfrage automatisch, ob Parallel Query verwendet werden soll.

Wenn parallele Abfragen in Versuchen in einer Entwicklungs- oder Testumgebung nicht verwendet werden, kann dies daran liegen, dass Ihre Tabellen zu klein sind (zu wenige Zeilen oder zu wenig

Datenvolumen). Die Daten für die Tabelle können sich auch vollständig im Pufferpool befinden, insbesondere bei Tabellen, die Sie kürzlich erstellt haben, um Experimente durchzuführen.

Während Sie die Cluster-Leistung überwachen oder optimieren, müssen Sie entscheiden, ob parallele Abfragen in den richtigen Kontexten verwendet werden. Sie haben die Möglichkeit, das Datenbankschema, die Einstellungen, die SQL-Abfragen oder sogar die Cluster-Topologie und die Anwendungsverbindungseinstellungen nachzubessern, um die Vorteile der Funktion nutzen zu können.

Um zu prüfen, ob eine Abfrage Parallel Query verwendet, prüfen Sie den Abfrageausführungsplan (auch als „Erläuterungsplan“ bezeichnet), indem Sie die Anweisung EXPLAIN ausführen. Anhand unserer Beispiele können Sie nachvollziehen, wie sich SQL-Anweisungen, SQL-Klauseln und SQL-Ausdrücke auf die `EXPLAIN`-Ausgabe von Parallel Query auswirken: Zusammenwirken von Parallel Query und SQL-Konstrukten

Das nachfolgende Beispiel verdeutlicht den Unterschied zwischen einem normalen Abfrageplan und einem parallelen Abfrageplan (Parallel Query). Dieser Erläuterungsplan stammt aus Abfrage 3 aus dem TPC-H-Benchmark. Viele der Beispielabfragen aus diesem Abschnitt verwenden die Tabellen aus dem TPC-H-Dataset. Sie können die Tabellendefinitionen, Abfragen und das `dbgen`-Programm abrufen, das Beispieldaten von der TPC-h-Website generiert.

```
EXPLAIN SELECT l_orderkey,
  sum(l_extendedprice * (1 - l_discount)) AS revenue,
  o_orderdate,
  o_shippriority
FROM customer,
  orders,
  lineitem
WHERE c_mktsegment = 'AUTOMOBILE'
AND c_custkey = o_custkey
AND l_orderkey = o_orderkey
AND o_orderdate < date '1995-03-13'
AND l_shipdate > date '1995-03-13'
GROUP BY l_orderkey,
  o_orderdate,
  o_shippriority
ORDER BY revenue DESC,
  o_orderdate LIMIT 10;
```

Standardmäßig hat die Abfrage möglicherweise einen Plan wie den folgenden. Wenn im Abfrageplan kein Hash-Join verwendet wird, stellen Sie sicher, dass zuerst die Optimierung aktiviert ist.

```
+----+-------------+----------+------------+------+---------------+------+---------
+------+----------+----------+----------------------------------------------------+
| id | select_type | table    | partitions | type | possible_keys | key  | key_len |
 ref  | rows     | filtered | Extra                                              |
+----+-------------+----------+------------+------+---------------+------+---------
+------+----------+----------+----------------------------------------------------+
|  1 | SIMPLE      | customer | NULL       | ALL  | NULL          | NULL | NULL    |
 NULL |  1480234 |    10.00 | Using where; Using temporary; Using filesort       |
|  1 | SIMPLE      | orders   | NULL       | ALL  | NULL          | NULL | NULL    |
 NULL | 14875240 |     3.33 | Using where; Using join buffer (Block Nested Loop) |
|  1 | SIMPLE      | lineitem | NULL       | ALL  | NULL          | NULL | NULL    |
 NULL | 59270573 |     3.33 | Using where; Using join buffer (Block Nested Loop) |
+----+-------------+----------+------------+------+---------------+------+---------
+------+----------+----------+----------------------------------------------------+
```

Sie können bei Aurora MySQL 3 den Hash-Join auf Sitzungsebene aktivieren, indem Sie die folgende Anweisung ausgeben.

```
SET optimizer_switch='block_nested_loop=on';
```

Für Aurora MySQL Version 2.09 und höher setzen Sie den`aurora_disable_hash_join`-DB-Parameter oder DB-Cluster-Parameter auf `0` (aus). Durch Deaktivierung von `aurora_disable_hash_join` wird der Wert von `optimizer_switch` auf `hash_join=on` gesetzt.

Nachdem Sie den Hash-Join aktiviert haben, versuchen Sie erneut, die `EXPLAIN`-Anweisung auszuführen. Informationen zur effektiven Verwendung von Hash-Joins finden Sie unter Optimierung von großen Aurora-MySQL-Join-Abfragen mit Hash-Joins.

Bei aktiviertem Hash-Join, aber deaktivierter paralleler Abfrage kann die Abfrage einen Plan wie den folgenden haben, der Hash-Join, aber keine parallele Abfrage verwendet.

```
+----+-------------+----------+...+-----------
+-------------------------------------------------------------+
| id | select_type | table    |...| rows      | Extra
                          |
+----+-------------+----------+...+-----------
+-------------------------------------------------------------+
|  1 | SIMPLE      | customer |...|   5798330 | Using where; Using index; Using
 temporary; Using filesort       |
```

```
|  1 | SIMPLE      | orders   |...| 154545408 | Using where; Using join buffer (Hash
 Join Outer table orders)   |
|  1 | SIMPLE      | lineitem |...| 606119300 | Using where; Using join buffer (Hash
 Join Outer table lineitem) |
+----+-------------+----------+...+-----------
+-------------------------------------------------------------------+
```

Nachdem die parallele Abfrage aktiviert wurde, können zwei Schritte in diesem Abfrageplan die parallele Abfrageoptimierung verwenden, wie unter der Spalte `Extra` in der Ausgabe `EXPLAIN` angezeigt. Die I/O-intensive und CPU-intensive Verarbeitung aus diesen Schritten wird in die Speicherschicht hinabgestuft.

```
+----+...
+-------------------------------------------------------------------------------------------------------
+
| id |...| Extra
                                                    |
+----+...
+-------------------------------------------------------------------------------------------------------
+
|  1 |...| Using where; Using index; Using temporary; Using filesort
                                                    |
|  1 |...| Using where; Using join buffer (Hash Join Outer table orders); Using
 parallel query (4 columns, 1 filters, 1 exprs; 0 extra)   |
|  1 |...| Using where; Using join buffer (Hash Join Outer table lineitem); Using
 parallel query (4 columns, 1 filters, 1 exprs; 0 extra) |
+----+...
+-------------------------------------------------------------------------------------------------------
+
```

Hinweise zur Interpretierung der `EXPLAIN`-Ausgabe einer Parallelabfrage und der Teile von SQL-Anweisungen, für die Parallel Query in Frage kommt, lesen Sie im Beitrag Zusammenwirken von Parallel Query und SQL-Konstrukten.

Aus der nachfolgenden Beispielausgabe geht hervor, welche Ergebnisse zustande kommen, wenn die vorherige Abfrage auf einer db.r4.2xlarge-Instance mit kaltem Bufferpool ausgeführt wird. Die Abfrage wird mit Parallel Query erheblich schneller ausgeführt.

> **Note**
>
> Weil Durchlaufzeiten von vielen Umgebungsfaktoren abhängen, können Ihre Ergebnisse anders lauten. Führen Sie deshalb stets eigene Leistungstests durch. Damit prüfen Sie die Ergebnisse gegen Ihre eigene Umgebung, Workloads und andere Faktoren.

```
-- Without parallel query
+------------+-------------+-------------+----------------+
| l_orderkey | revenue     | o_orderdate | o_shippriority |
+------------+-------------+-------------+----------------+
|   92511430 | 514726.4896 | 1995-03-06  |              0 |
.
.
|   28840519 | 454748.2485 | 1995-03-08  |              0 |
+------------+-------------+-------------+----------------+
10 rows in set (24 min 49.99 sec)
```

```
-- With parallel query
+------------+-------------+-------------+----------------+
| l_orderkey | revenue     | o_orderdate | o_shippriority |
+------------+-------------+-------------+----------------+
|   92511430 | 514726.4896 | 1995-03-06  |              0 |
.
.
|   28840519 | 454748.2485 | 1995-03-08  |              0 |
+------------+-------------+-------------+----------------+
10 rows in set (1 min 49.91 sec)
```

In vielen Beispielabfragen aus diesem Abschnitt werden Tabellen aus diesem TPC-H-Dataset verwendet, besonders häufig die PART-Tabelle mit 20 Millionen Zeilen und folgender Definition.

```
+---------------+---------------+------+-----+---------+-------+
| Field         | Type          | Null | Key | Default | Extra |
+---------------+---------------+------+-----+---------+-------+
| p_partkey     | int(11)       | NO   | PRI | NULL    |       |
| p_name        | varchar(55)   | NO   |     | NULL    |       |
| p_mfgr        | char(25)      | NO   |     | NULL    |       |
| p_brand       | char(10)      | NO   |     | NULL    |       |
| p_type        | varchar(25)   | NO   |     | NULL    |       |
| p_size        | int(11)       | NO   |     | NULL    |       |
```

```
| p_container   | char(10)      | NO   |     | NULL    |       |
| p_retailprice | decimal(15,2) | NO   |     | NULL    |       |
| p_comment     | varchar(23)   | NO   |     | NULL    |       |
+---------------+---------------+------+-----+---------+-------+
```

Durch Versuchsläufe mit Ihrer Workload gewinnen Sie ein Gefühl dafür, ob einzelne SQL-Anweisungen von Parallel Query profitieren. Anschließend können Sie mit den folgenden Überwachungstechniken nachprüfen, wie oft Parallel Query im Laufe der Zeit in echten Workloads verwendet wird. Für tatsächliche Workloads gelten zusätzliche Faktoren (z. B. Obergrenzen für gleichzeitige Abfragen).

Überwachen von Parallel Query

Wenn Ihr Aurora MySQL Cluster eine parallele Abfrage verwendet, wird möglicherweise eine Zunahme der `VolumeReadIOPS`-Werte. Parallel Query verwendet den Bufferpool nicht. Obwohl die Abfragen schnell sind, kann diese optimierte Verarbeitung zu einem Anstieg der Lesevorgänge und damit verbundenen Gebühren führen.

Neben den Amazon CloudWatch-Metriken (siehe Anzeigen von Metriken in der Amazon-RDS-Konsole) enthält Aurora auch verschiedene Statusvariable. Sie können diese globalen Statusvariablen verwenden, um die parallele Abfrageausführung zu überwachen. Sie können Ihnen Einblicke in die Gründe geben, warum der Optimierer die parallele Abfrage in einer bestimmten Situation verwendet oder nicht verwendet. Sie können diese Variablen mit dem Befehl `SHOW GLOBAL STATUS` abrufen. Eine Liste der Variablen finden Sie auch nachfolgend auf dieser Seite.

Eine parallele Abfragesitzung ist nicht notwendigerweise eine 1:1-Zuweisung mit den von der Datenbank durchgeführten Abfragen. Angenommen, Ihr Abfrageplan enthält zwei Schritte, die Parallel Query verwenden. In diesem Fall besteht die Abfrage aus zwei parallelen Sitzungen. Die Zähler für Aufrufversuche und erfolgreiche Aufrufe werden inkrementell jeweils um zwei erhöht.

Wenn Sie mit Parallel Query experimentieren und dabei `EXPLAIN`-Anweisungen herausgeben, kann sein, dass Zähleranstiege als "nicht ausgewählt" bezeichnet sind, obwohl die Abfragen nicht ausgeführt werden. Wenn Sie Parallel Query in einer Produktionsumgebung einsetzen, können Sie nachprüfen, ob die Meldung "nicht ausgewählt" schneller als erwartet zunimmt. An diesem Punkt können Sie sie so anpassen, dass die parallele Abfrage für die erwarteten Abfragen ausgeführt wird. Dazu können Sie Ihre Clustereinstellungen, den Abfragemix, DB-Instances, bei denen die parallele Abfrage aktiviert ist, usw. ändern.

Die Aktionen werden auf DB-Instance-Ebene nachverfolgt. Wenn Sie eine Verbindung zu einem anderen Endpunkt herstellen, könnten sich andere Metriken ergeben, weil jede DB-Instance ihre

eigenen Parallelabfragen ausführt. Unterschiedliche Metriken können sich auch dann ergeben, wenn sich der Leserendpunkt in jeder Sitzung mit einer anderen DB-Instance verbindet.

Name	Beschreibung
`Aurora_pq_bytes_returned`	Die Anzahl der Bytes, die in Zusammenhang mit Tupel-Datenstrukturen während der Parallelabfragen an den Hauptknoten übertragen wurden. Für den Abgleich mit durch 16 348 teile `Aurora_pq_pages_pushed_down` .
`Aurora_pq_max_concurrent_requests`	Die Höchstanzahl der Parallel Query-Sitzungen, die auf dieser Aurora-DB-Instance gleichzeitig ausgeführt werden können. Diese Zahl ist festgelegt und hängt von der AWS-DB-Instance-Klasse ab.
`Aurora_pq_pages_pushed_down`	Die Anzahl der Datenseiten (jeweils fix 16 KiB groß), auf denen Parallel Query eine netzwerkgebundene Übertragung an den Hauptknoten verhindert hat.
`Aurora_pq_request_attempted`	Die Anzahl der angeforderten Parallel Query-Sitzungen. Hinter diesem Wert können pro Abfrage mehrere Sitzungen stehen. Ausschlaggebend sind SQL-Konstrukte wie Unterabfragen und Join-Abfragen.
`Aurora_pq_request_executed`	Die Anzahl der erfolgreich ausgeführten Parallel Query-Sitzungen.
`Aurora_pq_request_failed`	Die Anzahl der Parallel Query-Sitzungen, die dem Client einen Fehler zurückgaben. Es kann vorkommen, dass eine angeforderte Parallelabfrage fehlschlägt – z. B. wegen eines Problems auf der Speicherschicht. In diesen Fällen wird der fehlgeschlagene Abfrageteil wiederholt. Dafür kommt der nicht-parallele

Name	Beschreibung
	Abfragemechanismus zum Einsatz. Wenn auch die wiederholte Abfrage fehlschlägt, wird dem Client ein Fehler zurückgegeben. Die Zähleranz eige erhöht sich.
`Aurora_pq_request_in_progress`	Die Anzahl der derzeit in Ausführung befindlic hen Parallel Query-Sitzungen. Die Zahl bezieht sich auf die angeschlossene Aurora-DB-Instance, mit der Sie verbunden sind, nicht auf das gesamte Aurora-DB-Cluster. Sie können prüfen, ob eine DB-Instance die Obergrenze für gleichzeitige Abfragen annähernd erreicht hat. Gleichen Sie dazu diesen Wert mit a `Aurora_pq_max_concurrent_re quests` .
`Aurora_pq_request_not_chosen`	Die Anzahl der Situationen, in denen Parallel Query nicht für die Abarbeitung einer Abfrage genutzt wurde. Dieser Wert setzt sich aus den Beiträgen mehrerer Zähler mit höherer Granularität zusammen. Die Zähleranzeige kann mit einer `EXPLAIN`-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächli ch ausgeführt wird.
`Aurora_pq_request_not_chose n_below_min_rows`	Die Anzahl der Situationen, in denen die Anzahl der Tabellenzeilen der Grund für den Nichteins atz von Parallel Query war. Die Zähleranzeige kann mit einer `EXPLAIN`-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächli ch ausgeführt wird.

Name	Beschreibung
`Aurora_pq_request_not_chosen_column_bit`	Die Anzahl der Parallelabfrageanforderungen, die aufgrund eines nicht unterstützten Datentyps in der Liste der projizierten Spalten den nicht-parallelen Abfrageverarbeitungspfad nutzen.
`Aurora_pq_request_not_chosen_column_geometry`	Die Anzahl der Parallelabfrageanforderungen, die den nicht-parallelen Abfrageverarbeitungspfad nutzen, da die Tabelle Spalten mit dem Datentyp `GEOMETRY` enthält. Informationen zu Aurora-MySQL-Versionen, die diese Einschränkung aufheben, finden Sie unter Upgrade paralleler Abfrage-Cluster auf Aurora-MySQL-Version 3.
`Aurora_pq_request_not_chosen_column_lob`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle Spalten mit einem `LOB`-Datentyp enthält oder `VARCHAR`-Spalten, die aufgrund der deklarierten Länge extern gespeichert werden. Informationen zu Aurora-MySQL-Versionen, die diese Einschränkung aufheben, finden Sie unter Upgrade paralleler Abfrage-Cluster auf Aurora-MySQL-Version 3.
`Aurora_pq_request_not_chosen_column_virtual`	Die Anzahl der Parallelabfrageanforderungen, die den nicht-parallelen Abfrageverarbeitungspfad nutzen, da die Tabelle eine virtuelle Spalte enthält.
`Aurora_pq_request_not_chosen_custom_charset`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle Spalten mit einem benutzerdefinierten Zeichensatz enthält.

Name	Beschreibung
`Aurora_pq_request_not_chose n_fast_ddl`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle zurzeit durch eine schnelle `ALTER`-DDL-Anweisung geändert wird.
`Aurora_pq_request_not_chosen_ few_pages_outside_buffer_pool`	Die Anzahl der Situationen, in denen Parallel Query nicht genutzt wurde, obwohl weniger als 95 Prozent der Tabellendaten im Bufferpool waren. Grund: Es gab zu wenig nicht gepufferte Tabellendaten. Eine Parallelabfrage lohnte sich deshalb nicht.
`Aurora_pq_request_not_chose n_full_text_index`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle Volltextindizes enthält.
`Aurora_pq_request_not_chosen_ high_buffer_pool_pct`	Die Anzahl der Situationen, in denen Parallel Query nicht genutzt wurde, weil ein hoher Anteil der Tabellendaten (derzeit >95 Prozent) bereits im Bufferpool war. In diesen Fällen entscheidet der Optimierer, dass das Lesen der Daten aus dem Bufferpool effizienter ist. Die Zähleranzeige kann mit einer `EXPLAIN`-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächlich ausgeführt wird.
`Aurora_pq_request_not_chose n_index_hint`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage einen Indexhinweis enthält.

Name	Beschreibung
`Aurora_pq_request_not_chosen_innodb_table_format`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle ein nicht unterstütztes InnoDB-Zeilenformat verwendet. Die parallele Aurora-Abfrage gilt nur für die `COMPACT`-, `REDUNDANT` - und `DYNAMIC`-Zeilenformate.
`Aurora_pq_request_not_chosen_long_trx`	Die Anzahl der Parallelabfrageanforderungen, die den nicht-parallelen Abfrageverarbeitungspfad nutzten, weil die Abfrage in einer lang laufenden Transaktion gestartet wurde. Die Zähleranzeige kann mit einer `EXPLAIN`-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächlich ausgeführt wird.
`Aurora_pq_request_not_chosen_no_where_clause`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage keine `WHERE`-Klausel enthält.
`Aurora_pq_request_not_chosen_range_scan`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage einen Bereichsscan für einen Index verwendet.
`Aurora_pq_request_not_chosen_row_length_too_long`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Gesamtlänge aller Spalten zu groß ist.

Name	Beschreibung
`Aurora_pq_request_not_chosen_small_table`	Die Anzahl der Situationen, in denen die Gesamtgröße der Tabelle (Zeilenanzahl und durchschnittliche Zeilenlänge) der Grund für den Nichteinsatz von Parallel Query war. Die Zähleranzeige kann mit einer `EXPLAIN`-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächlich ausgeführt wird.
`Aurora_pq_request_not_chosen_temporary_table`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage auf temporäre Tabellen verweist, die die nicht unterstützten Tabellentypen `MyISAM` oder `memory` verwenden.
`Aurora_pq_request_not_chosen_tx_isolation`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage eine nicht unterstützte Transaktionsisolationsstufe verwendet. Bei DB-Leser-Instances wird die parallele Abfrage nur auf die Isolationsstufen `REPEATABLE READ` und `READ COMMITTED` angewendet.
`Aurora_pq_request_not_chosen_update_delete_stmts`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage Teil einer `UPDATE`- oder `DELETE`-Anweisung ist.

Name	Beschreibung
`Aurora_pq_request_not_chosen_unsupported_access`	Die Anzahl der Parallelabfrageanforderungen, die den nicht-parallelen Abfrageverarbeitungspfad nutzen, weil die `WHERE`-Klausel nicht den Kriterien einer Parallelabfrage gerecht wird. Dieses Ergebnis kann eintreten, wenn für die Abfrage kein datenintensiver Scan erforderlich ist oder wenn es sich bei der Abfrage um eine `DELETE`- oder `UPDATE`-Anweisung handelt.
`Aurora_pq_request_not_chosen_unsupported_storage_type`	Die Anzahl der Parallelabfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da der DB-Cluster von Aurora MySQL keine unterstützte Aurora-Cluster-Speicherkonfiguration verwendet. Dieser Parameter ist in Aurora-MySQL-Version 3.04 und höher verfügbar. Weitere Informationen finden Sie unter Einschränkungen.
`Aurora_pq_request_throttled`	Die Anzahl der Situationen, in denen Parallel Query nicht genutzt wurde, weil die Höchstmenge gleichzeitiger Parallelabfragen bereits auf einer bestimmten Aurora-DB-Instance ausgeführt wird.

Zusammenwirken von Parallel Query und SQL-Konstrukten

Im folgenden Abschnitt finden Sie weitere Details dazu, warum bestimmte SQL-Anweisungen parallele Abfragen verwenden oder nicht verwenden. In diesem Abschnitt wird auch beschrieben, wie Aurora MySQL-Funktionen mit Parallel Query interagieren. Mit Hilfe dieser Informationen können Sie Leistungsprobleme in Clustern diagnostizieren, die Parallel Query verwenden. Außerdem können Sie nachvollziehen, wie Parallel Query auf Ihren spezifischen Workload angewendet wird.

Die Entscheidung für Parallel Query hängt von vielen Faktoren ab, die zu dem Zeitpunkt wirken, an dem die Anweisung ausgeführt wird. Es kann also sein, dass Parallel Query für bestimmte Abfragen immer, nie oder nur unter bestimmten Bedingungen zum Einsatz kommt.

> **Tip**
>
> Wenn Sie diese Beispiele in HTML anzeigen, können Sie das Widget Copy (Kopieren) in der oben rechts in jeder Codeverzeichnis verwenden, um den SQL-Code zu kopieren und es selbst zu versuchen. Durch die Verwendung des Widgets Copy (Kopieren) wird ein Kopieren der zusätzlichen Zeichen um die Aufforderung `mysql>` und die Fortsetzungszeilen `->` vermieden.

Themen

EXPLAIN-Anweisung

Wie aus den Beispielen aus diesem Abschnitt hervorgeht, gibt die `EXPLAIN`-Anweisung an, ob die jeweilige Stufe einer Abfrage derzeit parallelabfragetauglich ist. Darüber hinaus gibt sie auch an, welche Aspekte einer Abfrage auf die nächste Speicherschicht herabgestuft werden können. Die wichtigsten Bestandteile im Abfrageplan sind folgende:

- Wenn in der `NULL`-Spalte ein anderer Wert als `key` steht, liegt nahe, dass die Abfrage mit Index-Lookups effizient möglich ist. Der Einsatz von Parallel Query ist unwahrscheinlich.
- Wenn in der Spalte `rows` ein kleiner Wert steht (d. h. nicht im Millionenbereich), kann dies bedeuten, dass für die Abfrage zu wenig Daten verfügbar sind, als dass sich eine Parallelabfrage lohnen würde. Das bedeutet, dass eine parallele Abfrage unwahrscheinlich ist.
- Die Spalte `Extra` zeigt an, ob mit einer Parallelabfrage zu rechnen ist. Die Ausgabe kann in etwa wie im folgenden Beispiel aussehen.

  ```
  Using parallel query (A columns, B filters, C exprs; D extra)
  ```

  Die Zahl vor `columns` gibt an, wie viele Spalten im Abfrageblock hinterlegt sind.

  Die Zahl vor `filters` gibt an, wie viele `WHERE`-Prädikate einen einfachen Vergleich zwischen Spaltenwert und einer Konstante darstellen. Es können Größen wie „Gleichheit“ und „Ungleichheit“, aber auch Bereiche verglichen werden. Aurora parallelisiert diese Prädikattypen am effektivsten.

  Die Zahl vor `exprs` gibt die Anzahl der Ausdrücke (z. B. Funktionsaufrufe, Operatoren oder sonstige Ausdrücke) an, die auch parallelisiert werden können – wenn auch nicht so effektiv wie eine Filterbedingung.

  Die Zahl vor `extra` gibt an, wie viele Ausdrücke nicht herabgestuft werden können und deshalb vom Hauptknoten ausgeführt werden.

Betrachten Sie dazu die folgende `EXPLAIN`-Ausgabe.

```
mysql> explain select p_name, p_mfgr from part
    -> where p_brand is not null
    -> and upper(p_type) is not null
    -> and round(p_retailprice) is not null;
+----+-------------+-------+...+----------
+-------------------------------------------------------------------------------+
```

```
| id | select_type | table |...| rows     | Extra
                                |
+----+-------------+-------+...+----------
+-------------------------------------------------------------------------------+
|  1 | SIMPLE      | part  |...| 20427936 | Using where; Using parallel query (5
 columns, 1 filters, 2 exprs; 0 extra) |
+----+-------------+-------+...+----------
+-------------------------------------------------------------------------------+
```

Aus der `Extra`-Spalte geht hervor, dass aus jeder Zeile fünf Spalten extrahiert werden, mit denen die Abfragebedingungen bewertet und der Ergebnissatz konstruiert werden. Ein `WHERE`-Prädikat beinhaltet einen Filter – in diesem Fall eine Spalte, die direkt in der `WHERE`-Klausel getestet wird. Kommen zwei `WHERE`-Klauseln vor, müssen kompliziertere Ausdrücke bewertet werden (die in diesem Fall Funktionsaufrufe beinhalten). Das Feld `0 extra` bestätigt, dass alle Operationen in der `WHERE`-Klausel im Zuge der Parallelabfrageverarbeitung in die Speicherschicht herabgestuft werden.

Wird Parallel Query nicht ausgewählt, lässt sich der Grund dafür meist aus den anderen Spalten der `EXPLAIN`-Ausgabe ableiten. So kann möglicherweise sein, dass der `rows`-Wert zu klein ist oder dass die Spalte `possible_keys` angibt, dass die Abfrage statt auf einen datenintensiven Scan auf einen Index-Lookup zurückgreift. Das folgende Beispiel zeigt eine Abfrage, bei der der Optimierer schätzen kann, dass die Abfrage nur eine kleine Anzahl von Zeilen durchsucht. Dies erfolgt auf der Basis der Eigenschaften des Primärschlüssels. Eine Parallelabfrage ist deshalb nicht erforderlich.

```
mysql> explain select count(*) from part where p_partkey between 1 and 100;
+----+-------------+-------+-------+---------------+---------+---------+------+------
+--------------------------+
| id | select_type | table | type  | possible_keys | key     | key_len | ref  | rows |
 Extra                    |
+----+-------------+-------+-------+---------------+---------+---------+------+------
+--------------------------+
|  1 | SIMPLE      | part  | range | PRIMARY       | PRIMARY | 4       | NULL |   99 |
 Using where; Using index |
+----+-------------+-------+-------+---------------+---------+---------+------+------
+--------------------------+
```

Die Ausgabe mit Auskunft zur Verwendung von Parallel Query berücksichtigt alle Faktoren, die zu dem Zeitpunkt verfügbar waren, als die `EXPLAIN`-Anweisung ausgeführt wurde. Möglicherweise trifft der Optimierer zum Zeitpunkt der tatsächlichen Abfrageausführung eine andere Auswahl, wenn bis dahin eine andere Ausgangslage herrscht. `EXPLAIN` könnte beispielsweise melden, dass eine Anweisung Parallel Query verwendet. Wird die Abfrage später dann tatsächlich ausgeführt, könnte

sein, dass Parallel Query aufgrund der dann vorliegenden Bedingungen nicht nötig ist. Zu solchen Bedingungen können mehrere weitere parallele Abfragen gehören, die gleichzeitig ausgeführt werden. Es kann sich auch um Zeilen handeln, die aus der Tabelle gelöscht werden, um einen neuen Index, der erstellt wird, um zu viel Zeit, die in einer offenen Transaktion verstreicht, usw.

WHERE-Klausel

Damit die parallele Abfrageausführung genutzt werden kann, muss die Abfrage eine `WHERE`-Klausel enthalten.

Die parallele Abfrageausführung beschleunigt viele unterschiedliche Ausdrücke, die in der `WHERE`-Klausel vorkommen:

- Einfache Abgleiche zwischen einem Spaltenwert und einer Konstante (Filter). Bei diesen Abgleichen lohnt sich die Herabstufung auf die Speicherschicht am meisten. Wie viele Filterausdrücke in einer Abfrage vorkommen, ist in der `EXPLAIN`-Ausgabe zusammengefasst.
- Wo dies möglich ist, werden auch andere Ausdrücke aus der `WHERE`-Klausel in die Speicherschicht hinabgestuft. Wie viele solche Ausdrücke in einer Abfrage vorkommen, ist in der `EXPLAIN`-Ausgabe zusammengefasst. Bei diesen Ausdrücken kann es sich um Funktionsaufrufe, `LIKE`-Operatoren, `CASE`-Ausdrücke und Ähnliches handeln.
- Bestimmte Funktionen und Operatoren werden von Parallel Query derzeit noch nicht herabgestuft. Wie viele solche Ausdrücke in einer Abfrage vorkommen, wird mit dem `extra`-Zähler in der `EXPLAIN`-Ausgabe angegeben. Der Rest der Abfrage verwendet Parallel Query.
- Ausdrücke aus der Auswahlliste werden nicht herabgestuft. Für Abfragen mit solchen Funktionen kann es sich aber positiv auswirken, dass die Zwischenergebnisse von Parallelabfragen weniger Netzwerkdatenverkehr verursachen. So können beispielsweise Abfragen, die Aggregationsfunktionen aus der Auswahlliste aufrufen, von Parallelabfragen profitieren, selbst wenn die Aggregationsfunktionen selbst nicht herabgestuft werden.

Die nachfolgend abgebildete Abfrage scannt beispielsweise die gesamte Tabelle und verarbeitet alle Werte aus der `P_BRAND`-Spalte. Es handelt sich dabei allerdings nicht um eine Parallelabfrage, weil sie keine `WHERE`-Klausel enthält.

```
mysql> explain select count(*), p_brand from part group by p_brand;
+----+-------------+-------+------+---------------+------+---------+------+----------
+---------------------------------+
| id | select_type | table | type | possible_keys | key  | key_len | ref  | rows     |
 Extra                           |
```

```
+----+-------------+-------+------+---------------+------+---------+------+----------
+---------------------------------+
|  1 | SIMPLE      | part  | ALL  | NULL          | NULL | NULL    | NULL | 20427936 |
 Using temporary; Using filesort |
+----+-------------+-------+------+---------------+------+---------+------+----------
+---------------------------------+
```

Die nächste Abfrage enthält hingegen `WHERE`-Prädikate, die die Ergebnisse filtern. Deshalb ist eine Parallelabfrage möglich:

```
mysql> explain select count(*), p_brand from part where p_name is not null
    ->   and p_mfgr in ('Manufacturer#1', 'Manufacturer#3') and p_retailprice > 1000
    -> group by p_brand;
+----+...+----------
+-------------------------------------------------------------------------------------------
+
| id |...| rows     | Extra
                                          |
+----+...+----------
+-------------------------------------------------------------------------------------------
+
|  1 |...| 20427936 | Using where; Using temporary; Using filesort; Using parallel
 query (5 columns, 1 filters, 2 exprs; 0 extra) |
+----+...+----------
+-------------------------------------------------------------------------------------------
+
```

Wenn der Optimierer davon ausgeht, dass zu einem Abfrageblock nur wenige Zeilen zurückgegeben werden, wird Parallel Query für diesen Abfrageblock nicht verwendet. Im nachfolgenden Beispiel wird ein Größer-als-Operator in der Primärschlüssel-Spalte auf mehrere Millionen Zeilen angewendet. Das sorgt dafür, dass Parallel Query verwendet wird. Dagegen wird davon ausgegangen, dass die Kleiner-als-Gegenprobe nur auf wenige Zeilen anwendbar ist. Parallel Query kommt nicht zum Einsatz.

```
mysql> explain select count(*) from part where p_partkey > 10;
+----+...+----------
+-------------------------------------------------------------------------+
| id |...| rows     | Extra
          |
+----+...+----------
+-------------------------------------------------------------------------+
```

```
|  1 |...| 20427936 | Using where; Using parallel query (1 columns, 1 filters, 0 exprs;
 0 extra) |
+----+...+----------
+-------------------------------------------------------------------------------+

mysql> explain select count(*) from part where p_partkey < 10;
+----+...+------+--------------------------+
| id |...| rows | Extra                    |
+----+...+------+--------------------------+
|  1 |...|    9 | Using where; Using index |
+----+...+------+--------------------------+
```

Data Definition Language (DDL)

In Aurora-MySQL-Version 2 ist die parallele Abfrage nur für Tabellen verfügbar, für die keine schnellen DDL-Vorgänge (Data Definition Language) anstehen. In Aurora-MySQL-Version 3 können Sie eine parallele Abfrage für eine Tabelle gleichzeitig mit einem sofortigen DDL-Vorgang verwenden.

Instant DDL in Aurora-MySQL-Version 3 ersetzt die schnelle DDL-Funktion in Aurora-MySQL-Version 2. Informationen zu Instant-DDL finden Sie unter Sofortige DDL (Aurora MySQL Version 3).

Spaltendatentypen

In Aurora-MySQL-Version 3 kann die parallele Abfrage mit Tabellen arbeiten, die Spalten mit den Datentypen `TEXT`, `BLOB`, `JSON` und `GEOMETRY` enthalten. Es kann auch mit `VARCHAR`- und `CHAR`-Spalten mit einer maximalen deklarierten Länge von mehr als 768 Byte arbeiten. Wenn sich Ihre Abfrage auf Spalten bezieht, die so große Objekttypen enthalten, erhöht die zusätzliche Arbeit zum Abrufen der Abfrageverarbeitung einen gewissen Aufwand. Überprüfen Sie in diesem Fall, ob die Abfrage die Verweise auf diese Spalten weglassen kann. Wenn dies nicht der Fall ist, führen Sie Benchmarks aus, um zu bestätigen, ob solche Abfragen schneller sind, wenn die parallele Abfrage aktiviert oder deaktiviert ist.

In Aurora-MySQL-Version 2 hat die parallele Abfrage folgende Einschränkungen für große Objekttypen:

- Die Datentypen `TEXT`, `BLOB`, `JSON` und `GEOMETRY` werden von parallelen Abfragen nicht unterstützt. Eine Abfrage, die sich auf Spalten dieses Typs bezieht, kann keine parallelen Abfragen nutzen.
- Spalten unterschiedlicher Länge (Datentypen `VARCHAR` und `CHAR`) sind bis zur deklarierten Länge (max. 768 Byte) mit Parallel Query kompatibel. Eine Abfrage, die sich auf Spalten der Typen

bezieht, die mit mehr Höchstlänge deklariert sind, kann Parallel Query nicht nutzen. In Spalten, in denen Zeichensätze mit mehreren Byte Länge vorkommen, ist im Byte-Höchstwert die maximale Byte-Anzahl des Zeichensatzes berücksichtigt. Für eine `utf8mb4`-Spalte mit dem Zeichensatz `VARCHAR(192)` (maximal 4 Byte Zeichenlänge) kann beispielsweise eine Parallelabfrage gestartet werden, nicht jedoch für eine `VARCHAR(193)`-Spalte.

Partitionierte Tabellen

In Aurora-MySQL-Version 3 können Sie partitionierte Tabellen mit Parallel Query verwenden. Da partitionierte Tabellen intern als mehrere kleinere Tabellen dargestellt werden, verwendet eine Abfrage, die eine parallele Abfrage für eine nicht partitionierte Tabelle verwendet, möglicherweise keine parallele Abfrage für eine identische partitionierte Tabelle. Aurora MySQL prüft, ob jede Partition groß genug ist, um sich für die parallele Abfrageoptimierung zu qualifizieren, anstatt die Größe der gesamten Tabelle auszuwerten. Prüfen Sie, ob die Statusvariable `Aurora_pq_request_not_chosen_small_table` inkrementiert wird, wenn eine Abfrage in einer partitionierten Tabelle die parallele Abfrage nicht wie erwartet verwendet.

Betrachten Sie beispielsweise eine Tabelle, die mit `PARTITION BY HASH (`*`column`*`) PARTITIONS 2` partitioniert ist, und eine andere Tabelle, die mit `PARTITION BY HASH (`*`column`*`) PARTITIONS 10` partitioniert ist. In der Tabelle mit zwei Partititionen sind die Partitionen fünfmal so groß wie die Tabelle mit zehn Partitionen. Daher wird eine parallele Abfrage eher für Abfragen gegen die Tabelle mit weniger Partitionen verwendet. Im folgenden Beispiel hat die Tabelle `PART_BIG_PARTITIONS` zwei Partitionen und `PART_SMALL_PARTITIONS` hat zehn Partitionen. Bei identischen Daten wird eine parallele Abfrage eher für die Tabelle mit weniger großen Partitionen verwendet.

```
mysql> explain select count(*), p_brand from part_big_partitions where p_name is not
 null
    ->   and p_mfgr in ('Manufacturer#1', 'Manufacturer#3') and p_retailprice > 1000
 group by p_brand;
+----+-------------+--------------------+-----------
+-------------------------------------------------------------------------------------------------
+
| id | select_type | table              | partitions | Extra
                                                                                                 |
+----+-------------+--------------------+-----------
+-------------------------------------------------------------------------------------------------
+
```

```
|  1 | SIMPLE      | part_big_partitions | p0,p1      | Using where; Using temporary;
 Using parallel query (4 columns, 1 filters, 1 exprs; 0 extra; 1 group-bys, 1 aggrs) |
+----+-------------+---------------------+------------
+-------------------------------------------------------------------------------------
+

mysql> explain select count(*), p_brand from part_small_partitions where p_name is not
 null
    ->   and p_mfgr in ('Manufacturer#1', 'Manufacturer#3') and p_retailprice > 1000
 group by p_brand;
+----+-------------+----------------------+------------------------------
+------------------------------+
| id | select_type | table                | partitions                   | Extra
                   |
+----+-------------+----------------------+------------------------------
+------------------------------+
|  1 | SIMPLE      | part_small_partitions | p0,p1,p2,p3,p4,p5,p6,p7,p8,p9 | Using
 where; Using temporary |
+----+-------------+----------------------+------------------------------
+------------------------------+
```

Aggregationsfunktionen, GROUP BY-Klauseln und HAVING-Klauseln

In Abfragen mit Aggregationsfunktionen werden große Tabellen mit sehr vielen Zeilen gescannt. Sie eignen sich deshalb oft besonders gut für Parallelabfragen.

In Aurora MySQL 3 kann eine parallele Abfrage Aggregatfunktionsaufrufe in der Auswahlliste und der Klausel `HAVING` optimieren.

Vor Aurora MySQL 3 werden Aggregatfunktionsaufrufe in der Auswahlliste oder der Klausel `HAVING` nicht auf die Speicherschicht übertragen. Eine parallele Abfrage kann dennoch die Leistung solcher Abfragen mit Aggregationsfunktionen verbessern – indem sie zuerst auf der Speicherschicht Spaltenwerte aus den Rohdatenseiten parallel extrahiert. Anschließend überträgt Parallel Query diese Werte in einem kompakten Tupelformat an den Hauptknoten zurück und nicht als vollständige Datenseiten. Wie immer muss die Abfrage mindestens 1 `WHERE`-Prädikat enthalten, das für Parallel Query aktiviert ist.

Die nachfolgenden einfach gehaltenen Beispiele veranschaulichen, welche aggregierte Abfragen von Parallel Query profitieren. Dies gilt zum einen durch Rückgabe unmittelbarer, kompakt gehaltener Ergebnisse an den Hauptknoten und eventuell zusätzlich durch Herausfilterung nicht passender Zeilen aus den Zwischenergebnissen.

```
mysql> explain select sql_no_cache count(distinct p_brand) from part where p_mfgr =
 'Manufacturer#5';
+----+...+-----------------------------------------------------------------------------+
| id |...| Extra                                                                       |
+----+...+-----------------------------------------------------------------------------+
|  1 |...| Using where; Using parallel query (2 columns, 1 filters, 0 exprs; 0 extra) |
+----+...+-----------------------------------------------------------------------------+

mysql> explain select sql_no_cache p_mfgr from part where p_retailprice > 1000 group by
 p_mfgr having count(*) > 100;
+----+...
+-------------------------------------------------------------------------------------------------
+
| id |...| Extra
                                  |
+----+...
+-------------------------------------------------------------------------------------------------
+
|  1 |...| Using where; Using temporary; Using filesort; Using parallel query (3
 columns, 0 filters, 1 exprs; 0 extra) |
+----+...
+-------------------------------------------------------------------------------------------------
+
```

Funktionsaufrufe in WHERE-Klausel

Aurora kann die Optimierung der parallelen Abfrageausführung auf Aufrufe der meisten integrierten Funktionen der `WHERE`-Klausel anwenden. Durch die Parallelisierung dieser Funktionsaufrufe wird der Hauptknoten entlastet, weil etwas CPU-Arbeitslast entfällt. Die parallel ablaufende Bewertung der Prädikatfunktionen in der ersten Abfragephase ermöglicht es Aurora, die Datenmenge zu minimieren, die im späteren Verlauf übertragen und verarbeitet werden muss.

Aktuell werden nicht alle Funktionsaufrufe aus der Auswahlliste parallelisiert. Diese Funktionen werden vom Hauptknoten auch dann bewertet, wenn in der `WHERE`-Klausel dieselben Funktionsaufrufe enthalten sind. Die ursprünglichen Werte aus betroffenen Spalten werden in die Tupel aufgenommen, die vom Speicherknoten zum Hauptknoten zurückübertragen werden. Der Hauptknoten führt alle Transformationen aus, z. B. `UPPER`, `CONCATENATE` usw., und generiert die endgültigen Werte für den Abfragesatz.

Im folgenden Beispiel parallelisiert Parallel Query den Aufruf von LOWER, da diese Funktion in der WHERE-Klausel enthalten ist. Parallel Query wirkt sich nicht auf die Aufrufe von SUBSTR und UPPER aus, da sie in der Auswahlliste stehen.

```
mysql> explain select sql_no_cache distinct substr(upper(p_name),1,5) from part
    -> where lower(p_name) like '%cornflower%' or lower(p_name) like '%goldenrod%';
+----+...
+-------------------------------------------------------------------------------------------
+
| id |...| Extra
                |
+----+...
+-------------------------------------------------------------------------------------------
+
|  1 |...| Using where; Using temporary; Using parallel query (2 columns, 0 filters, 1
 exprs; 0 extra) |
+----+...
+-------------------------------------------------------------------------------------------
+
```

Die gleichen Überlegungen gelten für andere Ausdrücke wie CASE-Ausdrücke oder LIKE-Operatoren. Im der folgenden Beispiel ist beispielsweise zu sehen, dass die parallele Abfrage in der CASE-Klausel den LIKE-Ausdruck und die WHERE-Operatoren evaluiert.

```
mysql> explain select p_mfgr, p_retailprice from part
    -> where p_retailprice > case p_mfgr
    ->   when 'Manufacturer#1' then 1000
    ->   when 'Manufacturer#2' then 1200
    ->   else 950
    -> end
    -> and p_name like '%vanilla%'
    -> group by p_retailprice;
+----+...
+-------------------------------------------------------------------------------------------
+
| id |...| Extra
                                |
+----+...
+-------------------------------------------------------------------------------------------
+
|  1 |...| Using where; Using temporary; Using filesort; Using parallel query (4
 columns, 0 filters, 2 exprs; 0 extra) |
```

```
+----+...
+-------------------------------------------------------------------------------------------------
+
```

LIMIT-Klausel

Derzeit können Abfrageblöcke mit `LIMIT`-Klausel nicht parallel abgefragt werden. Parallel Query könnte jedoch für frühere Abfragephasen mit `GROUP BY`, `ORDER BY` oder Join-Abfragen geeignet sein.

Vergleichsoperatoren

Der Optimierer schätzt ab, wie viele Zeilen gescannt werden müssen, um die Vergleichsoperatoren bewerten zu können, und entscheidet ausgehend von dieser Schätzung, ob Parallel Query verwendet wird.

Das erste Beispiel belegt, dass ein Gleichheitsvergleich gegen die Hauptschlüsselspalte effizient ohne Parallel Query möglich ist. Das zweite Beispiel belegt, dass für einen ähnlichen Vergleich gegen eine nicht indizierte Spalte mehrere Millionen Zeilen gescannt werden müssen. Parallel Query lohnt sich deshalb.

```
mysql> explain select * from part where p_partkey = 10;
+----+...+------+-------+
| id |...| rows | Extra |
+----+...+------+-------+
|  1 |...|    1 | NULL  |
+----+...+------+-------+

mysql> explain select * from part where p_type = 'LARGE BRUSHED BRASS';
+----+...+----------
+-------------------------------------------------------------------------------+
| id |...| rows     | Extra
          |
+----+...+----------
+-------------------------------------------------------------------------------+
|  1 |...| 20427936 | Using where; Using parallel query (9 columns, 1 filters, 0 exprs;
 0 extra) |
+----+...+----------
+-------------------------------------------------------------------------------+
```

Die gleichen Kriterien gelten für "ist ungleich"-Prüfungen und Bereichsvergleiche (z. B. kleiner als, größer als, ist gleich oder `BETWEEN`. Der Optimierer schätzt ab, wie viele Zeilen zu scannen sind, und entscheidet dann, ob sich eine parallele Abfrage angesichts des E/A-Gesamt-Volumens lohnt.

Joins

Join-Abfragen mit großen Tabellen sind in der Regel datenintensive Operationen, die von der Optimierung der parallelen Abfrageausführung profitieren. Derzeit werden Vergleiche von Spaltenwerten aus mehreren Tabellen (also die Join-Prädikate) nicht parallelisiert. Parallel Query kann allerdings einen Teil der internen Verarbeitung aus anderen Join-Phasen herunterstufen – z. B. die Erstellung des Bloom-Filters während eines Hash-Join. Parallel Query kann auch ohne `WHERE`-Klausel auf Join-Abfragen angewendet werden. Join-Abfragen sind in dieser Hinsicht Ausnahmen von der Regel, dass Parallelabfragen ohne `WHERE`-Klausel nicht möglich sind.

Jede Phase der Join-Verarbeitung wird ausgewertet, um festzustellen, ob sie für eine Parallelabfrage in Frage kommt. Falls mehrere Phasen parallelabfragetauglich sind, werden sie nacheinander ausgeführt. Was die Obergrenze für gleichzeitige Abfragen angeht, bedeutet dies, dass jede Join-Abfrage als separate Parallelabfragesitzung zählt.

Wenn eine Join-Abfrage beispielsweise mit `WHERE`-Prädikaten die Zeilen einer verknüpften Tabelle filtert, kann diese Filteroption Parallel Query verwenden. Ein weiteres Beispiel ist die Verknüpfung einer großen mit einer kleinen Tabelle mittels Hash-Join in einer Join-Abfrage. In diesem Fall kann der Tabellenscan für die Generierung der Datenstruktur des Bloom-Filters Parallel Query möglicherweise verwenden.

> **Note**
>
> Parallele Abfragen werden typischerweise für ressourcenintensive Abfragen verwendet, die von der Hash-Join-Optimierung profitieren. Die Methode zum Einschalten der Hash-Join-Optimierung hängt von der Aurora-MySQL-Version ab. Einzelheiten zu den einzelnen Versionen finden Sie unter Hash-Join für parallele Abfrage-Cluster aktivieren. Informationen zur effektiven Verwendung von Hash-Joins finden Sie unter Optimierung von großen Aurora-MySQL-Join-Abfragen mit Hash-Joins.

```
mysql> explain select count(*) from orders join customer where o_custkey = c_custkey;
+----+...+----------+-------+--------------+-------------+...+-----------
+-------------------------------------------------------------------------------------------
+
```

```
| id |...| table    | type  | possible_keys | key         |...| rows      | Extra

              |
+----+...+----------+-------+---------------+-------------+...+-----------
+-------------------------------------------------------------------------------------------
+
|  1 |...| customer | index | PRIMARY       | c_nationkey |...|  15051972 | Using index

              |
|  1 |...| orders   | ALL   | o_custkey     | NULL        |...| 154545408 | Using join
 buffer (Hash Join Outer table orders); Using parallel query (1 columns, 0 filters, 1
 exprs; 0 extra) |
+----+...+----------+-------+---------------+-------------+...+-----------
+-------------------------------------------------------------------------------------------
+
```

In Join-Abfragen, die mit geschachtelten Schleifen arbeiten, könnte der äußerste geschachtelte Schleifenblock parallele Abfragen verwenden. Die Anwendung von parallelen Abfragen hängt von den gleichen Faktoren wie immer ab, z. B. dem Vorhandensein zusätzlicher Filterbedingungen in der `WHERE`-Klausel.

```
mysql> -- Nested loop join with extra filter conditions can use parallel query.
mysql> explain select count(*) from part, partsupp where p_partkey != ps_partkey and
 p_name is not null and ps_availqty > 0;
+----+-------------+----------+...+----------
+-------------------------------------------------------------------------------+
| id | select_type | table    |...| rows     | Extra
                                 |
+----+-------------+----------+...+----------
+-------------------------------------------------------------------------------+
|  1 | SIMPLE      | part     |...| 20427936 | Using where; Using parallel query (2
 columns, 1 filters, 0 exprs; 0 extra) |
|  1 | SIMPLE      | partsupp |...| 78164450 | Using where; Using join buffer (Block
 Nested Loop)                       |
+----+-------------+----------+...+----------
+-------------------------------------------------------------------------------+
```

Unterabfragen

Der äußere Abfrageblock und der innere Unterabfrageblock können jeweils parallele Abfragen verwenden oder nicht. Ob sie dies tun, ist für jeden Block von den gewöhnlichen Eigenschaften

der Tabelle, der WHERE-Klausel usw. abhängig. In der folgenden Abfrage kommt Parallel Query am Unterabfrageblock zum Einsatz, nicht jedoch am Außenblock.

```
mysql> explain select count(*) from part where
   --> p_partkey < (select max(p_partkey) from part where p_name like '%vanilla%');
+----+-------------+...+----------
+-------------------------------------------------------------------------------+
| id | select_type |...| rows     | Extra
                       |
+----+-------------+...+----------
+-------------------------------------------------------------------------------+
|  1 | PRIMARY     |...|     NULL | Impossible WHERE noticed after reading const tables
                      |
|  2 | SUBQUERY    |...| 20427936 | Using where; Using parallel query (2 columns, 0
 filters, 1 exprs; 0 extra) |
+----+-------------+...+----------
+-------------------------------------------------------------------------------+
```

Für korrelierte Unterabfragen steht die Optimierung der parallelen Abfrageausführung nicht zur Verfügung.

UNION

Jeder Abfrageblock einer UNION-Abfrage kann parallele Abfragen Query nutzen (oder nicht). Ausschlaggebend sind die Tabelleneigenschaften und die WHERE-Klausel usw. des jeweiligen UNION-Teils.

```
mysql> explain select p_partkey from part where p_name like '%choco_ate%'
    -> union select p_partkey from part where p_name like '%vanil_a%';
+----+---------------+...+----------
+-------------------------------------------------------------------------------+
| id | select_type   |...| rows     | Extra
                         |
+----+---------------+...+----------
+-------------------------------------------------------------------------------+
|  1 | PRIMARY       |...| 20427936 | Using where; Using parallel query (2 columns, 0
 filters, 1 exprs; 0 extra) |
|  2 | UNION         |...| 20427936 | Using where; Using parallel query (2 columns, 0
 filters, 1 exprs; 0 extra) |
| NULL | UNION RESULT | <union1,2> |...|     NULL | Using temporary
                       |
```

```
+----+--------------+...+----------
+-------------------------------------------------------------------------------+
```

> **Note**
>
> Die `UNION`-Klauseln in der Abfrage werden nacheinander ausgeführt. Selbst wenn die Abfrage mehrstufig ist und in jeder Phase Parallel Query zum Einsatz kommt, führt sie Parallel Query jedes Mal separat aus. Deshalb gilt mit Hinblick auf die Höchstzahl gleichzeitig zulässiger Parallelabfragen auch eine komplexe mehrstufige Abfrage nur als 1 Abfrage.

Ansichten

Der Optimierer verwendet beim Umschreiben jeder Abfrage eine Ansicht als längere Abfrage. Dazu werden die zugrunde liegenden Tabellen verwendet. Das bedeutet, dass die Funktionsweise von Parallel Query unabhängig von der Tabellenreferenz (Ansicht oder tatsächliche Tabelle) gleich ist. Für die fertige umgeschriebene Abfrage gelten die gleichen Kriterien hinsichtlich der Verwendung von Parallel Query für eine Abfrage und hinsichtlich der Herabstufung einzelner Teile.

Beispielsweise zeigt der folgende Abfrageplan eine Ansichtsdefinition, die Parallel Query in der Regel nicht verwendet. Erst wenn die Ansicht mit zusätzlichen `WHERE`-Klauseln abgefragt wird, verwendet Aurora MySQL Parallel Query.

```
mysql> create view part_view as select * from part;
mysql> explain select count(*) from part_view where p_partkey is not null;
+----+...+----------
+-------------------------------------------------------------------------------+
| id |...| rows     | Extra
          |
+----+...+----------
+-------------------------------------------------------------------------------+
|  1 |...| 20427936 | Using where; Using parallel query (1 columns, 0 filters, 0 exprs;
 1 extra) |
+----+...+----------
+-------------------------------------------------------------------------------+
```

DML-Anweisungen (Data Manipulation Language)

Die `INSERT`-Anweisung kann Parallel Query für die `SELECT`-Verarbeitungsphase verwenden, wenn der `SELECT`-Teil die sonstigen Bedingungen für eine Parallelabfrage erfüllt.

```
mysql> create table part_subset like part;
mysql> explain insert into part_subset select * from part where p_mfgr =
 'Manufacturer#1';
+----+...+----------
+-------------------------------------------------------------------------------+
| id |...| rows     | Extra
          |
+----+...+----------
+-------------------------------------------------------------------------------+
|  1 |...| 20427936 | Using where; Using parallel query (9 columns, 1 filters, 0 exprs;
 0 extra) |
+----+...+----------
+-------------------------------------------------------------------------------+
```

> **Note**
>
> In der Regel liegen die Daten zu den neu eingefügten Zeilen nach der `INSERT`-Anweisung im Bufferpool. Deshalb kann sein, dass eine Tabelle unmittelbar nach dem Einfügen vieler Zeilen nicht für Parallel Query in Frage kommt. Erst wenn die Daten im normalen Betrieb aus dem Bufferpool entfernt wurden, können in Abfragen gegen die Tabelle wieder Parallelabfragen zum Einsatz kommen.

Die `CREATE TABLE AS SELECT`-Anweisung greift nicht auf Parallel Query zurück – auch dann nicht, wenn der `SELECT`-Teil der Anweisung ansonsten parallelabfragefähig ist. Diese Anweisung ist wegen ihres DDL-Anteils nicht für die Parallelabfrageverarbeitung geeignet. Dagegen kann der `INSERT ... SELECT`-Teil der `SELECT`-Anweisung Parallel Query verwenden.

Parallel Query wird nie verwendet, wenn `DELETE`- oder `UPDATE`-Anweisungen vorliegen. Dies gilt unabhängig von der Größe der Tabelle und der Prädikate aus der `WHERE`-Klausel.

```
mysql> explain delete from part where p_name is not null;
+----+-------------+...+----------+-------------+
| id | select_type |...| rows     | Extra       |
+----+-------------+...+----------+-------------+
|  1 | SIMPLE      |...| 20427936 | Using where |
+----+-------------+...+----------+-------------+
```

Transaktionen und Sperren

Sie können alle Isolationsebenen auf der primären Aurora-Instance verwenden.

Auf Aurora-Reader-DB-Instances gilt die parallele Abfrage für Anweisungen, die unter der `REPEATABLE READ`-Isolierungsstufe ausgeführt werden. Aurora MySQL-Versionen 2.09 oder höher können die `READ COMMITTED`-Isolierungsstufe auch auf Reader-DB-Instances verwenden. `REPEATABLE READ` ist die Standardisolierungsstufe für Aurora-Reader-DB-Instances. Um die Isolierungsstufe `READ COMMITTED` auf DB-Leser-Instances anzuwenden, muss die Konfigurationsoption `aurora_read_replica_read_committed` auf Sitzungsebene festgelegt werden. Die Isolierungsstufe `READ COMMITTED` für Reader-Instances entspricht dem SQL-Standardverhalten. Die Isolierung ist jedoch bei Reader-Instances weniger streng als bei Abfragen, welche die `READ COMMITTED`-Isolierungsstufe bei der Writer-Instance verwenden.

Weitere Informationen zu Aurora-Isolierungsstufen, insbesondere zu den Unterschieden in `READ COMMITTED` zwischen Writer- und Reader-Instances, finden Sie unter Aurora MySQL-Isolierungsstufen.

Nach Abschluss einer großen Transaktion kann es sein, dass die Tabellenstatistik veraltet ist. Für solche Statistiken ist möglicherweise eine `ANALYZE TABLE`-Anweisung erforderlich, damit Aurora die Zeilenzahl zuverlässig schätzen kann. Auch mit Hilfe einer umfangreichen DML-Anweisung könnte ein beträchtlicher Teil der Tabellendaten in den Bufferpool gelangen. Sind diese Daten im Bufferpool kann sein, dass diese Tabelle weniger häufig von Parallel Query abgefragt wird. Dies ändert sich, wenn die Daten aus dem Pool entfernt sind.

Wenn Ihre Sitzung Teil einer langwierigen Transaktion (standardmäßig 10 Minuten) ist, verwenden weitere Abfragen aus dieser Sitzung keine Parallelabfragen. Eine einzelne lang laufende Abfrage kann auch wegen Zeitüberschreitung abgebrochen werden. Dieser Überschreitungsabbruch kann eintreten, wenn die Abfrage länger läuft als zulässig (Höchstdauer derzeit: 10 Minuten), bevor die Parallelverarbeitung der Abfragen beginnt.

Das Risiko, dass lang laufende Transaktionen ungewollt gestartet werden, kann reduziert werden. Legen Sie dazu in `autocommit=1`-Sitzungen, in denen Sie Ad-hoc-Abfragen durchführen, die Einstellung `mysql` fest. Selbst eine `SELECT`-Anweisung gegen eine Tabelle startet eine Transaktion, indem sie eine Leseansicht erstellt. Eine Leseansicht ist ein einheitlicher Datensatz für nachfolgende Abfragen. Dieser bleibt bestehen, bis die Transaktion übernommen wurde. Denken Sie an diese Einschränkung, wenn Aurora für JDBC- oder ODBC-Anwendungen verwendet wird. Solche Anwendungen könnten nämlich auch dann zur Ausführung kommen, wenn die Einstellung `autocommit` deaktiviert ist.

Im nachfolgenden Beispiel ist zu sehen, wie eine Abfrageausführung gegen eine Tabelle (Einstellung `autocommit` deaktiviert) eine Leseansicht erzeugt, die implizit eine Transaktion in Gang setzt. Abfragen, die kurz danach gestartet werden, können Parallel Query noch nutzen. Nach mehreren Minuten kommen Abfragen jedoch nicht mehr für Parallel Query in Frage. Wenn Sie ans Ende der Transaktion `COMMIT` oder `ROLLBACK` stellen, kann Parallel Query wieder ausgeführt werden.

```
mysql> set autocommit=0;

mysql> explain select sql_no_cache count(*) from part where p_retailprice > 10.0;
+----+...+---------
+-------------------------------------------------------------------------------+
| id |...| rows    | Extra
         |
+----+...+---------
+-------------------------------------------------------------------------------+
|  1 |...| 2976129 | Using where; Using parallel query (1 columns, 1 filters, 0 exprs;
 0 extra) |
+----+...+---------
+-------------------------------------------------------------------------------+

mysql> select sleep(720); explain select sql_no_cache count(*) from part where
 p_retailprice > 10.0;
+------------+
| sleep(720) |
+------------+
|          0 |
+------------+
1 row in set (12 min 0.00 sec)

+----+...+---------+-------------+
| id |...| rows    | Extra       |
+----+...+---------+-------------+
|  1 |...| 2976129 | Using where |
+----+...+---------+-------------+

mysql> commit;

mysql> explain select sql_no_cache count(*) from part where p_retailprice > 10.0;
+----+...+---------
+-------------------------------------------------------------------------------+
| id |...| rows    | Extra
         |
```

```
+----+...+---------
+-------------------------------------------------------------------------+
|  1 |...| 2976129 | Using where; Using parallel query (1 columns, 1 filters, 0 exprs;
 0 extra) |
+----+...+---------
+-------------------------------------------------------------------------+
```

Um festzustellen, wie oft Abfragen nicht für Parallel Query in Frage kamen, weil sie Teil lang laufender Transaktionen waren, untersuchen Sie die Statusvariable `Aurora_pq_request_not_chosen_long_trx`.

```
mysql> show global status like '%pq%trx%';
+---------------------------------------+-------+
| Variable_name                         | Value |
+---------------------------------------+-------+
| Aurora_pq_request_not_chosen_long_trx | 4     |
+-------------------------------+-------+
```

`SELECT`-Anweisungen, die Sperren annehmen (z. B. Syntax `SELECT FOR UPDATE` oder `SELECT LOCK IN SHARE MODE`), können Parallel Query nicht verwenden.

Parallel Query kann an Tabellen funktionieren, die mit einer `LOCK TABLES`-Anweisung gesperrt sind.

```
mysql> explain select o_orderpriority, o_shippriority from orders where o_clerk =
 'Clerk#000095055';
+----+...+-----------
+-------------------------------------------------------------------------+
| id |...| rows      | Extra
          |
+----+...+-----------
+-------------------------------------------------------------------------+
|  1 |...| 154545408 | Using where; Using parallel query (3 columns, 1 filters, 0
 exprs; 0 extra) |
+----+...+-----------
+-------------------------------------------------------------------------+

mysql> explain select o_orderpriority, o_shippriority from orders where o_clerk =
 'Clerk#000095055' for update;
+----+...+-----------+-------------+
| id |...| rows      | Extra       |
+----+...+-----------+-------------+
|  1 |...| 154545408 | Using where |
```

```
+----+...+-----------+-------------+
```

B-Baum-Indizes

Die von der `ANALYZE TABLE`-Anweisung erfassten Statistiken unterstützen den Optimierer bei der Entscheidung für Parallelabfragen oder Index-Lookups. Ausschlaggebend sind die Eigenschaften der Daten in den Spalten. Nach DML-Operationen können die Daten einer Tabelle nachhaltig verändert sein. Um die Statistiken auf dem aktuellen Stand zu halten, führen Sie nach der Operation `ANALYZE TABLE` aus.

Wenn Index-Lookups ausreichen, um eine Abfrage effizient ohne datenintensiven Scan auszuführen, verwendet Aurora möglicherweise Index-Lookups. Dadurch erübrigt sich der Zusatzaufwand der Parallelabfrageverarbeitung. Außerdem regeln Obergrenzen, wie viele Abfragen gleichzeitig in einem Aurora-DB-Cluster zulässig sind. Die Einhaltung bewährter Methoden bei der Indizierung von Tabellen trägt dazu bei, dass in den häufigsten und besonders oft gleichzeitig ausgeführten Abfragen Index-Lookups zur Anwendung kommen.

Volltextsuche (FTS)-Indizes

Zurzeit wird Parallel Query nicht für Tabellen mit Volltextsuchindex verwendet. Dies gilt unabhängig davon, ob sich die Abfrage auf solche indizierten Spalten bezieht oder ob sie den Operator `MATCH` verwendet.

Virtuelle Spalten

Zurzeit wird Parallel Query nicht für Tabellen verwendet, die eine virtuelle Spalte enthalten. Dies gilt unabhängig davon, ob die Abfrage auf virtuelle Spalten verweist.

Integrierte Caching-Mechanismen

Aurora enthält integrierte Caching-Mechanismen: den Bufferpool und den Abfrage-Cache. Der Aurora-Optimierer entscheidet, ob einer dieser Caching-Mechanismen oder Parallel Query für eine bestimmte Abfrage besser geeignet ist.

Wenn eine Parallelabfrage Zeilen filtert und Spaltenwerte transformiert/extrahiert, werden Daten als Tupel an den Hauptknoten zurückübertragen – nicht als Datenseiten. Das bedeutet also, dass bei Verwendung von Parallel Query dem Bufferpool keine Seiten hinzugefügt werden. Es werden auch keine Seiten entfernt, die bereits im Bufferpool sind.

Aurora überprüft die Anzahl der Tabellendatenseiten, die im Pufferpool vorhanden sind und welchen Anteil der Tabellendaten diese Zahl darstellt. Aurora verwendet diese Informationen, um

zu bestimmen, ob es effizienter ist, parallele Abfragen zu verwenden (und die Daten im Pufferpool zu umgehen). Es ist auch möglich, dass Aurora den nicht-parallelen Abfrageverarbeitungspfad verwendet, der auf Daten aus dem Bufferpool zurückgreift. Welche Seiten im Cache abgelegt sind und wie sich datenintensive Abfragen auf das Caching und die Bereinigung auswirken, hängt von den Konfigurationseinstellungen des Bufferpools ab. Es kann deshalb schwierig vorherzusagen sein, ob eine Abfrage mit Parallel Query ausgeführt wird. Dies hängt von den Daten im Bufferpool ab, deren Zusammensetzung sich ständig ändert.

Außerdem begrenzt Aurora, wie viele Parallelabfragen gleichzeitig möglich sind. Parallel Query kommt nicht für jede Abfrage zum Einsatz. Deshalb befinden sich die Daten von Tabellen, die von mehreren Abfragen gleichzeitig genutzt werden, zu einem beträchtlichen Teil im Bufferpool. Dementsprechend nutzt Aurora diese Tabellen nicht oft für Parallelabfragen.

In einer Abfolge nicht-paralleler Abfragen gegen dieselbe Tabelle ist die erste Abfrage möglicherweise langsam, weil die Daten nicht im Bufferpool sind. Die zweite und nachfolgende Abfragen laufen bereits schneller ab, weil der Bufferpool inzwischen sozusagen "warmgelaufen" ist. In der Regel zeigen Parallelabfragen ab der ersten Tabellenabfrage gleichbleibende Leistung Für Leistungstests empfehlen sich Vergleichswerte für einen kalten und einen warmen Bufferpool. In einigen Fällen sind die Ergebnisse des warmen Bufferpools eine gute Vergleichsbasis für Parallelabfragezeiten. Berücksichtigen Sie in diesen Fällen Faktoren wie die Häufigkeit von Abfragen für diese Tabelle. Überlegen Sie auch, ob es sich lohnt, die Daten für diese Tabelle im Pufferpool zu behalten.

Der Abfrage-Cache vermeidet die erneute Ausführung einer Abfrage, wenn eine identische Abfrage abgesendet wird und die zugrunde liegenden Tabellendaten nicht geändert wurden. Mit Parallel Query optimierte Abfragen können im Abfrage-Cache abgelegt werden. Wird die gleiche Abfrage noch einmal gestartet, liegt sofort ein Ergebnis vor.

> **Note**
>
> Bei Leistungsvergleichen können aufgrund des Abfrage-Cache künstlich niedrige Zeitangaben zustandekommen. Für Benchmark-ähnliche Aufgabenstellungen empfiehlt sich der `sql_no_cache`-Hinweis. Dieser verhindert, dass das Ergebnis aus dem Abfrage-Cache kommt. Auch dann nicht, wenn die gleiche Abfrage schon einmal ausgeführt wurde. Der Hinweis folgt in der Abfrage unmittelbar nach der `SELECT`-Anweisung. Viele Beispiele für parallele Abfragen in diesem Thema enthalten diesen Hinweis, um die Abfragezeiten zwischen den Versionen der Abfrage vergleichbar zu machen, für welche die parallele Abfrage aktiviert und deaktiviert ist.

Entfernen Sie diesen Hinweis aus Ihrem Quellcode, bevor Sie parallele Abfragen in einer Produktionsumgebung verwenden.

Optimierungshinweise

Eine andere Möglichkeit, den Optimierer zu steuern, besteht in der Verwendung von Optimierungshinweisen, die in einzelnen Anweisungen angegeben werden können. Sie können beispielsweise eine Optimierung für eine Tabelle in einer Anweisung aktivieren und dann die Optimierung für eine andere Tabelle deaktivieren. Weitere Informationen zu diesen Hinweisen finden Sie unter Optimierungshinweise im MySQL-Referenzhandbuch.

Sie können SQL-Hinweise mit Aurora-MySQL-Abfragen verwenden, um die Leistung zu optimieren. Sie können auch Hinweise verwenden, um zu verhindern, dass Ausführungspläne für wichtige Abfragen aufgrund unvorhersehbarer Bedingungen geändert werden.

Wir haben die Funktion für SQL-Hinweise erweitert, damit Sie die Optimiererauswahl für Ihre Abfragepläne besser kontrollieren können. Diese Hinweise gelten für Abfragen, bei denen die Parallelabfrageoptimierung verwendet wird. Weitere Informationen finden Sie unter Aurora-MySQL-Hinweise.

Temporäre MyISAM-Tabellen

Die parallele Abfrageausführung ist nur möglich, wenn InnoDB-Tabellen vorliegen. Aurora MySQL verwendet MyISAM im Hintergrund für temporäre Tabellen. Interne Abfragephasen mit temporären Tabellen werden nie parallel abgefragt. Diese Abfragephasen erkennen Sie am Code `Using temporary` in der `EXPLAIN`-Ausgabe.

Verwenden von Advanced Auditing in einem Amazon Aurora MySQL DB-Cluster

Sie können die Hochleistungsfunktion erweitertes Auditing in Amazon Aurora MySQL verwenden, um Datenbank-Aktivitäten zu überprüfen. Dafür müssen Sie die Sammlung der Prüfprotokolle aktivieren, indem Sie mehrere DB-Cluster-Parameter einstellen. Wenn erweitertes Auditing aktiviert ist, können Sie es verwenden, um eine beliebige Kombination von unterstützten Ereignissen zu protokollieren.

Sie können die Prüfprotokolle ansehen oder herunterladen, um die Prüfinformationen für jeweils eine DB-Instance zu überprüfen. Dazu können Sie die Verfahren in Überwachen von Amazon Aurora-Protokolldateien verwenden.

> **Tip**
>
> Für einen Aurora-DB-Cluster, der mehrere DB-Instances enthält, ist es möglicherweise praktischer, die Prüfprotokolle für alle Instances im Cluster zu untersuchen. Dazu können Sie CloudWatch Logs verwenden. Sie können eine Einstellung auf Cluster-Ebene aktivieren, um die Aurora MySQL-Audit-Log-Daten in einer Protokollgruppe in zu veröffentlichen CloudWatch. Anschließend können Sie die Audit-Logs über die CloudWatch Benutzeroberfläche anzeigen, filtern und durchsuchen. Weitere Informationen finden Sie unter Veröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs.

Aktivieren von erweitertem Auditing

Verwenden Sie die in diesem Abschnitt beschriebenen Parameter, um erweitertes Auditing für Ihr DB-Cluster zu aktivieren und zu konfigurieren.

Verwenden Sie den Parameter `server_audit_logging` zum Aktivieren oder Deaktivieren von Advanced Auditing.

Mit dem Parameter `server_audit_events` können Sie angeben, welche Ereignisse protokolliert werden.

Verwenden Sie die Parameter `server_audit_incl_users` und `server_audit_excl_users`, um anzugeben, wer überprüft werden soll. Standardmäßig werden alle Benutzer überprüft. Weitere Informationen darüber, wie diese Parameter funktionieren, wenn ein oder beide leer bleiben oder in

beiden die gleichen Benutzernamen angegeben sind, finden Sie unter server_audit_incl_users und server_audit_excl_users.

Konfigurieren Sie das erweiterte Auditing, indem Sie diese Parameter in der vom DB-Cluster verwendeten Parametergruppe festlegen. Sie können die in Ändern von Parametern in einer DB-Parametergruppe gezeigte Prozedur verwenden, um DB-Cluster-Parameter mithilfe der AWS Management Console zu ändern. Sie können den AWS CLI Befehl modify-db-cluster-parameter-group oder den Amazon RDS-API-Vorgang ModifyDB ClusterParameter Group verwenden, um DB-Cluster-Parameter programmgesteuert zu ändern.

Das Ändern dieser Parameter erfordert keinen Neustart des DB-Clusters, wenn die Parametergruppe Ihrem Cluster zugeordnet ist. Wenn Sie die Parametergruppe zum ersten Mal mit dem Cluster verknüpfen, ist ein Neustart des Clusters erforderlich.

Themen

- server_audit_logging
- server_audit_events
- server_audit_incl_users
- server_audit_excl_users

server_audit_logging

Aktiviert oder deaktiviert erweitertes Auditing. Dieser Parameter ist standardmäßig auf OFF eingestellt. Setzten Sie ihn auf ON, um erweiterte Prüfungen zu aktivieren.

In den Protokollen werden keine Prüfungsdaten angezeigt, es sei denn, Sie definieren auch eine oder mehrere Arten von Ereignissen mit dem Parameter `server_audit_events`.

Um sich zu vergewissern, dass Prüfungsdaten für eine DB-Instance protokolliert werden, sehen Sie nach, ob einige Protokolldateien für diese Instance Namen nach dem Schema `audit/audit.log.`*`other_identifying_information`* haben. Befolgen Sie zum Anzeigen der Namen der Protokolldateien die Anleitung unter Anzeigen und Auflisten von Datenbank-Protokolldateien.

server_audit_events

Beinhaltet die durch Kommas getrennte Liste von Ereignissen zum Protokollieren. Ereignisse müssen alle in Großbuchstaben angegeben werden und es sollte kein Leerraum zwischen

den Listenelementen bestehen, zum Beispiel: `CONNECT,QUERY_DDL`. Dieser Parameter ist standardmäßig auf eine leere Zeichenfolge eingestellt.

Sie können eine beliebige Kombination der folgenden Ereignisse protokollieren:

- CONNECT – Protokolliert sowohl erfolgreiche als auch fehlgeschlagene Verbindungen und Verbindungstrennungen. Dieses Ereignis beinhaltet Benutzerinformationen.
- QUERY – Protokolliert alle Abfragen in Klartext, einschließlich Abfragen, die aufgrund der Syntax oder Berechtigungsfehlern fehlschlagen.

> **Tip**
>
> Wenn dieser Ereignistyp aktiviert ist, enthalten die Prüfungsdaten Informationen über die kontinuierliche Überwachung und Zustandsprüfung, die Aurora automatisch durchführt. Wenn Sie nur an bestimmten Arten von Operationen interessiert sind, können Sie spezifischere Arten von Ereignissen verwenden. Sie können die CloudWatch Schnittstelle auch verwenden, um in den Protokollen nach Ereignissen zu suchen, die sich auf bestimmte Datenbanken, Tabellen oder Benutzer beziehen.

- QUERY_DCL – Ähnlich dem QUERY-Ereignis, aber gibt nur Data Control Language (DCL)-Abfragen zurück (GRANT, REVOKE usw.).
- QUERY_DDL – Ähnlich dem QUERY-Ereignis, aber gibt nur Data Definition Language (DDL)-Abfragen zurück (CREATE, ALTER usw.).
- QUERY_DML – Ähnlich dem QUERY-Ereignis, aber gibt nur Data Manipulation Language (DML)-Abfragen zurück (INSERT, UPDATE usw. und auch SELECT).
- TABLE – Protokolliert die Tabellen, die von der Ausführung von Abfragen betroffen sind.

> **Note**
>
> In Aurora gibt es keinen Filter, der bestimmte Abfragen aus den Audit-Logs ausschließt. Um `SELECT` Abfragen auszuschließen, müssen Sie alle DML-Anweisungen ausschließen. Wenn ein bestimmter Benutzer diese internen `SELECT` Abfragen in den Audit-Logs meldet, können Sie diesen Benutzer ausschließen, indem Sie den DB-Cluster-Parameter server_audit_excl_users festlegen. Wenn dieser Benutzer jedoch auch in anderen Aktivitäten verwendet wird und nicht weggelassen werden kann, gibt es keine andere Option zum Ausschließen von Abfragen. `SELECT`

server_audit_incl_users

Beinhaltet die durch Kommas getrennte Liste mit Benutzernamen für Benutzer, deren Aktivitäten überprüft werden. Zwischen den Listenelementen sollte kein Leerraum bestehen, zum Beispiel: `user_3,user_4`. Dieser Parameter ist standardmäßig auf eine leere Zeichenfolge eingestellt. Die maximale Länge beträgt 1024 Zeichen. Bestimmte Benutzernamen müssen mit entsprechenden Werten in der Spalte `User` der `mysql.user`-Tabelle übereinstimmen. Weitere Informationen zu Benutzernamen finden Sie unter Benutzernamen finden Sie unter Kontobenutzernamen und Passwörter in der MySQL-Dokumentation.

Wenn `server_audit_incl_users` und `server_audit_excl_users` keine Werte beinhalten (standardmäßige Einstellung), werden alle Benutzer überprüft.

Wenn Sie Benutzer zu `server_audit_incl_users` hinzufügen und für `server_audit_excl_users` keinen Wert eingeben, werden nur diese Benutzer überprüft.

Wenn Sie Benutzer zu `server_audit_excl_users` hinzufügen und für `server_audit_incl_users` keinen Wert eingeben, werden alle Benutzer überprüft, die nicht in `server_audit_excl_users` aufgeführt sind.

Wenn Sie dieselben Benutzer zu `server_audit_excl_users` und `server_audit_incl_users` hinzufügen, werden diese Benutzer überprüft. Wenn derselbe Benutzer in beiden Einstellungen aufgeführt ist, erhält `server_audit_incl_users` die höhere Priorität.

Verbinden und trennen Sie Ereignisse, die nicht von dieser Variable betroffen sind. Sie werden immer protokolliert, wenn dies festgelegt wurde. Ein Benutzer wird protokolliert, selbst wenn dieser Benutzer auch im Parameter `server_audit_excl_users` angegeben ist, da `server_audit_incl_users` höhere Priorität hat.

server_audit_excl_users

Beinhaltet die durch Kommas getrennte Liste mit Benutzernamen für Benutzer, deren Aktivitäten nicht überprüft werden. Zwischen den Listenelementen sollte kein Leerraum bestehen, zum Beispiel: `rdsadmin,user_1,user_2`. Dieser Parameter ist standardmäßig auf eine leere Zeichenfolge eingestellt. Die maximale Länge beträgt 1024 Zeichen. Bestimmte Benutzernamen müssen mit entsprechenden Werten in der Spalte `User` der `mysql.user`-Tabelle übereinstimmen. Weitere Informationen zu Benutzernamen finden Sie unter Benutzernamen finden Sie unter Kontobenutzernamen und Passwörter in der MySQL-Dokumentation.

Wenn `server_audit_incl_users` und `server_audit_excl_users` keine Werte beinhalten (standardmäßige Einstellung), werden alle Benutzer überprüft.

Wenn Sie Benutzer zu `server_audit_excl_users` hinzufügen und `server_audit_incl_users` leer lassen, werden nur die unter `server_audit_excl_users` aufgeführten Benutzer nicht überprüft. Alle anderen werden jedoch überprüft.

Wenn Sie dieselben Benutzer zu `server_audit_excl_users` und `server_audit_incl_users` hinzufügen, werden diese Benutzer überprüft. Wenn derselbe Benutzer in beiden Einstellungen aufgeführt ist, erhält `server_audit_incl_users` die höhere Priorität.

Verbinden und trennen Sie Ereignisse, die nicht von dieser Variable betroffen sind. Sie werden immer protokolliert, wenn dies festgelegt wurde. Ein Benutzer wird protokolliert, wenn dieser Benutzer auch im Parameter `server_audit_incl_users` festgelegt ist, da diese Einstellung eine höhere Priorität hat als `server_audit_excl_users`.

Anzeigen von Audit-Protokollen

Sie können Audit-Protokolle mithilfe der Konsole anzeigen und herunterladen. Wählen Sie auf der Seite Datenbanken die DB-Instance aus, um ihre Details anzuzeigen, und scrollen Sie dann in den Abschnitt Protokolle. Die von der Advanced-Auditing-Funktion erstellten Prüfprotokolle haben Namen nach dem Schema `audit/audit.log.`*`other_identifying_information`*.

Um eine Protokolldatei herunterzuladen, wählen Sie die Datei im Bereich Protokolle aus. Wählen Sie dann Herunterladen.

Sie können auch mit dem AWS CLI -Befehl describe-db-log-files eine Liste der Protokolldateien erhalten. Sie können den Inhalt einer Protokolldatei mit dem AWS CLI -Befehl download-db-log-file-portion herunterladen. Weitere Informationen erhalten Sie unter Anzeigen und Auflisten von Datenbank-Protokolldateien und Herunterladen einer Datenbank-Protokolldatei.

Details in Prüfprotokollen

Protokolldateien werden als CSV-Dateien (durch Kommata getrennte Werte) im UTF-8-Format dargestellt. Abfragen werden auch in einfache Anführungszeichen (') gesetzt.

Das Auditprotokoll wird separat im lokalen Speicher jeder Instanz gespeichert. Jede Aurora-Instance verteilt Schreibvorgänge auf vier Protokolldateien gleichzeitig. Die maximale Größe der Protokolle beträgt insgesamt 100 MB. Wenn dieses nicht konfigurierbare Limit erreicht ist, rotiert Aurora die Dateien und generiert vier neue Dateien.

> **Tip**
>
> Protokolldateieinträge folgen keiner sequenziellen Reihenfolge. Um die Einträge zu sortieren, verwenden Sie den Wert des Zeitstempels. Sie müssen eventuell alle Protokolldateien überprüfen, um die aktuellen Ereignisse zu sehen. Um mehr Flexibilität beim Sortieren und Durchsuchen der Protokolldaten zu erhalten, aktivieren Sie die Einstellung, in die Auditprotokolle hochzuladen CloudWatch und sie über die CloudWatch Benutzeroberfläche anzuzeigen.
> Um Prüfdaten mit mehreren Feldtypen und mit Ausgabe im JSON-Format anzuzeigen, können Sie auch die Funktion Datenbankaktivitäts-Streams verwenden. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.

Die Prüfprotokolldateien beinhalten die folgenden durch Kommata getrennten Informationen in Zeilen in der festgelegten Reihenfolge:

Feld	Beschreibung
timestamp	Der präzise Unix-Zeitstempel für das protokollierte Ereignis mit Mikrosekunden.
serverhost	Der Name der Instance, für die das Ereignis protokolliert wird.
username	Der verbundene Benutzername des Benutzers.
host	Der Host, von dem sich der Benutzer verbunden hat.
connectionid	Die Nummer der Verbindungs-ID für den protokollierte Vorgang.
queryid	Die Nummer der Abfragen-ID, die verwendet werden kann, um Ereignisse für relationale Tabellenereignisse und zugehörige Abfragen zu finden. Für `TABLE`-Ereignisse werden mehrere Zeilen hinzugefügt.
operation	Der dokumentierte Aktionstyp. Mögliche Werte sind: `CONNECT`, `QUERY`, `READ`, `WRITE`, `CREATE`, `ALTER`, `RENAME` und `DROP`.
Datenbank	Die aktive Datenbank, wie vom `USE`-Befehl eingestellt.

Feld	Beschreibung
Objekt	Bei QUERY-Ereignissen gibt dieser Wert die Abfrage an, die die Datenbank ausgeführt hat. Bei TABLE-Ereignissen gibt er den Tabellennamen an.
retcode	Der zurückgegebene Code des protokollierten Vorgangs.

Replikation mit Amazon Aurora My SQL

Die Aurora-MySQL-Replikationsfunktionen sind für die hohe Verfügbarkeit und Leistung Ihres Clusters entscheidend. Ein Aurora erleichtert das Erstellen und Skalieren von Clustern mit bis zu 15 Aurora-Replikaten.

Alle Replicas arbeiten mit denselben zugrunde liegenden Daten. Wenn einige Datenbank-Instances offline gehen, bleiben andere verfügbar, um die Verarbeitung von Abfragen fortzusetzen oder bei Bedarf als Writer zu übernehmen. Aurora verteilt Ihre schreibgeschützten Verbindungen automatisch auf mehrere Datenbank-Instances und hilft einem Aurora-Cluster, abfrageintensive Workloads zu unterstützen.

In den folgenden Themen finden Sie Informationen darüber, wie die Aurora-MySQL-Replikation funktioniert, und wie Sie die Replikationseinstellungen für beste Verfügbarkeit und Leistung anpassen.

Themen

Verwendung von Aurora-Replicas

Aurora-Replicas sind unabhängige Endpunkte in einem Aurora-DB-Cluster, die die beste Methode für das Skalieren von Leseoperationen und Erhöhen der Verfügbarkeit darstellen. Es können bis zu 15 Aurora-Replikate über die Availability Zones verteilt werden, über die sich ein DB-Cluster innerhalb einer AWS-Region erstreckt. Obwohl das DB-Cluster-Volume aus mehreren Kopien der

Daten in Ihrem DB-Cluster besteht, werden die Daten im Cluster-Volume als ein zusammengefasstes einzelnes logisches Volume der primären Instance und den Aurora Replicas im DB-Cluster dargestellt. Weitere Informationen über Aurora-Replicas finden Sie unter Aurora-Replikate.

Aurora Replicas funktionieren für das Skalieren von Lesevorgängen, da sie in Ihrem Cluster-Volume vollständig für Lesevorgänge bereit stehen. Schreibvorgänge werden von der primären Instance verwaltet. Da das Cluster-Volume zwischen allen Instances in Ihrem Aurora MySQL-DB-Cluster geteilt wird, ist kein zusätzlicher Arbeitsaufwand erforderlich, um eine Kopie Ihrer Daten für jedes Aurora-Replica zu erstellen. Im Gegensatz dazu müssen MySQL-Read Replicas in einem einzelnen Thread alle Schreiboperationen aus der Quell-DB-Instance in ihrem lokalen Datenspeicher wiedergeben. Dies kann sich auf die Leistungsfähigkeit der unterstützten Lesevorgänge im Datenverkehr mit großem Volumen in Ihren MySQL-Lesereplikaten auswirken.

Mit Aurora MySQL wird beim Löschen eines Aurora-Replica der Instance-Endpunkt sofort entfernt und das Aurora-Replica vom Leser-Endpunkt entfernt. Wenn Anweisungen vorhanden sind, die auf dem Aurora-Replica ausgeführt werden, das gerade gelöscht wird, besteht eine Übergangsfrist von drei Minuten. Vorhandene Anweisungen können während der Nachfrist geordnet beendet werden. Nach Ablauf der Nachfrist wird das Aurora-Replikat geschlossen und gelöscht.

Important

Aurora-Replicas für Aurora MySQL verwenden immer die standardmäßige Transaktionsisolationsebene `REPEATABLE READ` für Vorgänge in InnoDB-Tabellen. Sie können den Befehl `SET TRANSACTION ISOLATION LEVEL` verwenden, um die Transaktionsebene nur für die primäre Instance eines Aurora MySQL-DB-Clusters zu ändern. Diese Beschränkung vermeidet Sperren auf Benutzerebene in Aurora-Replicas und ermöglicht eine Skalierung der Aurora-Replicas, um tausende aktive Benutzerverbindungen bei gleichzeitig minimaler Replica-Verzögerung zu ermöglichen.

Note

Durch DDL-Anweisungen, die auf der primären Instance ausgeführt werden, können Datenbankverbindungen auf den verknüpften Aurora-Replikaten unterbrochen werden. Wenn eine Aurora-Replica-Verbindung aktiv ein Datenbankobjekt (z. B. eine Tabelle) verwendet und dieses Objekt auf der primären Instance mithilfe einer DDL-Anweisung geändert wird, führt das zu einer Unterbrechung der Aurora-Replica-Verbindung.

> **Note**
>
> Die Region China (Ningxia) unterstützt keine regionsübergreifenden Lesereplikate.

Replikationsoptionen für Amazon Aurora MySQL

Sie können eine Replikation zwischen allen folgenden Optionen einrichten:

- Zwei Aurora-MySQL-DB-Cluster in verschiedenen AWS-Regionen, indem Sie ein regionsübergreifendes Lesereplikat eines Aurora-MySQL-DB-Clusters erstellen.

  Weitere Informationen finden Sie unter Replizieren von Amazon-Aurora-MySQL-DB-Clustern über AWS-Regionen hinweg.
- Zwei Aurora-MySQL-DB-Cluster in der gleichen AWS-Region, indem Sie mit dem MySQL-Binärprotokoll (binlog) eine Replikation einrichten.

  Weitere Informationen finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).
- Eine RDS for MySQL-DB-Instance als Quelle und ein Aurora MySQL-DB-Cluster, indem Sie ein Aurora-Read Replica einer RDS for MySQL-DB-Instance erstellen.

  Sie können diesen Ansatz verwenden, um bestehende und laufende Datenänderungen in Aurora MySQL während der Migration zu Aurora zu bringen. Weitere Informationen finden Sie unter Migrieren von Daten aus einer RDS-für-MySQL-DB-Instance zu einem Amazon-Aurora-MySQL-DB-Cluster mittels einer Aurora Read Replica (Lesereplikat).

  Sie können diesen Ansatz auch verwenden, um die Skalierbarkeit von Leseabfragen für Ihre Daten zu erhöhen. Sie tun dies, indem Sie die Daten mit einer oder mehreren DB-Instances in einem schreibgeschützten Aurora MySQL-Cluster abfragen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora für das Skalieren von Lesevorgängen in Ihrer MySQL-Datenbank.
- Ein Aurora-MySQL-DB-Cluster in einer AWS-Region und bis zu fünf schreibgeschützte Aurora-MySQL-DB-Cluster in verschiedenen Regionen durch Erstellen einer globalen Aurora-Datenbank.

  Sie können eine Aurora globale Datenbank verwenden, um Anwendungen mit einem weltweiten Fußabdruck zu unterstützen. Der primäre Aurora MySQL-DB-Cluster verfügt über eine Writer-Instance und bis zu 15 Aurora Replikate. Die schreibgeschützten sekundären Aurora MySQL-DB-

Cluster können jeweils aus bis zu 16 Aurora Replikaten bestehen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Global Databases.

> **Note**
>
> Durch einen Neustart der primären Instance eines Amazon Aurora-DB-Clusters werden auch automatisch die Aurora-Replicas für diesen DB-Cluster neu gestartet, um einen Einstiegspunkt wiederherzustellen, der die Lese-/Schreibkonsistenz innerhalb des DB-Clusters hinweg gewährleistet.

Performance-Überlegungen zur Amazon Aurora MySQL-Replikation

Die folgenden Funktionen helfen Ihnen bei der Optimierung der Leistung der Aurora MySQL-Replikation.

Die Funktion Replica-Protokollkompression reduziert automatisch die Netzwerkbandbreite für Replikationsbenachrichtigungen. Weil jede Benachrichtigung an alle Aurora-Replicas gesendet wird, sind die Vorteile bei umfangreicheren Clustern größer. Diese Funktion beinhaltet einen gewissen CPU-Overhead im Schreiber-Knoten, um die Kompression durchzuführen. In Aurora MySQL Version 2 und Version 3 ist sie immer aktiviert.

Die Funktion Binärprotokollfilterung reduziert automatisch die Netzwerkbandbreite für Replikationsbenachrichtigungen. Da Aurora-Replicas die in den Replikationsbenachrichtigungen enthaltene Binärprotokollinformation nicht verwenden, sind diese Daten in den an diese Knoten gesendeten Benachrichtigungen nicht enthalten.

In Aurora MySQL Version 2 steuern Sie diese Funktion durch eine Änderung des `aurora_enable_repl_bin_log_filtering`-Parameters. Dieser Parameter ist standardmäßig aktiviert. Da diese Optimierung transparent sein soll, können Sie diese Einstellung nur während der Diagnose oder Fehlersuche bei Problemen im Zusammenhang mit der Replikation deaktivieren. Beispielsweise können Sie so das Verhalten eines älteren Aurora MySQL-Clusters anzupassen, bei dem diese Funktion nicht verfügbar war.

Die Binlog-Filterung ist in Aurora MySQL Version 3 immer aktiviert.

Neustart ohne Ausfallzeit (ZDR) für Amazon Aurora MySQL

Die Funktion „Neustart ohne Ausfallzeit“ (ZDR) kann einige oder alle aktiven Verbindungen zu DB-Instances während bestimmter Arten von Neustarts beibehalten. ZDR gilt für Neustarts, die Aurora automatisch durchführt, um Fehlerbedingungen zu beheben, beispielsweise wenn ein Replikat zu weit hinter der Quelle zurückbleibt.

> **Important**
>
> Der ZDR-Mechanismus arbeitet auf Best-Effort-Basis. Die Aurora MySQL-Versionen, Instance-Klassen, Fehlerbedingungen, kompatible SQL-Operationen und andere Faktoren, die bestimmen, wo die ZDR gilt, können sich jederzeit ändern.

ZDR für Aurora MySQL 2.x erfordert Version 2.10 und höher. ZDR ist in allen Nebenversionen von Aurora MySQL 3.x verfügbar. In Aurora-MySQL-Version 2 und 3 ist der ZDR-Mechanismus standardmäßig aktiviert und Aurora verwendet den Parameter `aurora_enable_zdr` nicht.

Aurora berichtet über Aktivitäten auf der Ereignisseite im Zusammenhang mit dem Neustart ohne Ausfallzeiten. Aurora zeichnet ein Ereignis auf, wenn ein Neustart versucht wird, indem der Neustartmechanismus ohne Ausfallzeit verwendet wird. Dieses Ereignis gibt an, warum Aurora den Neustart durchführt. Aurora zeichnet dann ein anderes Ereignis auf, wenn der Neustart abgeschlossen ist. Dieses letzte Ereignis gibt an, wie lange der Prozess gedauert hat und wie viele Verbindungen während des Neustarts erhalten oder abgebrochen wurden. Sie können das Datenbankfehlerprotokoll einsehen, um weitere Details darüber zu erfahren, was während des Neustarts passiert ist.

Obwohl Verbindungen nach einem erfolgreichen ZDR-Vorgang intakt bleiben, werden einige Variablen und Funktionen neu initialisiert. Die folgenden Arten von Informationen werden durch einen Neustart, der durch den Neustart ohne Ausfallzeiten verursacht wird, nicht beibehalten:

- Globale Variablen. Aurora stellt Sitzungsvariablen wieder her, stellt jedoch nach dem Neustart keine globalen Variablen wieder her.
- Statusvariablen. Insbesondere wird der vom Engine-Status gemeldete Verfügbarkeitswert zurückgesetzt.
- `LAST_INSERT_ID`.
- In-Memory-`auto_increment`-Status für Tabellen. Der Status des automatischen In-Memory-Inkrements wird neu initialisiert. Weitere Informationen zu automatischen Inkrementwerten finden Sie im MySQL-Referenzhandbuch.

- Diagnoseinformationen aus `INFORMATION_SCHEMA`- und `PERFORMANCE_SCHEMA`-Tabellen. Diese Diagnoseinformationen erscheinen auch in der Ausgabe von Befehlen wie `SHOW PROFILE` und `SHOW PROFILES`.

Die folgende Tabelle zeigt die Versionen, Instance-Rollen und andere Umstände, die bestimmen, ob Aurora den ZDR-Mechanismus beim Neustart von DB-Instances in Ihrem Cluster verwenden kann.

Aurora MySQL Version	ZDR gilt für den Writer?	ZDR gilt für Leser?	ZDR ist immer aktiviert?	Hinweise
2.x, niedriger als 2.10.0	Nein	Nein	N/A	ZDR ist für diese Versionen nicht verfügbar.
2.10.0–2.11.0	Ja	Ja	Ja	Aurora setzt alle Transaktionen zurück, die bei aktiven Verbindungen ausgeführt werden. Ihre Anwendung muss die Transaktionen erneut versuchen. Aurora bricht alle Verbindungen ab, die TLS/SSL, temporäre Tabellen, Tabellensperren oder Benutzersperren verwenden.
2.11.1 und höher	Ja	Ja	Ja	Aurora setzt alle Transaktionen zurück, die bei aktiven Verbindungen ausgeführt werden. Ihre Anwendung muss die Transaktionen erneut versuchen. Aurora bricht alle Verbindungen ab, die temporäre Tabellen, Tabellensperren oder Benutzersperren verwenden.
3.01–3.03	Ja	Ja	Ja	Aurora setzt alle Transaktionen zurück, die bei aktiven Verbindungen ausgeführt werden. Ihre Anwendung muss die Transaktionen erneut versuchen.

Aurora MySQL Version	ZDR gilt für den Writer?	ZDR gilt für Leser?	ZDR ist immer aktiviert?	Hinweise
				Aurora bricht alle Verbindungen ab, die TLS/SSL, temporäre Tabellen, Tabellensperren oder Benutzersperren verwenden.
3.04 und höher	Ja	Ja	Ja	Aurora setzt alle Transaktionen zurück, die bei aktiven Verbindungen ausgeführt werden. Ihre Anwendung muss die Transaktionen erneut versuchen. Aurora bricht alle Verbindungen ab, die temporäre Tabellen, Tabellensperren oder Benutzersperren verwenden.

Konfigurieren von Replikationsfiltern mit Aurora MySQL

Sie können Replikationsfilter verwenden, um anzugeben, welche Datenbanken und Tabellen mit einem Lesereplikat repliziert werden. Replikationsfilter können Datenbanken und Tabellen in die Replikation einbeziehen oder sie von der Replikation ausschließen.

Im Folgenden finden Sie einige Anwendungsfälle für Replikationsfilter:

- Reduzieren der Größe eines Lesereplikats. Mit Replikationsfiltern können Sie die Datenbanken und Tabellen ausschließen, die für das Lesereplikat nicht benötigt werden.
- Ausschließen von Datenbanken und Tabellen von Lesereplikaten aus Sicherheitsgründen.
- Replizieren verschiedener Datenbanken und Tabellen für spezifische Anwendungsfälle bei verschiedenen Lesereplikaten. Beispielsweise könnten Sie bestimmte Lesereplikate für Analysen oder Sharding verwenden.
- Für einen DB-Cluster mit Read Replicas in verschiedenen AWS-Regionen, um unterschiedliche Datenbanken oder Tabellen in verschiedenen AWS-Regionen zu replizieren.
- Um anzugeben, welche Datenbanken und Tabellen mit einem Aurora-MySQL-DB-Cluster repliziert werden, der als Replikat in einer eingehenden Replikationstopologie konfiguriert ist. Weitere Informationen zu dieser Konfiguration finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).

Themen

Einrichten der Parameter der Replikationsfilter für Aurora MySQL

Um Replikationsfilter zu konfigurieren, legen Sie die folgenden Parameter fest:

- `binlog-do-db` – Repliziert Änderungen in die angegebenen Binärprotokolle. Wenn Sie diesen Parameter für einen Binärprotokoll-Quellcluster festlegen, werden nur die im Parameter angegebenen Binärprotokolle repliziert.
- `binlog-ignore-db` – Repliziert keine Änderungen in die angegebenen Binärprotokolle. Wenn der `binlog-do-db` Parameter für einen Binärprotokoll-Quellcluster festgelegt ist, wird dieser Parameter nicht ausgewertet.
- `replicate-do-db` – Repliziert Änderungen der angegebenen Datenbanken. Wenn Sie diesen Parameter für einen Binlog-Replikat-Cluster festlegen, werden nur die im Parameter angegebenen Datenbanken repliziert.
- `replicate-ignore-db` – Repliziert keine Änderungen der angegebenen Datenbanken. Wenn der `replicate-do-db` Parameter für einen Binlog-Replikat-Cluster festgelegt ist, wird dieser Parameter nicht ausgewertet.
- `replicate-do-table` – Repliziert Änderungen der angegebenen Tabellen. Wenn Sie diesen Parameter für ein Lesereplikat festlegen, werden nur die im Parameter angegebenen Tabellen repliziert. Wenn der `replicate-ignore-db` Parameter `replicate-do-db` oder festgelegt ist, stellen Sie außerdem sicher, dass Sie die Datenbank, die die angegebenen Tabellen enthält, in die Replikation mit dem Binlog-Replikat-Cluster einbeziehen.
- `replicate-ignore-table` – Repliziert keine Änderungen der angegebenen Tabellen. Wenn der `replicate-do-table` Parameter für einen Binlog-Replikat-Cluster festgelegt ist, wird dieser Parameter nicht ausgewertet.
- `replicate-wild-do-table` – Repliziert Tabellen basierend auf den angegebenen Namensmustern für Datenbanken und Tabellen. Die Platzhalterzeichen `%` und `_` werden unterstützt. Wenn der `replicate-ignore-db` Parameter `replicate-do-db` oder festgelegt ist, stellen Sie sicher, dass Sie die Datenbank, die die angegebenen Tabellen enthält, in die Replikation mit dem Binlog-Replikat-Cluster einbeziehen.

- `replicate-wild-ignore-table` – Repliziert keine Tabellen basierend auf den angegebenen Namensmustern für Datenbanken und Tabellen. Die Platzhalterzeichen `%` und `_` werden unterstützt. Wenn der `replicate-wild-do-table` Parameter `replicate-do-table` oder für einen Binlog-Replikat-Cluster festgelegt ist, wird dieser Parameter nicht ausgewertet.

Die Parameter werden in der angegebenen Reihenfolge ausgewertet. Weitere Informationen zur Funktionsweise dieser Parameter finden Sie in der MySQL-Dokumentation:

- Allgemeine Informationen finden Sie unter Optionen und Variablen für Replikatserver.
- Informationen darüber, wie Filterparameter für die Datenbankreplikation ausgewertet werden, finden Sie unter Optionen zur Auswertung der Replikation auf Datenbankebene und für die binäre Protokollierung.
- Informationen darüber, wie Filterparameter für die Tabellenreplikation ausgewertet werden, finden Sie unter Optionen zur Auswertung der Replikation auf Tabellenebene.

Standardmäßig hat jeder dieser Parameter einen leeren Wert. Auf jedem Binärprotokoll-Cluster können Sie diese Parameter verwenden, um Replikationsfilter festzulegen, zu ändern und zu löschen. Wenn Sie einen dieser Parameter festlegen, trennen Sie die einzelnen Filter durch ein Komma voneinander.

Sie können die Platzhalterzeichen `%` und `_` in den Parametern `replicate-wild-do-table` und `replicate-wild-ignore-table` verwenden. Der Platzhalter `%` entspricht einer beliebigen Anzahl von Zeichen, und der Platzhalter `_` entspricht nur einem Zeichen.

Das binäre Protokollierungsformat der Quell-DB-Instance ist wichtig für die Replikation, da es den Datensatz der Datenänderungen bestimmt. Die Einstellung des Parameters `binlog_format` bestimmt, ob die Replikation zeilenbasiert oder anweisungsbasiert ist. Weitere Informationen finden Sie unter Konfiguration von Aurora MySQL.

> **Note**
>
> Alle DDL-Anweisungen (Data Definition Language) werden unabhängig von der Einstellung `binlog_format` für die Quell-DB-Instance als Anweisungen repliziert.

Einschränkungen der Replikationsfilter für Aurora MySQL

Folgende Einschränkungen gelten für Replikationsfilter bei Aurora MySQL:

- Replikationsfilter werden nur für Aurora MySQL Version 3 unterstützt.
- Jeder Filterparameter für die Replikation hat ein Limit von 2.000 Zeichen.
- Kommas werden in Replikationsfiltern nicht unterstützt.
- Die Replikationsfilterung unterstützt keine XA-Transaktionen.

  Weitere Informationen finden Sie unter Einschränkungen bei XA-Transaktionen in der MySQL-Dokumentation.

Beispiele für Replikationsfilter bei Aurora MySQL

Um die Replikationsfilter für ein Lesereplikat zu konfigurieren, ändern Sie die Parameter der Replikationsfilter in der DB-Cluster-Parametergruppe, die dem Lesereplikat zugeordnet ist.

> **Note**
>
> Eine Standard-DB-Cluster-Parametergruppe kann nicht modifiziert werden. Erstellen Sie eine neue Parametergruppe und ordnen Sie diese der Lesereplika zu, wenn die Lesereplika eine Standardparametergruppe verwendet. Weitere Informationen zu DB-Cluster-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Sie können Parameter in einer DB-Cluster-Parametergruppe mithilfe der AWS Management Console-, AWS CLI- oder der RDS-API festlegen. Weitere Informationen zum Festlegen von Parametern finden Sie unter Ändern von Parametern in einer DB-Parametergruppe. Wenn Sie Parameter in einer Parametergruppe festlegen, verwenden alle DB-Cluster, die der Parametergruppe zugeordnet sind, diese Parametereinstellungen. Wenn Sie Parameter der Replikationsfilter in einer Parametergruppe festlegen, stellen Sie sicher, dass die Parametergruppe nur Replica-Clustern zugeordnet ist. Lassen Sie die Parameter der Replikationsfilter für Quell-DB-Instances leer.

In den folgenden Beispielen werden die Parameter mithilfe von festgeleg AWS CLI. Diese Beispiele legen `ApplyMethod` auf `immediate` fest, sodass die Parameteränderungen unmittelbar nach Abschluss des CLI-Befehls erfolgen. Wenn Sie möchten, dass eine ausstehende Änderung nach dem Neustart des Lesereplikats angewendet wird, legen Sie `ApplyMethod` auf `pending-reboot` fest.

In den folgenden Beispielen werden Replikationsfilter festgelegt:

- Including databases in replication
- Including tables in replication

- Including tables in replication with wildcard characters
- Excluding databases from replication
- Excluding tables from replication
- Excluding tables from replication using wildcard characters

Example Einschließen von Datenbanken in die Replikation

Das folgende Beispiel schließt die Datenbanken `mydb1` und `mydb2` in die Replikation ein.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-do-
db,ParameterValue='mydb1,mydb2',ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-do-
db,ParameterValue='mydb1,mydb2',ApplyMethod=immediate"
```

Example Einschließen von Tabellen in die Replikation

Das folgende Beispiel schließt die Tabellen `table1` und `table2` in der Datenbank `mydb1` in die Replikation ein.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-do-
table,ParameterValue='mydb1.table1,mydb1.table2',ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
```

```
  --db-cluster-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-do-
table,ParameterValue='mydb1.table1,mydb1.table2',ApplyMethod=immediate"
```

Example Einschließen von Tabellen in die Replikation mit Platzhalterzeichen

Das folgende Beispiel schließt Tabellen mit Namen, die mit `order` und `return` beginnen, in Datenbank `mydb` in die Replikation ein.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-wild-do-table,ParameterValue='mydb.order
%,mydb.return%',ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-wild-do-table,ParameterValue='mydb.order
%,mydb.return%',ApplyMethod=immediate"
```

Example Ausschließen von Datenbanken von der Replikation

Das folgende Beispiel schließt die Datenbanken `mydb5` und `mydb6` von der Replikation aus.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-ignore-
db,ParameterValue='mydb5,mydb6',ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name myparametergroup ^
```

```
  --parameters "ParameterName=replicate-ignore-
db,ParameterValue='mydb5,mydb6,ApplyMethod=immediate"
```

Example Ausschließen von Tabellen von der Replikation

Das folgende Beispiel schließt die Tabellen `table1` in Datenbank `mydb5` und `table2` in Datenbank `mydb6` von der Replikation aus.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-ignore-
table,ParameterValue='mydb5.table1,mydb6.table2',ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-ignore-
table,ParameterValue='mydb5.table1,mydb6.table2',ApplyMethod=immediate"
```

Example Ausschließen von Tabellen von der Replikation mit Platzhalterzeichen

Das folgende Beispiel schließt Tabellen mit Namen, die mit `order` und `return` beginnen, in Datenbank `mydb7` von der Replikation aus.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-wild-ignore-table,ParameterValue='mydb7.order
%,mydb7.return%',ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-wild-ignore-table,ParameterValue='mydb7.order
%,mydb7.return%',ApplyMethod=immediate"
```

Anzeigen der Replikationsfilter für ein Lesereplikat

Sie können die Replikationsfilter für ein Lesereplikat wie folgt anzeigen:

- Überprüfen Sie die Einstellungen der Parameter der Replikationsfilter in der dem Lesereplikat zugeordneten Parametergruppe.

  Detaillierte Anweisungen finden Sie unter Anzeigen von Parameterwerten für eine DB-Parametergruppe.
- Stellen Sie in einem MySQL-Client eine Verbindung zum Read-Replikat her und führen Sie die`SHOW REPLICA STATUS` Anweisung aus.

  In der Ausgabe werden in den folgenden Feldern die Replikationsfilter für das Lesereplikat angezeigt:

  - `Binlog_Do_DB`
  - `Binlog_Ignore_DB`
  - `Replicate_Do_DB`
  - `Replicate_Ignore_DB`
  - `Replicate_Do_Table`
  - `Replicate_Ignore_Table`
  - `Replicate_Wild_Do_Table`
  - `Replicate_Wild_Ignore_Table`

  Weitere Informationen zu diesen Feldern finden Sie unter Überprüfen des Replikationsstatus in der MySQL-Dokumentation.

Überwachung der Amazon Aurora MySQL-Replikation

Skalieren von Lesevorgängen und hohe Verfügbarkeit hängen von der minimalen Verzögerungszeit ab. Sie können überwachen, wie weit ein Aurora-Replikat gegenüber der primären Instance Ihres Aurora MySQL-DB-Clusters zurückbleibt, indem Sie die Amazon CloudWatch `AuroraReplicaLag`-Metrik überwachen. Die `AuroraReplicaLag`-Metrik wird in jedem Aurora-Replikat aufgezeichnet.

Die primäre DB-Instance zeichnet auch die `AuroraReplicaLagMinimum` Amazon CloudWatch-Metriken `AuroraReplicaLagMaximum` und auf. Die `AuroraReplicaLagMaximum`-Metrik zeichnet die maximale Verzögerung zwischen der primären DB-Instance und jedem Aurora-Replikat im DB-

Cluster auf. Die `AuroraReplicaLagMinimum`-Metrik zeichnet die minimale Verzögerung zwischen der primären DB-Instance und jedem Aurora-Replikat im DB-Cluster auf.

Wenn Sie den aktuellen Wert für die Aurora-Replica-Verzögerung benötigen, können Sie die -`AuroraReplicaLag`Metrik in Amazon überprüfen CloudWatch. Die Aurora-Replica-Verzögerung wird auch für jedes Aurora-Replikat Ihres DB-Clusters von Aurora MySQL in der `information_schema.replica_host_status`-Tabelle aufgezeichnet. Weitere Informationen zu dieser Tabelle finden Sie unter information_schema.replica_host_status.

Weitere Informationen zur Überwachung von RDS-Instances und - CloudWatch Metriken finden Sie unter Überwachung von Metriken in einem Amazon-Aurora-Cluster.

Verwendung der lokalen Schreibweiterleitung in einem DB-Cluster von Amazon Aurora MySQL

Lokale (clusterinterne) Schreibweiterleitung ermöglicht Ihren Anwendungen, Lese-/Schreibtransaktionen direkt auf einem Aurora-Replikat durchzuführen. Diese Transaktionen werden dann zum Commit an die Writer-DB-Instance weitergeleitet. Sie können die lokale Schreibweiterleitung verwenden, wenn Ihre Anwendungen Lesen-nach-Schreiben-Konsistenz erfordern. Dies ist die Fähigkeit, den letzten Schreibvorgang in einer Transaktion zu lesen.

Lesereplikate erhalten asynchron Updates vom Writer. Ohne Schreibweiterleitung müssen Sie alle Lesevorgänge, die eine Lesen-nach-Schreiben-Konsistenz erfordern, auf der Writer-DB-Instance abwickeln. Oder Sie müssen eine komplexe benutzerdefinierte Anwendungslogik entwickeln, um aus Gründen der Skalierbarkeit mehrere Lesereplikate nutzen zu können. Ihre Anwendungen müssen den gesamten Lese- und Schreibverkehr vollständig aufteilen und zwei Gruppen von Datenbankverbindungen aufrechterhalten, um den Datenverkehr an den richtigen Endpunkt zu senden. Dieser Entwicklungsaufwand erschwert das Anwendungsdesign, wenn die Abfragen Teil einer einzelnen logischen Sitzung bzw. Transaktion innerhalb der Anwendung sind. Da die Replikationsverzögerung zwischen den Lesereplikaten unterschiedlich sein kann, ist es außerdem schwierig, eine globale Lesekonsistenz für alle Instances in der Datenbank zu erreichen.

Durch die Schreibweiterleitung müssen diese Transaktionen nicht aufgeteilt oder ausschließlich an den Writer gesendet werden, was die Anwendungsentwicklung vereinfacht. Diese neue Funktion macht es einfach, Leseskalierung für Workloads zu erreichen, die den letzten Schreibvorgang in einer Transaktion lesen müssen und nicht empfindlich auf Schreiblatenz reagieren.

Die lokale Schreibweiterleitung unterscheidet sich von der globalen Schreibweiterleitung, bei der Schreibvorgänge von einem sekundären DB-Cluster an den primären DB-Cluster in einer globalen Aurora-Datenbank weitergeleitet werden. Sie können die lokale Schreibweiterleitung in einem DB-Cluster verwenden, der Teil einer globalen Aurora-Datenbank ist. Weitere Informationen finden Sie unter Verwenden der Schreibweiterleitung in einer Amazon Aurora globalen Datenbank.

Die Schreibweiterleitung erfordert Aurora-MySQL-Version 3.04 oder höher.

Themen

- Anwendung und SQL-Kompatibilität mit Schreibweiterleitung
- Isolationsstufen für die Schreibweiterleitung
- Lesekonsistenz für die Schreibweiterleitung
- Ausführen von Multipart-Anweisungen mit Schreibweiterleitung
- Transaktionen mit Schreibweiterleitung
- Konfigurationsparameter für die Schreibweiterleitung
- Amazon-CloudWatch-Metriken und Aurora-MySQL-Statusvariablen für die Schreibweiterleitung
- Identifizieren weitergeleiteter Transaktionen und Abfragen

Aktivieren der lokalen Schreibweiterleitung

Standardmäßig ist die lokale Schreibweiterleitung für DB-Cluster von Aurora MySQL nicht aktiviert. Sie aktivieren die lokale Schreibweiterleitung auf Clusterebene, nicht auf Instance-Ebene.

> **Important**
>
> Sie können auch die lokale Schreibweiterleitung für regionsübergreifende Lesereplikate aktivieren, die Binärprotokollierung verwenden. Schreibvorgänge werden jedoch nicht an die Quelle AWS-Region weitergeleitet. Sie werden an die Writer-DB-Instance des Binärprotokoll-Lesereplikats-Clusters weitergeleitet.
> Verwenden Sie diese Methode nur, wenn Sie einen Anwendungsfall für das Schreiben in das Binärprotokoll-Lesereplikat in der sekundären AWS-Region haben. Andernfalls könnte es zu einem „Split-Brain“ -Szenario kommen, in dem replizierte Datensätze nicht miteinander konsistent sind.
> Es wird empfohlen, die globale Schreibweiterleitung für globale Datenbanken anstelle der lokalen Schreibweiterleitung für regionsübergreifende Lesereplikate zu verwenden, sofern dies nicht unbedingt erforderlich ist. Weitere Informationen finden Sie unter Verwenden der Schreibweiterleitung in einer Amazon Aurora globalen Datenbank.

Konsole

Wählen Sie in der AWS Management Console das Kontrollkästchen Lokale Schreibweiterleitung aktivieren unter Read-Replica-Schreibweiterleitung aktivieren aus, wenn Sie einen DB-Cluster erstellen oder ändern.

AWS CLI

Wenn Sie die Schreibweiterleitung über die AWS CLI aktivieren möchten, verwenden Sie die Option `--enable-local-write-forwarding`. Diese Option funktioniert, wenn Sie über den Befehl `create-db-cluster` einen neuen DB-Cluster erstellen. Sie funktioniert auch, wenn Sie einen vorhandenen DB-Cluster über den Befehl `modify-db-cluster` ändern. Sie können die Schreibweiterleitung deaktivieren, indem Sie die Option `--no-enable-local-write-forwarding` mit denselben CLI-Befehlen verwenden.

Im folgenden Beispiel wird ein DB-Cluster von Aurora MySQL mit aktivierter Schreibweiterleitung erstellt.

```
aws rds create-db-cluster \
  --db-cluster-identifier write-forwarding-test-cluster \
  --enable-local-write-forwarding \
  --engine aurora-mysql \
  --engine-version 8.0.mysql_aurora.3.04.0 \
  --master-username myuser \
  --master-user-password mypassword \
  --backup-retention 1
```

Anschließend erstellen Sie Writer- und Reader-DB-Instances, sodass Sie die Schreibweiterleitung verwenden können. Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

RDS-API

Um die Schreibweiterleitung über die Amazon RDS-API zu aktivieren, legen Sie den Parameter `EnableLocalWriteForwarding` auf `true` fest. Dieser Parameter funktioniert, wenn Sie über die Operation `CreateDBCluster` einen neuen DB-Cluster erstellen. Sie funktioniert auch, wenn Sie einen vorhandenen DB-Cluster über die Operation `ModifyDBCluster` ändern. Sie können die Schreibweiterleitung deaktivieren, indem Sie den Parameter `EnableLocalWriteForwarding` auf `false` festlegen.

Aktivieren der Schreibweiterleitung für Datenbanksitzungen

Der Parameter `aurora_replica_read_consistency` ist ein DB-Parameter und ein DB-Cluster-Parameter, der die Schreibweiterleitung ermöglicht. Sie können `EVENTUAL`, `SESSION` oder `GLOBAL` als Lesekonsistenzstufe angeben. Weitere Informationen über Konsistenzebenen finden Sie unter Lesekonsistenz für die Schreibweiterleitung.

Für diesen Parameter gelten die folgenden Regeln:

- Der Standardwert ist (null).
- Die Schreibweiterleitung ist nur verfügbar, wenn `aurora_replica_read_consistency` auf `EVENTUAL`, `SESSION` oder `GLOBAL` festgelegt ist. Dieser Parameter ist nur in Reader-Instances von DB-Clustern relevant, für die Schreibweiterleitung aktiviert ist.
- Sie können diesen Parameter (wenn leer) nicht innerhalb einer Multistatement-Transaktion festlegen oder die Einstellung (wenn er bereits eingestellt ist) nicht aufheben. Sie können ihn während einer solchen Transaktion von einem gültigen Wert in einen anderen gültigen Wert ändern. Diese Aktion wird jedoch nicht empfohlen.

Überprüfen, ob die Schreibweiterleitung für einen DB-Cluster aktiviert ist

Wenn Sie feststellen möchten, ob Sie die Schreibweiterleitung in einem DB-Cluster verwenden können, stellen Sie sicher, dass das Attribut `LocalWriteForwardingStatus` für den Cluster auf `enabled` eingestellt ist.

In der AWS Management Console sehen Sie auf der Registerkarte Konfiguration der Detailseite des Clusters den StatusAktiviert für Lokale Lesereplikat-Schreibweiterleitung.

Um den Status der Einstellung für die Schreibweiterleitung für alle Cluster anzuzeigen, führen Sie den folgenden AWS CLI-Befehl aus.

Example

```
aws rds describe-db-clusters \
--query '*[].
{DBClusterIdentifier:DBClusterIdentifier,LocalWriteForwardingStatus:LocalWriteForwardingStatus}

[
    {
        "LocalWriteForwardingStatus": "enabled",
        "DBClusterIdentifier": "write-forwarding-test-cluster-1"
    },
    {
        "LocalWriteForwardingStatus": "disabled",
        "DBClusterIdentifier": "write-forwarding-test-cluster-2"
    },
    {
        "LocalWriteForwardingStatus": "requested",
```

```
        "DBClusterIdentifier": "test-global-cluster-2"
    },
    {
        "LocalWriteForwardingStatus": "null",
        "DBClusterIdentifier": "aurora-mysql-v2-cluster"
    }
]
```

Für einen DB-Cluster sind folgende Werte `LocalWriteForwardingStatus` zulässig:

- `disabled` – Die Schreibweiterleitung ist deaktiviert.
- `disabling` – Die Schreibweiterleitung wird gerade deaktiviert.
- `enabled` – Die Schreibweiterleitung ist aktiviert.
- `enabling` – Die Schreibweiterleitung wird gerade aktiviert.
- `null` – Die Schreibweiterleitung ist für diesen DB-Cluster nicht verfügbar.
- `requested` – Die Schreibweiterleitung wurde angefordert, ist aber noch nicht aktiv.

Anwendung und SQL-Kompatibilität mit Schreibweiterleitung

Sie können die folgenden Arten von SQL-Anweisungen mit Schreibweiterleitung verwenden:

- Data Manipulation Language (DM)-Anweisungen wie `INSERT`, wie`DELETE` und `UPDATE`. Es gibt einige Einschränkungen für die Eigenschaften dieser Anweisungen, die Sie bei der Schreibweiterleitung verwenden können, wie im Folgenden beschrieben.
- `SELECT ... LOCK IN SHARE MODE`- und `SELECT FOR UPDATE`-Anweisungen.
- `PREPARE`- und `EXECUTE`-Anweisungen.

Bestimmte Anweisungen sind nicht zulässig oder können veraltete Ergebnisse erzeugen, wenn Sie sie in einem DB-Cluster mit Schreibweiterleitung verwenden. Somit ist die die Einstellung `EnableLocalWriteForwarding` für DB-Cluster standardmäßig deaktiviert. Stellen Sie vor der Aktivierung sicher, dass der Anwendungscode von keiner dieser Einschränkungen betroffen ist.

Die folgenden Einschränkungen gelten für die SQL-Anweisungen, die Sie für die Schreibweiterleitung verwenden. In einigen Fällen können Sie die Anweisungen in DB-Clustern verwenden, bei denen eine Schreibweiterleitung auf Clusterebene aktiviert ist. Dieser Ansatz funktioniert, wenn die Schreibweiterleitung nicht innerhalb der Sitzung durch den Konfigurationsparameter

`aurora_replica_read_consistency` aktiviert wird. Wenn Sie versuchen, eine Anweisung zu verwenden, obwohl diese aufgrund der Schreibweiterleitung nicht zulässig ist, wird eine Fehlermeldung ähnlich wie die folgende ausgegeben:

```
ERROR 1235 (42000): This version of MySQL doesn't yet support 'operation with write
 forwarding'.
```

Data Definition Language (DDL)

Stellen Sie eine Verbindung mit der Writer-DB-Instance her, um DDL-Anweisungen auszuführen. Sie können sie nicht von Reader-DB-Instances aus ausführen.

Aktualisieren einer permanenten Tabelle mit Daten aus einer temporären Tabelle

Sie können in DB-Clustern mit aktivierter Schreibweiterleitung temporäre Tabellen verwenden. Sie können jedoch keine DML-Anweisung verwenden, um eine permanente Tabelle zu ändern, wenn sich die Anweisung auf eine temporäre Tabelle bezieht. Beispielsweise können Sie keine `INSERT ... SELECT`-Anweisung verwenden, die die Daten aus einer temporären Tabelle übernimmt.

XA-Transaktionen

Sie können die folgenden Anweisungen nicht in einem DB-Cluster verwenden, wenn die Schreibweiterleitung innerhalb der Sitzung aktiviert wird. Sie können diese Anweisungen in DB-Clustern verwenden, bei denen die Schreibweiterleitung nicht aktiviert ist, oder innerhalb von Sitzungen mit leerer Einstellung `aurora_replica_read_consistency`. Bevor Sie die Schreibweiterleitung innerhalb einer Sitzung aktivieren, müssen Sie überprüfen, ob Ihr Code diese Anweisungen verwendet.

```
XA {START|BEGIN} xid [JOIN|RESUME]
XA END xid [SUSPEND [FOR MIGRATE]]
XA PREPARE xid
XA COMMIT xid [ONE PHASE]
XA ROLLBACK xid
XA RECOVER [CONVERT XID]
```

LOAD-Anweisungen für permanente Tabellen

Sie können die folgenden Anweisungen nicht in einem DB-Cluster mit aktivierter Schreibweiterleitung verwenden.

```
LOAD DATA INFILE 'data.txt' INTO TABLE t1;
LOAD XML LOCAL INFILE 'test.xml' INTO TABLE t1;
```

Plugin-Anweisungen

Sie können die folgenden Anweisungen nicht in einem DB-Cluster mit aktivierter Schreibweiterleitung verwenden.

```
INSTALL PLUGIN example SONAME 'ha_example.so';
UNINSTALL PLUGIN example;
```

SAVEPOINT-Anweisungen

Sie können die folgenden Anweisungen nicht in einem DB-Cluster verwenden, wenn die Schreibweiterleitung innerhalb der Sitzung aktiviert wird. Sie können diese Anweisungen in DB-Clustern ohne aktivierte Schreibweiterleitung oder in Sitzungen mit leerer Einstellung `aurora_replica_read_consistency` verwenden. Überprüfen Sie, ob Ihr Code diese Anweisungen verwendet, bevor Sie die Schreibweiterleitung innerhalb einer Sitzung aktivieren.

```
SAVEPOINT t1_save;
ROLLBACK TO SAVEPOINT t1_save;
RELEASE SAVEPOINT t1_save;
```

Isolationsstufen für die Schreibweiterleitung

In Sitzungen, die Schreibweiterleitung verwenden, können Sie nur die Isolationsstufe `REPEATABLE READ` verwenden. Obwohl Sie die Isolationsstufe `READ COMMITTED` auch mit Aurora Replicas verwenden können, funktioniert diese Isolationsstufe nicht mit Schreibweiterleitung. Weitere Informationen zu den Isolationsstufen `REPEATABLE READ` und `READ COMMITTED` finden Sie unter Aurora MySQL-Isolierungsstufen.

Lesekonsistenz für die Schreibweiterleitung

Sie können den Grad der Lesekonsistenz in einem DB-Cluster steuern. Die Lesekonsistenzstufe legt fest, wie lange der DB-Cluster vor jeder Leseoperation wartet, um sicherzustellen, dass einige oder alle Änderungen aus dem Writer repliziert werden. Sie können die Lesekonsistenzstufe anpassen, um sicherzustellen, dass alle aus Ihrer Sitzung weitergeleiteten Schreiboperationen im DB-Cluster vor nachfolgenden Abfragen angezeigt werden. Sie können diese Einstellung auch verwenden,

um sicherzustellen, dass Abfragen auf dem DB-Cluster stets die aktuellsten Updates des Writers angezeigt werden. Diese Einstellung gilt auch für Abfragen, die von anderen Sitzungen oder Clustern gesendet werden. Um diese Art von Verhalten für Ihre Anwendung anzugeben, wählen Sie einen Wert für den DB-Parameter `aurora_replica_read_consistency` oder den DB-Cluster-Parameter aus.

> **Important**
>
> Stellen Sie den DB-Parameter `aurora_replica_read_consistency` oder den DB-Cluster-Parameter immer ein, wenn Sie Schreibvorgänge weiterleiten möchten. Andernfalls leitet Aurora keine Schreibvorgänge weiter. Dieser Parameter hat standardmäßig einen leeren Wert, wählen Sie daher einen bestimmten Wert, wenn Sie diesen Parameter verwenden. Der Parameter `aurora_replica_read_consistency` wirkt sich nur auf DB-Cluster oder Instances aus, für die die Schreibweiterleitung aktiviert ist.

Wenn Sie die Konsistenzstufe erhöhen, verbringt Ihre Anwendung mehr Zeit mit dem Warten auf die Propagierung von Änderungen zwischen DB-Instances. Sie können das Verhältnis zwischen schneller Reaktionszeit und der Gewährleistung festlegen, dass vor der Ausführung Ihrer Abfragen Änderungen auf anderen DB-Instances vollständig verfügbar sind.

Sie können die folgenden Werte für den Parameter `aurora_replica_read_consistency` angeben:

- `EVENTUAL` – Ergebnisse von Schreibvorgängen in derselben Sitzung sind erst sichtbar, wenn der Schreibvorgang auf der Writer-DB-Instance ausgeführt wird. Die Abfrage wartet nicht, bis die aktualisierten Ergebnisse verfügbar sind. Daher könnte sie die älteren Daten oder die aktualisierten Daten abrufen, abhängig vom Zeitpunkt der Anweisungen und der Größe der Replikationsverzögerung. Dies entspricht der Konsistenz von DB-Clustern von Aurora MySQL, die keine Schreibweiterleitung verwenden.
- `SESSION` – Allen Abfragen, die die Schreibweiterleitung verwenden, werden die Ergebnisse sämtlicher in dieser Sitzung vorgenommenen Änderungen angezeigt. Die Änderungen werden unabhängig davon angezeigt, ob die Transaktion übergeben wurde. Wenn notwendig, wartet die Abfrage auf die Replikation der Ergebnisse weitergeleiteter Schreibvorgänge.
- `GLOBAL` – In einer Sitzung werden alle übernommenen Änderungen in allen Sitzungen und Instances im DB-Cluster angezeigt. Jede Abfrage kann für einen bestimmten Zeitraum warten, abhängig von der Sitzungsverzögerung. Die Abfrage wird fortgesetzt, wenn der DB-Cluster

mit allen übergebenen Daten aus dem Writer mit Stand zu dem Zeitpunkt, an dem die Abfrage gestartet wurde, aktualisiert ist.

Informationen zu den mit der Schreibweiterleitung verbundenen Parametern finden Sie unter Konfigurationsparameter für die Schreibweiterleitung.

> **Note**
>
> Sie können auch `aurora_replica_read_consistency` als Sitzungsvariable verwenden, zum Beispiel:
>
> ```
> mysql> set aurora_replica_read_consistency = 'session';
> ```

Beispiele für die Verwendung der Schreibweiterleitung

Die folgenden Beispiele zeigen die Auswirkungen des Parameters `aurora_replica_read_consistency` auf laufende `INSERT`-Anweisungen, gefolgt von `SELECT`-Anweisungen. Abhängig vom Wert der Einstellung `aurora_replica_read_consistency` und vom Zeitpunkt der Anweisungen können sich die Ergebnisse unterscheiden.

Um eine höhere Konsistenz zu erreichen, können Sie kurz warten, bevor Sie die Anweisung `SELECT` ausführen. Oder Aurora kann automatisch warten, bis die Ergebnisse fertig repliziert sind, bevor mit fortgefahren wir `SELECT`.

Informationen zum Einstellen von DB-Parametern finden Sie unter Arbeiten mit Parametergruppen.

Example mit der Einstellung von **`aurora_replica_read_consistency`** auf **`EVENTUAL`**

Durch Ausführen einer `INSERT`-Anweisung, auf die unmittelbar eine `SELECT`-Anweisung folgt, wird ein Wert für `COUNT(*)` mit der Anzahl der Zeilen zurückgegeben, bevor die neue Zeile eingefügt wird. Wenn Sie kurze Zeit später `SELECT` erneut ausführen, wird die aktualisierte Zeilenzahl zurückgegeben. Die `SELECT`-Anweisungen haben keine Wartezeit.

```
mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
```

```
|        5 |
+----------+
1 row in set (0.00 sec)

mysql> insert into t1 values (6); select count(*) from t1;
+----------+
| count(*) |
+----------+
|        5 |
+----------+
1 row in set (0.00 sec)

mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        6 |
+----------+
1 row in set (0.00 sec)
```

Example mit der Einstellung von **`aurora_replica_read_consistency`** auf **`SESSION`**

Eine `SELECT`-Anweisung wartet unmittelbar nach einer `INSERT`-Anweisung, bis die Änderungen aus der `INSERT`-Anweisung sichtbar sind. Nachfolgende `SELECT`-Anweisungen haben keine Wartezeit.

```
mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        6 |
+----------+
1 row in set (0.01 sec)

mysql> insert into t1 values (6); select count(*) from t1; select count(*) from t1;
Query OK, 1 row affected (0.08 sec)
+----------+
| count(*) |
+----------+
|        7 |
+----------+
1 row in set (0.37 sec)
+----------+
| count(*) |
```

```
+----------+
|        7 |
+----------+
1 row in set (0.00 sec)
```

Wenn die Lesekonsistenzeinstellung weiter auf `SESSION` festgelegt ist, wird durch die Einführung einer kurzen Wartezeit nach der Ausführung einer `INSERT`-Anweisung die aktualisierte Zeilenzahl zum Zeitpunkt der nächsten Ausführung der `SELECT`-Anweisung verfügbar.

```
mysql> insert into t1 values (6); select sleep(2); select count(*) from t1;
Query OK, 1 row affected (0.07 sec)
+----------+
| sleep(2) |
+----------+
|        0 |
+----------+
1 row in set (2.01 sec)
+----------+
| count(*) |
+----------+
|        8 |
+----------+
1 row in set (0.00 sec)
```

Example mit der Einstellung von **`aurora_replica_read_consistency`** auf **`GLOBAL`**

Jede `SELECT`-Anweisung wartet, um sicherzustellen, dass alle Datenänderungen mit Stand zur Startzeit der Anweisung angezeigt werden, bevor die Abfrage ausgeführt wird. Die Wartezeit für jede `SELECT`-Anweisung variiert je nach Dauer der Replikationsverzögerung.

```
mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        8 |
+----------+
1 row in set (0.75 sec)

mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
```

```
|        8 |
+----------+
1 row in set (0.37 sec)

mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        8 |
+----------+
1 row in set (0.66 sec)
```

Ausführen von Multipart-Anweisungen mit Schreibweiterleitung

Eine DML-Anweisung kann aus mehreren Teilen bestehen, z. B. einer `INSERT ... SELECT`-Anweisung oder einer `DELETE ... WHERE`-Anweisung. In diesem Fall wird die gesamte Anweisung an die Writer-DB-Instance weitergeleitet und dort ausgeführt.

Transaktionen mit Schreibweiterleitung

Wenn der Transaktionszugriffsmodus schreibgeschützt ist, wird die Schreibweiterleitung nicht verwendet. Sie können den Zugriffsmodus für die Transaktion durch Verwendung der Anweisungen `SET TRANSACTION` oder `START TRANSACTION` angeben. Sie können den Transaktionszugriffsmodus auch angeben, indem Sie den Wert der Sitzungsvariablen transaction_read_only ändern. Sie können diesen Sitzungswert nur ändern, wenn Sie mit einem DB-Cluster verbunden sind, für den die Schreibweiterleitung aktiviert ist.

Wenn eine Transaktion mit langer Laufzeit für einen beträchtlichen Zeitraum keine Anweisung ausgibt, kann sie Leerlaufzeitüberschreitung überschreiten. Dieser Zeitraum hat einen Standardwert von einer Minute. Sie können den Parameter `aurora_fwd_writer_idle_timeout` festlegen, um den Wert um bis zu einem Tag zu erhöhen. Eine Transaktion, die die Leerlaufzeitüberschreitung überschreitet, wird von der Writer-Instance abgebrochen. Die nächste nachfolgende Anweisung, die Sie übermitteln, empfängt einen Zeitüberschreitungsfehler. In diesem Fall rollt Aurora die Transaktion zurück.

Diese Art von Fehler kann in anderen Fällen auftreten, wenn die Schreibweiterleitung nicht mehr verfügbar ist. Beispielsweise bricht Aurora alle Transaktionen ab, die die Schreibweiterleitung verwenden, wenn Sie den DB-Cluster neu starten oder die Schreibweiterleitung deaktivieren.

Wenn eine Writer-Instance in einem Cluster, der die lokale Schreibweiterleitung verwendet, neu gestartet wird, werden alle aktiven, weitergeleiteten Transaktionen und Abfragen auf Reader-

Instances, die die lokale Schreibweiterleitung verwenden, automatisch geschlossen. Nachdem die Writer-Instance wieder verfügbar ist, können Sie diese Transaktionen erneut versuchen.

Konfigurationsparameter für die Schreibweiterleitung

Die Aurora-DB-Parametergruppen enthalten Einstellungen für die Schreibweiterleitung. Details zu diesen Parametern sind in der folgenden Tabelle zusammengefasst, mit Nutzungshinweisen unterhalb der Tabelle.

Parameter	Scope	Typ	Standardwert	Zulässige Werte
`aurora_fwd_writer_idle_timeout`	Cluster	Ganzzahl ohne Vorzeichen	60	1 – 86.400
`aurora_fwd_writer_max_connections_pct`	Cluster	Lange Ganzzahl ohne Vorzeichen	10	0 – 90
`aurora_replica_read_consistency`	Cluster oder Instances	Enum	" (null)	`EVENTUAL`, `SESSION`, `GLOBAL`

Verwenden Sie die folgenden Einstellungen, um eingehende Schreibanforderungen zu steuern:

- `aurora_fwd_writer_idle_timeout` – Die Anzahl der Sekunden, die die Writer-DB-Instance auf Aktivitäten bei einer Verbindung wartet, die von einer Reader-Instance weitergeleitet werden, bevor sie geschlossen wird. Wenn die Sitzung über diesen Zeitraum hinaus im Leerlauf ist, bricht Aurora die Sitzung ab.
- `aurora_fwd_writer_max_connections_pct` – Die obere Grenze für Datenbankverbindungen, die in einer Writer-DB-Instance für die Verarbeitung von Abfragen verwendet werden können, die von Reader-Instances weitergeleitet werden. Sie wird als Prozentsatz der Einstellung `max_connections` für den Writer ausgedrückt. Wenn beispielsweise `max_connections` 800 ist und `aurora_fwd_master_max_connections_pct` oder `aurora_fwd_writer_max_connections_pct` 10 ist, lässt der Writer maximal

80 weitergeleitete Sitzungen gleichzeitig zu. Diese Verbindungen stammen aus demselben, von der Einstellung `max_connections` verwalteten Verbindungspool.

Diese Einstellung gilt nur für den Writer, wenn dessen Schreibweiterleitung aktiviert ist. Wenn Sie den Wert verringern, sind vorhandene Verbindungen nicht betroffen. Aurora berücksichtigt den neuen Wert der Einstellung, wenn versucht wird, eine neue Verbindung von einem DB-Cluster aus zu erstellen. Der Standardwert ist 10, was 10 % des Werts für `max_connections` entspricht.

> **Note**
>
> Da es sich bei `aurora_fwd_writer_idle_timeout` und `aurora_fwd_writer_max_connections_pct` um Cluster-Parameter handelt, haben alle DB-Instances in allen Clustern die gleichen Werte für diese Parameter.

Mehr über `aurora_replica_read_consistency` erfahren Sie unter Lesekonsistenz für die Schreibweiterleitung.

Weitere Informationen zu DB-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Amazon-CloudWatch-Metriken und Aurora-MySQL-Statusvariablen für die Schreibweiterleitung

Die folgenden Amazon-CloudWatch-Metriken und Aurora-MySQL-Statusvariablen gelten, wenn Sie die Schreibweiterleitung in einem oder mehreren DB-Clustern verwenden. Diese Metriken und Statusvariablen werden alle auf der Writer-DB-Instance gemessen.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingWriterDMLLatency`	–	Millisekunden	Durchschnittliche Zeit für die Verarbeitung jeder weitergeleiteten DML-Anweisung auf der Writer-DB-Instance.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
			Nicht enthalten ist die Zeit, die der DB-Cluster benötigt, um die Schreibanforderung weiterzuleiten, oder die Zeit, um Änderungen zurück an den Writer zu replizieren.
`ForwardingWriterDMLThroughput`	–	Anzahl pro Sekunde	Anzahl der weitergeleiteten DML-Anweisungen, die pro Sekunde von dieser Writer-DB-Instance verarbeitet werden.
`ForwardingWriterOpenSessions`	`Aurora_fwd_writer_open_sessions`	Anzahl	Anzahl der weitergeleiteten Sitzungen auf der Writer-DB-Instance.
–	`Aurora_fwd_writer_dml_stmt_count`	Anzahl	Gesamtzahl der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden.
–	`Aurora_fwd_writer_dml_stmt_duration`	Mikrosekunden	Gesamtdauer der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
–	`Aurora_fwd_writer_select_stmt_count`	Anzahl	Gesamtzahl der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden.
–	`Aurora_fwd_writer_select_stmt_duration`	Mikrosekunden	Gesamtdauer der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden.

Die folgenden CloudWatch-Metriken und Aurora-MySQL-Statusvariablen werden auf jeder Reader-DB-Instance in einem DB-Cluster mit aktivierter Schreibweiterleitung gemessen.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingReplicaDMLLatency`	–	Millisekunden	Durchschnittliche Reaktionszeit weitergeleiteter DML-Anweisungen auf Replikaten.
`ForwardingReplicaDMLThroughput`	–	Anzahl pro Sekunde	Anzahl der weitergeleiteten DML-Anweisungen, die pro Sekunde verarbeitet werden.
`ForwardingReplicaOpenSessions`	`Aurora_fwd_replica_open_sessions`	Anzahl	Die Anzahl der Sitzungen, die die Schreibweiterleitung

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
			für eine Reader-DB-Instance verwenden.
`ForwardingReplicaReadWaitLatency`	–	Millisekunden	Durchschnittliche Wartezeit, die eine `SELECT`-Anweisung in einer Reader-DB-Instance darauf wartet, mit dem Writer aufzuschließen. Der Grad, in dem die Reader-DB-Instance vor der Verarbeitung einer Abfrage wartet, ist von der Einstellung `aurora_replica_read_consistency` abhängig.
`ForwardingReplicaReadWaitThroughput`	–	Anzahl pro Sekunde	Gesamtzahl der pro Sekunde in allen Sitzungen verarbeiteten `SELECT`-Anweisungen, die Schreibvorgänge weiterleiten.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingReplicaSelectLatency`	–	Millisekunden	Weitergeleitete `SELECT`-Latenz, als Durchschnitt über alle weitergeleiteten `SELECT`-Anweisungen innerhalb des Überwachungszeitraums.
`ForwardingReplicaSelectThroughput`	–	Anzahl pro Sekunde	Weitergeleiteter `SELECT`-Durchsatz, pro Sekunde, als Durchschnitt innerhalb des Überwachungszeitraums.
–	`Aurora_fwd_replica_dml_stmt_count`	Anzahl	Gesamtzahl der DML-Anweisungen, die aus dieser Reader-DB-Instance weitergeleitet werden.
–	`Aurora_fwd_replica_dml_stmt_duration`	Mikrosekunden	Gesamtdauer aller DML-Anweisungen, die aus dieser Reader-DB-Instance weitergeleitet werden.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
–	`Aurora_fwd_replica_errors_session_limit`	Anzahl	Anzahl der Sitzungen, die vom primären Cluster aufgrund einer der folgenden Fehlerbedingungen zurückgewiesen wurden: • Writer voll • Es sind zu viele weitergeleitete Anweisungen in Bearbeitung.
–	`Aurora_fwd_replica_read_wait_count`	Anzahl	Gesamtzahl der Lesen-Nach-Schreiben-Wartezeiten auf dieser Reader-DB-Instance.
–	`Aurora_fwd_replica_read_wait_duration`	Mikrosekunden	Gesamtdauer der Wartezeiten aufgrund der Lesekonsistenzeinstellung auf dieser Reader-DB-Instance.
–	`Aurora_fwd_replica_select_stmt_count`	Anzahl	Gesamtzahl der `SELECT`-Anweisungen, die aus dieser Reader-DB-Instance weitergeleitet werden.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
–	`Aurora_fwd_replica_select_stmt_duration`	Mikrosekunden	Gesamtdauer der `SELECT`-Anweisungen, die aus dieser Reader-DB-Instance weitergeleitet werden.

Identifizieren weitergeleiteter Transaktionen und Abfragen

Sie können die Tabelle `information_schema.aurora_forwarding_processlist` zur Identifizierung weitergeleiteter Transaktionen und Abfragen verwenden. Weitere Informationen zu dieser Tabelle finden Sie unter information_schema.aurora_forwarding_processlist.

Das folgende Beispiel zeigt alle weitergeleiteten Verbindungen auf einer Writer-DB-Instance.

```
mysql> select * from information_schema.AURORA_FORWARDING_PROCESSLIST where
 IS_FORWARDED=1 order by REPLICA_SESSION_ID;

+-----+----------+--------------------+----------+---------+------+--------------
+-------------------------------------------+--------------+-------------------
+---------------------------------+----------------------+----------------+
| ID  | USER     | HOST               | DB       | COMMAND | TIME | STATE        |
 INFO                                     | IS_FORWARDED | REPLICA_SESSION_ID |
 REPLICA_INSTANCE_IDENTIFIER     | REPLICA_CLUSTER_NAME | REPLICA_REGION |
+-----+----------+--------------------+----------+---------+------+--------------
+-------------------------------------------+--------------+-------------------
+---------------------------------+----------------------+----------------+
| 648 | myuser   | IP_address:port1   | sysbench | Query   |    0 | async commit |
 UPDATE sbtest58 SET k=k+1 WHERE id=4802579 |            1 |                637 | my-
db-cluster-instance-2        | my-db-cluster        | us-west-2      |
| 650 | myuser   | IP_address:port2   | sysbench | Query   |    0 | async commit |
 UPDATE sbtest54 SET k=k+1 WHERE id=2503953 |            1 |                639 | my-
db-cluster-instance-2        | my-db-cluster        | us-west-2      |
+-----+----------+--------------------+----------+---------+------+--------------
+-------------------------------------------+--------------+-------------------
+---------------------------------+----------------------+----------------+
```

Auf der weiterleitenden Reader-DB-Instance können Sie die Threads sehen, die diesen Writer-DB-Verbindungen zugeordnet sind, indem Sie `SHOW PROCESSLIST` ausführen. Die `REPLICA_SESSION_ID`-Werte auf dem Writer, 637 und 639, sind dieselben wie die `Id`-Werte auf dem Reader.

```
mysql> select @@aurora_server_id;

+--------------------------------+
| @@aurora_server_id             |
+--------------------------------+
| my-db-cluster-instance-2       |
+--------------------------------+
1 row in set (0.00 sec)

mysql> show processlist;

+-----+----------+--------------------+----------+---------+------+--------------
+-------------------------------------------+
| Id  | User     | Host               | db       | Command | Time | State        | Info
                                       |
+-----+----------+--------------------+----------+---------+------+--------------
+-------------------------------------------+
| 637 | myuser   | IP_address:port1   | sysbench | Query   |    0 | async commit |
 UPDATE sbtest12 SET k=k+1 WHERE id=4802579  |
| 639 | myuser   | IP_address:port2   | sysbench | Query   |    0 | async commit |
 UPDATE sbtest61 SET k=k+1 WHERE id=2503953  |
+-----+----------+--------------------+----------+---------+------+--------------
+-------------------------------------------+
12 rows in set (0.00 sec)
```

Replizieren von Amazon-Aurora-MySQL-DB-Clustern über AWS-Regionen hinweg

Sie können einen Amazon-Aurora-MySQL-DB-Cluster als Lesereplikat in einer anderen AWS-Region als der Ihres Quell-DB-Clusters erstellen. Durch diesen Ansatz können Sie das Potenzial von Notfallwiederherstellungen steigern, Lesevorgänge in einer Ihren Nutzern näher liegenden AWS-Region skalieren und einfacher zwischen einer AWS-Region und anderen Regionen migrieren.

Sie können Lesereplikate sowohl von verschlüsselten als auch von unverschlüsselten DB-Clustern erstellen. Das Lesereplikat muss verschlüsselt sein, wenn der Quell-DB-Cluster verschlüsselt ist.

Für jeden Quell-DB-Cluster können Sie über höchstens fünf regionsübergreifende DB-Cluster-Lesereplikate verfügen.

> **Note**
>
> Als Alternative zu regionsübergreifenden Lesereplikaten können Sie Lesevorgänge mit minimaler Verzögerung skalieren, indem Sie eine globale Aurora-Datenbank verwenden. Eine globale Aurora-Datenbank hat einen primären Aurora-DB-Cluster in einer AWS-Region und bis zu fünf sekundäre schreibgeschützte DB-Cluster in verschiedenen Regionen. Jeder sekundäre DB-Cluster kann bis zu 16 (statt 15) Aurora-Replikate enthalten. Die Replikation vom primären DB-Cluster zu allen sekundären wird von der Aurora-Speicherschicht und nicht von der Datenbank-Engine durchgeführt, so dass die Verzögerung für die Replikation von Änderungen in der Regel weniger als 1 Sekunde beträgt. Wenn Sie die Datenbank-Engine aus dem Replikationsprozess heraushalten, verarbeitet die Datenbank-Engine nur Workloads. Dies bedeutet auch, dass Sie die Aurora-MySQL-Binärprotokoll-Replikation (Binary Logging) nicht konfigurieren oder verwalten müssen. Weitere Informationen hierzu finden Sie unter Verwenden von Amazon Aurora Global Databases.

Wenn Sie eine Aurora-MySQL-DB-Cluster-Read-Replica in einer anderen AWS-Region erstellen, sollten Sie Folgendes beachten:

- Sowohl Ihr Quell-DB-Cluster als auch Ihr regionsübergreifender Lesereplikat-DB-Cluster kann bis zu 15 Aurora-Replikate zusammen mit der primären Instance im DB-Cluster haben. Dank dieser Funktionalität können Lesevorgänge sowohl für die Quell-AWS-Region als auch für die Ziel-AWS-Region der Replikation skaliert werden.

- In einem regionsübergreifenden Szenario besteht eine höhere Verzögerung zwischen dem Quell-DB-Cluster und der Read Replica aufgrund der längeren Netzwerkkanäle zwischen den AWS-Regionen.
- Für Daten, die für eine regionsübergreifende Replikation weitergeleitet werden, fallen Amazon RDS-Datenübertragungskosten an. Die folgenden regionsübergreifenden Replikationsaktionen generieren Gebühren für die übermittelten Daten aus der Quell-AWS-Region:
  - Wenn Sie das Lesereplikat erstellen, erstellt Amazon RDS einen Snapshot des Quell-Clusters und leitet den Snapshot an die AWS-Region weiter, die das Lesereplikat enthält.
  - Für jede in den Quell-Datenbanken durchgeführte Datenänderung übermittelt Amazon RDS Daten aus der Quellregion an die AWS-Region, die das Lesereplikat enthält.

  Weitere Informationen zu den Kosten von Amazon RDS-Datenübertragungen finden Sie unter Amazon Aurora – Preise.
- Sie können mehrere gleichzeitige Erstellungs- oder Löschaktionen für Lesereplikate ausführen, die auf den gleichen Quell-DB-Cluster verweisen. Sie müssen jedoch das Limit von höchstens fünf Lesereplikaten für jeden Quell-DB-Cluster einhalten.
- Damit die Replikation effektiv durchgeführt werden kann, sollte jedes Lesereplikat über dieselbe Menge an Ressourcen für Datenverarbeitung und Speicher wie der Quell-DB-Cluster verfügen. Wenn Sie den Quell-DB-Cluster skalieren, sollten Sie auch die Lesereplikate skalieren.

Themen

Bevor Sie beginnen

Bevor Sie einen Aurora-MySQL-DB-Cluster erstellen können, der ein regionsübergreifendes Lesereplikat darstellt, müssen Sie die Binärprotokollierung für Ihren Quell-Aurora-MySQL-DB-Cluster aktivieren. Die regionsübergreifende Replikation für Aurora MySQL verwendet die MySQL-Binärreplikation, um Änderungen im regionsübergreifenden Lesereplikat-DB-Cluster wiederzugeben.

Aktualisieren Sie den `binlog_format`-Parameter für Ihren Quell-DB-Cluster, um die Binärprotokollierung in einem Aurora-MySQL-DB-Cluster zu aktivieren. Der Parameter `binlog_format` ist ein Parameter auf Cluster-Ebene, der sich in der Cluster-Standardparametergruppe befindet. Wenn der DB-Cluster die Standard-DB-Cluster-Parametergruppe verwendet, müssen Sie eine neue DB-Cluster-Parametergruppe erstellen, um die `binlog_format`-Einstellungen ändern zu können. Wir empfehlen Ihnen, das `binlog_format` auf `MIXED` einzustellen. Jedoch können Sie `binlog_format` auch auf `ROW` oder auf `STATEMENT` einstellen, wenn Sie ein spezifisches Format des Binärprotokolls benötigen. Starten Sie Ihren Aurora-DB-Cluster neu, damit die Änderungen übernommen werden.

Weitere Informationen zur Verwendung der binären Protokollierung mit Aurora MySQL finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation). Weitere Informationen zum Ändern der Aurora MySQL-Konfigurationsparameter finden Sie unter Amazon Aurora-DB-Cluster und DB-Instance-Parameter und Arbeiten mit Parametergruppen.

Erstellen eines Amazon Aurora MySQL-DB-Clusters als regionsübergreifendes Lesereplikat

Sie können mithilfe der AWS Management Console, der AWS Command Line Interface (AWS CLI) oder der Amazon-RDS-API ein regionsübergreifendes Lesereplikat eines Aurora-DB-Clusters erstellen. Sie können regionsübergreifende Lesereplikate sowohl aus verschlüsselten als auch aus unverschlüsselten DB-Clustern erstellen.

Wenn Sie mithilfe der AWS Management Console ein regionsübergreifendes Lesereplikat für Aurora MySQL erstellen, erstellt Amazon RDS einen DB-Cluster in der Ziel-AWS-Region und anschließend automatisch eine DB-Instance als primäre Instance für diesen DB-Cluster.

Wenn Sie ein regionsübergreifendes Lesereplikat mithilfe der AWS CLI oder RDS-API erstellen, müssen Sie zuerst den DB-Cluster in der Ziel-AWS-Region erstellen und anschließend warten, bis er aktiviert wird. Sobald es aktiviert ist, erstellen Sie eine DB-Instance, die die primäre Instance für diesen DB-Cluster ist.

Die Replikation beginnt, wenn die primäre Instance des Lesereplikat-DB-Clusters verfügbar wird.

Verwenden Sie die folgenden Prozeduren, um ein regionsübergreifendes Lesereplikat für einen Aurora MySQL-DB-Cluster zu erstellen. Diese Prozeduren funktionieren für das Erstellen von Lesereplikaten aus verschlüsselten oder unverschlüsselten DB-Clustern.

Konsole

So erstellen Sie mithilfe der AWS Management Console einen Aurora-MySQL-DB-Cluster, der ein regionsübergreifendes Lesereplikat ist

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der rechten oberen Ecke der AWS Management Console die AWS-Region aus, die Ihr Quell-DB-Cluster hostet.
3. Wählen Sie im Navigationsbereich Datenbanken aus.
4. Wählen Sie den DB-Cluster aus, um ein regionsübergreifendes Lesereplikat dafür zu erstellen.
5. Wählen Sie unter Aktionen die Option Regionsübergreifende Read Replica erstellen aus.
6. Wählen Sie auf der Seite Regionsübergreifende Read Replica erstellen die Optionseinstellungen für Ihren regionsübergreifenden Lesereplikat-DB-Cluster aus, wie in der folgenden Tabelle beschrieben.

Option	Beschreibung
Zielregion	Wählen Sie die AWS-Region zum Hosten des neuen regionsübergreifenden Lesereplikat-DB-Clusters aus.
Zieladressen-DB-Subnetzgruppe	Wählen Sie die DB-Subnetzgruppe aus, die für den regionsübergreifenden Lesereplikat-DB-Cluster verwendet werden soll.
Öffentlich zugänglich	Wählen Sie Ja aus, um dem regionsübergreifenden Lesereplikat-DB-Cluster eine öffentliche IP-Adresse zuzuweisen, andernfalls wählen Sie Nein aus.
Verschlüsselung	Wählen Sie Enable Encryption (Verschlüsselung aktivieren) aus, um die Verschlüsselung im Ruhezustand für diesen DB-Cluster zu aktivieren. Weitere Informationen finden Sie unter Verschlüsseln von Amazon Aurora-Ressourcen.
AWS KMS key	Diese Option ist nur verfügbar, wenn Verschlüsselung auf Verschlüsselung aktivieren festgelegt wurde.

Option	Beschreibung
	Wählen Sie die AWS KMS key, die für die Verschlüsselung dieses DB-Clusters verwendet werden soll. Weitere Informationen finden Sie unter Verschlüsseln von Amazon Aurora-Ressourcen.
DB-Instance-Klasse	Wählen Sie eine DB-Instance-Klasse aus, die die Verarbeitungs- und Speicheranforderungen der primären Instance im DB-Cluster definiert. Weitere Informationen zu den Optionen für DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.
Multi-AZ-Bereitstellung	Wählen Sie Ja aus, um ein Lesereplikat des neuen DB-Clusters in einer anderen Availability Zone in der Ziel-AWS-Region für den Failover-Support zu erstellen. Weitere Informationen über die Multi-AZ-Bereitstellung finden Sie unter Regionen und Availability Zones.
Lese-Replikat-Quelle	Wählen Sie den Quell-DB-Cluster aus, um ein regionsübergreifendes Lesereplikat dafür zu erstellen.

Option	Beschreibung
DB-Instance-Kennung	Geben Sie einen Namen für die primäre Instance in Ihrem regionsübergreifenden Lesereplikat-DB-Cluster ein. Dieser Bezeichner wird in der Endpunktadresse für die primäre Instance des neuen DB-Clusters verwendet. Für den DB-Instance-Bezeichner gelten folgende Einschränkungen: • Sie darf 1 bis 63 alphanumerische Zeichen oder Bindestriche enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Es darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten. • Er muss für alle DB-Instances, jedes AWS-Konto und jede AWS-Region eindeutig sein. Da der regionsübergreifende Lesereplikat-DB-Cluster aus einem Snapshot des Quell-DB-Clusters erstellt wird, stimmen der Masterbenutzername und das Masterpasswort für das Lesereplikat mit denen des Quell-DB-Clusters überein.

Option	Beschreibung
DB-Cluster-Kennung	Geben Sie einen Namen für den regionsübergreifenden Lesereplikat-DB-Cluster ein, der für das Replikat in Ihrem Konto in der Ziel-AWS-Region eindeutig ist. Dieser Bezeichner wird in der Cluster-Endpunktadresse für den DB-Cluster verwendet. Weitere Informationen zum Cluster-Endpunkt finden Sie unter Amazon Aurora-Verbindungsverwaltung. Für den DB-Cluster-Bezeichner gelten folgende Einschränkungen: • Sie darf 1 bis 63 alphanumerische Zeichen oder Bindestriche enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Es darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten. • Es muss für alle DB-Cluster in jedem AWS-Konto und jeder AWS-Region eindeutig sein.
Priorität	Wählen Sie eine Failover-Priorität für die primäre Instance des DB-Clusters aus. Diese Priorität bestimmt die Reihenfolge, in der Aurora-Replikate bei der Wiederherstellung nach einem Ausfall der primären Instance hochgestuft werden. Wenn Sie keinen Wert auswählen, wird als Standard tier-1 eingestellt. Weitere Informationen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.

Option	Beschreibung
Datenbankport	Geben Sie den Port an, über den Anwendungen und Dienstprogramme auf die Datenbank zugreifen können. Aurora-DB-Cluster verwenden standardm äßig den MySQL-Standardport 3306. Die Firewalls einiger Unternehmen blockieren Verbindungen mit diesem Port. Wenn die Firewall Ihres Unternehmens den Standardport blockiert, wählen Sie einen anderen Port für den neuen DB-Cluster aus.
Verbesserte Überwachung	Wählen Sie Erweiterte Überwachung aktivieren aus, um die Erfassung von Metriken in Echtzeit für das Betriebssystem zu aktivieren, in dem Ihr DB-Cluste r ausgeführt wird. Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Übe rwachung).
Überwachungsrolle	Nur verfügbar, wenn Verbesserte Überwachung auf Erweiterte Überwachung aktivieren gesetzt ist. Wählen Sie die IAM-Rolle aus, die Sie erstellt haben, um Amazon RDS die Kommunikation mit Amazon CloudWatch Logs für Sie zu ermöglichen, oder wählen Sie Standard aus, damit RDS eine Rolle mit dem Namen für Sie erstellt`rds-monitoring-role` . Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).
Granularität	Nur verfügbar, wenn Verbesserte Überwachung auf Erweiterte Überwachung aktivieren gesetzt ist. Mit ihr können Sie die Zeitspanne zwischen den Erfassung en der Kennzahlen des DB-Clusters in Sekunden festlegen.

Option	Beschreibung
Kleinere Versions-Updates automatisch aktivieren	Diese Einstellung wird für Aurora MySQL-DB-Cluster nicht verwendet. Weitere Informationen über Engine-Updates für Aurora MySQL finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.

7. Wählen Sie Create (Erstellen) aus, um ein regionsübergreifendes Lesereplikat für Aurora zu erstellen.

AWS CLI

So erstellen Sie mithilfe der CLI einen Aurora MySQL-DB-Cluster, der ein regionsübergreifendes Lesereplikat ist:

1. Rufen Sie den AWS CLI-Befehl create-db-cluster in der AWS-Region auf, in der Sie den Lesereplikat-DB-Cluster erstellen möchten. Fügen Sie die Option `--replication-source-identifier` ein und legen Sie den Amazon-Ressourcennamen (ARN) des Quell-DB-Clusters fest, für den Sie ein Lesereplikat erstellen möchten.

   Für die regionsübergreifende Replikation, bei der der durch `--replication-source-identifier` identifizierte DB-Cluster verschlüsselt ist, geben Sie die Optionen `--kms-key-id` und `--storage-encrypted` an.

   > **Note**
   >
   > Sie können eine regionsübergreifende Replikation aus einem unverschlüsselten DB-Cluster zu einem verschlüsselten Lesereplikat einrichten, indem Sie `--storage-encrypted` festlegen und einen Wert für `--kms-key-id` angeben.

   Sie können die Parameter `--master-username` und `--master-user-password` nicht angeben. Diese Werte werden aus dem Quell-DB-Cluster übernommen.

   Im folgenden Code-Beispiel wird ein Lesereplikat in der Region us-east-1 aus einem unverschlüsselten DB-Cluster-Snapshot in der Region us-west-2 erstellt. Der Befehl wird in der

Region us-east-1 aufgerufen. In diesem Beispiel wird die Option `--manage-master-user-password` zum Generieren des Hauptbenutzerpassworts und zum Verwalten dieses Passworts in Secrets Manager angegeben. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager. Alternativ können Sie die Option `--master-password` verwenden, um das Passwort selbst festzulegen und zu verwalten.

Für Linux, macOSoder Unix:

```
aws rds create-db-cluster \
  --db-cluster-identifier sample-replica-cluster \
  --engine aurora \
  --replication-source-identifier arn:aws:rds:us-
west-2:123456789012:cluster:sample-master-cluster
```

Windows:

```
aws rds create-db-cluster ^
  --db-cluster-identifier sample-replica-cluster ^
  --engine aurora ^
  --replication-source-identifier arn:aws:rds:us-
west-2:123456789012:cluster:sample-master-cluster
```

Im folgenden Code-Beispiel wird ein Lesereplikat in der Region us-east-1 aus einem verschlüsselten DB-Cluster-Snapshot in der Region us-west-2 erstellt. Der Befehl wird in der Region us-east-1 aufgerufen.

Für Linux, macOSoder Unix:

```
aws rds create-db-cluster \
  --db-cluster-identifier sample-replica-cluster \
  --engine aurora \
  --replication-source-identifier arn:aws:rds:us-
west-2:123456789012:cluster:sample-master-cluster \
  --kms-key-id my-us-east-1-key \
  --storage-encrypted
```

Windows:

```
aws rds create-db-cluster ^
  --db-cluster-identifier sample-replica-cluster ^
```

```
  --engine aurora ^
  --replication-source-identifier arn:aws:rds:us-
west-2:123456789012:cluster:sample-master-cluster ^
  --kms-key-id my-us-east-1-key ^
  --storage-encrypted
```

Die `--source-region` Option ist für die regionsübergreifende Replikation zwischen den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (USA-West) erforderlich, in denen der durch identifizierte DB-Cluster verschlüsselt `--replication-source-identifier` ist. Geben Sie für `--source-region` die AWS-Region des Quell-DB-Clusters an.

Wenn `--source-region` nicht festgelegt ist, geben Sie einen `--pre-signed-url`-Wert an. Eine vorsignierte URL ist eine URL, die eine mit der Signaturversion 4 signierte Anforderung für den Befehl `create-db-cluster` enthält, der in der Quell-AWS-Region aufgerufen wird. Weitere Informationen zur `pre-signed-url` Option finden Sie unter create-db-cluster in der AWS CLI -Befehlsreferenz.

2. Überprüfen Sie die Verfügbarkeit des DB-Clusters, indem Sie den AWS CLI-Befehl describe-db-clusters verwenden, wie im folgenden Beispiel gezeigt.

```
aws rds describe-db-clusters --db-cluster-identifier sample-replica-cluster
```

Wenn der Befehl **`describe-db-clusters`** den Status `available` anzeigt, erstellen Sie die primäre Instance für den DB-Cluster, damit die Replikation gestartet werden kann. Verwenden Sie dafür den AWS CLI-Befehl create-db-instance, wie im folgenden Beispiel gezeigt.

Für Linux, macOSoder Unix:

```
aws rds create-db-instance \
  --db-cluster-identifier sample-replica-cluster \
  --db-instance-class db.r3.large \
  --db-instance-identifier sample-replica-instance \
  --engine aurora
```

Windows:

```
aws rds create-db-instance ^
  --db-cluster-identifier sample-replica-cluster ^
  --db-instance-class db.r3.large ^
  --db-instance-identifier sample-replica-instance ^
```

```
  --engine aurora
```

Wenn die DB-Instance erstellt wurde und verfügbar ist, wird die Replikation gestartet. Sie können feststellen, ob die DB-Instance verfügbar ist, indem Sie den AWS CLI-Befehl describe-db-instances aufrufen.

RDS-API

So erstellen Sie mithilfe der API einen Aurora MySQL-DB-Cluster, der ein regionsübergreifendes Lesereplikat ist:

1. Rufen Sie die RDS-API-Aktion CreateDBCluster in der AWS-Region auf, in der Sie einen Read-Replica-DB-Cluster erstellen möchten. Fügen Sie den Parameter `ReplicationSourceIdentifier` ein und legen Sie den Amazon-Ressourcennamen (ARN) des Quell-DB-Clusters fest, für den Sie ein Lesereplikat erstellen möchten.

   Für die regionsübergreifende Replikation, bei der der durch `ReplicationSourceIdentifier` identifizierte DB-Cluster verschlüsselt ist, geben Sie den Parameter `KmsKeyId` an und legen den Parameter `StorageEncrypted` auf `true` fest.

   > **Note**
   >
   > Sie können eine regionsübergreifende Replikation aus einem unverschlüsselten DB-Cluster zu einem verschlüsselten Lesereplikat einrichten, indem Sie für `StorageEncrypted` den Wert **`true`** festlegen und einen Wert für `KmsKeyId` angeben. In diesem Fall müssen Sie nicht festlege `PreSignedUrl`.

   Sie müssen die Parameter `MasterUsername` und `MasterUserPassword` nicht mit einschließen, da diese Werte aus dem Quell-DB-Cluster bezogen werden.

   Im folgenden Code-Beispiel wird ein Lesereplikat in der Region us-east-1 aus einem unverschlüsselten DB-Cluster-Snapshot in der Region us-west-2 erstellt. Die Aktion wird in der Region us-east-1 aufgerufen.

```
https://rds.us-east-1.amazonaws.com/
  ?Action=CreateDBCluster
```

```
  &ReplicationSourceIdentifier=arn:aws:rds:us-west-2:123456789012:cluster:sample-
master-cluster
  &DBClusterIdentifier=sample-replica-cluster
  &Engine=aurora
  &SignatureMethod=HmacSHA256
  &SignatureVersion=4
  &Version=2014-10-31
  &X-Amz-Algorithm=AWS4-HMAC-SHA256
  &X-Amz-Credential=AKIADQKE4SARGYLE/20161117/us-east-1/rds/aws4_request
  &X-Amz-Date=20160201T001547Z
  &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
  &X-Amz-Signature=a04c831a0b54b5e4cd236a90dcb9f5fab7185eb3b72b5ebe9a70a4e95790c8b7
```

Im folgenden Code-Beispiel wird ein Lesereplikat in der Region us-east-1 aus einem verschlüsselten DB-Cluster-Snapshot in der Region us-west-2 erstellt. Die Aktion wird in der Region us-east-1 aufgerufen.

```
https://rds.us-east-1.amazonaws.com/
  ?Action=CreateDBCluster
  &KmsKeyId=my-us-east-1-key
  &StorageEncrypted=true
  &PreSignedUrl=https%253A%252F%252Frds.us-west-2.amazonaws.com%252F
         %253FAction%253DCreateDBCluster
         %2526DestinationRegion%253Dus-east-1
         %2526KmsKeyId%253Dmy-us-east-1-key
         %2526ReplicationSourceIdentifier%253Darn%25253Aaws%25253Ards%25253Aus-
west-2%25253A123456789012%25253Acluster%25253Asample-master-cluster
         %2526SignatureMethod%253DHmacSHA256
         %2526SignatureVersion%253D4
         %2526Version%253D2014-10-31
         %2526X-Amz-Algorithm%253DAWS4-HMAC-SHA256
         %2526X-Amz-Credential%253DAKIADQKE4SARGYLE%252F20161117%252Fus-
west-2%252Frds%252Faws4_request
         %2526X-Amz-Date%253D20161117T215409Z
         %2526X-Amz-Expires%253D3600
         %2526X-Amz-SignedHeaders%253Dcontent-type%253Bhost%253Buser-agent%253Bx-
amz-content-sha256%253Bx-amz-date
         %2526X-Amz-Signature
%253D255a0f17b4e717d3b67fad163c3ec26573b882c03a65523522cf890a67fca613
  &ReplicationSourceIdentifier=arn:aws:rds:us-west-2:123456789012:cluster:sample-
master-cluster
  &DBClusterIdentifier=sample-replica-cluster
  &Engine=aurora
```

```
  &SignatureMethod=HmacSHA256
  &SignatureVersion=4
  &Version=2014-10-31
  &X-Amz-Algorithm=AWS4-HMAC-SHA256
  &X-Amz-Credential=AKIADQKE4SARGYLE/20161117/us-east-1/rds/aws4_request
  &X-Amz-Date=20160201T001547Z
  &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
  &X-Amz-Signature=a04c831a0b54b5e4cd236a90dcb9f5fab7185eb3b72b5ebe9a70a4e95790c8b7
```

Geben Sie für die regionsübergreifende Replikation zwischen den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (USA-West), in denen der durch identifizierte DB-Cluster verschlüsselt `ReplicationSourceIdentifier` ist, auch den `PreSignedUrl` Parameter an. Die vorsignierte URL muss eine gültige Anforderung für die API-Operation `CreateDBCluster` sein, die in der Quell-AWS-Region mit dem zu replizierenden verschlüsselten DB-Cluster ausgeführt werden kann. Der KMS-Schlüsselbezeichner wird zur Verschlüsselung des Lesereplikats verwendet und muss ein für die Ziel-AWS-Region gültiger KMS-Schlüssel sein. Verwenden Sie stattdessen den AWS CLI-Befehl create-db-cluster mit der Option `--source-region`, um automatisch (und nicht manuell) eine vorsignierte URL zu generieren.

2. Überprüfen Sie die Verfügbarkeit des DB-Clusters, indem Sie die RDS-API-Operation DescribeDBClusters verwenden, wie im folgenden Beispiel gezeigt.

```
https://rds.us-east-1.amazonaws.com/
  ?Action=DescribeDBClusters
  &DBClusterIdentifier=sample-replica-cluster
  &SignatureMethod=HmacSHA256
  &SignatureVersion=4
  &Version=2014-10-31
  &X-Amz-Algorithm=AWS4-HMAC-SHA256
  &X-Amz-Credential=AKIADQKE4SARGYLE/20161117/us-east-1/rds/aws4_request
  &X-Amz-Date=20160201T002223Z
  &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
  &X-Amz-Signature=84c2e4f8fba7c577ac5d820711e34c6e45ffcd35be8a6b7c50f329a74f35f426
```

Wenn die Ergebnisse von `DescribeDBClusters` den Status `available` anzeigen, erstellen Sie die primäre Instance für den DB-Cluster, damit die Replikation gestartet werden kann. Verwenden Sie dafür die RDS-API-Operation CreateDBInstance, wie im folgenden Beispiel gezeigt.

```
https://rds.us-east-1.amazonaws.com/
```

```
?Action=CreateDBInstance
&DBClusterIdentifier=sample-replica-cluster
&DBInstanceClass=db.r3.large
&DBInstanceIdentifier=sample-replica-instance
&Engine=aurora
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&Version=2014-10-31
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20161117/us-east-1/rds/aws4_request
&X-Amz-Date=20160201T003808Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=125fe575959f5bbcebd53f2365f907179757a08b5d7a16a378dfa59387f58cdb
```

Wenn die DB-Instance erstellt wurde und verfügbar ist, wird die Replikation gestartet. Sie können feststellen, ob die DB-Instance verfügbar ist, indem Sie den AWS CLI-Befehl DescribeDBInstances aufrufen.

Anzeigen von regionsübergreifenden Amazon Aurora MySQL-Replikaten

Sie können die regionsübergreifenden Replikationsbeziehungen für Ihre Amazon Aurora MySQL-DB-Cluster anzeigen, indem Sie den -describe-db-clustersAWS CLIBefehl oder die RDS-API-Operation DescribeDBClusters aufrufen. In der Antwort sind die DB-Clusterkennungen aller regionsübergreifenden Lesereplikat-DB-Cluster im Feld `ReadReplicaIdentifiers` aufgeführt. Das Element `ReplicationSourceIdentifier` gibt Aufschluss über den ARN des Quell-DB-Clusters, der die Replikationsquelle ist.

Hochstufen eines Lesereplikats zum DB-Cluster

Sie können ein Aurora MySQL-Lesereplikat zu einem eigenständigen DB-Cluster hochstufen. Wenn Sie ein Aurora MySQL-Lesereplikat hochstufen, werden ihre DB-Instances neu gestartet, bevor sie verfügbar werden.

Typischerweise stufen Sie ein Aurora MySQL-Lesereplikat zu einem eigenständigen DB-Cluster als Datenwiederherstellungsschema hoch, wenn der Quell-DB-Cluster ausfällt.

Erstellen Sie dazu zuerst ein Lesereplikat und überwachen Sie anschließend den Quell-DB-Cluster auf Fehler. Im Fall eines Ausfalls machen Sie Folgendes:

1. Stufen Sie das Lesereplikat hoch.

2. Leiten Sie den Datenverkehr der Datenbank an den hochgestuften DB-Cluster weiter.
3. Erstellen Sie ein Ersatz-Lesereplikat mit dem hochgestuften DB-Cluster als Quelle.

Wenn Sie ein Lesereplikat hochstufen, wird das Lesereplikat zu einem eigenständigen Aurora-DB-Cluster. Das Hochstufen kann einige Minuten oder mehr in Anspruch nehmen, abhängig von der Größe des Lesereplikats. Nachdem Sie das Lesereplikat zu einem neuen DB-Cluster hochgestuft haben, ist es wie bei jedem anderen DB-Cluster. Sie können beispielsweise Lesereplikate daraus erstellen und point-in-time Wiederherstellungsvorgänge durchführen. Sie können auch Aurora-Replicas für den DB-Cluster erstellen.

Da der hochgestufte DB-Cluster kein Lesereplikat mehr ist, können Sie ihn nicht mehr als Replikationsziel verwenden.

Die folgenden Schritte zeigen den allgemeinen Vorgang für das Hochstufen eines Lesereplikats zu einem DB-Cluster:

1. Halten Sie alle Schreibvorgänge von Transaktionen im Lesereplikat-Quell-DB-Cluster an und warten Sie anschließend, bis alle Updates für das Lesereplikat abgeschlossen wurden. Datenbank-Updates werden im Lesereplikat durchgeführt, nachdem Sie im Quell-DB-Cluster aufgetreten sind; diese Replikationsverzögerung kann beträchtlich variieren. Verwenden Sie die Metrik `ReplicaLag`, um zu bestimmen, wann alle Aktualisierungen am Lesereplikat vorgenommen wurden. Die Metrik `ReplicaLag` zeichnet die Zeit auf, die eine Lesereplikat-DB-Instance hinter der Quell-DB-Instance zurückbleibt. Wenn die Metrik `ReplicaLag` den Wert `0` erreicht, hat das Lesereplikat den Stand der Quell-DB-Instance erreicht.
2. Stufen Sie das Lesereplikat mithilfe der Option Hochstufen in der Amazon-RDS-Konsole, des AWS CLI Befehls promote-read-replica-db-Cluster oder der PromoteReadReplicaDBCluster-Amazon-RDS-API-Operation hoch.

   Sie wählen eine Aurora MySQL-DB-Instance aus, um das Lesereplikat hochzustufen. Nachdem das Lesereplikat hochgestuft wurde, wird der Aurora MySQL-DB-Cluster zu einem eigenständigen DB-Cluster hochgestuft. Die DB-Instance mit der höchsten Failover-Priorität wird zu der primären DB-Instance für den DB-Cluster hochgestuft. Die anderen dB-Instances werden zu Aurora-Replicas.

   > **Note**
   >
   > Das Hochstufen kann einige Minuten in Anspruch nehmen. Wenn Sie ein Lesereplikat hochstufen, wird die Replikation gestoppt und die DB-Instances werden neu gestartet.

Sobald der Neustart abgeschlossen ist, steht das Lesereplikat als neuer DB-Cluster zur Verfügung.

Konsole

So stufen Sie ein Aurora MySQL-Lesereplikat zu einem DB-Cluster hoch:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der Konsole Instances aus.

   Der Bereich Instance wird angezeigt.
3. Wählen Sie im Bereich Instances das Lesereplikat aus, das Sie hochstufen möchten.

   Die Lesereplikate werden als Aurora MySQL-DB-Instances angezeigt.
4. Wählen Sie unter Aktionen Promote read replica (Read Replica hochstufen) aus.
5. Wählen Sie auf der Bestätigungsseite Read Replica hochstufen aus.

AWS CLI

Verwenden Sie den Befehl AWS CLI -promote-read-replica-dbcluster, um ein Lesereplikat zu einem DB-Cluster hochzustufen.

Example

Für Linux, macOSoder Unix:

```
aws rds promote-read-replica-db-cluster \
    --db-cluster-identifier mydbcluster
```

Windows:

```
aws rds promote-read-replica-db-cluster ^
    --db-cluster-identifier mydbcluster
```

RDS-API

Um ein Lesereplikat zu einem DB-Cluster hochzustufen, rufen Sie PromoteReadReplicaDBCluster auf.

Fehlerbehebung für regionsübergreifende Amazon Aurora MySQL-Replikate

Im Folgenden finden Sie eine Liste der häufigen Fehlermeldungen, die Sie beim Erstellen eines regionsübergreifenden Amazon Aurora-Lesereplikats erhalten könnten, und wie Sie die angegebenen Fehler beheben können.

Für Quell-Cluster [DB-Cluster-ARN] sind Binärprotokolle nicht aktiviert

Um dieses Problem zu lösen, aktivieren Sie die Binärprotokollierung für das Quell-DB-Cluster. Weitere Informationen finden Sie unter Bevor Sie beginnen.

Quell-Cluster [DB-Cluster-ARN] verfügt über keine Cluster-Parametergruppe, die zu einem Writer synchron ist

Diese Fehlermeldung erhalten Sie, wenn Sie den DB-Cluster-Parameter `binlog_format` aktualisiert haben, aber die primäre Instance für das DB-Cluster nicht neu gestartet haben. Starten Sie die primäre Instance (die schreibende Instance) für das DB-Cluster neu und versuchen Sie es erneut.

Quell-Cluster [DB-Cluster-ARN] verfügt bereits über ein Lesereplikat in dieser Region

Sie können über bis zu fünf regionsübergreifende DB-Cluster verfügen, die Lesereplikate für jeden Quell-DB-Cluster in jeder AWS-Region darstellen. Wenn in einer bestimmten AWS-Region bereits die maximale Anzahl von Lesereplikaten für einen DB-Cluster vorhanden ist, müssen Sie ein vorhandenes löschen, bevor Sie einen neuen regionsübergreifenden DB-Cluster in dieser Region erstellen können.

Für DB-Cluster [DB-Cluster-ARN] ist ein Upgrade der Datenbank-Engine für die Unterstützung einer regionsübergreifenden Replikation erforderlich

Führen Sie ein Upgrade der Datenbank-Engine-Version für alle Instances im Quell-DB-Cluster auf die aktuelle Datenbank-Engine-Version durch und versuchen Sie erneut, eine regionsübergreifende Lesereplikat-DB zu erstellen.

Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation)

Da Amazon Aurora MySQL mit MySQL kompatibel ist, können Sie eine Replikation zwischen einer MySQL-Datenbank und einem Amazon Aurora MySQL-DB-Cluster einrichten. Bei diesem Replikationstyp wird die binäre MySQL-Protokoll-Replikation verwendet, die auch als Binärprotokoll-Replikation bezeichnet wird. Wenn Sie die binäre Protokollreplikation mit Aurora verwenden, sollte Ihre MySQL-Datenbank MySQL-Version 5.5 oder höher verwenden. Sie können eine Replikation einrichten, bei der Ihr Aurora MySQL DB-Cluster die Replikationsquelle oder das Replica ist. Sie können mit einer Amazon RDS-MySQL-DB-Instance, einer MySQL-Datenbank außerhalb von Amazon RDS oder einem anderen Aurora MySQL-DB-Cluster replizieren.

> **Note**
>
> Sie können die an bestimmte Arten von Aurora-Clustern gesendete oder davon empfangene Binlog-Replikation nicht verwenden. Insbesondere ist die Binlog-Replikation nicht für Aurora Serverless v1-Cluster verfügbar. Wenn die Anweisungen `SHOW MASTER STATUS` und `SHOW SLAVE STATUS` (Aurora-MySQLVersion 2) oder `SHOW REPLICA STATUS` (Aurora-MySQL-Version 3) keine Ausgabe zurückgeben, überprüfen Sie, ob der von Ihnen verwendete Cluster die Binlog-Replikation unterstützt.
>
> In Aurora MySQL Version 3 können Sie mit der binären Protokollreplikation nicht in eine `mysql`-Systemdatenbank replizieren. In Aurora MySQL Version 3 werden keine Passwörter und Konten durch die binäre Protokollreplikation repliziert. Daher werden Data Control Language (DCL)-Anweisungen wie `CREATE USER`, `GRANT` und `REVOKE` nicht repliziert.

Sie können eine Replikation auch mit einer RDS-for-MySQL-DB-Instance oder einem Aurora-MySQL-DB-Cluster in einer anderen AWS-Region vornehmen. Wenn Sie eine Replikation durchführen AWS-Regionen, stellen Sie sicher, dass Ihre DB-Cluster und DB-Instances öffentlich zugänglich sind. Wenn sich die Aurora MySQL-DB-Cluster in privaten Subnetzen in Ihrer VPC befinden, verwenden Sie VPC-Peering zwischen den AWS-Regionen. Weitere Informationen finden Sie unter Ein DB-Cluster in einer VPC, auf den eine EC2-Instanz in einer anderen VPC zugreift.

Wenn Sie die Replikation zwischen einem Aurora MySQL-DB-Cluster und einem Aurora MySQL-DB-Cluster in einem anderen konfigurieren möchten AWS-Region, können Sie einen Aurora MySQL-DB-Cluster als Read Replica in einem anderen als AWS-Region dem Quell-DB-Cluster erstellen. Weitere Informationen finden Sie unter Replizieren von Amazon-Aurora-MySQL-DB-Clustern über AWS-Regionen hinweg.

Mit Auror-MySQL-Version 2 und 3 können Sie eine Replikation zwischen Aurora MySQL und einer externen Quelle oder einem Ziel durchführen, die bzw. das globale Transaktionskennungen

(Global Transaction Identifiers, GTIDs) für die Replikation verwendet. Stellen Sie sicher, dass die Einstellungen der GTID-bezogenen Parameter im Aurora MySQL-DB-Cluster mit dem GTID-Staus der externen Datenbank kompatibel sind. Weitere Informationen zur Vorgehensweise finden Sie unter Verwenden der GTID-basierten Replikation. In Aurora-MySQL-Version 3.01 und höher können Sie auswählen, wie GTIDs Transaktionen zugewiesen werden, die von einer Quelle repliziert werden, die keine GTIDs verwendet. Informationen zur gespeicherten Prozedur, die diese Einstellung steuert, finden Sie unter mysql.rds_assign_gtids_to_anonymous_transactions (Aurora MySQL Version 3).

> **Warning**
>
> Wenn Sie zwischen Aurora MySQL und MySQL replizieren, dürfen Sie nur InnoDB-Tabellen verwenden. Wenn Sie MyISAM-Tabellen replizieren möchten, müssen Sie diese mit dem folgenden Befehl in das InnoDB-Format konvertieren, bevor Sie die Replikation einrichten.
>
> ```
> alter table <schema>.<table_name> engine=innodb, algorithm=copy;
> ```

Einrichten einer Replikation mit einem MySQL- oder einem anderen Aurora-DB-Cluster

Das Einrichten einer MySQL-Replikation mit Aurora MySQL umfasst die folgenden Schritte, die ausführlich erklärt werden:

1. Aktivieren der Binärprotokollierung für die Replikationsquelle
2. Beibehaltung der Binärprotokolle für die Replikationsquelle, bis diese nicht mehr erforderlich sind
3. Erstellen eines Snapshots oder Dumps Ihrer Replikationsquelle
4. Laden des Snapshots oder Dumps in das Replikat-Ziel
5. Erstellen Sie einen Replikationsbenutzer auf Ihrer Replikationsquelle
6. Aktivieren der Replikation für das Replikat-Ziel
7. Überwachen Ihres Replikats

1. Aktivieren der Binärprotokollierung für die Replikationsquelle

Im Folgenden finden Sie die Anweisungen zum Aktivieren der Binärprotokollierung an der Replikationsquelle für Ihre Datenbank-Engine.

Datenbank-Engine	Anweisungen
Aurora MySQL	So aktivieren Sie die Binärprotokollierung für einen Aurora-MySQL-DB-Cluster Legen Sie den Parameter `binlog_format` auf `ROW`, `STATEMENT` oder `MIXED` fest. `MIXED` wird empfohlen, sofern kein bestimmtes Format für das Binärprotokoll notwendig ist. (Der Standardwert ist `OFF`.) Um den`binlog_format` -Parameter zu ändern, erstellen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe und ordnen Sie diese benutzerdefinierte Parametergruppe Ihrem DB-Cluster zu. Sie können die Parameter in einer Standard-DB-Clusterparametergruppe nicht ändern. Wenn Sie den Parameter `binlog_format` von `OFF` zu einem anderen Wert ändern, müssen Sie Ihren Aurora-DB-Cluster neu starten, damit die Änderung wirksam wird. Weitere Informationen erhalten Sie unter Amazon Aurora-DB-Cluster und DB-Instance-Parameter und Arbeiten mit Parametergruppen.
RDS for MySQL	So aktivieren Sie die Binärprotokollierung für eine Amazon RDS-DB-Instance Sie können die Binärprotokollierung nicht direkt für eine Amazon RDS-DB-Instance aktivieren, aber Sie können diese Funktion aktivieren, indem Sie Folgendes tun: • Deaktivieren Sie die automatischen Backups für die DB-Instance. Sie können automatische Backups aktivieren, wenn Sie eine DB-Instance erstellen, oder Sie können Backups aktivieren, indem Sie eine bestehende DB-Instance ändern. Weitere Informationen finden Sie unter Erstellen einer DB-Instance im Amazon RDS-Benutzerhandbuch. • Erstellen Sie ein Lesereplikat für die DB-Instance. Weitere Informationen finden Sie unter Arbeiten mit Read Replicas im Amazon RDS-Benutzerhandbuch.
MySQL (extern)	So richten Sie eine verschlüsselte Replikation ein Wenn Sie Daten sicher mit Aurora-MySQL-Version 2 replizieren möchten, verwenden Sie eine verschlüsselte Replikation.

Datenbank-Engine	Anweisungen

> **Note**
>
> Wenn Sie keine verschlüsselte Replikation benötigen, können Sie diese Schritte überspringen.

Folgende Voraussetzungen gelten für die Verwendung einer verschlüsselten Replikation:

- Secure Sockets Layer (SSL) muss in der externen MySQL-Quelldatenbank aktiviert sein.
- Ein Clientschlüssel und ein Clientzertifikat müssen für das Aurora MySQL-DB-Cluster vorbereitet werden.

Während der verschlüsselten Replikation dient das Aurora MySQL-DB-Cluster als Client für den MySQL-Datenbankserver. Die Zertifikate und Schlüssel für den Aurora MySQL-Client befinden sich in Dateien im PEM-Format.

1. Stellen Sie sicher, dass alle Vorbereitungen für die verschlüsselte Replikation getroffen wurden:

   - Wenn SSL auf dem externen Server mit der MySQL-Quelldatenbank nicht aktiviert ist und Sie keinen Clientschlüssel und kein Clientzertifikat vorbereitet haben, aktivieren Sie SSL auf dem MySQL-Datenbankserver und generieren Sie den Clientschlüssel und das Clientzertifikat.
   - Wenn SSL auf der externen Quelle aktiviert ist, geben Sie einen Clientschlüssel und ein Clientzertifikat für das Aurora MySQL-DB-Cluster an. Wenn Sie diese Werte nicht haben, erstellen Sie ein einen neuen Schlüssel und ein neues Zertifikat für das Aurora MySQL-DB-Cluster. Sie benötigen zur Signierung des Clientzertifikats den Zertifizierungsstellenschlüssel, den Sie zum Konfigurieren von SSL auf der externen MySQL-Quelldatenbank verwendet haben.

Datenbank-Engine	Anweisungen

Weitere Informationen finden Sie unter Creating SSL Certificates and Keys Using openssl in der MySQL-Dokumentation.

Sie benötigen das Zertifizierungsstellenzertifikat, den Clientschlüssel und das Clientzertifikat.

2. Stellen Sie als Masterbenutzer über SSL eine Verbindung zum Aurora MySQL-DB-Cluster her.

   Informationen zum Herstellen einer Verbindung mit einem Aurora MySQL-DB-Cluster über SSL finden Sie unter Verwenden von TLS mit DB-Clustern von Aurora MySQL.

3. Führen Sie die gespeicherte Prozedur `mysql.rds_import_binlog_ssl_material` aus, um die SSL-Informationen in das Aurora MySQL-DB-Cluster zu importieren.

   Fügen Sie die Informationen aus den PEM-Dateien für das Aurora MySQL-DB-Cluster in die korrekte JSON-Nutzlast für den Parameter `ssl_material_value` ein.

   Im folgenden Beispiel werden SSL-Informationen in ein Aurora MySQL-DB-Cluster importiert. Der Code in den PEM-Dateien ist in der Regel länger als in diesem Beispiel.

```
call mysql.rds_import_binlog_ssl_material(
'{"ssl_ca":"-----BEGIN CERTIFICATE-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcj
qP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96
xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz22
1CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Datenbank-Engine	Anweisungen

```
-----END CERTIFICATE-----\n","ssl_cert":"-----BEGIN CERTIFICA
TE-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcj
qP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96
xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz22
1CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END CERTIFICATE-----\n","ssl_key":"-----BEGIN RSA PRIVATE
 KEY-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pc
jqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSF
JuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJ
tjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMu
cxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END RSA PRIVATE KEY-----\n"}');
```

Weitere Informationen finden Sie unter mysql.rds_import_binlog_ssl_material und Verwenden von TLS mit DB-Clustern von Aurora MySQL.

> **Note**
>
> Nach dem Ausführen der Prozedur werden die SSL-Informationen in Dateien gespeichert. Um die Dateien später zu löschen, können Sie die mysql.rds_remove_binlog_ssl_material gespeicherte Prozedur ausführen.

So aktivieren Sie die Binärprotokollierung für eine externe MySQL-Datenbank

1. Halten Sie mit dieser Befehlszeile den mysql-Service an.

Datenbank-Engine	Anweisungen

```
sudo service mysqld stop
```

2. Bearbeiten Sie die `my.cnf`-Datei (diese Datei befindet sich üblicherweise unter `/etc`).

```
sudo vi /etc/my.cnf
```

Fügen Sie die Optionen `log_bin` und `server_id` zum Abschnitt `[mysqld]` hinzu. Die Option `log_bin` bietet eine Dateinamenkennung für Binärprotokolldateien. Die Option `server_id` stellt eine eindeutige Kennung für den Server für Quelle-Replica-Beziehungen bereit.

Wenn keine verschlüsselte Replikation erforderlich ist, muss die externe MySQL-Datenbank mit aktivierten Binärprotokollen und aktiviertem SSL gestartet werden.

Dies sind die relevanten Einträge für unverschlüsselte Daten in der Datei `/etc/my.cnf` .

```
log-bin=mysql-bin
server-id=2133421
innodb_flush_log_at_trx_commit=1
sync_binlog=1
```

Wenn die verschlüsselte Replikation erforderlich ist, muss die externe MySQL-Datenbank mit aktivierten Binärprotokollen und aktiviertem SSL gestartet werden.

Die Einträge in der Datei `/etc/my.cnf` müssen dann die Speicherorte der PEM-Dateien für den MySQL-Datenbankserver enthalten.

```
log-bin=mysql-bin
server-id=2133421
innodb_flush_log_at_trx_commit=1
sync_binlog=1

# Setup SSL.
ssl-ca=/home/sslcerts/ca.pem
```

Datenbank-Engine	Anweisungen

```
ssl-cert=/home/sslcerts/server-cert.pem
ssl-key=/home/sslcerts/server-key.pem
```

Zusätzlich muss die Option `sql_mode` für Ihre MySQL-DB-Instance auf 0 gesetzt oder in Ihrer my.cnf-Datei enthalten sein.

Zeichnen Sie die Position der Binärprotokolle der externen MySQL-Datenbank auf, während Sie mit der Datenbank verbunden sind.

```
mysql> SHOW MASTER STATUS;
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
+------------------+----------+--------------+------------------
+-------------------+
| File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
 Executed_Gtid_Set |
+------------------+----------+--------------+------------------
+-------------------+
| mysql-bin.000031 |      107 |              |                  |
               |
+------------------+----------+--------------+------------------
+-------------------+
1 row in set (0.00 sec)
```

Weitere Informationen finden Sie unter Setting the replication source configuration in der MySQL-Dokumentation.

3. Starten Sie den mysql-Service.

```
sudo service mysqld start
```

2. Beibehaltung der Binärprotokolle für die Replikationsquelle, bis diese nicht mehr erforderlich sind

Wenn Sie die binäre MySQL-Protokollreplikation verwenden, verwaltet Amazon RDS den Replikationsvorgang nicht. Daher müssen Sie sicherstellen, dass die Binärprotokolldateien an Ihre

Replikationsquelle so lange aufbewahrt werden, bis die Änderungen auf das Replica angewandt wurden. Durch diese Pflege können Sie Ihre Quelldatenbank im Fall eines Ausfalls wiederherstellen.

Verwenden Sie folgende Anweisungen zur Beibehaltung von Binärprotokollen für Ihre Datenbank-Engine.

Datenbank-Engine	Anweisungen
Aurora MySQL	So bewahren Sie Binärprotokolle für einen Aurora MySQL-DB-Cluster auf Sie haben keinen Zugriff auf die Binärprotokolldateien eines Aurora-MySQL-DB-Clusters. Daher müssen Sie für die Aufbewahrung der Binärprotokolldateien an Ihrer Replikationsquelle ein ausreichend langes Zeitfenster festlegen, um sicherzustellen, dass die Änderungen auf Ihr Replica angewandt wurden, bevor die Binärprotokolldatei von Amazon RDS gelöscht wird. Sie können diese Binärprotokolldateien in einem Aurora MySQL-DB-Cluster für bis zu 90 Tage aufbewahren. Wenn Sie eine Replikation mit einer MySQL-Datenbank oder einer RDS für MySQL-DB-Instance als Replica einrichten und die Datenbank, für die Sie eine Replica erstellen, sehr groß ist, wählen Sie ein großes Zeitfenster, um Binärprotokolldateien aufzubewahren, bis die erste Kopie der Datenbank in der Replica abgeschlossen ist und die Replica-Verzögerung den Wert 0 erreicht hat. Verwenden Sie zur Festlegung der Aufbewahrungszeit für Binärprotokolldateien die Prozedur mysql.rds_set_configuration und legen Sie einen Konfigurationsparameter für `'binlog retention hours'` zusammen mit der Stundenanzahl für die Aufbewahrung der Binärprotokolldateien im DB-Cluster fest. Der maximal zulässige Wert für Aurora MySQL Version 2.11.0 und höher sowie Version 3 ist 2 160 (90 Tage). Beim folgenden Beispiel wird der Aufbewahrungszeitraum für binäre Protokolle auf 6 Tage festgelegt: `CALL mysql.rds_set_configuration('binlog retention hours', 144);` Nachdem die Replikation gestartet wurde, können Sie nach dem Ausführen des Befehls `SHOW SLAVE STATUS` (Aurora-MySQL-Version 2) oder `SHOW REPLICA`

Datenbank-Engine	Anweisungen
	`STATUS` (Aurora-MySQL-Version 3) für das Read Replica im Feld `Seconds behind master` überprüfen, ob Änderungen auf Ihr Replica angewandt wurden. Wenn der Wert im Feld `Seconds behind master` 0 ist, gibt es keine Replikatverzögerung. Wenn keine Replica-Verzögerung vorliegt, reduzieren Sie den Aufbewahrungszeitraum für die Binärprotokolldateien, indem Sie den Konfigurationsparameter `binlog retention hours` auf ein kleineres Zeitfenster einstellen. Wenn diese Einstellung nicht angegeben wird, ist der Standardwert für Aurora MySQL 24 (1 Tag). Wenn Sie einen Wert für `'binlog retention hours'` angeben, der den maximal zulässigen Wert überschreitet, dann wird von Aurora MySQL der maximale Wert verwendet.
RDS for MySQL	So bewahren Sie Binärprotokolle einer Amazon RDS-DB-Instance auf Sie können binäre Protokolldateien auf einer Amazon-RDS-DB-Instance aufbewahren, indem Sie die Stundenanzahl für die Aufbewahrung einstellen, so wie es bereits für einen Aurora-MySQL-DB-Cluster im vorherigen Anschnitt erläutert wurde. Sie können auch Binärprotokolldateien für eine Amazon RDS-DB-Instance aufbewahren, indem Sie ein Lesereplikat von dieser DB-Instance erstellen. Dieses Lesereplikat ist temporär und lediglich dazu gedacht, Binärprotokolldateien aufzubewahren. Nachdem das Lesereplikat erstellt wurde, rufen Sie die Prozedur mysql.rds_stop_replication für das Lesereplikat auf. Während die Replikation angehalten wird, löscht Amazon RDS keine der Binärprotokolldateien für die Replikationsquelle. Nachdem Sie die Replikation mit Ihrem permanenten Replikat eingerichtet haben, können Sie das Read-Replikat löschen, sobald die Replikat-Verzögerung (Feld `Seconds behind master`) zwischen Ihrer Replikationsquelle und Ihrem permanenten Replikat den Wert 0 erreicht hat.

Datenbank-Engine	Anweisungen
MySQL (extern)	So bewahren Sie Binärprotokolle in einer externen MySQL-Datenbank Da die Binärprotokolldateien in einer externen MySQL-Datenbank nicht von Amazon RDS verwaltet werden, werden diese aufbewahrt, bis Sie sie selbst löschen. Nachdem die Replikation gestartet wurde, können Sie nach dem Ausführen des Befehls `SHOW SLAVE STATUS` (Aurora-MySQL-Version 2) oder `SHOW REPLICA STATUS` (Aurora-MySQL-Version 3) für das Read Replica im Feld `Seconds behind master` überprüfen, ob Änderungen auf Ihr Replica angewandt wurden. Wenn der Wert im Feld `Seconds behind master` 0 ist, gibt es keine Replikatverzögerung. Wenn keine Replica-Verzögerung besteht, können Sie alte Binärprotokolldateien löschen.

3. Erstellen eines Snapshots oder Dumps Ihrer Replikationsquelle

Sie verwenden einen Snapshot oder Dump Ihrer Replikationsquelle, um die Baseline-Kopie Ihrer Daten in Ihr Replica zu kopieren und starten die Replikation dann ab diesem Punkt.

Verwenden Sie folgende Anweisungen zum Erstellen eines Snapshots oder Dumps der Replikationsquelle für Ihre Datenbank-Engine.

Datenbank-Engine	Anweisungen
Aurora MySQL	So erstellen Sie einen Snapshot eines Aurora MySQL-DB-Clusters 1. Erstellen Sie einen DB-Cluster-Snapshot Ihres Amazon Aurora-DB-Clusters. Weitere Informationen finden Sie unter Erstellen eines DB-Cluster-Snapshots. 2. Erstellen Sie ein neues Aurora-DB-Cluster, indem Sie eine Wiederherstellung aus einem kürzlich erstellten DB-Cluster-Snapshot durchführen. Stellen Sie sicher, dass Sie dieselbe DB-Parametergruppe für Ihr wiederhergestelltes DB-Cluster wie für Ihr ursprüngliches DB-Cluster aufbewahren. Dadurch wird sichergestellt, dass die Binärprotokollierung für die Kopie des DB-Clusters aktiviert ist. Weitere Informationen finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.

Datenbank-Engine	Anweisungen

3. Wählen Sie in der Konsole Databases (Datenbanken) und anschließend die primäre Instance (Writer) für Ihren wiederhergestellten Aurora-DB-Cluster aus, um Details anzuzeigen. Scrollen Sie zu Recent Events (Aktuelle Ereignisse). Eine Ereignismeldung zeigt den Namen und die Position der Binärprotokolldatei an. Die Ereignismeldung liegt im folgenden Format vor.

```
Binlog position from crash recovery is binlog-file-name  binlog-po
sition
```

Speichern Sie den Binärprotokolldateinamen- und die -positionswerte für den Beginn einer Replikation.

Sie erhalten den Binärprotokolldateinamen und die -position auch, indem Sie den AWS CLI-Befehl describe-events ausführen. Im folgenden Beispiel wird der Befehl `describe-events` mit einer Beispielausgabe gezeigt.

```
PROMPT> aws rds describe-events
```

```
{
    "Events": [
        {
            "EventCategories": [],
            "SourceType": "db-instance",
            "SourceArn": "arn:aws:rds:us-west-2:123456789012:
db:sample-restored-instance",
            "Date": "2016-10-28T19:43:46.862Z",
            "Message": "Binlog position from crash recovery is mysql-
bin-changelog.000003 4278",
            "SourceIdentifier": "sample-restored-instance"
        }
    ]
}
```

Sie erhalten den Namen und die Position der Binärprotokolldateien, indem Sie im MySQL-Fehlerprotokoll nach der letzten MySQL-Binärprotokolldatei suchen.

Datenbank-Engine	Anweisungen
	4. Wenn Ihr Replikatziel eine externe MySQL-Datenbank oder eine RDS for MySQL-DB-Instance ist, können Sie die Daten nicht aus einem Amazon Aurora Aurora-DB-Cluster-Snapshot laden. Erstellen Sie stattdessen eine Dumpdatei des DB-Clusters von Amazon Aurora, indem Sie über einen MySQL-Client eine Verbindung mit dem DB-Cluster herstellen und den Befehl `mysqldump` ausführen. Stellen Sie sicher, dass der Befehl `mysqldump` für die Kopie des von Ihnen erstellten DB-Clusters von Amazon Aurora ausgeführt wird. Im Folgenden wird ein Beispiel gezeigt. `PROMPT> mysqldump --databases <database_name> --single-transaction --order-by-primary -r backup.sql -u <local_user> -p` 5. Wenn Sie mit dem Erstellen des Auszugs Ihrer Daten aus dem neu erstellten Aurora-DB-Cluster fertig sind, löschen Sie dieses DB-Cluster, da es nicht länger benötigt wird.
RDS for MySQL	So erstellen Sie einen Snapshot Ihrer Amazon RDS-DB-Instance Erstellen Sie ein Lesereplikat Ihrer Amazon RDS-DB-Instance. Weitere Informationen finden Sie unter Erstellen einer Read Replica im Amazon Relational Database Service-Benutzerhandbuch. 1. Verbinden Sie sich mit Ihrem Lesereplikat und halten Sie die Replikation mithilfe der Prozedur mysql.rds_stop_replication an. 2. Während die Read Replica angehalten ist, stellen Sie eine Verbindung zur Read Replica her und führen Sie den Befehl `SHOW SLAVE STATUS` (Aurora-MySQL-Version 2) oder `SHOW REPLICA STATUS` (Aurora-MySQL-Version 3) aus. Rufen Sie den aktuellen Namen der Binärprotokolldatei aus dem Feld `Relay_Master_Log_File` und die Position aus dem Feld `Exec_Master_Log_Pos` ab. Speichern Sie diese Werte für den Start einer Replikation. 3. Solange das Lesereplikat im Status Stopped (Angehalten) verweilt, erstellen Sie einen DB-Snapshot dieses Lesereplikats. Weitere Informationen finden Sie unter Erstellen eines DB-Snapshots im Amazon Relational Database Service-Benutzerhandbuch. 4. Löschen Sie das Read Replica.

Datenbank-Engine	Anweisungen

MySQL (extern)	So erstellen Sie einen Dump einer externen MySQL-Datenbank
	1. Bevor Sie einen Dump erstellen, müssen Sie sicherstellen, dass der Speicherort Ihres Binärprotokolls für den Dump auf dem aktuellen Stand der Daten Ihrer Quell-Instance ist. Hierfür müssen Sie als Erstes alle Schreibvorgänge für diese Instance mithilfe des folgenden Befehls anhalten:
	`mysql> FLUSH TABLES WITH READ LOCK;`
	2. Erstellen Sie einen Dump Ihrer MySQL-Datenbank mithilfe des Befehls `mysqldump` , wie im Folgenden gezeigt:
	`PROMPT> sudo mysqldump --databases <database_name> --master-data=2 --single-transaction \ --order-by-primary -r backup.sql -u <local_user> -p`
	3. Nachdem Sie den Dump erstellt haben, entsperren Sie die Tabellen in Ihrer MySQL-Datenbank mit dem folgenden Befehl:
	`mysql> UNLOCK TABLES;`

4. Laden des Snapshots oder Dumps in das Replikat-Ziel

Wenn Sie Daten aus einem Dump einer Amazon RDS-externen MySQL-Datenbank laden möchten, können Sie eine EC2-Instance erstellen, die Dumpdateien dorthin kopieren und die Daten anschließend aus dieser EC2-Instance in das DB-Cluster oder die DB-Instance laden. Bei Verwendung dieses Ansatzes können Sie die Dumpdateien komprimieren, bevor Sie sie in eine EC2-Instance kopieren, um Netzwerkkosten zu minimieren, die in Verbindung mit dem Kopieren von Dateien nach Amazon RDS entstehen. Sie können die Dumpdatei oder -dateien auch verschlüsseln, um sie beim Übermitteln im Netzwerk zu schützen.

Verwenden Sie folgende Anweisungen, um den Snapshot Ihrer Replikationsquelle in das Replikat-Ziel für Ihre Datenbank-Engine zu laden.

Datenbank-Engine	Anweisungen

Aurora MySQL	So laden Sie einen Snapshot oder Dump in einen DB-Cluster von Aurora MySQL
	• Wenn der Snapshot der Replikationsquelle ein DB-Cluster-Snapshot ist, können Sie aus dem DB-Cluster-Snapshot wiederherstellen, um ein neues Aurora MySQL-DB-Cluster als Replica-Ziel erstellen. Weitere Informationen finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.
	• Wenn der Snapshot Ihrer Replikationsquelle ein DB-Snapshot ist, können Sie die Daten aus dem DB-Snapshot in ein neues Aurora MySQL-DB-Cluster migrieren . Weitere Informationen finden Sie unter Migrieren von Daten zu einem Amazon Aurora MySQL-DB-Cluster.
	• Wenn die Daten Ihrer Replikationsquelle der Ausgabe des `mysqldump` -Befehls entsprechen, führen Sie folgende Schritte aus:
	1. Kopieren Sie die Ausgabe des Befehls `mysqldump` von der Replikationsquelle an einen Speicherort, der auch eine Verbindung zum Aurora MySQL-DB-Cluster herstellen kann.
	2. Verbinden Sie sich mithilfe des `mysql`-Befehls mit Ihrem Aurora MySQL-DB-Cluster. Im Folgenden wird ein Beispiel gezeigt.
	`PROMPT> mysql -h <host_name> -port=3306 -u <db_master_user> -p`
	3. Führen Sie in der `mysql`-Eingabeaufforderung den Befehl `source` aus und geben Sie den Namen Ihrer Datenbank-Dumpdatei ein, um die Daten in den Aurora MySQL-DB-Cluster zu laden, zum Beispiel:
	`mysql> source backup.sql;`

RDS for MySQL	So laden Sie einen Dump in eine DB-Instance von Amazon RDS 1. Kopieren Sie die Ausgabe des Befehls `mysqldump` von Ihrer Replikationsquelle an einen Speicherort, der auch eine Verbindung mit Ihrer MySQL-DB-Instance herstellen kann. 2. Verbinden Sie sich mit Ihrer MySQL-DB-Instance mithilfe des `mysql`-Befehls. Im Folgenden wird ein Beispiel gezeigt.

Datenbank-Engine	Anweisungen
	``` PROMPT> mysql -h <host_name> -port=3306 -u <db_master_user> -p ``` 3. Führen Sie in der `mysql`-Eingabeaufforderung den Befehl `source` aus und geben Sie den Namen Ihrer Datenbank-Dumpdatei mit, um deren Daten in die My-DB-Instance zu laden, zum Beispiel: ``` mysql> source backup.sql; ```
MySQL (extern)	So laden Sie einen Dump in eine externe MySQL-Datenbank Sie können keinen DB-Snapshot oder DB-Cluster-Snapshot in eine externe MySQL-Datenbank laden. Stattdessen müssen Sie die Ausgabe des `mysqldump` -Befehls verwenden. 1. Kopieren Sie die Ausgabe des Befehls `mysqldump` von der Replikationsquelle an einen Speicherort, der auch eine Verbindung zur MySQL-Datenbank herstellen kann. 2. Verbinden Sie sich mit Ihrer MySQL-Datenbank mithilfe des `mysql`-Befehls. Im Folgenden wird ein Beispiel gezeigt. ``` PROMPT> mysql -h <host_name> -port=3306 -u <db_master_user> -p ``` 3. Führen Sie an der `mysql`-Eingabeaufforderung den Befehl `source` aus und übergeben Sie den Namen der Datenbank-Dumpdatei, deren Daten in die MySQL-Datenbank geladen werden sollen. Im Folgenden wird ein Beispiel gezeigt. ``` mysql> source backup.sql; ```

5. Erstellen Sie einen Replikationsbenutzer auf Ihrer Replikationsquelle

Erstellen Sie eine Benutzer-ID an der Quelle, die ausschließlich für die Replikation verwendet wird. Das folgende Beispiel bezieht sich auf RDS für MySQL oder externe MySQL-Quelldatenbanken.

```
mysql> CREATE USER 'repl_user'@'domain_name' IDENTIFIED BY 'password';
```

Für Aurora MySQL-Quelldatenbanken ist der `skip_name_resolve` DB-Cluster-Parameter auf 1 (0N) gesetzt und kann nicht geändert werden. Sie müssen also eine IP-Adresse für den Host anstelle eines Domainnamens verwenden. Weitere Informationen finden Sie unter skip_name_resolve in der MySQL-Dokumentation.

```
mysql> CREATE USER 'repl_user'@'IP_address' IDENTIFIED BY 'password';
```

Der Benutzer benötigt die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE`. Gewähren Sie dem Benutzer diese Berechtigungen.

Wenn die Replikation verschlüsselt durchgeführt werden muss, fordern Sie für den Replikationsbenutzer eine SSL-Verbindung an. Sie können beispielsweise eine der folgenden Anweisungen verwenden, um SSL-Verbindungen für das Benutzerkonto vorzuschreiben. `repl_user`

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'IP_address';
```

```
GRANT USAGE ON *.* TO 'repl_user'@'IP_address' REQUIRE SSL;
```

> **Note**
>
> Wenn `REQUIRE SSL` nicht angegeben wird, kann die Replikationsverbindung ohne entsprechende Meldung auf eine unverschlüsselte Verbindung zurückgesetzt werden.

6. Aktivieren der Replikation für das Replikat-Ziel

Bevor Sie die Replikation aktivieren, empfehlen wir, manuell einen Snapshot des Aurora-MySQL-DB-Clusters oder des RDS for MySQL-DB-Instance Replica-Ziels zu erstellen. Wenn ein Problem auftritt und Sie den Replikationsvorgang mit dem DB-Cluster oder dem DB-Instance-Replica-Ziel wieder einrichten müssen, können Sie das DB-Cluster bzw. die DB-Instance aus diesem Snapshot wiederherstellen, anstatt erneut Daten in das Replica-Ziel zu importieren.

Verwenden Sie folgende Anweisungen zum Aktivieren der Replikation für Ihre Datenbank-Engine.

Datenbank-Engine	Anweisungen

Aurora MySQL	So aktivieren Sie die Replikation aus einem Aurora-MySQL-DB-Cluster
	1. Suchen Sie den Startpunkt für die Replikation. Sie benötigen den Namen der Binärprotokolldatei und die Binärprotokollposition.
	Wenn Ihr DB-Cluster-Replikatziel auf Folgendem erstellt wurde:
	• DB-Cluster-Snapshot – Rufen Sie den Namen und die Position der Binärprotokolldatei aus den letzten Ereignissen für Ihren wiederhergestellten DB-Cluster ab, wie unter 3. Erstellen eines Snapshots oder Dumps Ihrer Replikationsquelle gezeigt.
	• DB-Snapshot – Sie haben den Binärprotokoll-Dateinamen und die -position aus dem Befehl `SHOW SLAVE STATUS` (Aurora MySQL Version 2) oder `SHOW REPLICA STATUS` (Aurora MySQL Version 3) abgerufen, als Sie den Snapshot Ihrer Replikationsquelle erstellt haben.
	2. Stellen Sie eine Verbindung mit dem DB-Cluster her und rufen Sie die folgenden Prozeduren auf, um eine Replikation mit Ihrer Replikationsquelle unter Verwendung des Namens und des Speicherorts der Binärprotokolldatei aus dem vorherigen Schritt zu starten:
	• mysql.rds_set_external_source (Aurora MySQL Version 3)
	• mysql.rds_set_external_master (Aurora-MySQL-Version 2)
	• mysql.rds_start_replication (alle Versionen)
	Das folgende Beispiel gilt für Aurora MySQL Version 3.
	`CALL mysql.rds_set_external_source ('mydbinstance.123456789012.us-east-1.rds.amazonaws.com', 3306, 'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 0);`
	`CALL mysql.rds_start_replication;`
	Zur Verwendung der SSL-Verschlüsselung legen Sie den endgültigen Wert auf 1 statt auf `0` fest.

Datenbank-Engine	Anweisungen

RDS for MySQL	So aktivieren Sie die Replikation aus einer Amazon RDS-DB-Instance
	1. Wenn das DB-Instance-Replica-Ziel aus einem DB-Snapshot erstellt wurde, benötigen Sie den Namen der Binärprotokolldatei und die Position in der Datei, ab der die Replikation durchgeführt werden soll. Sie haben diese Werte aus dem Befehl `SHOW SLAVE STATUS` (Aurora-MySQL-Version 2) oder `SHOW REPLICA STATUS` (Aurora-MySQL-Version 3) abgerufen, als Sie den Snapshot Ihrer Replikationsquelle erstellt haben.
	2. Stellen Sie eine Verbindung zur DB-Instance her und rufen Sie die Prozeduren mysql.rds_set_external_master (Aurora-MySQL-Version 2) odermysql.rds_set_external_source (Aurora MySQL Version 3) und mysql.rds_start_replication auf, um eine Replikation mit Ihrer Replikationsquelle zu starten. Verwenden Sie den Namen und den Speicherort der Binärprotokolldatei aus dem vorherigen Schritt. Im Folgenden wird ein Beispiel gezeigt.
	`CALL mysql.rds_set_external_master ('mydbcluster.cluster-123456789012.us-east-1.rds.amazonaws.com', 3306, 'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 0);`
	`CALL mysql.rds_start_replication;`
	Zur Verwendung der SSL-Verschlüsselung legen Sie den endgültigen Wert auf 1 statt auf `0` fest.

Datenbank-Engine	Anweisungen

MySQL (extern)	So aktivieren Sie die Replikation aus einer externen MySQL-Datenbank
	1. Erhalten Sie den Namen und die Position der Binärprotokolldatei, die der Ausgangspunkt für eine Replikation sind. Sie haben diese Werte aus dem Befehl `SHOW SLAVE STATUS` (Aurora-MySQL-Version 2) oder `SHOW REPLICA STATUS` (Aurora-MySQL-Version 3) abgerufen, als Sie den Snapshot Ihrer Replikationsquelle erstellt haben. Wenn das externe MySQL-Replica-Ziel durch den `mysqldump` -Befehl mit der Option `--master-data=2` mit Daten gefüllt wurde, sind der Name und die Position der Binärprotokolldatei in den ausgegebenen Informationen enthalten. Im Folgenden wird ein Beispiel gezeigt.
	`-- -- Position to start replication or point-in-time recovery from -- -- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031', MASTER_LOG_POS=107;`
	2. Stellen Sie eine Verbindung zum externen MySQL-Replica-Ziel her und führen Sie die Befehle `CHANGE MASTER TO` und `START SLAVE` (Aurora-MySQL-Version 2) oder `START REPLICA` (Aurora-MySQL-Version 3) aus, um eine Replikation mit der Replikationsquelle mithilfe des Namens und der Position der Binärprotokolldatei aus dem vorherigen Schritt zu starten. Beispiel:
	`CHANGE MASTER TO MASTER_HOST = 'mydbcluster.cluster-123456789012.us-east-1.rds.amazonaws.com', MASTER_PORT = 3306, MASTER_USER = 'repl_user', MASTER_PASSWORD = 'password', MASTER_LOG_FILE = 'mysql-bin-changelog.000031', MASTER_LOG_POS = 107; -- And one of these statements depending on your engine version: START SLAVE; -- Aurora MySQL version 2 START REPLICA; -- Aurora MySQL version 3`

Wenn die Replikation fehlschlägt, kann dies zu einem starken Anstieg der unbeabsichtigten I/O auf dem Replikat führen, was die Leistung beeinträchtigen kann. Wenn die Replikation fehlschlägt oder nicht mehr benötigt wird, können Sie das gespeicherte Verfahren mysql.rds_reset_external_master (Aurora-MySQL-Version 2) oder mysql.rds_reset_external_source (Aurora MySQL Version 3) zum Entfernen der Replikationskonfiguration durchführen.

Festlegen einer Position zum Stoppen der Replikation zu einer Read Replica

In der Aurora MySQL-Version 3.04 und höher können Sie die Replikation starten und dann an einem bestimmten Ort in der Binär-Protokolldatei mit der gespeicherten mysql.rds_start_replication_until (Aurora-MySQL-Version 3)-Prozedur anhalten.

Starten Sie die Replikation für ein Lesereplikat und stoppen Sie die Replikation an einer bestimmten Position wie folgt:

1. Stellen Sie über einen MySQL-Client als Masterbenutzer eine Verbindung zum Replikat-Aurora-MySQL-DB-Cluster her.
2. Führen Sie die gespeicherte Prozedur mysql.rds_start_replication_until (Aurora-MySQL-Version 3) aus.

   Das folgende Beispiel initiiert die Replikation und repliziert die Änderungen, bis die Position `120` in der Binärprotokolldatei `mysql-bin-changelog.000777` erreicht wird. Beispiel: In einem Szenario der Notfallwiederherstellung liegt die Position `120` unmittelbar vor der Katastrophe.

   ```
   call mysql.rds_start_replication_until(
     'mysql-bin-changelog.000777',
     120);
   ```

Die Replikation stoppt automatisch, sobald der Stopppunkt erreicht ist. Das folgende RDS-Ereignis wird generiert: `Replication has been stopped since the replica reached the stop point specified by the rds_start_replication_until stored procedure`.

Wenn Sie die GTID-basierte Replikation verwenden, nutzen Sie die gespeicherte Prozedur mysql.rds_start_replication_until_gtid (Aurora-MySQL-Version 3) anstelle der gespeicherten Prozedur mysql.rds_start_replication_until (Aurora-MySQL-Version 3). Weitere Informationen zu GTID-basierten Replikationen finden Sie unter Verwenden der GTID-basierten Replikation.

7. Überwachen Ihres Replikats

Wenn Sie eine MySQL-Replikation mit einem Aurora MySQL-DB-Cluster eingerichtet haben, müssen Sie Failover-Ereignisse für den Aurora MySQL-DB-Cluster überwachen, wenn dieser ein Replica-Ziel ist. Im Falle eines Failovers kann dann das DB-Cluster (das Replica-Ziel) auf einem neuen Host mit einer anderen Netzwerkadresse erneut erstellt werden. Weitere Informationen zum Überwachen von Failover-Ereignissen finden Sie unter Arbeiten mit Amazon-RDS-Ereignisbenachrichtigungen.

Sie können außerdem überwachen, wie weit das Replica-Ziel hinter der Replikationsquelle zurückliegt, indem Sie eine Verbindung zum Replica-Ziel herstellen und den Befehl `SHOW SLAVE STATUS` (Aurora-MySQL-Version 2) oder `SHOW REPLICA STATUS` (Aurora-MySQL-Version 3) ausführen. In der Befehlsausgabe wird im Feld `Seconds Behind Master` angezeigt, wie weit das Replica-Ziel hinter der Quelle zurückliegt.

Synchronisierung von Passwörtern zwischen Replikationsquelle und -ziel

Wenn Sie Benutzerkonten und Kennwörter auf der Replikationsquelle mithilfe von SQL-Anweisungen ändern, werden diese Änderungen automatisch auf das Replikationsziel repliziert.

Wenn Sie die AWS Management Console, die oder die RDS-API verwenden AWS CLI, um das Master-Passwort für die Replikationsquelle zu ändern, werden diese Änderungen nicht automatisch auf das Replizierungsziel repliziert. Wenn Sie den Master-Benutzer und das Master-Kennwort zwischen dem Quell- und dem Zielsystem synchronisieren möchten, müssen Sie die gleiche Änderung auf dem Replikationsziel selbst vornehmen.

Anhalten einer Replikation zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster

Folgen Sie diesen im folgenden Verlauf detailliert beschriebenen Schritten, um eine binäre Protokollreplikation mit einer MySQL-DB-Instance, einer externen MySQL-Datenbank oder einem anderen Aurora-DB-Cluster anzuhalten.

1. Anhalten der binären Protokollreplikation für das Replikat-Ziel

2. Deaktivieren der Binärprotokollierung für die Replikationsquelle

1. Anhalten der binären Protokollreplikation für das Replikat-Ziel

Im Folgenden finden Sie die Anweisungen zum Anhalten der binären Protokollreplikation für Ihre Datenbank-Engine.

Datenbank-Engine	Anweisungen
Aurora MySQL	So können Sie die binären Protokollreplikation in einem Aurora MySQL-DB-Cluster-Replica-Ziel anhalten Stellen Sie eine Verbindung mit dem als Replica-Ziel verwendeten Aurora-DB-Cluster her und rufen Sie die Prozedur mysql.rds_stop_replication auf.
RDS for MySQL	So können Sie eine binären Protokollreplikation in einer Amazon RDS-DB-Instance anhalten Stellen Sie eine Verbindung mit der als Replica-Ziel verwendeten RDS-DB-Instance her und rufen Sie die Prozedur mysql.rds_stop_replication auf.
MySQL (extern)	So halten Sie die binären Protokollreplikation für eine externe MySQL-Datenbank an Stellen Sie eine Verbindung mit der MySQL-Datenbank her und führen Sie den Befehl `STOP SLAVE` (Version 5.7) oder `STOP REPLICA` (Version 8.0) aus.

2. Deaktivieren der Binärprotokollierung für die Replikationsquelle

Im Folgenden finden Sie die Anweisungen zum Deaktivieren der Binärprotokollierung an der Replikationsquelle für Ihre Datenbank-Engine.

Datenbank-Engine	Anweisungen
Aurora MySQL	So deaktivieren Sie die Binärprotokollierung für einen Amazon-Aurora-DB-Cluster 1. Stellen Sie eine Verbindung mit dem als Replikationsquelle verwendeten Aurora-DB-Cluster her. 2. Verwenden Sie das Verfahren mysql.rds_set_configuration und geben Sie den Konfigurationsparameter `binlog retention hours` mit dem Wert `NULL` an, wie im folgenden Beispiel gezeigt. `CALL mysql.rds_set_configuration('binlog retention hours', NULL);`

Datenbank-Engine	Anweisungen
	> **Note** Sie können den Wert `0` nicht für `binlog retention hours` verwenden. 3. Stellen Sie den Parameter `binlog_format` für die Replikationsquelle auf `OFF` ein. Der`binlog_format` -Parameter befindet sich in der benutzerdefinierten Parametergruppe, die Ihrem DB-Cluster zugeordnet ist. Nachdem Sie den Parameterwert `binlog_format` geändert haben, starten Sie Ihren DB-Cluster neu, damit die Änderungen übernommen werden. Weitere Informationen erhalten Sie unter Amazon Aurora-DB-Cluster und DB-Instance-Parameter und Ändern von Parametern in einer DB-Parametergruppe.
RDS for MySQL	So deaktivieren Sie die Binärprotokollierung für eine Amazon RDS-DB-Instance Sie können die Binärprotokollierung nicht direkt für eine Amazon RDS-DB-Instance deaktivieren, aber Sie können diese Funktion deaktivieren, indem Sie Folgendes tun: 1. Deaktivieren Sie die automatischen Backups für die DB-Instance. Sie können die automatischen Backups deaktivieren, indem Sie eine bestehende DB-Instance ändern und Backup Retention Period (Aufbewahrungszeitraum für Sicherungen) auf den Wert 0 setzen. Weitere Informationen finden Sie unter Ändern einer Amazon RDS-DB-Instance und unter Arbeiten mit Sicherungen im Amazon Relational Database Service-Benutzerhandbuch. 2. Löschen Sie alle Lesereplikate für die DB-Instance. Weitere Informationen finden Sie unter Arbeiten mit Read Replicas von MariaDB, MySQL und PostgreSQL DB-Instances im Amazon Relational Database Service-Benutzerhandbuch.

Datenbank-Engine	Anweisungen
MySQL (extern)	So deaktivieren Sie die Binärprotokollierung für eine externe MySQL-Datenbank Verbinden Sie sich mit der MySQL-Datenbank und rufen Sie den Befehl `STOP REPLICATION` auf. 1. Halten Sie aus einer Command-Shell den Service `mysqld` an. ``` sudo service mysqld stop ``` 2. Bearbeiten Sie die `my.cnf`-Datei (diese Datei befindet sich üblicherweise unter `/etc`). ``` sudo vi /etc/my.cnf ``` Löschen Sie die Optionen `log_bin` und `server_id` aus dem Abschnitt `[mysqld]`. Weitere Informationen finden Sie unter Setting the replication source configuration in der MySQL-Dokumentation. 3. Starten Sie den mysql-Service. ``` sudo service mysqld start ```

Verwenden von Amazon Aurora für das Skalieren von Lesevorgängen in Ihrer MySQL-Datenbank

Sie können Amazon Aurora mit Ihrer MySQL-DB-Instance verwenden, um die Möglichkeiten der Skalierung von Lesevorgängen von Amazon Aurora zu nutzen und den Lese-Workload für Ihre MySQL-DB-Instance zu erweitern. Erstellen Sie einen Amazon-Aurora MySQL-DB-Cluster und machen Sie ihn zum Read Replica Ihrer MySQL-DB-Instance, um Aurora für die Skalierung von Lesevorgängen Ihrer MySQL-DB-Instance zu verwenden. Dies gilt für eine RDS for MySQL-DB-Instance oder eine MySQL-Datenbank, die außerhalb von Amazon RDS ausgeführt wird.

Weitere Informationen zum Erstellen eines Amazon Aurora-DB-Clusters finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Wenn Sie eine Replikation zwischen Ihrer MySQL-DB-Instance und Ihrem Amazon Aurora-DB-Cluster einrichten, folgen Sie sicherheitshalber bitte diesen Anweisungen:

- Verwenden Sie die Amazon Aurora-DB-Cluster-Endpunkt-Adresse, wenn Sie Ihr Amazon Aurora MySQL-DB-Cluster referenzieren. Bei einem Failover verwendet die Aurora-Replica, die zur primären Instance for das Aurora MySQL-DB-Cluster hochgestuft wird, weiterhin die DB-Cluster-Endpunkt-Adresse.
- Bewahren Sie die Binärprotokolle auf Ihrer Schreiber-Instance auf, bis Sie sichergestellt haben, dass sie auf das Aurora Replica angewandet wurden. Durch das Aufbewahren können Sie sicherstellen, dass Sie Ihre Schreiber-Instance im Fall eines Ausfalls wiederherstellen können.

Important

Wenn Sie eine von Ihnen verwaltete Replikation verwenden, sind Sie für die Überwachung und Lösung jeglicher auftretender Probleme bei der Replikation verantwortlich. Weitere Informationen finden Sie unter Diagnose und Lösung bei Verzögerungen zwischen Read Replicas (Lesereplikaten).

Note

Die erforderlichen Berechtigungen zum Starten einer Replikation in einem Amazon-Aurora-MySQL-DB-Cluster sind beschränkt und für Ihren Amazon-RDS-Hauptbenutzer nicht verfügbar. Aus diesem Grund müssen Sie die Prozedurenmysql.rds_set_external_master (Aurora-MySQL-Version 2), mysql.rds_set_external_source (Aurora MySQL Version 3) und mysql.rds_start_replication verwenden, um eine Replikation zwischen Ihrem Aurora-MySQL-DB-Cluster und Ihrer MySQL-DB-Instance einzurichten.

Starten der Replikation zwischen einer externen Quell-Instance und einem MySQL-DB-Cluster

1. Legen Sie die Quell-MySQL-DB-Instance als schreibgeschützt fest:

```
mysql> FLUSH TABLES WITH READ LOCK;
```

```
mysql> SET GLOBAL read_only = ON;
```

2. Führen Sie den Befehl `SHOW MASTER STATUS` in der Quell-MySQL-DB-Instance aus, um den Speicherort des Binärprotokolls zu bestimmen. Sie erhalten eine Ausgabe, ähnlich der im folgenden Beispiel:

```
File                          Position
-----------------------------------
 mysql-bin-changelog.000031      107
-----------------------------------
```

3. Kopieren Sie die Datenbank mithilfe von aus der externen MySQL-DB-Instance in das Amazon Aurora MySQL-DB-Cluster `mysqldump`. Bei sehr großen Datenbanken empfiehlt es sich, das Verfahren zu verwenden, das im Abschnitt zum Importieren von Daten in eine MySQL- oder MariaDB-DB-Instance mit reduzierter Ausfallzeit im Amazon Relational Database Service-Benutzerhandbuch beschrieben ist.

   Für LinuxmacOS, oderUnix:

```
mysqldump \
    --databases <database_name> \
    --single-transaction \
    --compress \
    --order-by-primary \
    -u local_user \
    -p local_password | mysql \
        --host aurora_cluster_endpoint_address \
        --port 3306 \
        -u RDS_user_name \
        -p RDS_password
```

   Windows:

```
mysqldump ^
    --databases <database_name> ^
    --single-transaction ^
    --compress ^
    --order-by-primary ^
    -u local_user ^
    -p local_password | mysql ^
        --host aurora_cluster_endpoint_address ^
```

```
        --port 3306 ^
        -u RDS_user_name ^
        -p RDS_password
```

> **Note**
>
> Stellen Sie sicher, dass kein Leezeichen zwischen der Option `-p` und dem eingegebenen Passwort vorhanden ist.

Verwenden Sie die Optionen `--host`, `--user (-u)` `--port` und `-p` im Befehl `mysql`, um den Host-Namen, Benutzernamen, Port und das Passwort für die Verbindung mit Ihrem Aurora-DB-Cluster anzugeben. Der Host-Name ist der DNS-Name aus dem Amazon Aurora-DB-Cluster-Endpunkt, z. B, `mydbcluster.cluster-123456789012.us-east-1.rds.amazonaws.com`. Sie finden den Endpunktwert in den Cluster-Details in der Amazon RDS-Managementkonsole.

4. Legen Sie die Quell-MySQL-DB-Instance als wieder beschreibbar fest:

```
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

Weitere Informationen zum Erstellen von Backups zur Verwendung mit der Replikation finden Sie unter Backing up a source or replica by making it read only in der MySQL-Dokumentation.

5. Fügen Sie in der Amazon RDS-Management Console die IP-Adresse des Servers, der die Quell-MySQL-Datenbank hostet, zu der VPC-Sicherheitsgruppe für das Amazon Aurora-DB-Cluster hinzu. Weitere Informationen zum Ändern einer VPC-Sicherheitsgruppe finden Sie unter Sicherheitsgruppen für Ihre VPC im Amazon Virtual Private Cloud-Benutzerhandbuch.

   Es könnte sein, dass Sie Ihr lokales Netzwerk so konfigurieren müssen, dass es Verbindungen von der IP-Adresse Ihres Amazon Aurora-DB-Clusters zulässt, damit Sie mit Ihrer Quell-MySQL-Datenbank kommunizieren können. Verwenden Sie den Befehl `host`, um die IP-Adresse des Amazon Aurora-DB-Clusters herauszufinden.

```
host aurora_endpoint_address
```

   Der Hostname ist der DNS-Name aus dem Amazon Aurora-DB-Cluster-Endpunkt.

6. Verbinden Sie sich mithilfe eines Clients Ihrer Wahl mit der externen MySQL-Instance und erstellen Sie einen MySQL-Benutzer, der für die Replikation verwendet werden soll. Dieses Konto

wird ausschließlich für die Replikation verwendet und muss auf Ihre Domäne beschränkt sein, um die Sicherheit zu erhöhen. Im Folgenden wird ein Beispiel gezeigt.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

7. Erteilen Sie Ihrem Replikationsbenutzer für die externe MySQL-Instance die Sonderrechte `REPLICATION CLIENT` und `REPLICATION SLAVE`. Erteilen Sie beispielsweise die Sonderrechte `REPLICATION CLIENT` und `REPLICATION SLAVE` in allen Datenbank für den '`repl_user`'-Benutzer für Ihre Domäne, mit dem folgenden Befehl.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
       IDENTIFIED BY 'password';
   ```

8. Machen Sie einen manuellen Snapshot des Aurora MySQL-DB-Clusters, der das Read Replica sein soll, bevor Sie eine Replikation einrichten. Wenn Sie erneut eine Replikation mit dem DB-Cluster als Read Replica einrichten müssen, können Sie das Aurora MySQL-DB-Cluster aus diesem Snapshot wiederherstellen, anstatt die Daten aus Ihrer-MySQL-DB-Instance in ein neues Aurora MySQL-DB-Cluster importieren zu müssen.
9. Legen Sie das Amazon Aurora-DB-Cluster als Replica fest. Verbinden Sie sich als Hauptbenutzer mit dem Amazon-Aurora-DB-Cluster und bestimmen Sie die MySQL-Quelldatenbank mithilfe der Prozeduren mysql.rds_set_external_master (Aurora-MySQL-Version 2) oder mysql.rds_set_external_source (Aurora MySQL Version 3) und mysql.rds_start_replication als Replikationsmaster.

   Verwenden Sie den Namen und die Position der Protokolldatei, die Sie in Schritt 2 festgelegt haben. Im Folgenden wird ein Beispiel gezeigt.

   ```
   For Aurora MySQL version 2:
   CALL mysql.rds_set_external_master ('mymasterserver.mydomain.com', 3306,
       'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 0);

   For Aurora MySQL version 3:
   CALL mysql.rds_set_external_source ('mymasterserver.mydomain.com', 3306,
       'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 0);
   ```

10. Rufen Sie auf dem Amazon-Aurora-DB-Cluster die mysql.rds_start_replication-Prozedur auf, um die Replikation zu starten.

    ```
    CALL mysql.rds_start_replication;
    ```

Nachdem Sie die Replikation zwischen Ihrer Quell-MySQL-DB-Instance und Ihrem Amazon Aurora-DB-Cluster erneut eingerichtet haben, können Sie Aurora-Replicas zu Ihrem Amazon Aurora-DB-Cluster hinzufügen. Sie können sich anschließend mit dem Aurora Replicas verbinden, um die Lesevorgänge Ihrer Daten zu skalieren. Weitere Informationen über das Erstellen einer Aurora-Replica finden Sie unter Hinzufügen von Aurora-Replicas zu einem DB-Cluster.

Optimieren der binären Protokollreplikation

Im Folgenden erfahren Sie, wie Sie die Leistung der binären Protokollreplikation optimieren und damit zusammenhängende Probleme in Aurora MySQL beheben können.

> **Tip**
>
> In dieser Erörterung wird davon ausgegangen, dass Sie mit dem Mechanismus der binären MySQL-Protokollreplikation und dessen Funktionsweise vertraut sind. Hintergrundinformationen finden Sie unter Replication Implementation (Implementierung der Replikation) in der MySQL-Dokumentation.

Replikation von binären Protokollen mit mehreren Threads

Bei der Multithread-Replikation für binäre Protokolle liest ein SQL-Thread Ereignisse aus dem Relay-Log und stellt sie in die Warteschlange, damit SQL-Worker-Threads angewendet werden können. Die SQL-Worker-Threads werden von einem Koordinator-Thread verwaltet. Die binären Protokollereignisse werden nach Möglichkeit parallel angewendet.

Die Multithread-Binärprotokollreplikation wird in Aurora MySQL Version 3 und in Aurora MySQL Version 2.12.1 und höher unterstützt.

Wenn eine Aurora MySQL-DB-Instance für die Verwendung der binären Protokollreplikation konfiguriert ist, verwendet die Replikat-Instance standardmäßig die Single-Thread-Replikation für Aurora MySQL-Versionen unter 3.04. Um die Multithread-Replikation zu aktivieren, aktualisieren Sie den `replica_parallel_workers`-Parameter in Ihrer benutzerdefinierten Parametergruppe auf einen Wert größer als Null.

Für Aurora MySQL Version 3.04 und höher erfolgt die Replikation standardmäßig in mehreren Threads, wobei die Einstellung auf `replica_parallel_workers` gesetzt ist. 4 Sie können diesen Parameter in Ihrer benutzerdefinierten Parametergruppe ändern.

Die folgenden Konfigurationsoptionen helfen Ihnen bei der Optimierung der Multithread-Replikation. Informationen zur Verwendung finden Sie unter Replikations- und binäre Protokollierungsoptionen und -Variablen im MySQL-Verweishandbuch.

Die optimale Konfiguration hängt von mehreren Faktoren ab. Beispielsweise wird die Leistung für die Binärprotokollreplikation von Ihren Datenbank-Workload-Merkmalen und der DB-Instanzklasse beeinflusst, auf der das Replikat ausgeführt wird. Wir empfehlen Ihnen daher, alle Änderungen an diesen Konfigurationsparametern gründlich zu testen, bevor Sie neue Parametereinstellungen auf eine Produktionsinstanz anwenden:

- `binlog_group_commit_sync_delay`
- `binlog_group_commit_sync_no_delay_count`
- `binlog_transaction_dependency_history_size`
- `binlog_transaction_dependency_tracking`
- `replica_preserve_commit_order`
- `replica_parallel_type`
- `replica_parallel_workers`

In Aurora MySQL Version 3.06 und höher können Sie die Leistung für binäre Protokollreplikate verbessern, wenn Sie Transaktionen für große Tabellen mit mehr als einem sekundären Index replizieren. Diese Funktion führt einen Threadpool ein, um sekundäre Indexänderungen parallel auf ein Binlog-Replikat anzuwenden. Die Funktion wird durch den `aurora_binlog_replication_sec_index_parallel_workers` DB-Cluster-Parameter gesteuert, der die Gesamtzahl der parallel Threads steuert, die für die Anwendung der sekundären Indexänderungen verfügbar sind. Der Parameter ist standardmäßig auf `0` (deaktiviert) gesetzt. Für die Aktivierung dieser Funktion ist kein Instanzneustart erforderlich. Um diese Funktion zu aktivieren, beenden Sie die laufende Replikation, legen Sie die gewünschte Anzahl parallel Worker-Threads fest und starten Sie die Replikation dann erneut.

Sie können diesen Parameter auch als globale Variable verwenden, wobei *n* die Anzahl der parallel Worker-Threads ist:

```
SET global aurora_binlog_replication_sec_index_parallel_workers=n;
```

Optimierung der Binlog-Replikation (Aurora MySQL 2.10 und höher)

In Aurora MySQL 2.10 und höher wendet Aurora automatisch eine Optimierung an, die als Binlog-I/O-Cache bekannt ist, auf die Binärlog-Replikation. Durch Zwischenspeichern der zuletzt festgeschriebenen Binlog-Ereignisse soll diese Optimierung die Leistung des Binlog-Dump-Threads verbessern und gleichzeitig die Auswirkungen auf Vordergrundtransaktionen auf der Binlog-Quell-Instance begrenzen.

> **Note**
>
> Dieser für diese Funktion verwendete Speicher ist unabhängig von der `binlog_cache` MySQL-Einstellung.
> Diese Funktion gilt nicht für Aurora DB-Instances, die die `db.t2`- und `db.t3`-Instanceklassen verwenden.

Sie müssen keine Konfigurationsparameter anpassen, um diese Optimierung zu aktivieren. Insbesondere wenn Sie den Konfigurationsparameter `aurora_binlog_replication_max_yield_seconds` in früheren Aurora MySQL-Versionen auf einen Wert ungleich null eingestellt haben, setzen Sie ihn für Aurora MySQL 2.10 und höher auf null zurück.

Die Statusvariablen `aurora_binlog_io_cache_reads` und `aurora_binlog_io_cache_read_requests` sind in Aurora MySQL 2.10 und höher verfügbar. Diese Statusvariablen helfen Ihnen zu überwachen, wie oft die Daten aus dem Binlog-I/O-Cache gelesen werden.

- `aurora_binlog_io_cache_read_requests` zeigt die Anzahl der Binlog-I/O-Leseanfragen aus dem Cache an.
- `aurora_binlog_io_cache_reads` zeigt die Anzahl der Binlog-I/O-Lesevorgänge an, die Informationen aus dem Cache abrufen.

Die folgende SQL-Abfrage berechnet den Prozentsatz der Binlog-Leseanforderungen, die die zwischengespeicherten Informationen nutzen. In diesem Fall ist es umso besser, je näher das Verhältnis an 100 liegt.

```
mysql> SELECT
  (SELECT VARIABLE_VALUE FROM INFORMATION_SCHEMA.GLOBAL_STATUS
    WHERE VARIABLE_NAME='aurora_binlog_io_cache_reads')
  / (SELECT VARIABLE_VALUE FROM INFORMATION_SCHEMA.GLOBAL_STATUS
```

```
    WHERE VARIABLE_NAME='aurora_binlog_io_cache_read_requests')
  * 100
  as binlog_io_cache_hit_ratio;
+--------------------------+
| binlog_io_cache_hit_ratio |
+--------------------------+
|         99.99847949080622 |
+--------------------------+
```

Die Binlog-I/O-Cache-Funktion enthält auch neue Metriken im Zusammenhang mit den Binlog-Dump-Threads. Dump-Threads sind die Threads, die erstellt werden, wenn neue Binlog-Replikate mit der Binlog-Quell-Instance verbunden sind.

Die Metriken des Dump-Threads werden alle 60 Sekunden mit dem Präfix in das Datenbankprotokoll gedruck `[Dump thread metrics]`. Die Metriken umfassen Informationen für jedes Binlog-Replikat wie `Secondary_id`, `Secondary_uuid`, den Namen der Binlog-Datei und die Position, die jedes Replikat liest. Zu den Metriken gehört auch `Bytes_behind_primary`, das den Abstand in Byte zwischen Replikationsquelle und Replikat darstellt. Diese Metrik misst die Verzögerung des Replikat-I/O-Threads. Diese Zahl unterscheidet sich von der Verzögerung des Replikat-SQL-Applier-Threads, der durch die `seconds_behind_master` Metrik auf dem Binlog-Replikat dargestellt wird. Sie können feststellen, ob Binlog-Replikate die Quelle aufholen oder zurückfallen, indem Sie überprüfen, ob die Entfernung abnimmt oder zunimmt.

Optimierung der Binlog-Replikation (Aurora-MySQL-Version 2 bis 2.09)

Um die binäre Protokollreplikation für Aurora MySQL zu optimieren, passen Sie die folgenden Optimierungsparameter auf Clusterebene an. Diese Parameter helfen Ihnen, das richtige Gleichgewicht zwischen Latenz für die Binärprotokoll-Quell-Instance und Replikationsverzögerung anzugeben.

- `aurora_binlog_use_large_read_buffer`
- `aurora_binlog_read_buffer_size`
- `aurora_binlog_replication_max_yield_seconds`

> **Note**
>
> Für MySQL 5.7-kompatible Cluster können Sie diese Parameter in Aurora-MySQL-Version 2 bis 2.09* verwenden. In Aurora MySQL 2.10.0 und höher werden diese Parameter durch die Binlog-I/O-Cache-Optimierung ersetzt und Sie müssen sie nicht verwenden.

Themen

Überblick über den großen Lese-Puffer und die Max-Yield-Optimierung

Es kann zu einer verringerten Leistung der binären Protokollreplikation kommen, wenn der binäre Protokoll-Dump-Thread auf das Aurora Cluster-Volume zugreift, während der Cluster eine hohe Anzahl von Transaktionen verarbeitet Sie können die Parameter `aurora_binlog_use_large_read_buffer`, `aurora_binlog_replication_max_yield_seconds` und `aurora_binlog_read_buffer_size` verwenden, um diese Art von Konflikt zu minimieren.

Angenommen, Sie haben eine Situation, in der `aurora_binlog_replication_max_yield_seconds` auf größer als 0 gesetzt ist und die aktuelle Binlog-Datei des Dump-Threads aktiv ist. In diesem Fall wartet der binäre Protokoll-Dump-Thread bis zu einer bestimmten Anzahl von Sekunden, bis die aktuelle Binärprotokolldatei durch Transaktionen gefüllt wird. Diese Wartezeit vermeidet Konflikte, die sich aus der Replikation jedes Binärprotokoll-Ereignisses ergeben können. Dies erhöht jedoch die Replica-Verzögerung für binäre Protokollreplikationen. Diese Replicas können um die gleiche Anzahl von Sekunden wie die `aurora_binlog_replication_max_yield_seconds`-Einstellung hinter die Quelle zurückfallen.

Die aktuelle Binärprotokolldatei ist die Binärprotokolldatei, die der Dump-Thread gerade liest, um die Replikation durchzuführen. Wir berücksichtigen, dass eine Binärprotokolldatei aktiv ist, wenn die Binärprotokolldatei aktualisiert oder geöffnet wird, um durch eingehende Transaktionen aktualisiert zu werden. Nach dem Aurora MySQL die aktive Binärprotokolldatei ausfüllt, erstellt MySQL eine neue

Binärprotokolldatei und wechselt dieser Binärprotokolldatei. Die alte Binärprotokolldatei wird inaktiv. Es wird nicht mehr von eingehenden Transaktionen aktualisiert.

> **Note**
>
> Bevor Sie diese Parameter anpassen, messen Sie Ihre Transaktionslatenz und Ihren Durchsatz über die Zeit. Möglicherweise stellen Sie fest, dass die Leistung der binären Protokollreplikation stabil ist und eine geringe Latenz aufweist, selbst wenn gelegentliche Konflikte auftreten.

`aurora_binlog_use_large_read_buffer`

Wenn dieser Parameter auf 1 gesetzt ist, wird Aurora MySQL die binäre Protokollreplikation basierend auf den Einstellungen der Parameter `aurora_binlog_read_buffer_size` und `aurora_binlog_replication_max_yield_seconds` optimieren. Wenn `aurora_binlog_use_large_read_buffer` 0 ist, ignoriert Aurora MySQL die Werte der Parameter `aurora_binlog_read_buffer_size` und `aurora_binlog_replication_max_yield_seconds`.

`aurora_binlog_read_buffer_size`

Binäre Protokoll-Dump-Threads mit größerem Lesepuffer minimieren die Anzahl der Lese-I/O-Vorgänge, indem sie weitere Ereignisse für jede I/O lesen. Der Parameter `aurora_binlog_read_buffer_size` legt die Größe des Lesepuffers fest. Der große Lesepuffer kann den Konflikt zwischen Binärprotokollen für Workloads reduzieren, die eine große Menge an Binärprotokoll-Daten erzeugen.

> **Note**
>
> Dieser Parameter hat nur Auswirkungen, wenn der Cluster auch die Einstellung ha `aurora_binlog_use_large_read_buffer=1`.
> Eine Erhöhung der Größe des Lesepuffers hat keinen Einfluss auf die Leistung der binären Protokollreplikation. Binäre Protokoll-Dump-Threads warten nicht darauf, dass die Aktualisierung von Transaktionen den Lesepuffer füllt.

`aurora_binlog_replication_max_yield_seconds`

Wenn Ihr Workload eine geringe Transaktionslatenz erfordert und Sie eine gewisse Replikationsverzögerung tolerieren können, können Sie den Parameter `aurora_binlog_replication_max_yield_seconds` erhöhen. Dieser Parameter steuert die Eigenschaft „Maximum Yield“ der binären Protokollreplikation in Ihrem Cluster.

> **Note**
>
> Dieser Parameter hat nur Auswirkungen, wenn der Cluster auch die Einstellung ha `aurora_binlog_use_large_read_buffer=1`.

Aurora MySQL erkennt jede Änderung des `aurora_binlog_replication_max_yield_seconds`-Parameterwerts sofort. Sie müssen die DB-Instance nicht neu starten. Wenn Sie diese Einstellung aktivieren, beginnt der Dump-Thread jedoch erst dann zu arbeiten, wenn die aktuelle Binärprotokolldatei ihre maximale Größe von 128 MB erreicht und in eine neue Datei gedreht wird.

Zugehörige Parameter

Verwenden Sie die folgenden DB-Cluster-Parameter, um die Binärprotokoll-Optimierung zu aktivieren.

Parameter	Standard	Zulässige Werte	Beschreibung
`aurora_binlog_use_large_read_buffer`	1	0, 1	Schalter zum Einschalten der Replikationsverbesserung. Wenn der Wert 1 ist, verwendet der binäre Protokoll-Dump-Thread `aurora_binlog_read_buffer_size` für die binäre Protokollreplikation, andernfal

Parameter	Standard	Zulässige Werte	Beschreibung
			ls wird die Standardp uffergröße (8 K) verwendet. In Aurora-MySQL-Version 3 nicht verwendet.
`aurora_bi nlog_read _buffer_size`	5242880	8192-536870912	Liest die Puffergrö ße, die vom binären Protokoll-Dump-Thr ead verwendet wird, wenn der Parameter `aurora_bi nlog_use_ large_rea d_buffer` auf 1 gesetzt ist. In Aurora-MySQL-Version 3 nicht verwendet.

Parameter	Standard	Zulässige Werte	Beschreibung
`aurora_binlog_replication_max_yield_seconds`	0	0 -36000	Der maximal zulässige Wert für Aurora-MySQL-Version 2.07* ist 45. Unter 2.09 und späteren Versionen können Sie einen höheren Wert einstellen. Für Version 2 funktioniert dieser Parameter nur, wenn der Parameter `aurora_binlog_use_large_read_buffer` auf 1 gesetzt ist.

Aktivieren des Max-Yield-Mechanismus für die binäre Protokollreplikation

Sie können die Max-Yield-Optimierung der binären Protokollreplikation wie folgt aktivieren. Dadurch wird die Latenz für Transaktionen auf der Binärprotokoll-Quell-Instance minimiert. Es kann jedoch zu einer höheren Verzögerung bei der Replikation kommen.

Aktivieren der Max-Yield-Binlog-Optimierung für einen Aurora-MySQL-Cluster

1. Erstellen oder bearbeiten Sie eine DB-Clusterparametergruppe unter Verwendung der folgenden Parametereinstellungen:

   - `aurora_binlog_use_large_read_buffer`: schaltet sich mit einem Wert von `ON` oder 1 ein.
   - `aurora_binlog_replication_max_yield_seconds`: Geben Sie einen Wert größer als 0 ein.

2. Ordnen Sie die DB-Cluster-Parametergruppe dem Aurora MySQL-Cluster zu, der als Binärprotokoll-Quelle arbeitet. Befolgen Sie hierzu die Verfahren unter Arbeiten mit Parametergruppen.
3. Bestätigen Sie, dass die Parameteränderung wirksam wird. Führen Sie dazu die folgende Abfrage für die Binärprotokoll-Quell-Instance aus.

```
SELECT @@aurora_binlog_use_large_read_buffer,
 @@aurora_binlog_replication_max_yield_seconds;
```

Die Ausgabe sollte in etwa wie folgt aussehen.

```
+---------------------------------------
+-----------------------------------------------+
| @@aurora_binlog_use_large_read_buffer |
 @@aurora_binlog_replication_max_yield_seconds |
+---------------------------------------
+-----------------------------------------------+
|                                     1 |
  45 |
+---------------------------------------
+-----------------------------------------------+
```

Deaktivieren der Max-Yield-Optimierung der binären Protokollreplikation

Sie können die Max-Yield-Optimierung der binären Protokollreplikation wie folgt deaktivieren. Dadurch wird die Verzögerung bei der Replikation minimiert. Es kann jedoch zu einer höheren Latenz für Transaktionen auf der Binärprotokoll-Quell-Instance kommen.

Deaktivieren der Max-Yield-Optimierung für einen Aurora MySQL-Cluster

1. Stellen Sie sicher, das bei der DB-Clusterparametergruppe, die dem Aurora MySQL-Cluster zugeordnet ist, `aurora_binlog_replication_max_yield_seconds` auf 0 eingestellt ist. Weitere Informationen zum Einstellen von Konfigurationsparametern unter Verwendung von Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.
2. Bestätigen Sie, dass die Parameteränderung wirksam wird. Führen Sie dazu die folgende Abfrage für die Binärprotokoll-Quell-Instance aus.

```
SELECT @@aurora_binlog_replication_max_yield_seconds;
```

Die Ausgabe sollte in etwa wie folgt aussehen.

```
+-----------------------------------------------+
| @@aurora_binlog_replication_max_yield_seconds |
+-----------------------------------------------+
|                                             0 |
+-----------------------------------------------+
```

Ausschalten des großen Lesepuffers

Sie können die gesamte Funktion für große Lesepuffer wie folgt deaktivieren.

So schalten Sie den großen Lesepuffer für das binäre Protokoll für einen Aurora MySQL Cluster aus

1. Setzen Sie `aurora_binlog_use_large_read_buffer` auf `OFF` oder 0 zurück:

   Stellen Sie sicher, das bei der DB-Clusterparametergruppe, die dem Aurora MySQL-Cluster zugeordnet ist, `aurora_binlog_use_large_read_buffer` auf 0 eingestellt ist. Weitere Informationen zum Einstellen von Konfigurationsparametern unter Verwendung von Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

2. On the binlog source instance, run the following query.

   ```
   SELECT @@ aurora_binlog_use_large_read_buffer;
   ```

   Die Ausgabe sollte in etwa wie folgt aussehen.

   ```
   +--------------------------------------+
   | @@aurora_binlog_use_large_read_buffer |
   +--------------------------------------+
   |                                    0 |
   +--------------------------------------+
   ```

Einrichten eines erweiterten Binärprotokolls

Das erweiterte Binärprotokoll reduziert den durch die Aktivierung des Binärprotokolls verursachten Rechenleistungs-Overhead, der in bestimmten Fällen bis zu 50 % betragen kann. Mit einem erweiterten Binärprotokoll kann dieser Overhead auf etwa 13 % reduziert werden. Damit der

Overhead reduziert wird, schreibt das erweiterte Binärprotokoll die Binär- und Transaktionsprotokolle parallel in den Speicher, wodurch die zum Zeitpunkt des Transaktions-Commits geschriebenen Daten minimiert werden.

Die Verwendung des erweiterten Binärprotokolls verbessert außerdem die Datenbankwiederherstellungszeit nach Neustarts und Failovers um bis zu 99 % im Vergleich zum Community-MySQL-Binärprotokoll. Das erweiterte Binärprotokoll ist mit bestehenden binlogbasierten Workloads kompatibel und Sie interagieren damit genauso wie mit dem Community-MySQL-Binärprotokoll.

Das erweiterte Binlog ist auf Aurora MySQL Version 3.03.1 und höher verfügbar.

Themen

Konfiguration erweiterter Binärprotokollparameter

Sie können zwischen Community-MySQL-Binärprotokoll und erweitertem Binärprotokoll wechseln, indem Sie die Parameter für das erweiterte Binärprotokoll aktivieren/deaktivieren. Die bestehenden Binärprotokollbenutzer können die Binärprotokolldateien weiterhin lesen und verarbeiten, ohne dass es zu Lücken in der Binärprotokolldateifolge kommt.

So aktivieren Sie das erweiterte Binärprotokoll

Parameter	Standard	Beschreibung
`binlog_format`	–	Legen Sie den Parameter `binlog_format` auf das binäre Protokollierungsformat Ihrer Wahl fest, um das erweiterte Binärprotokoll zu aktivieren. Stellen Sie sicher, dass der `binlog_format`

Parameter	Standard	Beschreibung
		`parameter` nicht auf AUS eingestellt ist. Weitere Informationen finden Sie unter Konfiguration der binären Protokollierung mit Aurora MySQL.
`aurora_enhanced_binlog`	`0`	Legen Sie den Wert dieses Parameters in der Parametergruppe des DB-Clusters, die mit dem Aurora-MySQL-Cluster verknüpft ist, auf 1 fest. Wenn Sie den Wert dieses Parameters ändern, müssen Sie die Writer-Instance neu starten, wenn für den Wert `DBClusterParameterGroupStatus` `pending-reboot` angezeigt wird.
`binlog_backup`	`1`	Deaktivieren Sie diesen Parameter, um das erweiterte Binärprotokoll zu aktivieren. Legen Sie dazu den Wert dieses Parameters auf `0` fest.
`binlog_replication_globaldb`	`1`	Deaktivieren Sie diesen Parameter, um das erweiterte Binärprotokoll zu aktivieren. Legen Sie dazu den Wert dieses Parameters auf `0` fest.

> **Important**
>
> Sie können die Parameter `binlog_backup` und `binlog_replication_globaldb` nur deaktivieren, wenn Sie das erweiterte Binärprotokoll verwenden.

So deaktivieren Sie das erweiterte Binärprotokoll

Parameter	Beschreibung
`aurora_enhanced_binlog`	Legen Sie den Wert dieses Parameters in der Parametergruppe des DB-Clusters, die mit dem Aurora-MySQL-Cluster verknüpft ist, auf `0` fest. Sobald Sie den Wert dieses Parameters ändern, müssen Sie die Writer-Instance neu starten, wenn für den Wert `DBClusterParameterGroupStatus` `pending-reboot` angezeigt wird.
`binlog_backup`	Aktivieren Sie diesen Parameter, wenn Sie das erweiterte Binärprotokoll deaktivieren. Legen Sie dazu den Wert dieses Parameters auf 1 fest.
`binlog_replication_globaldb`	Aktivieren Sie diesen Parameter, wenn Sie das erweiterte Binärprotokoll deaktivieren. Legen Sie dazu den Wert dieses Parameters auf 1 fest.

Um zu überprüfen, ob das erweiterte Binärprotokoll aktiviert ist, verwenden Sie den folgenden Befehl im MySQL-Client:

```
mysql>show status like 'aurora_enhanced_binlog';

+-------------------------+--------+
| Variable_name           | Value  |
+-------------------------+--------+
| aurora_enhanced_binlog | ACTIVE |
```

```
+-------------------------+--------+
1 row in set (0.00 sec)
```

Wenn das erweiterte Binärprotokoll aktiviert ist, wird in der Ausgabe `ACTIVE` für `aurora_enhanced_binlog` angezeigt.

Sonstige zugehörige Parameter

Wenn Sie das erweiterte Binärprotokoll aktivieren, sind folgende Parameter betroffen:

- Der Parameter `max_binlog_size` ist sichtbar, kann aber nicht geändert werden. Sein Standardwert `134217728` wird automatisch in `268435456` geändert, wenn das erweiterte Binärprotokoll aktiviert ist.
- Im Gegensatz zum Community-MySQL-Binärprotokoll fungiert `binlog_checksum` nicht als dynamischer Parameter, wenn das erweiterte Binärprotokoll aktiviert ist. Damit die Änderung an diesem Parameter wirksam wird, müssen Sie den DB-Cluster manuell neu starten, auch wenn für `ApplyMethod` `immediate` festgelegt ist.
- Der Wert, den Sie für den Parameter `binlog_order_commits` festlegen, hat keinen Einfluss auf die Reihenfolge der Commits, wenn das erweiterte Binärprotokoll aktiviert ist. Die Commits werden immer ohne weitere Auswirkungen auf die Leistung angeordnet.

Unterschiede zwischen erweitertem Binärprotokoll und Community-MySQL-Binärprotokoll

Das erweiterte Binlog interagiert anders mit Klonen, Backups und der globalen Aurora-Datenbank als das Community-MySQL-Binlog. Bevor Sie das erweiterte Binärprotokoll verwenden, sollten Sie sich mit den folgenden Unterschieden vertraut machen.

- Verbesserte Binlogdateien aus dem Quell-DB-Cluster sind auf einem geklonten DB-Cluster nicht verfügbar.
- Verbesserte Binlogdateien sind nicht in Aurora-Backups enthalten. Daher sind erweiterte Binärprotokolldateien aus dem Quell-DB-Cluster nach der Wiederherstellung eines DB-Clusters trotz einer für ihn festgelegten Aufbewahrungsfrist nicht verfügbar.
- Bei Verwendung mit einer globalen Aurora-Datenbank werden die erweiterten Binärprotokolldateien des primären DB-Clusters nicht auf den DB-Cluster in den sekundären Regionen repliziert.

Beispiele

Die folgenden Beispiele veranschaulichen die Unterschiede zwischen dem erweiterten Binärprotokoll und dem Community-MySQL-Binärprotokoll.

Auf einem wiederhergestellten oder geklonten DB-Cluster

Wenn das erweiterte Binärprotokoll aktiviert ist, sind die historischen Binärprotokolldateien im wiederhergestellten oder geklonten DB-Cluster nicht verfügbar. Wenn das Binärprotokoll aktiviert ist, beginnt der neue DB-Cluster nach einem Wiederherstellungs- oder Klonvorgang, seine eigene Reihenfolge von Binärprotokolldateien zu schreiben, beginnend mit 1 (mysql-bin-changelog.000001).

Um das erweiterte Binärprotokoll nach einem Wiederherstellungs- oder Klonvorgang zu aktivieren, legen Sie die erforderlichen DB-Cluster-Parameter auf dem wiederhergestellten oder geklonten DB-Cluster fest. Weitere Informationen finden Sie unter Konfiguration erweiterter Binärprotokollparameter.

Example Ausführung des Klon- oder Wiederherstellungsvorgangs, wenn das erweiterte Binärprotokoll aktiviert ist

Quell-DB-Cluster:

```
mysql> show binary logs;

+---------------------------+-----------+-----------+
| Log_name                  | File_size | Encrypted |
+---------------------------+-----------+-----------+
| mysql-bin-changelog.000001 |       156 | No        |
| mysql-bin-changelog.000002 |       156 | No        |
| mysql-bin-changelog.000003 |       156 | No        |
| mysql-bin-changelog.000004 |       156 | No        | --> Enhanced Binlog turned on
| mysql-bin-changelog.000005 |       156 | No        | --> Enhanced Binlog turned on
| mysql-bin-changelog.000006 |       156 | No        | --> Enhanced Binlog turned on
+---------------------------+-----------+-----------+
6 rows in set (0.00 sec)
```

In einem wiederhergestellten oder geklonten DB-Cluster werden Binärprotokolldateien nicht gesichert, wenn das erweiterte Binärprotokoll aktiviert ist. Um Unterbrechungen in den Binärprotokolldaten zu vermeiden, sind die Binärprotokolldateien, die vor dem Aktivieren des erweiterten Binärprotokolls geschrieben wurden, ebenfalls nicht verfügbar.

```
mysql>show binary logs;
```

```
+---------------------------+-----------+-----------+
| Log_name                  | File_size | Encrypted |
+---------------------------+-----------+-----------+
| mysql-bin-changelog.000001 |       156 | No        | --> New sequence of Binlog files
+---------------------------+-----------+-----------+
1 row in set (0.00 sec)
```

Example Der Vorgang zum Klonen oder Wiederherstellen wird ausgeführt, wenn das erweiterte Binlog ausgeschaltet ist

Quell-DB-Cluster:

```
mysql>show binary logs;

+---------------------------+-----------+-----------+
| Log_name                  | File_size | Encrypted |
+---------------------------+-----------+-----------+
| mysql-bin-changelog.000001 |       156 | No        |
| mysql-bin-changelog.000002 |       156 | No        | --> Enhanced Binlog enabled
| mysql-bin-changelog.000003 |       156 | No        | --> Enhanced Binlog enabled
| mysql-bin-changelog.000004 |       156 | No        |
| mysql-bin-changelog.000005 |       156 | No        |
| mysql-bin-changelog.000006 |       156 | No        |
+---------------------------+-----------+-----------+
6 rows in set (0.00 sec)
```

In einem wiederhergestellten oder geklonten DB-Cluster sind Binärprotokolldateien verfügbar, die nach dem Deaktivieren des erweiterten Binärprotokoll geschrieben wurden.

```
mysql>show binary logs;

+---------------------------+-----------+-----------+
| Log_name                  | File_size | Encrypted |
+---------------------------+-----------+-----------+
| mysql-bin-changelog.000004 |       156 | No        |
| mysql-bin-changelog.000005 |       156 | No        |
| mysql-bin-changelog.000006 |       156 | No        |
+---------------------------+-----------+-----------+
```

```
1 row in set (0.00 sec)
```

In einer Amazon Aurora Global Database

In einer Amazon Aurora Global Database werden die Binärprotokolldaten des primären DB-Clusters nicht auf den sekundären DB-Cluster repliziert. Nach einem regionsübergreifenden Failover-Prozess sind die Binärprotokolldaten im neu hochgestuften primären DB-Cluster nicht verfügbar. Wenn das Binärprotokoll aktiviert ist, beginnt der neu hochgestufte DB-Cluster mit seiner eigenen Reihenfolge von Binärprotokolldateien, beginnend mit 1 (mysql-bin-changelog.000001).

Um das erweiterte Binärprotokoll nach einem Failover zu aktivieren, müssen Sie die erforderlichen DB-Cluster-Parameter auf dem sekundären DB-Cluster festlegen. Weitere Informationen finden Sie unter Konfiguration erweiterter Binärprotokollparameter.

Example Ausführen eines globalen Datenbank-Failovers, wenn das erweiterte Binärprotokoll aktiviert ist

Alter primärer DB-Cluster (vor dem Failover):

```
mysql>show binary logs;

+----------------------------+-----------+-----------+
| Log_name                   | File_size | Encrypted |
+----------------------------+-----------+-----------+
| mysql-bin-changelog.000001 |       156 | No        |
| mysql-bin-changelog.000002 |       156 | No        |
| mysql-bin-changelog.000003 |       156 | No        |
| mysql-bin-changelog.000004 |       156 | No        | --> Enhanced Binlog enabled
| mysql-bin-changelog.000005 |       156 | No        | --> Enhanced Binlog enabled
| mysql-bin-changelog.000006 |       156 | No        | --> Enhanced Binlog enabled
+----------------------------+-----------+-----------+
6 rows in set (0.00 sec)
```

Neuer primärer DB-Cluster (nach dem Failover):

Binärprotokolldateien werden nicht in sekundäre Regionen repliziert, wenn das erweiterte Binärprotokoll aktiviert ist. Um Unterbrechungen in den Binärprotokolldaten zu vermeiden, sind die Binärprotokolldateien, die vor dem Aktivieren des erweiterten Binärprotokolls geschrieben wurden, nicht verfügbar.

```
mysql>show binary logs;

+----------------------------+-----------+-----------+
| Log_name                   | File_size | Encrypted |
+----------------------------+-----------+-----------+
| mysql-bin-changelog.000001 |       156 | No        | --> Fresh sequence of Binlog
 files
+----------------------------+-----------+-----------+
1 row in set (0.00 sec)
```

Example Ausführen eines globalen Datenbank-Failovers, wenn das erweiterte Binärprotokoll deaktiviert ist

Quell-DB-Cluster:

```
mysql>show binary logs;

+----------------------------+-----------+-----------+
| Log_name                   | File_size | Encrypted |
+----------------------------+-----------+-----------+
| mysql-bin-changelog.000001 |       156 | No        |
| mysql-bin-changelog.000002 |       156 | No        | --> Enhanced Binlog enabled
| mysql-bin-changelog.000003 |       156 | No        | --> Enhanced Binlog enabled
| mysql-bin-changelog.000004 |       156 | No        |
| mysql-bin-changelog.000005 |       156 | No        |
| mysql-bin-changelog.000006 |       156 | No        |
+----------------------------+-----------+-----------+
6 rows in set (0.00 sec)
```

Wiederhergestellter oder geklonter DB-Cluster:

Binärprotokolldateien, die nach dem Deaktivieren des erweiterten Binärprotokolls geschrieben wurden, werden repliziert und sind im neu hochgestuften DB-Cluster verfügbar.

```
mysql>show binary logs;

+----------------------------+-----------+-----------+
| Log_name                   | File_size | Encrypted |
```

```
+----------------------------+-----------+-----------+
| mysql-bin-changelog.000004 |       156 | No        |
| mysql-bin-changelog.000005 |       156 | No        |
| mysql-bin-changelog.000006 |       156 | No        |
+----------------------------+-----------+-----------+
3 rows in set (0.00 sec)
```

CloudWatch Amazon-Metriken für erweitertes Binlog

Die folgenden CloudWatch Amazon-Metriken werden nur veröffentlicht, wenn das erweiterte Binlog aktiviert ist.

CloudWatch Metrik	Beschreibung	Einheiten
ChangeLogBytesUsed	Die Menge des vom Speicherplatzes, der vom erweiterten Binärprotokoll belegt wird.	Bytes
ChangeLogLesen Sie IOPS	Die Anzahl von Lese-I/O-Operationen, die im erweiterten Binärprotokoll in einem fünfminütigen Intervalls durchgeführt wurden.	Anzahl pro 5 Minuten
ChangeLogSchreiben Sie IOPS	Die Anzahl von Schreib-I/O-Operationen, die im erweiterten Binärprotokoll in einem fünfminütigen Intervalls durchgeführt wurden.	Anzahl pro 5 Minuten

Beschränkungen für das erweiterte Binärprotokoll

Die folgenden Einschränkungen gelten für DB-Cluster von Amazon Aurora, wenn das erweiterte Binärprotokoll aktiviert ist.

- Das erweiterte Binlog wird nur auf Aurora MySQL Version 3.03.1 und höher unterstützt.
- Die auf dem primären DB-Cluster geschriebenen erweiterten Binärprotokolldateien werden nicht in die geklonten oder wiederhergestellten DB-Cluster kopiert.

- Bei Verwendung mit Amazon Aurora Global Database werden die erweiterten Binärprotokolldateien des primären DB-Clusters nicht auf sekundäre DB-Cluster repliziert. Daher sind die historischen Binärprotokolldaten nach dem Failover-Prozess im neuen primären DB-Cluster nicht verfügbar.
- Die folgenden Binärprotokoll-Konfigurationsparameter werden ignoriert:
  - `binlog_group_commit_sync_delay`
  - `binlog_group_commit_sync_no_delay_count`
  - `binlog_max_flush_queue_time`
- Sie können eine beschädigte Tabelle in einer Datenbank nicht löschen oder umbenennen. Um diese Tabellen zu löschen, können Sie Kontakt aufnehmen. AWS Support
- Der Binärprotokoll-I/O-Cache ist deaktiviert, wenn das erweiterte Binärprotokoll aktiviert ist. Weitere Informationen finden Sie unter Optimieren der binären Protokollreplikation .

> **Note**
>
> Das erweiterte Binärprotokoll bietet ähnliche Verbesserungen der Leseleistung wie der Binärprotokoll-I/O-Cache und deutliche Verbesserungen der Schreibleistung.

- Die Rückverfolgungsfunktion wird nicht unterstützt. Das erweiterte Binärprotokoll kann in einem DB-Cluster unter den folgenden Bedingungen nicht aktiviert werden:
  - Für den DB-Cluster ist derzeit die Rückverfolgungsfunktion aktiviert.
  - DB-Cluster, in dem die Backtrack-Funktion zuvor aktiviert war, jetzt aber deaktiviert ist.
  - Der DB-Cluster wurde aus einem Quell-DB-Cluster oder einem Snapshot mit aktivierter Rückverfolgungsfunktion wiederhergestellt.

Verwenden der GTID-basierten Replikation

Im folgenden Inhalt wird erklärt, wie Sie Global Transaction Identifiers (GTIDs) mit der Binärprotokollreplikation (Binlog) MySQL MySQL-DB-Instances verwenden. zwischen einem Aurora MySQL-Cluster und einer externen Quelle.

> **Note**
>
> Bei Aurora können Sie diese Funktion nur mit Aurora-MySQL-Clustern verwenden, welche die binlog-Replikation in eine externe oder aus einer externen MySQL-Datenbank nutzen. Bei der anderen Datenbank kann es sich um eine Amazon-RDS-MySQL-Instance, eine

lokale MySQL-Datenbank oder einen Aurora-DB-Cluster in einer anderen AWS-Region handeln. Weitere Informationen zum Konfigurieren dieser Art von Replikation finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).

Wenn Sie die Binlog-Replikation verwenden und mit der GTID-basierten Replikation mit MySQL nicht vertraut sind, finden Sie weitere Informationen unter Replikation mit globalen Transaktions-Identifikatoren in der MySQL-Dokumentation.

Die GTID-basierte Replikation wird für Aurora-MySQL-Version 2 und 3 unterstützt.

Themen

- Übersicht über globale Transaktionskennungen (GTIDs)
- Parameter für die GTID-basierte Replikation
- Konfigurieren einer GTID-basierten Replikation für einen Aurora MySQL-Cluster
- Deaktivieren einer GTID-basierten Replikation für einen Aurora MySQL-DB-Cluster

Übersicht über globale Transaktionskennungen (GTIDs)

Globale Transaktionskennungen (GTIDs) sind eindeutige IDs, die für festgeschriebene MySQL-Transaktionen generiert werden. Sie können GTIDs verwenden, um die Fehlerbehebung für die binlog-Replikation zu erleichtern.

> **Note**
>
> Wenn Aurora Daten unter den DB-Instances in einem Cluster synchronisiert, steht dieser Replikationsmechanismus in keinem Zusammenhang mit dem Binärprotokoll (binlog). Bei Aurora MySQL ist die GTID-basierte Replikation nur anwendbar, wenn Sie auch eine binlog-Replikation verwenden, um eine Replikation aus einer externen MySQL-kompatiblen Datenbank in einen oder aus einem Aurora MySQL-DB-Cluster durchführen.

MySQL verwendet für die binlog-Replikation zwei verschiedene Arten von Transaktionen:

- GTID-Transaktionen – Transaktionen, die durch eine GTID gekennzeichnet sind.
- Anonyme Transaktionen – Transaktionen, denen keine GTID zugeordnet ist.

In einer Replikationskonfiguration sind GTIDs bei allen DB-Instances eindeutig. GTIDs vereinfachen die Replikationskonfiguration, weil Sie nicht auf die Protokolldateipositionen verweisen müssen, wenn Sie diese verwenden. GTIDs erleichtern das Verfolgen von replizierten Transaktionen und legen fest, ob die Quellinstance und Replikate konsistent sind.

Sie verwenden die GTID-basierte Replication gewöhnlich mit Aurora, wenn Sie eine Replikation aus einer externen MySQL-kompatiblen Datenbank in einen Aurora-Cluster durchführen. Sie können diese Replikationskonfiguration als Teil einer Migration von einer lokalen oder einer Amazon RDS-Datenbank in Aurora MySQL einrichten. Wenn die externe Datenbank bereits GTIDs verwendet, kann der Replikationsvorgang durch Aktivieren der GTID-basierten Replikation für den Aurora-Cluster vereinfacht werden.

Sie konfigurieren die GTID-basierte Replikation für einen Aurora MySQL-Cluster, indem Sie zuerst die relevanten Konfigurationsparameter in einer DB-Clusterparametergruppe festlegen. Sie ordnen diese Parametergruppe dann dem Cluster zu.

Parameter für die GTID-basierte Replikation

Mit den folgenden Parametern konfigurieren Sie die GTID-basierte Replikation.

Parameter	Zulässige Werte	Beschreibung
`gtid_mode`	`OFF`, `OFF_PERMISSIVE` , `ON_PERMISSIVE` , `ON`	`OFF` gibt an, dass neue Transaktionen anonyme Transaktionen sind (d. h. keine GTIDs haben). Eine Transaktion muss anonym sein, um repliziert werden zu können. `OFF_PERMISSIVE` gibt an, dass neue Transaktionen anonyme Transaktionen sind und alle Transaktionen repliziert werden können. `ON_PERMISSIVE` gibt an, dass neue Transaktionen GTID-Transaktionen sind und alle Transaktionen repliziert werden können. `ON` gibt an, dass neue Transaktionen GTID-Transaktionen sind. Eine Transaktion muss eine GTID-Transaktion sein, um repliziert zu werden.

Parameter	Zulässige Werte	Beschreibung
`enforce_gtid_consistency`	`OFF`, `ON`, `WARN`	`OFF` erlaubt es Transaktionen, gegen die GTID-Konsistenz zu verstoßen. `ON` verhindert das Verstoßen von Transaktionen gegen die GTID-Konsistenz. `WARN` erlaubt es Transaktionen, gegen die GTID-Konsistenz zu verstoßen, generiert aber eine Warnung, wenn ein Verstoß auftritt.

> **Note**
>
> In der wird der Parameter als AWS Management Console angezeigt. `gtid_mode` `gtid-mode`

Bei einer GTID-basierten Replikation verwenden Sie diese Einstellungen für die DB-Cluster-Parametergruppe für Ihren Aurora MySQL-DB-Cluster:

- `ON` und `ON_PERMISSIVE` gelten nur für die ausgehende Replikation von einem Aurora-MySQL-Cluster. Beide Werte bewirken, dass Ihr Aurora-DB-Cluster GTIDs für Transaktionen verwenden, die zu einer externen Datenbank repliziert werden. `ON` erfordert, dass die externe Datenbank ebenfalls die GTID-basierte Replikation verwendet. Mit `ON_PERMISSIVE` ist die GTID-basierte Replikation auf der externen Datenbank optional.
- Wenn `OFF_PERMISSIVE` eingestellt ist, bedeutet dies, dass Ihr Aurora-DB-Cluster die eingehende Replikation von einer externen Datenbank akzeptieren kann. Dies ist ungeachtet davon möglich, ob die externe Datenbank eine GTID-basierte Replikation verwendet oder ob nicht.
- Wenn `OFF` eingestellt ist, bedeutet dies, dass Ihr Aurora-DB-Cluster nur eingehende Replikation von externen Datenbanken akzeptiert, die keine GTID-basierte Replikation verwenden.

> **Tip**
>
> Eingehende Replikation ist das geläufigste binlog-Replikationsszenario für Aurora MySQL-Cluster. Für eine eingehende Replikation empfehlen wir, dass Sie den GTID-Modus auf

einzustelle `OFF_PERMISSIVE`. Diese Einstellung ermöglicht eine eingehende Replikation aus externen Datenbanken ungeachtete der GTID-Einstellungen an der Replikationsquelle.

Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Konfigurieren einer GTID-basierten Replikation für einen Aurora MySQL-Cluster

Wenn die GTID-basierte Replikation für einen Aurora MySQL-DB-Cluster aktiviert ist, gelten die GTID-Einstellungen sowohl für eine eingehende als auch für eine ausgehende binlog-Replikation.

So aktivieren Sie eine GTID-basierte Replikation für einen Aurora MySQL-Cluster

1. Erstellen oder bearbeiten Sie eine DB-Clusterparametergruppe unter Verwendung der folgenden Parametereinstellungen:
   - `gtid_mode` – `ON` oder `ON_PERMISSIVE`
   - `enforce_gtid_consistency` – `ON`
2. Ordnen Sie die DB-Clusterparametergruppe dem Aurora MySQL-Cluster zu. Befolgen Sie hierzu die Verfahren unter Arbeiten mit Parametergruppen.
3. (Optional) Geben Sie an, wie GTIDs Transaktionen zugewiesen werden, die sie nicht enthalten. Rufen Sie dazu die Gespeicherte Prozedur in mysql.rds_assign_gtids_to_anonymous_transactions (Aurora MySQL Version 3) auf.

Deaktivieren einer GTID-basierten Replikation für einen Aurora MySQL-DB-Cluster

Sie können eine GTID-basierte Replikation für einen Aurora-MySQL-DB-Cluster deaktivieren. Dies bedeutet, dass der Aurora-Cluster keine ein- oder ausgehende binlog-Replikation mit externen Datenbanken ausführen kann, die .

> **Note**
>
> Im folgenden Verfahren bezieht sich Lesereplikat auf das Replikationsziel in einer Aurora-Konfiguration mit binlog-Replikation in eine externe oder aus einer externen Datenbank. Es bezieht sich nicht auf die schreibgeschützten Aurora Replica-DB-Instances. Wenn ein Aurora-Cluster beispielsweise eine eingehende Replikation aus einer externen Quelle akzeptiert, dann fungiert die primäre Aurora-Instance als Lesereplikat der binlog-Replikation.

Weitere Informationen zu den in diesem Abschnitt erwähnten gespeicherten Verfahren finden Sie unter Von Aurora MySQL gespeicherte Prozeduren.

GTID-basierte Replikation für einen Aurora-MySQL-DB-Cluster deaktivieren

1. Führen Sie auf den Aurora-Repliken das folgende Verfahren aus:

   Für Version 3

   ```
   CALL mysql.rds_set_source_auto_position(0);
   ```

   Für Version 2

   ```
   CALL mysql.rds_set_master_auto_position(0);
   ```

2. Setzen Sie den Wert für `gtid_mode` auf `ON_PERMISSIVE` zurück.

   a. Stellen Sie sicher, das bei der DB-Clusterparametergruppe, die dem Aurora MySQL-Cluster zugeordnet ist, `gtid_mode` auf `ON_PERMISSIVE` eingestellt ist.

      Weitere Informationen zum Einstellen von Konfigurationsparametern unter Verwendung von Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

   b. Starten Sie den Aurora MySQL-DB-Cluster neu.

3. Setzen Sie den Wert für `gtid_mode` auf `OFF_PERMISSIVE` zurück.

   a. Stellen Sie sicher, das bei der DB-Clusterparametergruppe, die dem Aurora MySQL-Cluster zugeordnet ist, `gtid_mode` auf `OFF_PERMISSIVE` eingestellt ist.

   b. Starten Sie den Aurora MySQL-DB-Cluster neu.

4. Warten Sie, bis alle GTID-Transaktionen auf die primäre Aurora-Instance angewendet wurden. Gehen Sie wie folgt vor, um zu überprüfen, ob diese angewendet werden:

   a. Führen Sie auf der primären Aurora-Instance den Befehl `SHOW MASTER STATUS` aus.

      Ihre Ausgabe sollte der folgenden Ausgabe ähneln.

      ```
      File                        Position
      ------------------------------------
      mysql-bin-changelog.000031      107
      ```

```
-----------------------------------
```

Notieren Sie die Datei und Position in Ihrer Ausgabe.

b. Verwenden Sie für jedes Read Replica die Datei- und Positionsinformationen aus der Quellinstanz im vorherigen Schritt, um die folgende Abfrage auszuführen:

Für Version 3

```
SELECT SOURCE_POS_WAIT('file', position);
```

Für Version 2

```
SELECT MASTER_POS_WAIT('file', position);
```

Wenn der Dateiname beispielsweise lautet `mysql-bin-changelog.000031` und die Position lautet`107`, führen Sie die folgende Anweisung aus:

Für Version 3

```
SELECT SOURCE_POS_WAIT('mysql-bin-changelog.000031', 107);
```

Für Version 2

```
SELECT MASTER_POS_WAIT('mysql-bin-changelog.000031', 107);
```

5. Setzen Sie die GTID-Parameter zurück, um die GTID-basierte Replikation zu deaktivieren.

a. Die DB-Clusterparametergruppe, die dem Aurora MySQL-Cluster zugeordnet ist, muss über die folgenden Parametereinstellungen verfügen:

- `gtid_mode` – `OFF`
- `enforce_gtid_consistency` – `OFF`

b. Starten Sie den Aurora MySQL-DB-Cluster neu.

Integrieren von Amazon Aurora MySQL in anderen AWS-Services

Amazon Aurora MySQL ist auch in anderen AWS-Services integriert, damit Sie Ihren Aurora-MySQL-DB-Cluster erweitern können, um zusätzliche Funktionen in der AWS Cloud zu verwenden. Ihr Aurora-MySQL-DB-Cluster kann AWS-Services verwenden, um Folgendes durchzuführen:

- Rufen Sie synchron oder asynchron eine AWS Lambda-Funktion mit den nativen Funktionen `lambda_sync` oder `lambda_async` auf. Weitere Informationen finden Sie unter Aufrufen einer Lambda-Funktion aus einem Amazon Aurora MySQL-DB-Cluster.
- Laden Sie Daten aus Text- und XML-Dateien, die in einem Amazon Simple Storage Service (Amazon S3)-Bucket gespeichert sind, mithilfe des Befehls `LOAD DATA FROM S3` oder `LOAD XML FROM S3` in Ihren DB-Cluster. Weitere Informationen finden Sie unter Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket.
- Speichern Sie Daten in die Textdateien, die in einem Amazon S3-Bucket aus Ihrem DB-Cluster gespeichert sind, mithilfe des Befehls `SELECT INTO OUTFILE S3`. Weitere Informationen finden Sie unter Speichern von Daten aus einem Amazon Aurora MySQL-DB-Cluster in Textdateien in einem Amazon S3-Bucket.
- Automatisches Hinzufügen oder Entfernen von Aurora-Replicas mit Application Auto Scaling. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Auto Scaling mit Aurora Replicas.
- Führen Sie Stimmungsanalysen mit Amazon Comprehend oder eine Vielzahl von Machine-Learning-Algorithmen mit durch SageMaker. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Machine Learning.

Mit Aurora können Sie auf andere AWS-Services mithilfe von AWS Identity and Access Management (IAM) zugreifen. Sie können die Erlaubnis erteilen, auf andere AWS-Services zuzugreifen, indem Sie eine IAM-Rolle mit den notwendigen Berechtigungen erstellen und diese dann Ihrem DB-Cluster zuordnen. Weitere Details und Anweisungen, wie Sie selbst Ihren Aurora-MySQL-DB-Cluster für den Zugriff auf andere AWS-Services berechtigen, finden Sie unter Autorisierung von Amazon Aurora MySQL zum Zugriff auf andere AWS-Services für Sie.

Autorisierung von Amazon Aurora MySQL zum Zugriff auf andere AWS-Services für Sie

Damit der Aurora-MySQL-DB-Cluster in Ihrem Auftrag auf andere Services zugreifen kann, erstellen und konfigurieren Sie eine AWS Identity and Access Management-(IAM)-Rolle. Diese Rolle

autorisiert Datenbankbenutzer in Ihrem DB-Cluster, auf andere AWS-Services zuzugreifen. Weitere Informationen finden Sie unter Einrichten von IAM-Rollen für den Zugriff auf AWS-Services.

Sie müssen auch Ihr Aurora-DB-Cluster so konfigurieren, dass ausgehende Verbindungen zum Ziel-AWS-Service erlaubt werden. Weitere Informationen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.

Wenn Sie dies tun, können Ihre Datenbankbenutzer folgende Aktionen mit anderen AWS-Services durchführen:

- Rufen Sie synchron oder asynchron eine AWS Lambda-Funktion mit den nativen Funktionen `lambda_sync` oder `lambda_async` auf. Oder rufen Sie asynchron eine AWS Lambda-Funktion mit der Prozedur `mysql.lambda_async` auf. Weitere Informationen finden Sie unter Aufrufen einer Lambda-Funktion mit einer nativen Aurora MySQL-Funktion.
- Laden Sie Daten aus Text- und XML-Dateien, die in einem Amazon S3-Bucket gespeichert sind, mithilfe der Anweisungen `LOAD DATA FROM S3` oder `LOAD XML FROM S3` in Ihren DB-Cluster. Weitere Informationen finden Sie unter Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket.
- Speichern Sie Daten aus Ihrem DB-Cluster in Textdateien, die in einem Amazon S3-Bucket gespeichert sind, mithilfe der Anweisung `SELECT INTO OUTFILE S3`. Weitere Informationen finden Sie unter Speichern von Daten aus einem Amazon Aurora MySQL-DB-Cluster in Textdateien in einem Amazon S3-Bucket.
- Exportieren Sie Protokolldaten in Amazon CloudWatch Logs MySQL. Weitere Informationen finden Sie unter Veröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs.
- Automatisches Hinzufügen oder Entfernen von Aurora-Replicas mit Application Auto Scaling. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Auto Scaling mit Aurora Replicas.

Einrichten von IAM-Rollen für den Zugriff auf AWS-Services

Führen Sie die folgenden Schritte aus, um Ihrem Aurora-DB-Cluster zu erlauben, auf einen anderen AWS-Service zuzugreifen:

1. Erstellen Sie eine IAM-Zugriffsrichtlinie, die Berechtigungen für den AWS-Service erteilt. Weitere Informationen finden Sie unter:
   - Erstellen einer IAM-Zugriffsrichtlinie für Amazon S3-Ressourcen
   - Erstellen einer IAM-Zugriffsrichtlinie für AWS Lambda-Ressourcen

- Erstellen einer IAM-Zugriffsrichtlinie für CloudWatch Logs-Ressourcen
- Erstellen einer IAM-Zugriffsrichtlinie für AWS KMS-Ressourcen

2. Erstellen Sie eine IAM-Rolle und fügen Sie die erstellte Zugriffsrichtlinie an. Weitere Informationen finden Sie unter Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.
3. Weisen Sie diese IAM-Rolle Ihrem Aurora-DB-Cluster zu. Weitere Informationen finden Sie unter Zuweisen einer IAM-Rolle zu einem Amazon-Aurora-MySQL-DB-Cluster.

Erstellen einer IAM-Zugriffsrichtlinie für Amazon S3-Ressourcen

Aurora kann auf Amazon S3-Ressourcen zugreifen, um entweder Daten zu laden oder Daten aus einem Aurora-DB-Cluster zu speichern. Jedoch müssen Sie zuerst eine IAM-Zugriffsrichtlinie erstellen, die die Bucket- und Objektberechtigungen bereitstellt, um Aurora den Zugriff auf Amazon S3 zu erlauben.

In der folgenden Tabelle sind die Aurora-Funktionen gelistet, die in Ihrem Auftrag auf ein Amazon S3-Bucket zugreifen können, und das Minimum der erforderlichen Bucket- und Objektberechtigungen, die für jede Funktion benötigt werden.

Funktion	Bucket-Berechtigungen	Objektberechtigungen
`LOAD DATA FROM S3`	`ListBucket`	`GetObject` `GetObjectVersion`
`LOAD XML FROM S3`	`ListBucket`	`GetObject` `GetObjectVersion`

`SELECT INTO OUTFILE S3`	`ListBucket`	`AbortMultipartUpload`
		`DeleteObject`
		`GetObject`
		`ListMultipartUploadParts`
		`PutObject`

Die folgende Richtlinie fügt die Berechtigungen hinzu, die Aurora möglicherweise für den Zugriff auf einen Amazon S3-Bucket in Ihrem Namen benötigt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAuroraToExampleBucket",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
            ]
        }
    ]
}
```

> **Note**
>
> Achten Sie darauf, dass beide Einträge für den Wert `Resource` eingeschlossen sind. Aurora benötigt die Berechtigungen sowohl für den Bucket selbst als auch für alle Objekte im Bucket. Basierend auf Ihrem Anwendungsfall müssen Sie möglicherweise nicht alle Berechtigungen in der Beispielrichtlinie hinzufügen. Möglicherweise sind auch weitere Berechtigungen erforderlich. Wenn Ihr Amazon S3-Bucket beispielsweise verschlüsselt ist, müssen Sie `kms:Decrypt`-Berechtigungen hinzufügen.

Sie können die folgenden Schritte ausführen, um eine IAM-Zugriffsrichtlinie zu erstellen, die das Minimum der erforderlichen Berechtigungen für Aurora bereitstellt, um in Ihrem Auftrag auf einen Amazon S3-Bucket zuzugreifen. Um Aurora den Zugriff auf alle Ihre Amazon S3-

Buckets zu erlauben, können Sie diese Schritte überspringen und die vordefinierte IAM-Richtlinie `AmazonS3ReadOnlyAccess` oder `AmazonS3FullAccess` verwenden, anstatt eigene zu erstellen.

So können Sie eine IAM-Zugriffsrichtlinie erstellen, um Zugriff auf Ihre Amazon S3-Ressourcen zu erlauben

1. Öffnen Sie die IAM-Managementkonsole.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie auf der Registerkarte Visueller Editor die Option Service auswählen und dann S3 aus.
5. Wählen Sie unter Actions (Aktionen) die Option Expand all (Alle expandieren). Wählen Sie dann die Bucket-Berechtigungen und Objektberechtigungen aus, die für die IAM-Richtlinie benötigt werden.

   Objektberechtigungen sind Berechtigungen für Objektoperationen in Amazon S3 und müssen für Objekte in einem Bucket und nicht für das Bucket selbst erteilt werden. Weitere Informationen über Berechtigungen für Objektoperationen in Amazon S3 finden Sie unter Berechtigungen für Objektoperationen.
6. Wählen Sie Resources (Ressourcen) und dann Add ARN (ARN hinzufügen) für Bucket (Bucket) aus.
7. Geben Sie im Dialogfeld ARN(s) hinzufügen die Details zu Ihrer Ressource an, und wählen Sie Hinzufügen.

   Geben Sie das Amazon S3-Bucket an, wofür der Zugriff erlaubt werden soll. Wenn Sie Aurora beispielsweise Zugriff auf den Amazon S3 S3-Bucket mit dem Namen *`DOC-EXAMPLE-BUCKET`* gewähren möchten, setzen Sie den Wert Amazon Resource Name (ARN) auf. `arn:aws:s3:::`*`DOC-EXAMPLE-BUCKET`*
8. Wenn die Ressource Objekt aufgelistet ist, wählen Sie ARN hinzufügen für Objekt.
9. Geben Sie im Dialogfeld ARN(s) hinzufügen die Details zu Ihrer Ressource an.

   Geben Sie für den Amazon S3-Bucket den Amazon S3-Bucket an, für den der Zugriff erlaubt werden soll. Sie können für das Objekt Beliebig auswählen, um Berechtigungen für alle Objekte im Bucket bereitzustellen.

> **Note**
>
> Sie können Amazon-Ressourcenname (ARN) auf einen spezifischen ARN-Wert einstellen, um Aurora nur den Zugriff auf spezifische Dateien oder Ordern in einem Amazon S3-Bucket zu erlauben. Weitere Informationen über das Definieren von Zugriffsrichtlinien für Amazon S3 finden Sie unter Verwaltung der Zugriffsberechtigungen zu Ihren Amazon S3-Ressourcen.

10. (Optional) Wählen Sie Add ARN (ARN hinzufügen) für Bucket, um der Richtlinie einen weiteren Amazon S3-Bucket hinzuzufügen, und wiederholen Sie die vorherigen Schritte für den Bucket.

> **Note**
>
> Sie können diesen Schritt wiederholen, um Ihrer Richtlinie die entsprechenden Bucket-Berechtigungsanweisungen für jeden Amazon S3-Bucket hinzuzufügen, auf den Aurora zugreifen soll. Alternativ können Sie auch Zugriff auf alle Buckets und Objekte in Amazon S3 erlauben.

11. Wählen Sie Richtlinie prüfen.
12. Geben Sie unter Name einen Namen für Ihre IAM-Richtlinie ein, z. B. `AllowAuroraToExampleBucket`. Sie verwenden diesen Namen, wenn Sie eine IAM-Rolle erstellen, um sie Ihrem Aurora-DB-Cluster zuzuweisen. Sie können auch einen optionalen Wert für Description (Beschreibung) hinzufügen.
13. Wählen Sie Richtlinie erstellen aus.
14. Führen Sie die Schritte unter au Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.

Erstellen einer IAM-Zugriffsrichtlinie für AWS Lambda-Ressourcen

Sie können eine IAM-Zugriffsrichtlinie zu erstellen, die das Minimum der erforderlichen Berechtigungen für Aurora bereitstellt, um für Sie eine AWS Lambda-Funktion aufzurufen.

Die folgende Richtlinie fügt die Berechtigungen hinzu, die Aurora benötigt, um in Ihrem Namen eine AWS Lambda-Funktion aufzurufen.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowAuroraToExampleFunction",
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource":
 "arn:aws:lambda:<region>:<123456789012>:function:<example_function>"
        }
    ]
}
```

Sie können die folgenden Schritte ausführen, um eine IAM-Zugriffsrichtlinie zu erstellen, die das Minimum der erforderlichen Berechtigungen für Aurora bereitstellt, um für Sie eine AWS Lambda-Funktion aufzurufen. Um Aurora zu erlauben alle Ihre AWS Lambda-Funktionen aufzurufen, können Sie diese Schritte überspringen und die vordefinierte Zugriffsrichtlinie `AWSLambdaRole` verwenden, anstatt Ihre eigene zu erstellen.

So können Sie eine IAM-Zugriffrichtlinie erstellen, um den Aufruf Ihrer AWS Lambda-Funktionen zu genehmigen

1. Öffnen Sie die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Policies aus.
3. Wählen Sie Create Policy (Richtlinie erstellen) aus.
4. Wählen Sie auf der Registerkarte Visueller Editor die Option Service auswählen und dann Lambda aus.
5. Wählen Sie für Actions (Aktionen) die Option Expand all (Alle erweitern) und danach die für die IAM-Richtlinie erforderlichen AWS Lambda-Berechtigungen aus.

   Stellen Sie sicher, dass `InvokeFunction` ausgewählt ist. Diese Berechtigung sind das erforderliche Minimum, um Amazon Aurora zu ermöglichen, eine AWS Lambda-Funktion aufzurufen.
6. Wählen Sie Ressourcen und dann ARN hinzufügen für Funktion.
7. Geben Sie im Dialogfeld ARN(s) hinzufügen die Details zu Ihrer Ressource an.

   Geben Sie die Lambda-Funktion an, wofür der Zugriff erlaubt werden soll.
   Wenn Sie beispielsweise Aurora den Zugriff auf eine Lambda-Funktion mit dem Namen `example_function` erlauben möchten, stellen Sie den ARN-Wert auf `arn:aws:lambda:::function:example_function` ein.

Weitere Informationen über das Definieren einer Zugriffsrichtlinie für AWS Lambda finden Sie unter Authentifizierung und Zugriffskontrolle für AWS Lambda.

8. Wählen Sie optional Add additional permissions (Zusätzliche Berechtigungen hinzufügen) um der Richtlinie eine weitere AWS Lambda-Funktion hinzuzufügen, und wiederholen Sie die vorherigen Schritte für die Funktion.

> **Note**
>
> Sie können diesen Schritt wiederholen, um Ihrer Richtlinie die entsprechenden Funktionsberechtigungsanweisungen für jede AWS Lambda-Funktion hinzuzufügen, auf die Aurora zugreifen soll.

9. Wählen Sie Review policy (Richtlinie prüfen).
10. Stellen Sie Name auf einen Namen für Ihre IAM-Zugriffsrichtlinie ein, zum Beispiel `AllowAuroraToExampleFunction`. Sie verwenden diesen Namen, wenn Sie eine IAM-Rolle erstellen, um sie Ihrem Aurora-DB-Cluster zuzuweisen. Sie können auch einen optionalen Wert für Description (Beschreibung) hinzufügen.
11. Wählen Sie Create Policy (Richtlinie erstellen) aus.
12. Führen Sie die Schritte unter au Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.

Erstellen einer IAM-Zugriffsrichtlinie für CloudWatch Logs-Ressourcen

Aurora kann auf CloudWatch Logs zugreifen, um Auditprotokolldateien aus einem Aurora-DB-Cluster zu exportieren. Jedoch müssen Sie zuerst eine IAM-Richtlinie erstellen, die der Protokollgruppe und dem Protokollstream Berechtigungen erteilt, damit Aurora auf CloudWatch Logs zugreifen kann.

Die folgende Richtlinie fügt die erforderlichen Berechtigungen hinzu, damit Aurora auf Amazon CloudWatch Logs in Ihrem Namen zugreifen darf, sowie die mindestens erforderlichen Berechtigungen zur Erstellung von Protokollgruppen und zum Exportieren von Daten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableCreationAndManagementOfRDSCloudwatchLogEvents",
            "Effect": "Allow",
```

```
            "Action": [
                "logs:GetLogEvents",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
        },
        {
            "Sid": "EnableCreationAndManagementOfRDSCloudwatchLogGroupsAndStreams",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:PutRetentionPolicy",
                "logs:CreateLogGroup"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/rds/*"
        }
    ]
}
```

Sie können die ARNs in der Richtlinie ändern, um den Zugriff auf eine bestimmte AWS-Region und ein bestimmtes Konto einzuschränken.

Mit den folgenden Schritten können Sie eine IAM-Richtlinie erstellen, die die mindestens erforderlichen Berechtigungen für Aurora bereitstellt, um in Ihrem Namen auf CloudWatch Logs zuzugreifen. Um Aurora den uneingeschränkten Zugriff auf CloudWatch Logs zu erlauben, können Sie diese Schritte überspringen und die vordefinierten IAM-Richtlinie `CloudWatchLogsFullAccess` verwenden, anstatt eine eigene zu erstellen. Weitere Informationen finden Sie unter Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für CloudWatch Logs im Amazon CloudWatch-Benutzerhandbuch.

So können Sie eine IAM-Zugriffsrichtlinie erstellen, um Zugriff auf Ihre CloudWatch Logs-Ressourcen zu erlauben

1. Öffnen Sie die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Policies aus.
3. Wählen Sie Create Policy (Richtlinie erstellen) aus.
4. Wählen Sie auf der Registerkarte Visueller Editor die Option Service auswählen und dann CloudWatch Logs (CloudWatch-Protokolle) aus.

5. Wählen Sie für Actions (Aktionen) die Option Expand all (Alle erweitern) (auf er rechten Seite) und danach die für die IAM-Richtlinie erforderlichen Amazon CloudWatch Logs-Berechtigungen aus.

   Vergewissern Sie sich, dass die folgenden Berechtigungen ausgewählt sind:

   - `CreateLogGroup`
   - `CreateLogStream`
   - `DescribeLogStreams`
   - `GetLogEvents`
   - `PutLogEvents`
   - `PutRetentionPolicy`
6. Wählen Sie Ressourcen und dann ARN hinzufügen für log-group (Protokollgruppe).
7. Geben Sie im Dialogfeld ARN(s) hinzufügen die folgenden Werte ein:

   - Region – Eine AWS-Region oder *
   - Konto – Eine Kontonummer oder *
   - Protokollgruppenname – `/aws/rds/*`
8. Wählen Sie im Dialogfeld Add ARN(s) (ARN(s) hinzufügen) Add (Hinzufügen).
9. Wählen Sie ARN hinzufügen für log-stream (Protokollstream).
10. Geben Sie im Dialogfeld ARN(s) hinzufügen die folgenden Werte ein:

    - Region – Eine AWS-Region oder *
    - Konto – Eine Kontonummer oder *
    - Protokollgruppenname – `/aws/rds/*`
    - Protokollstreamname – *
11. Wählen Sie im Dialogfeld Add ARN(s) (ARN(s) hinzufügen) Add (Hinzufügen).
12. Wählen Sie Review policy (Richtlinie prüfen).
13. Stellen Sie Name auf einen Namen für Ihre IAM-Zugriffsrichtlinie ein, zum Beispiel `AmazonRDSCloudWatchLogs`. Sie verwenden diesen Namen, wenn Sie eine IAM-Rolle erstellen, um sie Ihrem Aurora-DB-Cluster zuzuweisen. Sie können auch einen optionalen Wert für Description (Beschreibung) hinzufügen.
14. Wählen Sie Create Policy (Richtlinie erstellen) aus.

15. Führen Sie die Schritte unter au Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.

Erstellen einer IAM-Zugriffsrichtlinie für AWS KMS-Ressourcen

Aurora kann auf die AWS KMS keys zugreifen, die für die Verschlüsselung ihrer Datenbanksicherungen verwendet wird. Sie müssen jedoch zunächst eine IAM-Richtlinie erstellen, die Aurora den Zugriff auf KMS-Schlüssel erlaubt.

Die folgende Richtlinie fügt die Berechtigungen hinzu, die Aurora für den Zugriff auf KMS-Schlüssel in Ihrem Namen benötigt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:<region>:<123456789012>:key/<key-ID>"
        }
    ]
}
```

Anhand der folgenden Schritte können Sie eine IAM-Richtlinie erstellen, die Aurora die erforderlichen Mindestberechtigungen für den Zugriff auf KMS-Schlüssel in Ihrem Namen erteilt.

So erstellen Sie eine IAM-Richtlinie zum Gewähren des Zugriffs auf Ihre KMS-Schlüssel

1. Öffnen Sie die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Policies aus.
3. Wählen Sie Create Policy (Richtlinie erstellen) aus.
4. Wählen Sie auf der Registerkarte Visueller Editor die Option Service auswählen und dann KMS aus.
5. Wählen Sie unter Actions (Aktionen) die Option Write (Schreiben) und danach Decrypt (Entschlüsseln) aus.
6. Wählen Sie Ressourcen und danach ARN hinzufügen.

7. Geben Sie im Dialogfeld ARN(s) hinzufügen die folgenden Werte ein:
   - Region – Geben Sie die AWS-Region ein, wie etwa `us-west-2`.
   - Konto – Geben Sie die Nummer des Benutzerkontos ein.
   - Log Stream Name - Geben Sie den KMS-Schlüsselbezeichner ein.
8. Wählen Sie im Dialogfeld Add ARN(s) (ARN(s) hinzufügen) Add (Hinzufügen).
9. Wählen Sie Review policy (Richtlinie prüfen).
10. Stellen Sie Name auf einen Namen für Ihre IAM-Zugriffsrichtlinie ein, zum Beispiel `AmazonRDSKMSKey`. Sie verwenden diesen Namen, wenn Sie eine IAM-Rolle erstellen, um sie Ihrem Aurora-DB-Cluster zuzuweisen. Sie können auch einen optionalen Wert für Description (Beschreibung) hinzufügen.
11. Wählen Sie Create Policy (Richtlinie erstellen) aus.
12. Führen Sie die Schritte unter au Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.

Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben

Nachdem Sie eine IAM-Zugriffsrichtlinie erstellt haben, um Aurora Zugriff auf AWS-Ressourcen zu erlauben, müssen Sie eine IAM-Rolle erstellen und der IAM-Zugriffsrichtlinie die neue IAM-Rolle anfügen.

Gehen Sie wie folgt vor, um eine IAM-Rolle zu erstellen, die Ihrem Amazon-RDS-Cluster die Kommunikation mit anderen AWS-Services für Sie ermöglicht.

So erstellen Sie eine IAM-Rolle, um Amazon RDS; den Zugriff auf AWS-Services zu ermöglichen:

1. Öffnen Sie die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Roles aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie unter AWS-ServiceRDS.
5. Wählen Sie unter Select your use case (Anwendungsfall auswählen) die Option RDS – Add Role to Database (RDS Rolle zur Datenbank hinzufügen) aus.
6. Wählen Sie Next (Weiter).
7. Geben Sie auf der Seite Attach permissions policies (Berechtigungsrichtlinien anfügen) den Namen Ihrer Richtlinie im Feld Search (Suchen) ein.

8. Wenn die zuvor definierte Richtlinie in der Liste angezeigt wird, wählen Sie diese entsprechend den Anweisungen in einem der folgenden Abschnitte aus:

   - Erstellen einer IAM-Zugriffsrichtlinie für Amazon S3-Ressourcen
   - Erstellen einer IAM-Zugriffsrichtlinie für AWS Lambda-Ressourcen
   - Erstellen einer IAM-Zugriffsrichtlinie für CloudWatch Logs-Ressourcen
   - Erstellen einer IAM-Zugriffsrichtlinie für AWS KMS-Ressourcen
9. Wählen Sie Next (Weiter).
10. Geben Sie unter Role name (Rollenname) einen Namen für Ihre IAM-Rolle ein, z. B. `RDSLoadFromS3`. Sie können auch einen optionalen Wert für Description (Beschreibung) hinzufügen.
11. Wählen Sie Create Role aus.
12. Führen Sie die Schritte unter au Zuweisen einer IAM-Rolle zu einem Amazon-Aurora-MySQL-DB-Cluster.

Zuweisen einer IAM-Rolle zu einem Amazon-Aurora-MySQL-DB-Cluster

Weisen Sie die IAM-Rolle, die Sie in Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben erstellt haben, einem DB-Cluster zu, um Datenbankbenutzern in diesem DB-Cluster von Amazon Aurora den Zugriff auf andere AWS-Services zu erlauben. Sie können auch eine neue IAM-Rolle durch AWS erstellen lassen, indem Sie den Service direkt zuordnen.

> **Note**
>
> Sie können keine IAM-Rolle mit einem Aurora Serverless v1-DB-Cluster verknüpfen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Serverless v1.
> Sie können eine IAM-Rolle mit einem DB-Cluster von Aurora Serverless v2verknüpfen.

Sie müssen zwei Dinge tun, um eine IAM-Rolle mit einem DB-Cluster zu verbinden:

1. Fügen Sie die Rolle zu der Liste mit den zugewiesenen Rollen für ein DB-Cluster mithilfe der RDS-Konsole und dem AWS CLI-Befehl add-role-to-db-cluster oder der RDS-API-Operation AddRoleToDBCluster hinzu.

   Sie können maximal fünf IAM-Rollen für jeden Aurora-DB-Cluster hinzufügen.

2. Stellen Sie den Cluster-Level-Parameter für den zugehörigen AWS-Service auf den ARN für die zugeordnete IAM-Rolle ein.

   Die folgende Tabelle beschreibt die Cluster-Level-Parameter-Namen für die IAM-Rollen, die für den Zugriff auf andere AWS-Services verwendet werden.

Parameter auf Clusterebene	Beschreibung
`aws_default_lambda_role`	Wird beim Aufrufen einer Lambda-Funktion aus dem DB-Cluster verwendet.
`aws_default_logs_role`	Dieser Parameter ist nicht mehr erforderlich, um Protokolldaten von Ihrem DB-Cluster in Amazon CloudWatch Logs zu exportieren. Aurora MySQL verwendet jetzt eine serviceverknüpfte Rolle für die erforderlichen Berechtigungen. Weitere Informationen zu Service-verknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Aurora.
`aws_default_s3_role`	Wird beim Aufrufen der Anweisung `LOAD DATA FROM S3`, `LOAD XML FROM S3` oder `SELECT INTO OUTFILE S3` aus Ihrem DB-Cluster verwendet. Bei Aurora-MySQL-Version 2 wird die in diesem Parameter festgelegte IAM-Rolle verwendet, wenn keine IAM-Rolle für `aurora_load_from_s3_role` oder `aurora_select_into_s3_role` für die entsprechende Anweisung festgelegt ist. Bei Aurora-MySQL-Version 3 wird die für diesen Parameter festgelegte IAM-Rolle immer verwendet.

Parameter auf Clusterebene	Beschreibung
`aurora_load_from_s3_role`	Wird beim Aufrufen der Anweisung `LOAD DATA FROM S3` oder `LOAD XML FROM S3` aus Ihrem DB-Cluster verwendet. Wenn keine IAM-Rolle für diesen Parameter festgelegt ist, wird die in `aws_default_s3_role` festgelegte IAM-Rolle verwendet. Bei Aurora MySQL Version 3 ist dieser Parameter nicht verfügbar.
`aurora_select_into_s3_role`	Wird beim Aufrufen der Anweisung `SELECT INTO OUTFILE S3` aus Ihrem DB-Cluster verwendet. Wenn keine IAM-Rolle für diesen Parameter festgelegt ist, wird die in `aws_default_s3_role` festgelegte IAM-Rolle verwendet. Bei Aurora MySQL Version 3 ist dieser Parameter nicht verfügbar.

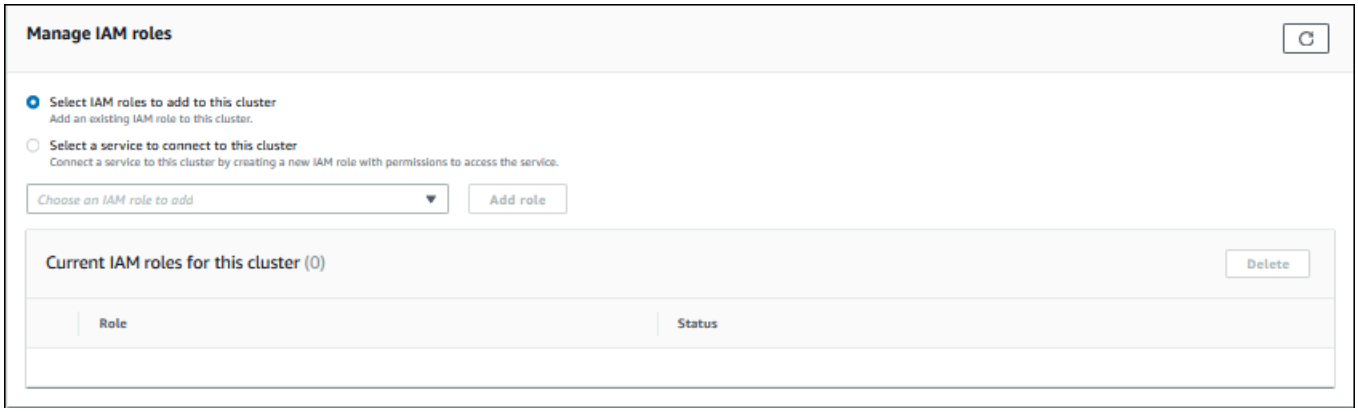
Gehen Sie wie folgt vor, um einer IAM-Rolle die Erlaubnis, Ihrem Amazon-RDS-Cluster die Kommunikation mit anderen AWS-Services für Sie zu ermöglichen, zuzuweisen.

Konsole

Sie müssen zwei Dinge tun, um eine IAM-Rolle einem Aurora-DB-Cluster mithilfe der Konsole zuzuweisen:

1. Öffnen Sie die RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Datenbanken aus.
3. Wählen Sie den Namen des Aurora-DB-Clusters, den Sie einer IAM-Rolle zuweisen möchten, aus, um die entsprechenden Details anzuzeigen.
4. Führen Sie auf der Registerkarte Konnektivität und Sicherheit im Abschnitt IAM-Rollen verwalten eine der folgenden Aktionen aus:

- IAM-Rollen auswählen, die diesem Cluster hinzugefügt werden sollen (Standard)
- Einen Service zum Herstellen einer Verbindung mit diesem Cluster auswählen



5. Wenn Sie eine vorhandene IAM-Rolle verwenden möchten, wählen Sie diese aus dem Menü aus und klicken Sie dann auf Add role (Rolle hinzufügen).

   Wenn die Rolle erfolgreich hinzugefügt wurde, wird ihr Status als `Pending` und dann als `Available` angezeigt.

6. So verbinden Sie einen Service direkt:

   a. Wählen Sie Select a service to connect to this cluster (Einen Service zum Herstellen einer Verbindung mit diesem Cluster auswählen) aus.

   b. Wählen Sie den Service aus dem Menü aus und klicken Sie dann auf Connect service (Service verbinden).

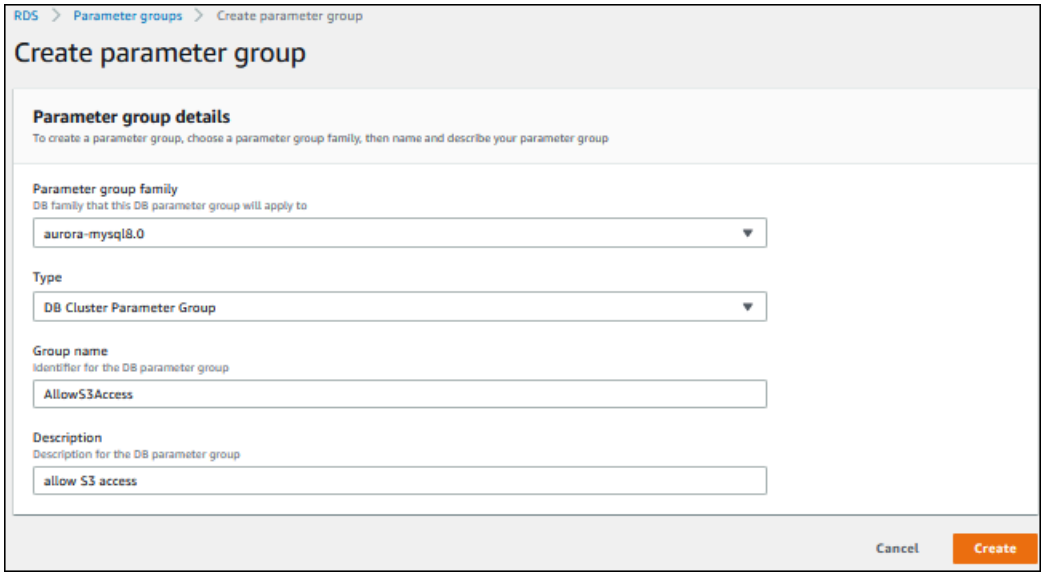
   c. Geben Sie unter Connect cluster to ***`Service Name`*** (Cluster mit „Servicename“ verbinden) den Amazon-Ressourcennamen (ARN) ein, der für die Verbindung mit dem Service verwendet werden soll, und wählen Sie dann Connect service (Service verbinden) aus.

   AWS erstellt eine neue IAM-Rolle für die Verbindung mit dem Service. Der Status wird als `Pending` und dann als `Available` angezeigt.

7. (Optional) Wenn Sie die Zuordnung einer IAM-Rolle mit einem DB-Cluster aufheben und die zugehörige Berechtigung entziehen möchten, wählen Sie die Rolle und dann Delete (Löschen) aus.

So legen Sie den Cluster-Level-Parameter für die zugeordnete Rolle fest

1. Wählen Sie in der RDS-Konsole Parametergruppen im Navigationsbereich aus.
2. Wenn Sie bereits eine benutzerdefinierte DB-Parametergruppe verwenden, können Sie diese Gruppe auswählen, statt eine neue DB-Cluster-Parametergruppe zu erstellen. Wenn Sie die Standard-DB-Cluster-Parametergruppe verwenden, erstellen Sie eine neue DB-Cluster-Parametergruppe, wie in den folgenden Schritten beschrieben ist:
   a. Wählen Sie Parametergruppe erstellen.
   b. Wählen Sie für Parametergruppenfamilie für einen mit Aurora MySQL 5.6 kompatiblen DB-Cluster `aurora-mysql8.0`, oder `aurora-mysql5.7` für einen mit Aurora MySQL 5.7 kompatiblen DB-Cluster.
   c. Wählen Sie für Typ die Option DB-Cluster-Parametergruppe.
   d. Geben Sie für Gruppenname den Namen Ihrer neuen DB-Cluster-Parametergruppe ein.
   e. Geben Sie unter Beschreibung die Beschreibung für Ihre neue DB-Cluster-Parametergruppe ein.



   f. Wählen Sie Create aus.
3. Wählen Sie auf der Seite Parameter Groups (Parametergruppen) Ihre DB-Cluster-Parametergruppe und danach die Option Edit (Bearbeiten) unter Parameter group actions (Parametergruppenaktionen) aus.
4. Legen Sie die entsprechenden Cluster-Level-Parameter für die zugehörigen ARN-Werte der IAM-Rolle fest.

Sie können beispielsweise den Parameter `aws_default_s3_role` auf `arn:aws:iam::123456789012:role/AllowS3Access` einstellen.

5. Wählen Sie Änderungen speichern.
6. Um die DB-Cluster-Parametergruppe für Ihren DB-Cluster zu ändern, führen Sie die folgenden Schritte aus:

   a. Wählen Sie Datenbanken aus und wählen Sie dann Ihren Aurora DB-Cluster aus.

   b. Wählen Sie Ändern aus.

   c. Blättern Sie zu Datenbankoptionen und legen Sie DB-Cluster-Parametergruppe auf die DB-Cluster-Parametergruppe fest.

   d. Klicken Sie auf Weiter.

   e. Überprüfen Sie Ihre Änderungen, und klicken Sie anschließend auf Sofort anwenden.

   f. Wählen Sie Modify Cluster (Cluster ändern) aus.

   g. Wählen Sie Databases (Datenbanken) und anschließend die primäre Instance für Ihren DB-Cluster aus.

   h. Wählen Sie unter Aktionen die Option Neustart aus.

      Wenn die Instance neu gestartet wurde, wird Ihre IAM-Rolle Ihrem DB-Cluster zugewiesen.

      Weitere Informationen zu Cluster-Parametergruppen finden Sie unter Aurora MySQL Konfigurationsparameter.

CLI

So weisen Sie eine IAM-Rolle einem DB-Cluster mithilfe der AWS CLI zu:

1. Rufen Sie den Befehl `add-role-to-db-cluster` aus der AWS CLI auf, um die ARNs für Ihre IAM-Rollen zum DB-Cluster hinzuzufügen, wie im Folgenden gezeigt.

```
PROMPT> aws rds add-role-to-db-cluster --db-cluster-identifier my-cluster --role-
arn arn:aws:iam::123456789012:role/AllowAuroraS3Role
PROMPT> aws rds add-role-to-db-cluster --db-cluster-identifier my-cluster --role-
arn arn:aws:iam::123456789012:role/AllowAuroraLambdaRole
```

2. Wenn Sie die Standard-DB-Cluster-Parametergruppe verwenden, erstellen Sie eine neue DB-Cluster-Parametergruppe. Wenn Sie bereits eine benutzerdefinierte DB-

Parametergruppe verwenden, können Sie diese Gruppe verwenden, anstatt eine neue DB-Cluster-Parametergruppe zu erstellen.

Rufen Sie den Befehl `create-db-cluster-parameter-group` aus der AWS CLI auf, um eine neue DB-Cluster-Parametergruppe zu erstellen, wie im Folgenden gezeigt.

```
PROMPT> aws rds create-db-cluster-parameter-group  --db-cluster-parameter-group-
name AllowAWSAccess \
     --db-parameter-group-family aurora5.7 --description "Allow access to Amazon S3
 and AWS Lambda"
```

Für einen mit Aurora MySQL 5.7 kompatiblen DB-Cluster geben Sie `aurora-mysql5.7` für `--db-parameter-group-family` an. Für einen mit Aurora MySQL 8.0 kompatiblen DB-Cluster geben Sie `aurora-mysql8.0` für `--db-parameter-group-family` an.

3. Stellen Sie den/die entsprechenden Cluster-Level-Parameter und die zugehörigen ARN-Werte der IAM-Rolle in Ihrer DB-Cluster-Parametergruppe ein, wie im Folgenden gezeigt.

```
PROMPT> aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-name
 AllowAWSAccess \
    --parameters
 "ParameterName=aws_default_s3_role,ParameterValue=arn:aws:iam::123456789012:role/
AllowAuroraS3Role,method=pending-reboot" \
    --parameters
 "ParameterName=aws_default_lambda_role,ParameterValue=arn:aws:iam::123456789012:role/
AllowAuroraLambdaRole,method=pending-reboot"
```

4. Ändern Sie das DB-Cluster, um die neue DB-Clusterparametergruppe zu verwenden und starten Sie das Cluster anschließend neu, wie im Folgenden gezeigt.

```
PROMPT> aws rds modify-db-cluster --db-cluster-identifier my-cluster --db-cluster-
parameter-group-name AllowAWSAccess
PROMPT> aws rds reboot-db-instance --db-instance-identifier my-cluster-primary
```

Wenn die Instance neu gestartet ist, sind Ihre IAM-Rollen Ihrem DB-Cluster zugewiesen.

Weitere Informationen zu Cluster-Parametergruppen finden Sie unter Aurora MySQL Konfigurationsparameter.

Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services

Um bestimmte andere AWS-Services mit Amazon Aurora nutzen zu können, muss die Netzwerkkonfiguration Ihres Aurora-DB-Clusters ausgehende Verbindungen zu Endpunkten für diese Services zulassen. Für die folgenden Operationen ist diese Netzwerkkonfiguration erforderlich.

- Aufrufen von AWS Lambda-Funktionen Weitere Informationen zu dieser Funktion finden Sie unter Aufrufen einer Lambda-Funktion mit einer nativen Aurora MySQL-Funktion.
- Zugriff auf Dateien von Amazon S3. Weitere Informationen zu dieser Funktion finden Sie unter Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket und Speichern von Daten aus einem Amazon Aurora MySQL-DB-Cluster in Textdateien in einem Amazon S3-Bucket.
- Zugriff auf AWS KMS-Endpunkte. AWS KMS-Zugriff ist erforderlich, um Datenbankaktivitäts-Streams mit Aurora MySQL verwenden zu können. Weitere Informationen zu dieser Funktion finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.
- Zugriff auf SageMaker-Endpunkte. SageMaker-Zugriff ist erforderlich, um SageMaker Machine Learning mit Aurora MySQL verwenden zu können. Weitere Informationen zu dieser Funktion finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.

Aurora gibt die folgenden Fehlermeldungen zurück, wenn keine Verbindung mit einem Service-Endpunkt hergestellt werden kann.

```
ERROR 1871 (HY000): S3 API returned error: Network Connection
```

```
ERROR 1873 (HY000): Lambda API returned error: Network Connection. Unable to connect to
 endpoint
```

```
ERROR 1815 (HY000): Internal error: Unable to initialize S3Stream
```

Bei Datenbankaktivitäts-Streams, die Aurora MySQL verwenden, funktioniert der Aktivitäts-Stream nicht mehr, wenn der DB-Cluster nicht auf den AWS KMS-Endpunkt zugreifen kann. Sie werden von Aurora über dieses Problem mithilfe von RDS-Ereignissen benachrichtigt.

Wenn Sie bei der Nutzung der entsprechenden AWS-Services auf diese Meldungen stoßen, prüfen Sie, ob Ihr Aurora-DB-Cluster öffentlich oder privat ist. Wenn Ihr Aurora-DB-Cluster privat ist, müssen Sie es konfigurieren, um die Verbindungen zu aktivieren.

Damit ein Aurora-DB-Cluster öffentlich ist, muss es als öffentlich zugänglich markiert sein. Wenn Sie in den Details für das DB-Cluster in der AWS Management Console nachsehen, sollte für Publicly Accessible (Öffentlich zugänglich) Ja ausgewählt sein, wenn dies der Fall ist. Das DB-Cluster muss sich auch in einem Amazon VPC-öffentlichen Subnetz befinden. Weitere Informationen über öffentlich zugängliche DB-Instances finden Sie unter Arbeiten mit einer DB-Cluster in einer VPC. Weitere Informationen zu öffentlichen Amazon VPC-Subnetzen finden Sie unter Ihre VPC und Subnetze.

Wenn Ihr Aurora-DB-Cluster nicht öffentlich zugänglich ist und sich nicht in einem öffentlichen VPC-Subnetz befindet, ist er privat. Möglicherweise verfügen Sie über einen DB-Cluster, der privat ist, und möchten eine der Funktionen nutzen, für die diese Netzwerkkonfiguration erforderlich ist. Konfigurieren Sie dazu den Cluster so, dass er sich mit Internetadressen über Network Address Translation (NAT) verbinden kann. Als Alternative zu Amazon S3, Amazon SageMaker und AWS Lambda können Sie stattdessen die VPC so konfigurieren, dass sie einen VPC-Endpunkt für den anderen Service besitzt, der der Routing-Tabelle des DB-Clusters zugeordnet ist, vgl. Arbeiten mit einer DB-Cluster in einer VPC. Weitere Informationen über das Konfigurieren von NAT in Ihrer VPC finden Sie unter NAT Gateways. Weitere Informationen über das Konfigurieren von VPC-Endpunkten finden Sie unter VPC-Endpunkte. Sie können auch einen S3-Gateway-Endpunkt erstellen, um auf Ihren S3-Bucket zuzugreifen. Weitere Informationen finden Sie unter Gateway-Endpunkte für Amazon S3.

Möglicherweise müssen Sie auch die kurzlebigen Ports für Ihre Netzwerkzugriffssteuerungslisten (ACLs) in den ausgehenden Regeln für Ihre VPC-Sicherheitsgruppe öffnen. Weitere Informationen zu kurzlebigen Ports für Netzwerk-ACLs finden Sie unter Kurzlebige Ports im Benutzerhandbuch für Amazon Virtual Private Cloud.

Verwandte Themen

- Integrieren von Aurora in anderen AWS-Services
- Verwalten eines Amazon Aurora-DB-Clusters

Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket

Sie können den Ausdruck `LOAD DATA FROM S3` oder `LOAD XML FROM S3` verwenden, um Daten aus Dateien zu laden, die in einem Amazon S3-Bucket gespeichert sind. In Aurora MySQL werden die Dateien zuerst auf der lokalen Festplatte gespeichert und dann in die Datenbank importiert. Nachdem die Importe in die Datenbank abgeschlossen sind, werden die lokalen Dateien gelöscht.

> **Note**
>
> Für Aurora Serverless v1 wird das Laden von Daten aus Textdateien in eine Tabelle nicht unterstützt. Für Aurora Serverless v2 wird sie unterstützt.

Inhalt

Gewähren von Zugriff auf Amazon S3 für Aurora

Bevor Sie Daten aus einem Amazon S3-Bucket laden können, müssen Sie Ihrem Aurora MySQL-DB-Cluster die Berechtigung für den Zugriff auf Amazon S3 erteilen.

So gewähren Sie Aurora MySQL Zugriff auf Amazon S3:

1. Erstellen Sie eine AWS Identity and Access Management (IAM-) Richtlinie, die die Bucket- und Objektberechtigungen bereitstellt, die Ihrem Aurora MySQL-DB-Cluster den Zugriff auf Amazon S3 ermöglichen. Anweisungen finden Sie unter Erstellen einer IAM-Zugriffsrichtlinie für Amazon S3-Ressourcen.

> **Note**
>
> In Aurora MySQL Version 3.05 und höher können Sie Objekte laden, die mit vom Kunden verwalteten AWS KMS keys verschlüsselt sind. Nehmen Sie dazu die Berechtigung `kms:Decrypt` in Ihre IAM-Richtlinie auf. Weitere Informationen finden Sie unter Erstellen einer IAM-Zugriffsrichtlinie für AWS KMS-Ressourcen.
> Sie benötigen diese Berechtigung nicht, um Objekte zu laden, die mit Von AWS verwaltete Schlüssel Amazon S3 S3-verwalteten Schlüsseln (SSE-S3) verschlüsselt wurden.

2. Erstellen Sie eine IAM-Rolle und fügen Sie der neuen IAM-Rolle die IAM-Richtlinie hinzu, die Sie in Erstellen einer IAM-Zugriffsrichtlinie für Amazon S3-Ressourcen erstellt haben. Detaillierte Anweisungen finden Sie unter Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.
3. Stellen Sie sicher, dass der DB-Cluster eine benutzerdefinierte DB-Cluster-Parametergruppe verwendet.

   Weitere Informationen über das Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe finden Sie unter Erstellen einer DB-Cluster-Parametergruppe.
4. Legen Sie in Aurora MySQL Version 2 einen der DB-Cluster-Parameter `aurora_load_from_s3_role` oder `aws_default_s3_role` auf den Amazon-Ressourcennamen (ARN) der neuen IAM-Rolle fest. Wenn für `aurora_load_from_s3_role` keine IAM-Rolle angegeben wird, verwendet Aurora die unter `aws_default_s3_role` angegebene IAM-Rolle.

   Verwenden Sie `aws_default_s3_role` in Aurora MySQL Version 3.

   Wenn das Cluster Teil einer globalen Aurora-Datenbank ist, legen Sie diesen Parameter für jedes Aurora-Cluster in der globalen Datenbank fest. Auch wenn nur das primäre Cluster in einer globalen Aurora-Datenbank Daten laden kann, kann ein anderes Cluster durch den Failover-Mechanismus zum primären Cluster hochgestuft werden.

   Weitere Informationen zu DB-Cluster-Parametern finden Sie unter Amazon Aurora-DB-Cluster und DB-Instance-Parameter.
5. Weisen Sie die Rolle, die Sie in Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben erstellt haben, diesem DB-Cluster zu, um Datenbankbenutzern in einem Aurora MySQL DB-Cluster den Zugriff auf Amazon S3 zu erlauben. Bei einer globalen

Aurora-Datenbank verknüpfen Sie die Rolle mit jedem Aurora-Cluster in der globalen Datenbank. Weitere Informationen zum Zuordnen einer IAM-Rolle zu einem DB-Cluster finden Sie unter Zuweisen einer IAM-Rolle zu einem Amazon-Aurora-MySQL-DB-Cluster.

6. Konfigurieren Sie Ihren Aurora MySQL-DB-Cluster so, dass er ausgehende Verbindungen zu Amazon S3 zulässt. Detaillierte Anweisungen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.

   Wenn Ihr -DB-Cluster nicht öffentlich zugänglich ist und sich nicht in einem öffentlichen VPC-Subnetz befindet, ist er privat. Sie können einen S3-Gateway-Endpunkt für den Zugriff auf Ihren S3-Bucket erstellen. Weitere Informationen finden Sie unter Gateway-Endpunkte für Amazon S3.

   Bei einer globalen Aurora-Datenbank aktivieren Sie ausgehende Verbindungen für jeden Aurora-Cluster in der globalen Datenbank.

Erteilen von Berechtigungen für das Laden von Daten in Amazon Aurora MySQL

Der Datenbankbenutzer, der die `LOAD DATA FROM S3`- oder `LOAD XML FROM S3`-Anweisung ausgibt, muss über eine bestimmte Rolle oder Berechtigung verfügen, um eine der Anweisungen auszugeben. In Aurora MySQL Version 3 gewähren Sie die Rolle `AWS_LOAD_S3_ACCESS`. In Aurora MySQL Version 2 gewähren Sie die Berechtigung `LOAD FROM S3`. Dem Administratorbenutzer für ein DB-Cluster wird die entsprechende Rolle oder -Berechtigung standardmäßig gewährt. Sie können die Berechtigung einem anderen Benutzer erteilen, indem Sie eine der folgenden Anweisungen verwenden.

Verwenden Sie die folgende Anweisung für Aurora MySQL Version 3:

```
GRANT AWS_LOAD_S3_ACCESS TO 'user'@'domain-or-ip-address'
```

> **Tip**
>
> Wenn Sie die Rollentechnik in Aurora MySQL Version 3 verwenden, können Sie die Rolle auch mit der Anweisung `SET ROLE role_name` oder `SET ROLE ALL` aktivieren. Wenn Sie mit dem MySQL 8.0-Rollensystem nicht vertraut sind, finden Sie in Rollenbasiertes Berechtigungsmodell weitere Informationen. Weitere Informationen finden Sie unter Rollen verwenden im MySQL-Referenzhandbuch.
> Dies gilt nur für die aktuelle aktive Sitzung. Wenn Sie die Verbindung wieder herstellen, müssen Sie die `SET ROLE` Anweisung erneut ausführen, um Rechte zu gewähren. Weitere Informationen finden Sie unter SET ROLE-Anweisung im MySQL-Referenzhandbuch.

Sie können den DB-Cluster-Parameter `activate_all_roles_on_login` zum automatischen Aktivieren aller Rollen verwenden, wenn ein Benutzer eine Verbindung mit einer DB-Instance herstellt. Wenn dieser Parameter festgelegt ist, müssen Sie die `SET ROLE` Anweisung im Allgemeinen nicht explizit aufrufen, um eine Rolle zu aktivieren. Weitere Informationen finden Sie unter activate_all_roles_on_login im MySQL-Referenzhandbuch. Sie müssen jedoch zu Beginn einer gespeicherten Prozedur `SET ROLE ALL` explizit aufrufen, um die Rolle zu aktivieren, wenn die gespeicherte Prozedur von einem anderen Benutzer aufgerufen wird.

Verwenden Sie die folgende Anweisung für Aurora MySQL Version 2:

```
GRANT LOAD FROM S3 ON *.* TO 'user'@'domain-or-ip-address'
```

Die Rolle `AWS_LOAD_S3_ACCESS` und die Berechtigung `LOAD FROM S3` sind spezifisch für Amazon Aurora und nicht für externe MySQL-Datenbanken oder DB-Instances von RDS für MySQL verfügbar. Wenn Sie die Replikation zwischen einem Aurora-DB-Cluster als Haupt-Replikation und einer MySQL-Datenbank als Replikations-Client eingerichtet haben, führt die `GRANT`-Anweisung für die Rolle oder Berechtigung dazu, dass die Replikation mit einem Fehler beendet wird. Sie können diese Fehlermeldung ignorieren und mit der Replikation fortfahren. Verwenden Sie das Verfahren mysql_rds_skip_repl_error, um die Fehlermeldung für eine Instance von RDS für MySQL zu überspringen. Um den Fehler in einer externen MySQL-Datenbank zu überspringen, verwenden Sie die Systemvariable slave_skip_errors (Aurora MySQL Version 2) oder die Systemvariable replica_skip_errors (Aurora MySQL Version 3).

> **Note**
>
> Der Datenbankbenutzer muss über `INSERT` Rechte für die Datenbank verfügen, in die er Daten lädt.

Angeben des Pfads (URI) zu einem Amazon-S3-Bucket

Mit folgender Syntax wird der Pfad (URI) zu Dateien angegeben, die in einem Amazon-S3-Bucket gespeichert sind.

```
s3-region://DOC-EXAMPLE-BUCKET/file-name-or-prefix
```

Der Pfad enthält die folgenden Werte:

- `region`(optional) — Die AWS Region, die den Amazon S3 S3-Bucket enthält, aus dem geladen werden soll. Dieser Wert ist optional. Falls Sie keinen Wert für `region` angeben, lädt Aurora die Datei aus Amazon S3 in derselben Region wie Ihr DB-Cluster.
- `bucket-name` – Der Name des Amazon S3-Buckets mit den zu ladenden Daten. Objekt-Präfixe, die einen virtuellen Ordnerpfad identifizieren, werden unterstützt.
- `file-name-or-prefix` – Der Name der Amazon S3-Textdatei oder XML-Datei oder ein Präfix, das eine oder mehrere Text- oder XML-Dateien zum Laden bestimmt. Sie können auch eine Manifestdatei festlegen, die eine oder mehrere Textdateien zum Laden angibt. Weitere Informationen darüber, wie Sie mit einer Manifestdatei Textdateien aus Amazon S3 laden, finden Sie unter Verwenden eines Manifests für zu ladende Dateien.

So kopieren Sie den URI für Dateien in einem S3-Bucket

1. Melden Sie sich bei der Amazon S3 S3-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/s3/.
2. Wählen Sie im Navigationsbereich Buckets und dann den Bucket aus, dessen URI Sie kopieren möchten.
3. Wählen Sie das Präfix oder die Datei aus, die Sie aus S3 laden möchten.
4. Wählen Sie S3-URI kopieren aus.

LOAD DATA FROM S3

Mit der Anweisung `LOAD DATA FROM S3` können Sie Daten in jedem Textdateiformat laden, das von der MySQL-Anweisung LOAD DATA INFILE unterstützt wird (z. B. durch Komma-getrennte Textdaten). Komprimierte Dateien werden nicht unterstützt.

> **Note**
>
> Stellen Sie sicher, dass Ihr Aurora-MySQL-DB-Cluster ausgehende Verbindungen zu S3 zulässt. Weitere Informationen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.

Syntax

```
LOAD DATA [FROM] S3 [FILE | PREFIX | MANIFEST] 'S3-URI'
    [REPLACE | IGNORE]
    INTO TABLE tbl_name
    [PARTITION (partition_name,...)]
    [CHARACTER SET charset_name]
    [{FIELDS | COLUMNS}
        [TERMINATED BY 'string']
        [[OPTIONALLY] ENCLOSED BY 'char']
        [ESCAPED BY 'char']
    ]
    [LINES
        [STARTING BY 'string']
        [TERMINATED BY 'string']
    ]
    [IGNORE number {LINES | ROWS}]
    [(col_name_or_user_var,...)]
    [SET col_name = expr,...]
```

> **Note**
>
> In Aurora MySQL Version 3.05 und höher ist das Schlüsselwort `FROM` optional.

Parameter

Die Anweisung `LOAD DATA FROM S3` verwendet die folgenden erforderlichen und optionalen Parameter. Weitere Informationen zu einigen der Parameter finden Sie unter LOAD DATA-Anweisung in der MySQL-Dokumentation.

FILE | PREFIX | MANIFEST

Gibt an, ob die Daten aus einer einzelnen Datei, aus allen Dateien mit einem bestimmten Präfix oder aus allen Dateien in einem angegebenen Manifest geladen werden sollen. `FILE` ist der Standardwert.

S3-URI

Gibt den URI der zu ladenden Text- oder Manifestdatei oder das zu verwendende Amazon-S3-Präfix an. Legen Sie den URI mithilfe der unter beschriebenen Syntax fes Angeben des Pfads (URI) zu einem Amazon-S3-Bucket.

REPLACE | IGNORE

Gibt an, welche Aktion ausgeführt werden soll, falls eine Eingabezeile die gleichen eindeutigen Schlüsselwerte aufweist wie eine vorhandene Zeile in der Datenbanktabelle.

- Geben Sie `REPLACE` an, wenn die Eingabezeile die bestehende Zeile überschreiben soll.
- Geben Sie `IGNORE` an, wenn die Eingabezeile verworfen werden soll.

INTO TABLE

Gibt den Namen der Datenbanktabelle an, in welche die Eingabezeilen geladen werden sollen.

PARTITION

Gibt vor, dass alle Eingabezeilen in die Partitionen, die in der Liste mit durch Komma getrennten Partitionsnamen angegeben sind, eingefügt werden müssen. Lässt sich eine Eingabezeile nicht in eine der angegebenen Partitionen einfügen, schlägt die Anweisung fehl und eine Fehlermeldung wird zurückgegeben.

CHARACTER SET

Gibt den Zeichensatz der Daten in der Eingabedatei an.

FIELDS | COLUMNS

Gibt an, wie die Felder oder Spalten in der Eingabedatei getrennt werden. Für Felder wird standardmäßig ein Tabulator als Trennzeichen verwendet.

LINES

Gibt an, wie die Zeilen in der Eingabedatei getrennt werden. Zeilen werden standardmäßig durch ein Zeilenumbruchzeichen (`'\n'`) getrennt.

IGNORE ***number*** LINES | ROWS

Gibt an, dass eine bestimmte Anzahl an Zeilen am Anfang der Eingabedatei ignoriert werden sollen. Sie können beispielsweise mit `IGNORE 1 LINES` die erste Headerzeile mit den Spaltennamen überspringen oder mit `IGNORE 2 ROWS` die ersten beiden Datenzeilen der Eingabedatei auslassen. Wenn Sie auch `PREFIX` verwenden, überspringt `IGNORE` eine bestimmte Anzahl von Zeilen am Anfang der ersten Eingabedatei.

col_name_or_user_var, ...

Gibt eine durch Komma getrennte Liste mit einem oder mehreren Spaltennamen bzw. einer oder mehreren Benutzervariablen an, die die Namen der zu ladenden Elemente identifizieren. Der Name einer Benutzervariable, der für diesen Zweck verwendet wird, muss mit dem

Namen eines Elements aus der Textdatei übereinstimmen, welcher ein @ als Präfix hat. Sie können Benutzervariablen einsetzen, um die entsprechenden Feldwerte für die spätere Wiederverwendung zu speichern.

Beispielsweise wird mit folgender Anweisung die erste Spalte aus der Eingabedatei in die erste Spalte von `table1` geladen, zudem wird der Wert der Spalte `table_column2` in `table1` auf den Eingabewert der zweiten Spalte geteilt durch 100 gesetzt.

```
LOAD DATA FROM S3 's3://DOC-EXAMPLE-BUCKET/data.txt'
    INTO TABLE table1
    (column1, @var1)
    SET table_column2 = @var1/100;
```

SET

Gibt eine durch Komma getrennte Liste mit Zuweisungsvorgängen an, die die Werte von Spalten in der Tabelle auf Werte setzen, die nicht in der Eingabedatei enthalten sind.

Beispielsweise setzt die folgende Anweisung die ersten beiden Spalten von `table1` auf die Werte in den ersten beiden Spalten aus der Eingabedatei und anschließend den Wert von `column3` in `table1` auf den aktuellen Zeitstempel.

```
LOAD DATA FROM S3  's3://DOC-EXAMPLE-BUCKET/data.txt'
    INTO TABLE table1
    (column1, column2)
    SET column3 = CURRENT_TIMESTAMP;
```

Auf der rechten Seite von SET-Zuweisungen können Sie Unterabfragen formulieren. Für eine Unterabfrage, die einen Wert zurückgibt, der einer Spalte zugewiesen werden soll, kommt ausschließlich eine skalare Unterabfrage infrage. Des Weiteren können Sie mit einer Unterabfrage keine Daten aus der zu ladenden Tabelle auswählen.

Sie können nicht das Schlüsselwort `LOCAL` der Anweisung `LOAD DATA FROM S3` verwenden, wenn Sie Daten aus einem Amazon-S3-Bucket laden.

Verwenden eines Manifests für zu ladende Dateien

Sie können mit der Anweisung `LOAD DATA FROM S3` und dem Schlüsselwort `MANIFEST` eine Manifestdatei im JSON-Format angeben, in der die Textdateien aufgeführt sind, die in eine Tabelle im DB-Cluster geladen werden sollen.

Das folgende JSON-Schema beschreibt das Format und den Inhalt einer Manifestdatei.

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "additionalProperties": false,
    "definitions": {},
    "id": "Aurora_LoadFromS3_Manifest",
    "properties": {
        "entries": {
            "additionalItems": false,
            "id": "/properties/entries",
            "items": {
                "additionalProperties": false,
                "id": "/properties/entries/items",
                "properties": {
                    "mandatory": {
                        "default": "false",
                        "id": "/properties/entries/items/properties/mandatory",
                        "type": "boolean"
                    },
                    "url": {
                        "id": "/properties/entries/items/properties/url",
                        "maxLength": 1024,
                        "minLength": 1,
                        "type": "string"
                    }
                },
                "required": [
                    "url"
                ],
                "type": "object"
            },
            "type": "array",
            "uniqueItems": true
        }
    },
    "required": [
        "entries"
    ],
    "type": "object"
}
```

Jeder `url`-Wert im Manifest muss eine URL mit dem Bucket-Namen und dem vollständigen Objektpfad zur Datei angeben (nicht nur ein Präfix). Sie können ein Manifest verwenden, um Dateien aus verschiedenen Buckets, verschiedenen Regionen oder mit unterschiedlichen Präfixen zu laden. Falls in der URL keine Region angegeben ist, wird die Region des Ziel-DB-Clusters in Aurora verwendet. Das folgende Beispiel zeigt eine Manifestdatei, mit der vier Dateien aus unterschiedlichen Buckets geladen werden.

```
{
  "entries": [
    {
      "url":"s3://aurora-bucket/2013-10-04-customerdata",
      "mandatory":true
    },
    {
      "url":"s3-us-west-2://aurora-bucket-usw2/2013-10-05-customerdata",
      "mandatory":true
    },
    {
      "url":"s3://aurora-bucket/2013-10-04-customerdata",
      "mandatory":false
    },
    {
      "url":"s3://aurora-bucket/2013-10-05-customerdata"
    }
  ]
}
```

Das optionale Flag `mandatory` gibt an, ob `LOAD DATA FROM S3` eine Fehlermeldung zurückgeben soll, wenn die Datei nicht gefunden wird. Das Flag `mandatory` ist standardmäßig auf `false` gesetzt. Wenn keine Dateien gefunden werden, wird `mandatory` beendet, und zwar unabhängig vom `LOAD DATA FROM S3`-Wert.

Manifestdateien können eine beliebige Erweiterung haben. Im folgenden Beispiel wird die Anweisung `LOAD DATA FROM S3` mit dem Manifest aus dem vorherigen Beispiel ausgeführt, das den Namen **`customer.manifest`** trägt.

```
LOAD DATA FROM S3 MANIFEST 's3-us-west-2://aurora-bucket/customer.manifest'
    INTO TABLE CUSTOMER
    FIELDS TERMINATED BY ','
    LINES TERMINATED BY '\n'
    (ID, FIRSTNAME, LASTNAME, EMAIL);
```

Nachdem die Anweisung beendet ist, wird ein Eintrag für jede erfolgreich geladene Datei in die Tabelle `aurora_s3_load_history` geschrieben.

Überprüfen der geladenen Dateien mit der Tabelle „aurora_s3_load_history“

Mit jeder erfolgreich ausgeführten Anweisung `LOAD DATA FROM S3` wird die Tabelle `aurora_s3_load_history` im Schema `mysql` mit einem Eintrag für jede geladene Datei aktualisiert.

Nach der Ausführung der Anweisung `LOAD DATA FROM S3` können Sie überprüfen, welche Dateien geladen wurden. Dazu führen Sie eine Abfrage für die Tabelle `aurora_s3_load_history` aus. Um die Dateien anzuzeigen, die aus einer Iteration der Anweisung geladen wurden, verwenden Sie die Klausel `WHERE`, um die Datensätze auf dem Amazon S3-URI für die in der Anweisung verwendete Manifestdatei zu filtern. Wenn Sie zuvor dieselbe Manifestdatei verwendet haben, filtern Sie die Ereignisse mithilfe des Felds `timestamp`.

```
select * from mysql.aurora_s3_load_history where load_prefix = 'S3_URI';
```

In der folgenden Tabelle werden die Felder der Tabelle `aurora_s3_load_history` beschrieben.

Feld	Beschreibung
`load_prefix`	Der URI, der in der Load-Anweisung angegeben wurde. Dieser URI kann alle der folgenden Elemente abbilden: • Eine einzelne Datei für ein Statement `LOAD DATA FROM S3 FILE` • Ein Amazon S3-Präfix, das auf mehrere Dateien für eine `LOAD DATA FROM S3 PREFIX`-Anweisung verweist • Eine einzelne Manifestdatei, die die zu ladenden Namen der Dateien für ein Statement `LOAD DATA FROM S3 MANIFEST` enthält
`file_name`	Der Name der Datei, die – mithilfe des im Feld `load_prefix` angegebenen URI – aus Amazon S3 in Aurora geladen wurde.

Feld	Beschreibung
`version_number`	Die Versionsnummer der im Feld `file_name` bezeichneten Datei, die geladen wurde, wenn der Amazon S3-Bucket eine Versionsnummer hat.
`bytes_loaded`	Die Größe der geladenen Datei in Bytes.
`load_timestamp`	Der Zeitstempel, zu dem die Anweisung `LOAD DATA FROM S3` abgeschlossen ist.

Beispiele

Mit folgender Anweisung werden Daten aus einem Amazon S3-Bucket geladen, der sich in derselben Region befindet wie der Aurora-DB-Cluster. Die Anweisung liest die kommagetrennten Daten in der Datei`customerdata.txt`, die sich im Amazon S3 *S3-Bucket DOC-EXAMPLE-BUCKET befindet, und* lädt die Daten dann in die Tabelle. `store-schema.customer-table`

```
LOAD DATA FROM S3 's3://DOC-EXAMPLE-BUCKET/customerdata.csv'
    INTO TABLE store-schema.customer-table
    FIELDS TERMINATED BY ','
    LINES TERMINATED BY '\n'
    (ID, FIRSTNAME, LASTNAME, ADDRESS, EMAIL, PHONE);
```

Mit folgender Anweisung werden Daten aus einem Amazon S3-Bucket geladen, der sich in einer anderen Region befindet als der Aurora-DB-Cluster. Die Anweisung liest die kommagetrennten Daten aus allen Dateien, die dem `employee-data` Objektpräfix im Amazon *S3-Bucket DOC-EXAMPLE-BUCKET* in der `us-west-2` Region entsprechen, und lädt die Daten dann in die Tabelle. `employees`

```
LOAD DATA FROM S3 PREFIX 's3-us-west-2://DOC-EXAMPLE-BUCKET/employee_data'
    INTO TABLE employees
    FIELDS TERMINATED BY ','
    LINES TERMINATED BY '\n'
    (ID, FIRSTNAME, LASTNAME, EMAIL, SALARY);
```

Mit folgender Anweisung werden Daten aus Dateien, die in einer JSON-Manifestdatei mit dem Namen "q1_sales.json" angegeben sind, in die Tabelle `sales` geladen.

```
LOAD DATA FROM S3 MANIFEST 's3-us-west-2://DOC-EXAMPLE-BUCKET1/q1_sales.json'
```

```
    INTO TABLE sales
    FIELDS TERMINATED BY ','
    LINES TERMINATED BY '\n'
    (MONTH, STORE, GROSS, NET);
```

LOAD XML FROM S3

Mit der Anweisung `LOAD XML FROM S3` können Sie Daten aus XML-Dateien, die in einem Amazon S3-Bucket gespeichert sind, in drei verschiedenen XML-Formaten laden:

- Spaltennamen als Attribute des Elements `<row>`. Der Attributwert bestimmt die Inhalte des Tabellenfeldes.

  ```
  <row column1="value1" column2="value2" .../>
  ```

- Spaltennamen als untergeordnete Elemente des Elements `<row>`. Der Wert des untergeordneten Elements bestimmt die Inhalte des Tabellenfeldes.

  ```
  <row>
    <column1>value1</column1>
    <column2>value2</column2>
  </row>
  ```

- Spaltennamen im Attribut `name` des Elements `<field>` im Element `<row>`. Der Wert des Elements `<field>` bestimmt die Inhalte des Tabellenfeldes.

  ```
  <row>
    <field name='column1'>value1</field>
    <field name='column2'>value2</field>
  </row>
  ```

Syntax

```
LOAD XML FROM S3 'S3-URI'
    [REPLACE | IGNORE]
    INTO TABLE tbl_name
    [PARTITION (partition_name,...)]
    [CHARACTER SET charset_name]
    [ROWS IDENTIFIED BY '<element-name>']
    [IGNORE number {LINES | ROWS}]
    [(field_name_or_user_var,...)]
```

```
    [SET col_name = expr,...]
```

Parameter

Die Anweisung `LOAD XML FROM S3` verwendet die folgenden erforderlichen und optionalen Parameter. Weitere Informationen zu einigen der Parameter finden Sie unter LOAD XML-Anweisung in der MySQL-Dokumentation.

FILE | PREFIX

Gibt an, ob die Daten aus einer einzelnen Datei oder aus allen Dateien mit einem bestimmten Präfix geladen werden sollen. `FILE` ist der Standardwert.

REPLACE | IGNORE

Gibt an, welche Aktion ausgeführt werden soll, falls eine Eingabezeile die gleichen eindeutigen Schlüsselwerte aufweist wie eine vorhandene Zeile in der Datenbanktabelle.

- Geben Sie `REPLACE` an, wenn die Eingabezeile die bestehende Zeile überschreiben soll.
- Geben Sie `IGNORE` an, wenn Sie die Eingabezeile verwerfen möchten. `IGNORE` ist der Standardwert.

INTO TABLE

Gibt den Namen der Datenbanktabelle an, in welche die Eingabezeilen geladen werden sollen.

PARTITION

Gibt vor, dass alle Eingabezeilen in die Partitionen, die in der Liste mit durch Komma getrennten Partitionsnamen angegeben sind, eingefügt werden müssen. Lässt sich eine Eingabezeile nicht in eine der angegebenen Partitionen einfügen, schlägt die Anweisung fehl und eine Fehlermeldung wird zurückgegeben.

CHARACTER SET

Gibt den Zeichensatz der Daten in der Eingabedatei an.

ROWS IDENTIFIED BY

Gibt den Elementnamen an, der eine Zeile in der Eingabedatei bestimmt. Der Standardwert ist `<row>`.

IGNORE ***number*** LINES | ROWS

Gibt an, dass eine bestimmte Anzahl an Zeilen am Anfang der Eingabedatei ignoriert werden sollen. Sie können beispielsweise mit `IGNORE 1 LINES` die erste Zeile in der Textdatei

überspringen oder mit `IGNORE 2 ROWS` die ersten beiden Datenzeilen der XML-Eingabedatei auslassen.

field_name_or_user_var, ...

Gibt eine durch Komma getrennte Liste mit einem oder mehreren XML-Elementnamen bzw. einer oder mehreren Benutzervariablen an, die die Namen der zu ladenden Elemente identifizieren. Der Name einer Benutzervariable, die für diesen Zweck verwendet wird, muss mit dem Namen eines Elements aus der XML-Datei übereinstimmen, welcher ein @ als Präfix hat. Sie können Benutzervariablen einsetzen, um die entsprechenden Feldwerte für die spätere Wiederverwendung zu speichern.

Beispielsweise wird mit folgender Anweisung die erste Spalte aus der Eingabedatei in die erste Spalte von `table1` geladen, zudem wird der Wert der Spalte `table_column2` in `table1` auf den Eingabewert der zweiten Spalte geteilt durch 100 gesetzt.

```
LOAD XML FROM S3 's3://DOC-EXAMPLE-BUCKET/data.xml'
   INTO TABLE table1
   (column1, @var1)
   SET table_column2 = @var1/100;
```

SET

Gibt eine durch Komma getrennte Liste mit Zuweisungsvorgängen an, die die Werte von Spalten in der Tabelle auf Werte setzen, die nicht in der Eingabedatei enthalten sind.

Beispielsweise setzt die folgende Anweisung die ersten beiden Spalten von `table1` auf die Werte in den ersten beiden Spalten aus der Eingabedatei und anschließend den Wert von `column3` in `table1` auf den aktuellen Zeitstempel.

```
LOAD XML FROM S3 's3://DOC-EXAMPLE-BUCKET/data.xml'
   INTO TABLE table1
   (column1, column2)
   SET column3 = CURRENT_TIMESTAMP;
```

Auf der rechten Seite von SET-Zuweisungen können Sie Unterabfragen formulieren. Für eine Unterabfrage, die einen Wert zurückgibt, der einer Spalte zugewiesen werden soll, kommt ausschließlich eine skalare Unterabfrage infrage. Darüber hinaus können Sie mit einer Unterabfrage keine Daten aus der zu ladenden Tabelle auswählen.

Speichern von Daten aus einem Amazon Aurora MySQL-DB-Cluster in Textdateien in einem Amazon S3-Bucket

Sie können die `SELECT INTO OUTFILE S3` Anweisung verwenden, um Daten aus einem Amazon Aurora MySQL-DB-Cluster abzufragen und sie in Textdateien zu speichern, die in einem Amazon S3 S3-Bucket gespeichert sind. In Aurora MySQL werden die Dateien zuerst auf der lokalen Festplatte gespeichert und dann nach S3 exportiert. Nach Abschluss der Exporte werden die lokalen Dateien gelöscht.

Sie können den Amazon S3-Bucket mit einem von Amazon S3 verwalteten Schlüssel (SSE-S3) oder AWS KMS key (SSE-KMS: Von AWS verwalteter Schlüssel oder vom Kunden verwalteten Schlüssel) verschlüsseln.

Die `LOAD DATA FROM S3` Anweisung kann Dateien verwenden, die durch die `SELECT INTO OUTFILE S3` Anweisung erstellt wurden, um Daten in einen Aurora-DB-Cluster zu laden. Weitere Informationen finden Sie unter Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket.

> **Note**
>
> Diese Funktion wird für DB-Cluster von Aurora Serverless v1 nicht unterstützt. Sie wird für DB-Cluster von Aurora Serverless v2 unterstützt.
> Sie können auch DB-Cluster-Daten und DB-Cluster-Snapshot-Daten mit der AWS Management Console AWS CLI, oder Amazon RDS-API in Amazon S3 speichern. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Daten nach Amazon S3 und Exportieren von DB-Cluster-Snapshot-Daten nach Amazon S3.

Inhalt

- Überlegungen
- Beispiele

Gewähren von Zugriff auf Amazon S3 für Aurora MySQL

Bevor Sie Daten in einem Amazon S3-Bucket speichern können, müssen Sie Ihrem Aurora MySQL-DB-Cluster die Berechtigung für den Zugriff auf Amazon S3 erteilen.

So gewähren Sie Aurora MySQL Zugriff auf Amazon S3:

1. Erstellen Sie eine AWS Identity and Access Management (IAM-) Richtlinie, die die Bucket- und Objektberechtigungen bereitstellt, die Ihrem Aurora MySQL-DB-Cluster den Zugriff auf Amazon S3 ermöglichen. Anweisungen finden Sie unter Erstellen einer IAM-Zugriffsrichtlinie für Amazon S3-Ressourcen.

   > **Note**
   >
   > In Aurora MySQL Version 3.05 und höher können Sie Objekte mit vom AWS KMS Kunden verwalteten Schlüsseln verschlüsseln. Nehmen Sie dazu die Berechtigung `kms:GenerateDataKey` in Ihre IAM-Richtlinie auf. Weitere Informationen finden Sie unter Erstellen einer IAM-Zugriffsrichtlinie für AWS KMS-Ressourcen.
   > Sie benötigen diese Berechtigung nicht, um Objekte mithilfe Von AWS verwaltete Schlüssel von Amazon S3 S3-verwalteten Schlüsseln (SSE-S3) zu verschlüsseln.

2. Erstellen Sie eine IAM-Rolle und fügen Sie der neuen IAM-Rolle die IAM-Richtlinie hinzu, die Sie in Erstellen einer IAM-Zugriffsrichtlinie für Amazon S3-Ressourcen erstellt haben. Detaillierte Anweisungen finden Sie unter Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.
3. Legen Sie in Aurora MySQL Version 2 einen der DB-Cluster-Parameter `aurora_select_into_s3_role` oder `aws_default_s3_role` auf den Amazon-Ressourcennamen (ARN) der neuen IAM-Rolle fest. Wenn für `aurora_select_into_s3_role` keine IAM-Rolle angegeben wird, verwendet Aurora die unter `aws_default_s3_role` angegebene IAM-Rolle.

   Verwenden Sie `aws_default_s3_role` in Aurora MySQL Version 3.

   Wenn das Cluster Teil einer globalen Aurora-Datenbank ist, legen Sie diesen Parameter für jedes Aurora-Cluster in der globalen Datenbank fest.

Weitere Informationen zu DB-Cluster-Parametern finden Sie unter Amazon Aurora-DB-Cluster und DB-Instance-Parameter.

4. Weisen Sie die Rolle, die Sie in Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben erstellt haben, diesem DB-Cluster zu, um Datenbankbenutzern in einem Aurora MySQL DB-Cluster den Zugriff auf Amazon S3 zu erlauben.

   Bei einer globalen Aurora-Datenbank verknüpfen Sie die Rolle mit jedem Aurora-Cluster in der globalen Datenbank.

   Weitere Informationen zum Zuordnen einer IAM-Rolle zu einem DB-Cluster finden Sie unter Zuweisen einer IAM-Rolle zu einem Amazon-Aurora-MySQL-DB-Cluster.

5. Konfigurieren Sie Ihren Aurora MySQL-DB-Cluster so, dass er ausgehende Verbindungen zu Amazon S3 zulässt. Detaillierte Anweisungen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.

   Bei einer globalen Aurora-Datenbank aktivieren Sie ausgehende Verbindungen für jeden Aurora-Cluster in der globalen Datenbank.

Gewähren von Rechten für das Speichern von Daten in Aurora MySQL

Der Datenbankbenutzer, der die `SELECT INTO OUTFILE S3`-Anweisung ausgibt, muss über eine bestimmte Rolle oder Berechtigung verfügen. In Aurora MySQL Version 3 gewähren Sie die Rolle `AWS_SELECT_S3_ACCESS`. In Aurora MySQL Version 2 gewähren Sie die Berechtigung `SELECT INTO S3`. Dem Administratorbenutzer für ein DB-Cluster wird die entsprechende Rolle oder -Berechtigung standardmäßig gewährt. Sie können die Berechtigung einem anderen Benutzer erteilen, indem Sie eine der folgenden Anweisungen verwenden.

Verwenden Sie die folgende Anweisung für Aurora MySQL Version 3:

```
GRANT AWS_SELECT_S3_ACCESS TO 'user'@'domain-or-ip-address'
```

> **Tip**
>
> Wenn Sie die Rollentechnik in Aurora MySQL Version 3 verwenden, können Sie die Rolle auch mit der Anweisung `SET ROLE role_name` oder `SET ROLE ALL` aktivieren. Wenn Sie mit dem MySQL 8.0-Rollensystem nicht vertraut sind, finden Sie in Rollenbasiertes

Berechtigungsmodell weitere Informationen. Weitere Informationen finden Sie unter Rollen verwenden im MySQL-Referenzhandbuch.
Dies gilt nur für die aktuelle aktive Sitzung. Wenn Sie die Verbindung wieder herstellen, müssen Sie die `SET ROLE` Anweisung erneut ausführen, um Rechte zu gewähren. Weitere Informationen finden Sie unter SET ROLE-Anweisung im MySQL-Referenzhandbuch.
Sie können den DB-Cluster-Parameter `activate_all_roles_on_login` zum automatischen Aktivieren aller Rollen verwenden, wenn ein Benutzer eine Verbindung mit einer DB-Instance herstellt. Wenn dieser Parameter festgelegt ist, müssen Sie die `SET ROLE` Anweisung im Allgemeinen nicht explizit aufrufen, um eine Rolle zu aktivieren. Weitere Informationen finden Sie unter activate_all_roles_on_login im MySQL-Referenzhandbuch.
Sie müssen jedoch zu Beginn einer gespeicherten Prozedur `SET ROLE ALL` explizit aufrufen, um die Rolle zu aktivieren, wenn die gespeicherte Prozedur von einem anderen Benutzer aufgerufen wird.

Verwenden Sie die folgende Anweisung für Aurora MySQL Version 2:

```
GRANT SELECT INTO S3 ON *.* TO 'user'@'domain-or-ip-address'
```

Die Rolle `AWS_SELECT_S3_ACCESS` und Berechtigung `SELECT INTO S3` gelten speziell für Amazon Aurora MySQL und sind nicht für MySQL-Datenbanken oder RDS für MySQL-DB-Instances verfügbar. Wenn Sie die Replikation zwischen einem Aurora MySQL DB-Cluster als Haupt-Replikation und einer MySQL-Datenbank als Replikations-Client eingerichtet haben, führt die Anweisung `GRANT` für die Rolle oder Berechtigung dazu, dass die Replikation mit einem Fehler beendet wird. Sie können diese Fehlermeldung ignorieren und mit der Replikation fortfahren. Verwenden Sie das Verfahren mysql_rds_skip_repl_error, um die Fehlermeldung für eine RDS für MySQL-DB-Instance zu überspringen. Um den Fehler in einer externen MySQL-Datenbank zu überspringen, verwenden Sie die Systemvariable slave_skip_errors (Aurora MySQL Version 2) oder die Systemvariable replica_skip_errors (Aurora MySQL Version 3).

Angeben eines Pfades zu einem Amazon S3-Bucket

Die Syntax für das Bestimmen eines Pfades zu einem Speicherort für Daten und Manifestdateien in einem Amazon S3-Bucket ist ähnlich der in der Anweisung `LOAD DATA FROM S3 PREFIX`, wie im Folgenden zu sehen ist.

```
s3-region://bucket-name/file-prefix
```

Der Pfad enthält die folgenden Werte:

- `region`(optional) — Die AWS Region, die den Amazon S3 S3-Bucket enthält, in dem die Daten gespeichert werden sollen. Dieser Wert ist optional. Wenn Sie keinen `region`-Wert festlegen, speichert Aurora Ihre Datei in Amazon S3, das sich in derselben Region befindet wie Ihr DB-Cluster.
- `bucket-name` – Der Name des Amazon S3-Buckets, in dem die Daten gespeichert werden sollen. Objekt-Präfixe, die einen virtuellen Ordnerpfad identifizieren, werden unterstützt.
- `file-prefix` – Das Amazon S3-Objektpräfix, das die Dateien identifiziert, die in Amazon S3 gespeichert werden sollen.

Die Dateien, die durch die Anweisung `SELECT INTO OUTFILE S3` erstellt wurden, verwenden den folgenden Pfad, in welchem *`00000`* eine fünfstellige, nullbasierte Ganzzahl ist.

```
s3-region://bucket-name/file-prefix.part_00000
```

Nehmen wir beispielsweise an, dass ein Statement `SELECT INTO OUTFILE S3` `s3-us-west-2://bucket/prefix` als den Pfad festlegt, in dem Dateien gespeichert und drei Datendateien erstellt werden sollen. Das festgelegte Amazon S3-Bucket beinhaltet die folgenden Dateien.

- s3-us-west-2://bucket/prefix.part 00000
- s3-us-west-2://bucket/prefix.part 00001
- s3-us-west-2://bucket/prefix.part 00002

Erstellen eines Manifests für das Auflisten von Dateien

Sie können das Statement `SELECT INTO OUTFILE S3` mit der Option `MANIFEST ON` verwenden, um eine Manifestdatei im JSON-Format zu erstellen, die die mithilfe des Statements erstellten Textdateien auflistet. Die Anweisung `LOAD DATA FROM S3` kann die Manifestdatei verwenden, um Dateien zurück in ein Aurora MySQL-DB-Cluster zu laden. Weitere Informationen über die Verwendung eines Manifests für das Laden von Dateien aus Amazon S3 in einen Aurora MySQL-DB-Cluster finden Sie unter Verwenden eines Manifests für zu ladende Dateien.

Die im Manifest beinhalteten Dateien, die mithilfe des Statements `SELECT INTO OUTFILE S3` erstellt wurden, werden in der Reihenfolge gelistet, in der sie mit dem Statement erstellt wurden.

Nehmen wir beispielsweise an, dass ein Statement `SELECT INTO OUTFILE S3 s3-us-west-2://bucket/prefix` als den Pfad angegeben hat, in dem Dateien gespeichert und drei Dateien und eine Manifestdatei erstellt werden sollen. Der angegebene Amazon S3-Bucket beinhaltet eine Manifestdatei mit dem Namen `s3-us-west-2://bucket/prefix.manifest`, die die folgenden Informationen beinhaltet.

```
{
  "entries": [
    {
      "url":"s3-us-west-2://bucket/prefix.part_00000"
    },
    {
      "url":"s3-us-west-2://bucket/prefix.part_00001"
    },
    {
      "url":"s3-us-west-2://bucket/prefix.part_00002"
    }
  ]
}
```

SELECT INTO OUTFILE S3

Sie können die Anweisung `SELECT INTO OUTFILE S3` verwenden, um Daten aus einem DB-Cluster abzufragen und diese direkt in separierten Textdateien in einem Amazon S3-Bucket zu speichern.

Komprimierte Dateien werden nicht unterstützt. Verschlüsselte Dateien werden ab Aurora MySQL Version 2.09.0 unterstützt.

Syntax

```
SELECT
    [ALL | DISTINCT | DISTINCTROW ]
        [HIGH_PRIORITY]
        [STRAIGHT_JOIN]
        [SQL_SMALL_RESULT] [SQL_BIG_RESULT] [SQL_BUFFER_RESULT]
        [SQL_CACHE | SQL_NO_CACHE] [SQL_CALC_FOUND_ROWS]
    select_expr [, select_expr ...]
    [FROM table_references
        [PARTITION partition_list]
    [WHERE where_condition]
```

```
    [GROUP BY {col_name | expr | position}
        [ASC | DESC], ... [WITH ROLLUP]]
    [HAVING where_condition]
    [ORDER BY {col_name | expr | position}
         [ASC | DESC], ...]
    [LIMIT {[offset,] row_count | row_count OFFSET offset}]
INTO OUTFILE S3 's3_uri'
[CHARACTER SET charset_name]
    [export_options]
    [MANIFEST {ON | OFF}]
    [OVERWRITE {ON | OFF}]
    [ENCRYPTION {ON | OFF | SSE_S3 | SSE_KMS ['cmk_id']}]

export_options:
    [FORMAT {CSV|TEXT} [HEADER]]
    [{FIELDS | COLUMNS}
        [TERMINATED BY 'string']
        [[OPTIONALLY] ENCLOSED BY 'char']
        [ESCAPED BY 'char']
    ]
    [LINES
        [STARTING BY 'string']
        [TERMINATED BY 'string']
]
```

Parameter

Die Anweisung `SELECT INTO OUTFILE S3` verwendet die folgenden erforderlichen und optionalen Parameter, die für Aurora spezifisch sind.

s3-uri

Gibt den URI für ein zu verwendendes Amazon-S3-Präfix an. Verwenden Sie die unter Angeben eines Pfades zu einem Amazon S3-Bucket beschriebene Syntax.

FORMAT {CSV|TEXT} [HEADER]

Speichert die Daten optional im CSV-Format.

Die Option `TEXT` ist die Standardeinstellung und erzeugt das vorhandene MySQL-Exportformat.

Die Option `CSV` erzeugt kommagetrennte Datenwerte. Das CSV-Format entspricht der Spezifikation in RFC-4180. Wenn Sie das optionale Schlüsselwort `HEADER` angeben, enthält die

Ausgabedatei eine Kopfzeile. Die Beschriftungen in der Kopfzeile entsprechen den Spaltennamen aus der `SELECT`-Anweisung. Sie können die CSV-Dateien zum Trainieren von Datenmodellen für die Verwendung mit AWS ML-Services verwenden. Weitere Informationen zur Verwendung exportierter Aurora-Daten mit AWS ML-Diensten finden Sie unterExportieren von Daten nach Amazon S3 für SageMaker Modelltraining (Fortgeschritten).

MANIFEST {ON | OFF}

Gibt an, ob eine Manifestdatei in Amazon S3 erstellt wird. Die Manifestdatei ist eine JSON-Datei (JavaScript Object Notation), die verwendet werden kann, um Daten mit der `LOAD DATA FROM S3 MANIFEST` Anweisung in einen Aurora-DB-Cluster zu laden. Mehr über `LOAD DATA FROM S3 MANIFEST` erfahren Sie unter Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket.

Wenn `MANIFEST ON` in der Abfrage angegeben ist, wird die Manifestdatei in Amazon S3 erstellt, nachdem alle Dateien erstellt und hochgeladen wurden. Die Manifestdatei wird unter Verwendung des folgenden Pfads erstellt:

```
s3-region://bucket-name/file-prefix.manifest
```

Weitere Informationen über das Format der Inhalte der Manifestdatei finden Sie unter Erstellen eines Manifests für das Auflisten von Dateien.

OVERWRITE {ON | OFF}

Gibt an, ob bestehende Dateien im angegebenen Amazon-S3-Bucket überschrieben werden. Wenn `OVERWRITE ON` festgelegt ist, werden bestehende Dateien, die mit dem Präfix des im `s3-uri`-URI angegebenen Präfixes übereinstimmen, überschrieben. Andernfalls tritt ein Fehler auf.

ENCRYPTION {ON | OFF | SSE_S3 | SSE_KMS ['*cmk_id*']}

Gibt an, ob serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) oder AWS KMS keys (SSE-KMS, einschließlich Von AWS verwaltete Schlüssel und vom Kunden verwalteter Schlüssel) verwendet werden soll. Die Einstellungen `SSE_S3` und `SSE_KMS` sind in Aurora MySQL Version 3.05 und höher verfügbar.

Sie können auch die Sitzungsvariable `aurora_select_into_s3_encryption_default` anstelle der Klausel `ENCRYPTION` verwenden, wie im folgenden Beispiel gezeigt. Verwenden Sie entweder die SQL-Klausel oder die Sitzungsvariable, aber nicht beide.

```
set session set session aurora_select_into_s3_encryption_default={ON | OFF | SSE_S3
 | SSE_KMS};
```

Die Einstellungen SSE_S3 und SSE_KMS sind in Aurora MySQL Version 3.05 und höher verfügbar.

Wenn Sie aurora_select_into_s3_encryption_default auf folgende Werte einstellen, gilt:

- OFF: Es wird die Standardverschlüsselungsrichtlinie des S3-Buckets befolgt. Der Standardwert von aurora_select_into_s3_encryption_default ist OFF.
- ON oder SSE_S3: Das S3-Objekt wird mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) verschlüsselt.
- SSE_KMS— Das S3-Objekt ist mit einem verschlüsselt. AWS KMS key

  In diesem Fall fügen Sie auch die Sitzungsvariable aurora_s3_default_cmk_id hinzu, beispielsweise:

  ```
  set session aurora_select_into_s3_encryption_default={SSE_KMS};
  set session aurora_s3_default_cmk_id={NULL | 'cmk_id'};
  ```

  - Wenn aurora_s3_default_cmk_id NULL ist, wird das S3-Objekt mit einem Von AWS verwalteter Schlüssel verschlüsselt.
  - Wenn es sich bei aurora_s3_default_cmk_id um eine nicht leere Zeichenfolge cmk_id handelt, wird das S3-Objekt mit einem vom Kunden verwalteten Schlüssel verschlüsselt.

    Der Wert von cmk_id kann keine leere Zeichenfolge sein.

Wenn Sie den Befehl SELECT INTO OUTFILE S3 verwenden, bestimmt Aurora die Verschlüsselung wie folgt:

- Wenn die Klausel ENCRYPTION im SQL-Befehl vorhanden ist, stützt sich Aurora nur auf den Wert für ENCRYPTION und verwendet keine Sitzungsvariable.
- Wenn die Klausel ENCRYPTION nicht vorhanden ist, stützt sich Aurora auf den Wert der Sitzungsvariablen.

Weitere Informationen finden Sie unter Verwenden der serverseitigen Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln (SSE-S3) und Verwenden der serverseitigen

Verschlüsselung mit AWS KMS Schlüsseln (SSE-KMS) im Amazon Simple Storage Service-Benutzerhandbuch.

Weitere Details zu anderen Parametern finden Sie unter SELECT-Anweisung und LOAD DATA-Anweisung in der MySQL-Dokumentation.

Überlegungen

Die Anzahl der im Amazon S3-Bucket geschriebenen Dateien hängt von der Datenmenge, die von der Anweisung `SELECT INTO OUTFILE S3` ausgewählt wurde, und dem Schwellenwert der Dateigröße für Aurora MySQL ab. Der Standard-Schwellenwert für die Dateigröße liegt bei 6 GB. Wenn die vom Statement ausgewählte Datei kleiner ist als der Schwellenwert für die Dateigröße, wird eine einzelne Datei erstellt, andernfalls werden mehrere Dateien erstellt. Außerdem sollte Folgendes für Dateien, die von diesem Statement erstellt wurden, beachtet werden:

- Aurora MySQL garantiert, dass Zeilen in Dateien nicht über Dateigrenzen aufgeteilt werden. Bei mehreren Dateien liegt die Dateigröße jeder Datei, außer der Letzten, normalerweise sehr dicht am Schwellenwert. Jedoch kann es gelegentlich vorkommen, dass die Zeilen von Dateien, deren Größe unter dem Schwellenwert liegt, zwischen zwei Dateien aufgeteilt werden. In diesem Fall erstellt Aurora MySQL eine Datei, die die Zeile intakt hält, aber dadurch größer als der Schwellenwert ist.
- Da jede `SELECT`-Anweisung in Aurora MySQL als eine atomare Transaktion ausgeführt wird, kann eine `SELECT INTO OUTFILE S3`-Anweisung, die einen großen Datensatz auswählt, einige Zeit in Anspruch nehmen. Wenn die Anweisung aus irgendeinem Grund fehlschlägt, müssen Sie möglicherweise erneut starten und die Anweisung nochmals ausstellen. Wenn die Anweisung fehlschlägt, bleiben Dateien, die bereits in Amazon S3 hochgeladen wurden, im angegebenen Amazon S3-Bucket bestehen. Sie können ein anderes Statement verwenden, um die übrigen Daten hochzuladen, anstatt von Neuem zu starten.
- Wenn die auszuwählende Datenmenge groß ist (mehr als 25 GB), empfehlen wir Ihnen, mehrere `SELECT INTO OUTFILE S3`-Anweisungen zu verwenden, um die Daten in Amazon S3 zu speichern. Jedes Statement sollte eine andere Partition für die zu speichernden Daten auswählen und auch ein anderes `file_prefix` im `s3-uri`-Parameter angeben, wenn die Daten gespeichert werden. Die Partitionierung der zu selektierenden Daten mit mehreren Anweisungen erleichtert die Behebung eines Fehlers in einer Anweisung. Wenn bei einer Aussage ein Fehler auftritt, muss nur ein Teil der Daten neu ausgewählt und in Amazon S3 hochgeladen werden. Die Verwendung von mehreren Statements hilft auch eine lange dauernde Einzeltransaktion zu vermeiden, was die Leistung verbessern kann.

- Wenn mehrere `SELECT INTO OUTFILE S3`-Anweisungen, die das selbe `file_prefix` im `s3-uri`-Parameter verwenden, parallel ausgeführt werden, um Daten nach Amazon S3 auszuwählen, kann das Verhalten nicht eingeschätzt werden.
- Metadaten, wie z. B. Tabellenschemata oder Metadatendateien werden nicht von Aurora MySQL nach Amazon S3 hochgeladen.
- In einigen Fällen können Sie eine `SELECT INTO OUTFILE S3`-Abfrage erneut tätigen, um beispielsweise nach einem Fehler wiederherzustellen. In diesen Fällen müssen Sie entweder alle bestehenden Dateien mit dem selben Präfix, wie in `s3-uri` angegeben, aus dem Amazon S3-Bucket entfernen oder `OVERWRITE ON` in die `SELECT INTO OUTFILE S3`-Abfrage einbinden.

Das Statement `SELECT INTO OUTFILE S3` gibt eine typische MySQL-Fehlernummer und -Antwort bei Erfolg oder Fehler zurück. Wenn Sie keinen Zugang zur MySQL-Fehlernummer oder -Antwort haben, ist es der einfachste Weg, nach Abschluss `MANIFEST ON` im Statement anzugeben. Die Manifestdatei ist die letzte Datei, die vom Statement geschrieben wurde. Mit anderen Worten, wenn Sie über eine Manifestdatei verfügen, hat die Anweisung die Ausführung abgeschlossen.

Aktuell gibt es keine Möglichkeit, den Fortschritt der `SELECT INTO OUTFILE S3`-Anweisung bei der Ausführung direkt zu überwachen. Nehmen wir jedoch an, Sie schreiben mithilfe dieser Anweisung eine große Datenmenge aus Aurora MySQL zu Amazon S3 und Sie kennen die Größe der von der Anweisung ausgewählten Daten. In diesem Fall können Sie den Fortschritt schätzen, indem Sie die Erstellung der Dateien in Amazon S3 überwachen.

Dabei können Sie sich die Tatsache zunutze machen, dass eine Datei im festgelegten Amazon S3-Bucket für je 6 GB Daten, die vom Statement ausgewählt wurden, erstellt wird. Teilen Sie diese ausgewählte Datengröße durch 6 GB, um eine geschätzte Anzahl der zu erstellenden Dateien zu erhalten. So können Sie den Fortschritt der Anweisung einschätzen, wenn Sie die Anzahl der in Amazon S3 hochgeladenen Dateien während der Ausführung der Anweisung überwachen.

Beispiele

Die folgende Anweisung wählt alle Daten in der Tabelle `employees` aus und speichert die Daten in einem Amazon S3-Bucket, der sich in einer anderen Region als der Aurora MySQL-DB-Cluster befindet. Das Statement erstellt Dateien, bei denen jedes Feld durch ein Komma (`,`) und jede Zeile durch einen Zeilenumbruch (\n) beendet wird. Die Anweisung gibt einen Fehler zurück, wenn sich Dateien, die mit dem Dateipräfix `sample_employee_data` übereinstimmen, im angegebenen Amazon S3-Bucket befinden.

```
SELECT * FROM employees INTO OUTFILE S3 's3-us-west-2://aurora-select-into-s3-pdx/
sample_employee_data'
    FIELDS TERMINATED BY ','
    LINES TERMINATED BY '\n';
```

Die folgende Anweisung wählt alle Daten in der Tabelle `employees` aus und speichert die Daten in einem Amazon S3-Bucket, der sich in der selben Region, wie der Aurora MySQL-DB-Cluster befindet. Das Statement erstellt Dateien bei denen jedes Feld durch ein Komma (`,`) und jede Zeile durch einen Zeilenumbruch (`\n`) beendet wird. Zudem wird eine Manifestdatei erstellt. Die Anweisung gibt einen Fehler zurück, wenn sich Dateien, die mit dem Dateipräfix `sample_employee_data` übereinstimmen, im angegebenen Amazon S3-Bucket befinden.

```
SELECT * FROM employees INTO OUTFILE S3 's3://aurora-select-into-s3-pdx/
sample_employee_data'
    FIELDS TERMINATED BY ','
    LINES TERMINATED BY '\n'
    MANIFEST ON;
```

Die folgende Anweisung wählt alle Daten in der Tabelle `employees` aus und speichert die Daten in einem Amazon S3-Bucket, der sich in einer anderen Region als der Aurora-DB-Cluster befindet. Das Statement erstellt Dateien, bei denen jedes Feld durch ein Komma (`,`) und jede Zeile durch einen Zeilenumbruch (`\n`) beendet wird. Die Anweisung überschreibt alle bestehenden Dateien, die mit dem Dateipräfix `sample_employee_data` im angegebenen Amazon S3-Bucket übereinstimmen.

```
SELECT * FROM employees INTO OUTFILE S3 's3-us-west-2://aurora-select-into-s3-pdx/
sample_employee_data'
    FIELDS TERMINATED BY ','
    LINES TERMINATED BY '\n'
    OVERWRITE ON;
```

Die folgende Anweisung wählt alle Daten in der Tabelle `employees` aus und speichert die Daten in einem Amazon S3-Bucket, der sich in der selben Region, wie der Aurora MySQL-DB-Cluster befindet. Das Statement erstellt Dateien bei denen jedes Feld durch ein Komma (`,`) und jede Zeile durch einen Zeilenumbruch (`\n`) beendet wird. Zudem wird eine Manifestdatei erstellt. Die Anweisung überschreibt alle bestehenden Dateien, die mit dem Dateipräfix `sample_employee_data` im angegebenen Amazon S3-Bucket übereinstimmen.

```
SELECT * FROM employees INTO OUTFILE S3 's3://aurora-select-into-s3-pdx/
sample_employee_data'
```

```
    FIELDS TERMINATED BY ','
    LINES TERMINATED BY '\n'
    MANIFEST ON
    OVERWRITE ON;
```

Aufrufen einer Lambda-Funktion aus einem Amazon Aurora MySQL-DB-Cluster

Sie können eine AWS Lambda Funktion aus einem Amazon Aurora MySQL-Compatible Edition-DB-Cluster mit der nativen Funktion oder aufrufen. `lambda_sync` `lambda_async` Damit Sie eine Lambda-Funktion von einem Aurora MySQL aufrufen können, benötigt der Aurora-DB-Cluster Zugriff auf Lambda. Details zum Gewähren des Zugriffs auf Aurora MySQL finden Sie unter Gewähren von Zugriff auf Lambda für Aurora. Informationen zu den gespeicherten `lambda_sync`- und `lambda_async`-Funktionen finden Sie unter Aufrufen einer Lambda-Funktion mit einer nativen Aurora MySQL-Funktion.

Sie können eine AWS Lambda Funktion auch mithilfe einer gespeicherten Prozedur aufrufen. Die Verwendung einer gespeicherten Prozedur ist jedoch veraltet. Wir empfehlen nachdrücklich die Verwendung einer Aurora MySQL-nativen Funktion, wenn Sie eine der folgenden Aurora MySQL-Versionen nutzen:

- Aurora MySQL Version 2 für MySQL 5.7-kompatible Cluster.
- Aurora MySQL Version 3.01 und höher für MySQL 8.0-kompatible Cluster. Die gespeicherte Prozedur ist in Aurora MySQL Version 3 nicht verfügbar.

Themen

Gewähren von Zugriff auf Lambda für Aurora

Bevor Sie Lambda-Funktionen von einem Aurora MySQL DB-Cluster aufrufen können, stellen Sie sicher, dass Sie Ihrem Cluster zuerst die Berechtigung für den Zugriff auf Lambda erteilen.

So gewähren Sie Aurora MySQL Zugriff auf Lambda:

1. Erstellen Sie eine AWS Identity and Access Management (IAM-) Richtlinie, die die Berechtigungen bereitstellt, die es Ihrem Aurora MySQL-DB-Cluster ermöglichen, Lambda-Funktionen aufzurufen. Detaillierte Anweisungen finden Sie unter Erstellen einer IAM-Zugriffsrichtlinie für AWS Lambda-Ressourcen.
2. Erstellen Sie eine IAM-Rolle und fügen Sie der neuen IAM-Rolle die IAM-Richtlinie hinzu, die Sie in Erstellen einer IAM-Zugriffsrichtlinie für AWS Lambda-Ressourcen erstellt haben. Detaillierte Anweisungen finden Sie unter Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben.
3. Sie müssen für den Amazon-Ressourcennamen (ARN) der neuen IAM-Rolle den DB-Cluster-Parameter `aws_default_lambda_role` festlegen.

   Wenn das Cluster Teil einer globalen Aurora-Datenbank ist, wenden Sie dieselbe Einstellung auf jeden Aurora-Cluster in der globalen Datenbank an.

   Weitere Informationen zu DB-Cluster-Parametern finden Sie unter Amazon Aurora-DB-Cluster und DB-Instance-Parameter.
4. Weisen Sie die Rolle, die Sie in Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben erstellt haben, diesem DB-Cluster zu, um Datenbankbenutzern in einem Aurora MySQL DB-Cluster den Aufruf von Lambda-Funktionen zu erlauben. Weitere Informationen zum Zuordnen einer IAM-Rolle zu einem DB-Cluster finden Sie unter Zuweisen einer IAM-Rolle zu einem Amazon-Aurora-MySQL-DB-Cluster.

   Wenn das Cluster Teil einer globalen Aurora-Datenbank ist, verknüpfen Sie die Rolle mit jedem Aurora-Cluster in der globalen Datenbank.
5. Konfigurieren Sie Ihren Aurora MySQL-DB-Cluster so, dass er ausgehende Verbindungen zu Lambda zulässt. Detaillierte Anweisungen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.

   Wenn das Cluster Teil einer globalen Aurora-Datenbank ist, aktivieren Sie ausgehende Verbindungen für jeden Aurora-Cluster in der globalen Datenbank.

Aufrufen einer Lambda-Funktion mit einer nativen Aurora MySQL-Funktion

> **Note**
>
> Sie können die nativen Funktionen `lambda_sync` und `lambda_async` aufrufen, wenn Sie Aurora MySQL Version 2 oder Aurora MySQL Version 3.01 und höher verwenden. Weitere Informationen zu den Aurora MySQL-Versionen erhalten Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.

Sie können eine AWS Lambda Funktion aus einem Aurora MySQL-DB-Cluster aufrufen, indem Sie die nativen Funktionen `lambda_sync` und `lambda_async` aufrufen. Dieser Ansatz kann nützlich sein, wenn Sie Ihre Datenbank, die auf Aurora MySQL läuft, in andere AWS Dienste integrieren möchten. Beispielsweise soll jedes Mal, wenn eine Zeile in eine bestimmte Tabelle der Datenbank eingefügt wird, eine Benachrichtigung mit Amazon Simple Notification Service (Amazon SNS) gesendet werden.

Inhalt

Arbeiten mit nativen Funktionen zum Aufrufen einer Lambda-Funktion

Die Funktionen `lambda_sync` und `lambda_async` sind eingebaute, native Funktionen, die eine Lambda-Funktion synchron oder asynchron aufrufen. Wenn Sie das Ergebnis der Ausführung der aufgerufenen Lambda-Funktion kennen müssen, bevor Sie zu einer anderen Aktion übergehen, verwenden Sie die synchrone Funktion `lambda_sync`. Wenn Sie das Ergebnis der Ausführung der

aufgerufenen Lambda-Funktion nicht kennen müssen, bevor Sie zu einer anderen Aktion übergehen, verwenden Sie die asynchrone Funktion `lambda_async`.

Gewähren der Rolle in Aurora MySQL Version 3

In Aurora MySQL Version 3 muss dem Benutzer, der eine native Funktion aufruft, die `AWS_LAMBDA_ACCESS`-Rolle gewährt werden. Um einem Benutzer diese Rolle zuzuweisen, stellen Sie als Administrator eine Verbindung zur DB-Instance her und führen Sie die folgende Anweisung aus.

```
GRANT AWS_LAMBDA_ACCESS TO user@domain-or-ip-address
```

Sie können diese Rolle widerrufen, indem Sie die folgende Anweisung ausführen.

```
REVOKE AWS_LAMBDA_ACCESS FROM user@domain-or-ip-address
```

> **Tip**
>
> Wenn Sie die Rollentechnik in Aurora MySQL Version 3 verwenden, können Sie die Rolle auch mit der Anweisung `SET ROLE role_name` oder `SET ROLE ALL` aktivieren. Wenn Sie mit dem MySQL 8.0-Rollensystem nicht vertraut sind, finden Sie in Rollenbasiertes Berechtigungsmodell weitere Informationen. Weitere Informationen finden Sie unter Rollen verwenden im MySQL-Referenzhandbuch.
> Dies gilt nur für die aktuelle aktive Sitzung. Wenn Sie die Verbindung wieder herstellen, müssen Sie die `SET ROLE` Anweisung erneut ausführen, um Rechte zu gewähren. Weitere Informationen finden Sie unter SET ROLE-Anweisung im MySQL-Referenzhandbuch.
> Sie können den DB-Cluster-Parameter `activate_all_roles_on_login` zum automatischen Aktivieren aller Rollen verwenden, wenn ein Benutzer eine Verbindung mit einer DB-Instance herstellt. Wenn dieser Parameter festgelegt ist, müssen Sie die `SET ROLE` Anweisung im Allgemeinen nicht explizit aufrufen, um eine Rolle zu aktivieren. Weitere Informationen finden Sie unter activate_all_roles_on_login im MySQL-Referenzhandbuch.
> Sie müssen jedoch zu Beginn einer gespeicherten Prozedur `SET ROLE ALL` explizit aufrufen, um die Rolle zu aktivieren, wenn die gespeicherte Prozedur von einem anderen Benutzer aufgerufen wird.

Wenn Sie beim Versuch, eine Lambda-Funktion aufzurufen, eine Fehlermeldung wie die folgende erhalten, führen Sie eine `SET ROLE`-Anweisung aus.

```
SQL Error [1227] [42000]: Access denied; you need (at least one of) the Invoke Lambda
 privilege(s) for this operation
```

Gewähren der Berechtigung in Aurora MySQL Version 2

In Aurora MySQL Version 2 muss dem Benutzer, der eine native Funktion aufruft, die `INVOKE LAMBDA`-Berechtigung gewährt werden. Um einem Benutzer diese Berechtigung zu erteilen, stellen Sie als Administrator eine Verbindung zur DB-Instance her und führen Sie die folgende Anweisung aus.

```
GRANT INVOKE LAMBDA ON *.* TO user@domain-or-ip-address
```

Sie können das Recht für einen anderen Benutzer mithilfe der folgenden Anweisung erteilen.

```
REVOKE INVOKE LAMBDA ON *.* FROM user@domain-or-ip-address
```

Syntax für die lambda_sync-Funktion

Sie rufen die Funktion `lambda_sync` synchron zum Aufruftyp `RequestResponse` auf. Die Funktion gibt das Ergebnis des Aufrufs von Lambda in einer JSON-Nutzlast zurück. Die Funktion weist die folgende Syntax auf.

```
lambda_sync (
  lambda_function_ARN,
  JSON_payload
)
```

Parameter für die lambda_sync-Funktion

Die Funktion `lambda_sync` hat die folgenden Parameter.

lambda_function_ARN

Der Amazon-Ressourcenname (ARN) der aufzurufenden Lambda-Funktion.

JSON-Nutzlast

Die Nutzlast für die aufgerufene Lambda-Funktion im JSON-Format.

> **Note**
>
> Aurora MySQL Version 3 unterstützt die JSON-Parsingfunktionen von MySQL 8.0. Aurora MySQL-Version 2 enthält diese Funktionen jedoch nicht. JSON-Parsing ist nicht erforderlich, wenn eine Lambda-Funktion einen atomaren Wert zurückgibt, wie z. B. eine Zahl oder einen String.

Beispiel für die lambda_sync-Funktion

Die folgende Abfrage, die auf `lambda_sync` basiert, ruft die Lambda-Funktion `BasicTestLambda` synchron mithilfe der ARN-Funktion auf. Die Nutzlast für die Funktion ist `{"operation": "ping"}`.

```
SELECT lambda_sync(
    'arn:aws:lambda:us-east-1:123456789012:function:BasicTestLambda',
    '{"operation": "ping"}');
```

Syntax für die lambda_async-Funktion

Sie rufen die Funktion `lambda_async` asynchron zum Aufruftyp `Event` auf. Die Funktion gibt das Ergebnis des Aufrufs von Lambda in einer JSON-Nutzlast zurück. Die Funktion weist die folgende Syntax auf.

```
lambda_async (
  lambda_function_ARN,
  JSON_payload
)
```

Parameter für die lambda_async-Funktion

Die Funktion `lambda_async` hat die folgenden Parameter.

lambda_function_ARN

Der Amazon-Ressourcenname (ARN) der aufzurufenden Lambda-Funktion.

JSON-Nutzlast

Die Nutzlast für die aufgerufene Lambda-Funktion im JSON-Format.

> **Note**
>
> Aurora MySQL Version 3 unterstützt die JSON-Parsingfunktionen von MySQL 8.0. Aurora MySQL-Version 2 enthält diese Funktionen jedoch nicht. JSON-Parsing ist nicht erforderlich, wenn eine Lambda-Funktion einen atomaren Wert zurückgibt, wie z. B. eine Zahl oder einen String.

Beispiel für die lambda_async-Funktion

Die folgende Abfrage, die auf `lambda_async` basiert, ruft die Lambda-Funktion `BasicTestLambda` asynchron mithilfe der ARN-Funktion auf. Die Nutzlast für die Funktion ist `{"operation": "ping"}`.

```
SELECT lambda_async(
    'arn:aws:lambda:us-east-1:123456789012:function:BasicTestLambda',
    '{"operation": "ping"}');
```

Aufrufen einer Lambda-Funktion innerhalb eines Auslösers

Sie können Auslöser verwenden, um Lambda für datenmodifizierende Anweisungen aufzurufen. Das folgende Beispiel verwendet die native `lambda_async`-Funktion und speichert das Ergebnis in einer Variablen.

```
mysql>SET @result=0;
mysql>DELIMITER //
mysql>CREATE TRIGGER myFirstTrigger
      AFTER INSERT
          ON Test_trigger FOR EACH ROW
      BEGIN
      SELECT lambda_async(
          'arn:aws:lambda:us-east-1:123456789012:function:BasicTestLambda',
          '{"operation": "ping"}')
          INTO @result;
      END; //
mysql>DELIMITER ;
```

> **Note**
>
> Auslöser werden nicht einmal pro SQL-Anweisung ausgeführt, sondern einmal pro geänderter Zeile, jeweils für eine einzelne Zeile. Wenn ein Trigger ausgeführt wird, ist der Prozess synchron. Die datenmodifizierende Anweisung wird nur zurückgegeben, wenn der Trigger abgeschlossen ist.
> Seien Sie vorsichtig, wenn Sie eine AWS Lambda Funktion über Trigger in Tabellen aufrufen, die viel Schreibverkehr haben. `INSERT`,`UPDATE`, und `DELETE` Trigger werden pro Zeile aktiviert. Eine umfangreiche Arbeitslast in einer Tabelle mit `INSERTUPDATE`, oder `DELETE` Triggern führt zu einer großen Anzahl von Aufrufen Ihrer AWS Lambda Funktion.

Aufrufen einer Lambda-Funktion mit einer Aurora MySQL-Stored Procedure (veraltet)

Sie können eine AWS Lambda Funktion aus einem Aurora MySQL-DB-Cluster aufrufen, indem Sie die `mysql.lambda_async` Prozedur aufrufen. Dieser Ansatz kann nützlich sein, wenn Sie Ihre Datenbank, die auf Aurora MySQL läuft, in andere AWS Dienste integrieren möchten. Beispielsweise soll jedes Mal, wenn eine Zeile in eine bestimmte Tabelle der Datenbank eingefügt wird, eine Benachrichtigung mit Amazon Simple Notification Service (Amazon SNS) gesendet werden.

Inhalt

Überlegungen zu Aurora MySQL-Versionen

Ab Aurora MySQL Version 2 können Sie die native Funktionsmethode anstelle dieser gespeicherten Prozeduren verwenden, um eine Lambda-Funktion aufzurufen. Weitere Informationen zu den nativen Funktionen finden Sie unter Arbeiten mit nativen Funktionen zum Aufrufen einer Lambda-Funktion.

In Aurora MySQL Version 2 wird die gespeicherte Prozedur `mysql.lambda_async` nicht mehr unterstützt. Es wird dringend empfohlen, stattdessen native Lambda-Funktionen zu verwenden.

In Aurora MySQL Version 3 ist die gespeicherte Prozedur nicht verfügbar.

Verwenden der Prozedur „mysql.lambda async“ zum Aufrufen einer Lambda-Funktion (veraltet)

Bei `mysql.lambda_async` handelt es sich um eine integrierte gespeicherte Prozedur, mit der eine Lambda-Funktion asynchron aufgerufen wird. Zur Nutzung dieser Prozedur muss der Datenbankbenutzer über die `EXECUTE`-Berechtigung für die gespeicherte Prozedur `mysql.lambda_async` verfügen.

Syntax

Die Prozedur `mysql.lambda_async` verwendet die folgende Syntax.

```
CALL mysql.lambda_async (
  lambda_function_ARN,
  lambda_function_input
)
```

Parameter

Die Prozedur `mysql.lambda_async` hat die folgenden Parameter.

lambda_function_ARN

Der Amazon-Ressourcenname (ARN) der aufzurufenden Lambda-Funktion.

lambda_function_input

Die Eingabezeichenfolge im JSON-Format für die aufgerufene Lambda-Funktion.

Beispiele

Als bewährte Methode wird empfohlen, Aufrufe der Prozedur `mysql.lambda_async` in einer gespeicherten Prozedur zu verpacken, die aus verschiedenen Quellen aufgerufen werden kann, wie zum Beispiel Auslöser oder Clientcode. Mit dieser Methode werden Probleme mit Impedanzfehlanpassungen vermieden, zudem wird der Aufruf von Lambda-Funktionen vereinfacht.

> **Note**
>
> Seien Sie vorsichtig, wenn Sie eine AWS Lambda Funktion über Trigger in Tabellen aufrufen, die einen hohen Schreibverkehr haben. `INSERT`,`UPDATE`, und `DELETE` Trigger werden pro Zeile aktiviert. Ein Workload mit hohem Schreibdatenverkehr in einer Tabelle mit den Auslösern `INSERT`, `UPDATE` oder `DELETE` führt zu einer hohen Anzahl von Aufrufen Ihrer AWS Lambda -Funktion.

Die Aufrufe der Prozedur `mysql.lambda_async` sind asynchron, Auslöser jedoch synchron. Eine Anweisung, die zu einer hohen Anzahl an Auslöseraktivierungen führt, wartet nicht, bis der AWS Lambda -Funktionsaufruf abgeschlossen ist – sie wartet jedoch, bis die Auslöser abgeschlossen sind, bevor die Kontrolle an den Client zurückgegeben wird.

Example Beispiel: Rufen Sie eine AWS Lambda Funktion zum Senden von E-Mails auf

Im folgenden Beispiel wird eine gespeicherte Prozedur erstellt, die Sie in Ihrem Datenbankcode aufrufen können, um eine E-Mail mit einer Lambda-Funktion zu senden.

AWS Lambda Funktion

```
import boto3

ses = boto3.client('ses')

def SES_send_email(event, context):

    return ses.send_email(
        Source=event['email_from'],
        Destination={
            'ToAddresses': [
            event['email_to'],
            ]
        },

        Message={
            'Subject': {
            'Data': event['email_subject']
            },
            'Body': {
                'Text': {
                    'Data': event['email_body']
                }
            }
        }
    )
```

Gespeicherte Prozedur

```
DROP PROCEDURE IF EXISTS SES_send_email;
```

```
DELIMITER ;;
  CREATE PROCEDURE SES_send_email(IN email_from VARCHAR(255),
                                  IN email_to VARCHAR(255),
                                  IN subject VARCHAR(255),
                                  IN body TEXT) LANGUAGE SQL
  BEGIN
    CALL mysql.lambda_async(
         'arn:aws:lambda:us-west-2:123456789012:function:SES_send_email',
         CONCAT('{"email_to" : "', email_to,
             '", "email_from" : "', email_from,
             '", "email_subject" : "', subject,
             '", "email_body" : "', body, '"}')
     );
  END
  ;;
DELIMITER ;
```

Abrufen der gespeicherten Prozedur zum Aufrufen der AWS Lambda -Funktion

```
mysql> call SES_send_email('example_from@amazon.com', 'example_to@amazon.com', 'Email
 subject', 'Email content');
```

Example Beispiel: Rufen Sie eine AWS Lambda Funktion auf, um ein Ereignis über einen Trigger zu veröffentlichen

Im folgenden Beispiel wird eine gespeicherte Prozedur erstellt, die ein Ereignis mithilfe von Amazon SNS veröffentlicht. Der Code ruft die Prozedur von einem Auslöser auf, wenn eine Zeile zu einer Tabelle hinzugefügt wird.

AWS Lambda Funktion

```
import boto3

sns = boto3.client('sns')

def SNS_publish_message(event, context):

    return sns.publish(
        TopicArn='arn:aws:sns:us-west-2:123456789012:Sample_Topic',
        Message=event['message'],
        Subject=event['subject'],
        MessageStructure='string'
```

```
    )
```

Gespeicherte Prozedur

```
DROP PROCEDURE IF EXISTS SNS_Publish_Message;
DELIMITER ;;
CREATE PROCEDURE SNS_Publish_Message (IN subject VARCHAR(255),
                                      IN message TEXT) LANGUAGE SQL
BEGIN
  CALL mysql.lambda_async('arn:aws:lambda:us-
west-2:123456789012:function:SNS_publish_message',
     CONCAT('{ "subject" : "', subject,
            '", "message" : "', message, '" }')
     );
END
;;
DELIMITER ;
```

Tabelle

```
CREATE TABLE 'Customer_Feedback' (
  'id' int(11) NOT NULL AUTO_INCREMENT,
  'customer_name' varchar(255) NOT NULL,
  'customer_feedback' varchar(1024) NOT NULL,
  PRIMARY KEY ('id')
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Auslöser

```
DELIMITER ;;
CREATE TRIGGER TR_Customer_Feedback_AI
  AFTER INSERT ON Customer_Feedback
  FOR EACH ROW
BEGIN
  SELECT CONCAT('New customer feedback from ', NEW.customer_name),
 NEW.customer_feedback INTO @subject, @feedback;
  CALL SNS_Publish_Message(@subject, @feedback);
END
;;
DELIMITER ;
```

Einfügen einer Tabellenzeile zum Auslösen der Benachrichtigung

```
mysql> insert into Customer_Feedback (customer_name, customer_feedback) VALUES ('Sample
 Customer', 'Good job guys!');
```

Veröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs

Sie können Ihren Aurora MySQL-DB-Cluster so konfigurieren, dass er allgemeine, langsame Protokolldaten, Prüfdaten und Fehlerprotokolldaten in einer Protokollgruppe in Amazon CloudWatch Logs veröffentlicht. Mit CloudWatch Logs können Sie eine Echtzeitanalyse der Protokolldaten durchführen und diese CloudWatch zur Erstellung von Alarmen und zur Anzeige von Metriken verwenden. Sie können CloudWatch Logs verwenden, um Ihre Protokolldatensätze in einem äußerst langlebigen Speicher zu speichern.

Um Logs in CloudWatch Logs zu veröffentlichen, müssen die entsprechenden Logs aktiviert sein. Fehlerprotokolle sind standardmäßig aktiviert, Protokolle anderer Typen müssen dagegen explizit aktiviert werden. Informationen zum Aktivieren der Protokolle in MySQL finden Sie unter Auswahl von allgemeinen Abfrage- und langsamen Abfrage-Protokollausgabezielen in der MySQL-Dokumentation. Weitere Informationen über das Aktivieren von Aurora MySQL-Audit-Protokollen finden Sie unter Aktivieren von erweitertem Auditing.

> **Note**
>
> - Wenn der Export von Protokolldaten deaktiviert ist, löscht Aurora keine existierenden Protokollgruppen oder Protokollstreams. Wenn der Export von Protokolldaten deaktiviert ist, bleiben vorhandene Protokolldaten je nach Aufbewahrung der CloudWatch Protokolle in Logs verfügbar, und es fallen weiterhin Gebühren für gespeicherte Audit-Log-Daten an. Sie können Protokollstreams und Protokollgruppen mithilfe der CloudWatch Logs-Konsole AWS CLI, der oder der CloudWatch Logs-API löschen.
> - Eine alternative Möglichkeit, Audit-Logs in Logs zu CloudWatch veröffentlichen, besteht darin, Advanced Auditing zu aktivieren, dann eine benutzerdefinierte DB-Cluster-Parametergruppe zu erstellen und den `server_audit_logs_upload` Parameter auf zu setzen`1`. Die Standardeinstellung für den `server_audit_logs_upload` DB-Cluster-Parameter ist`0`. Informationen zur Aktivierung von Advanced Auditing finden Sie unterVerwenden von Advanced Auditing in einem Amazon Aurora MySQL DB-Cluster.
>
>   Wenn Sie diese alternative Methode verwenden, müssen Sie über eine IAM-Rolle für den Zugriff auf CloudWatch Logs verfügen und den Parameter auf `aws_default_logs_role`

Clusterebene auf den ARN für diese Rolle festlegen. Weitere Informationen zum Erstellen der Rolle finden Sie unter Einrichten von IAM-Rollen für den Zugriff auf AWS-Services. Wenn Sie jedoch über die `AWSServiceRoleForRDS` serviceverknüpfte Rolle verfügen, bietet sie Zugriff auf CloudWatch Logs und setzt alle benutzerdefinierten Rollen außer Kraft. Informationen zu serviceverknüpften Rollen für Amazon RDS finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Aurora.

- Wenn Sie Audit-Logs nicht in Logs exportieren möchten, stellen Sie sicher, dass alle Methoden zum CloudWatch Exportieren von Audit-Logs deaktiviert sind. Bei diesen Methoden handelt es sich um die AWS Management Console, die AWS CLI, die RDS-API und den Parameter `server_audit_logs_upload`.
- Das Verfahren unterscheidet sich für Aurora Serverless v1 DB-Cluster geringfügig von dem für DB-Cluster mit bereitgestellten oder Aurora Serverless v2 DB-Instances. Aurora Serverless v1Cluster laden automatisch alle Protokolle hoch, die Sie über Konfigurationsparameter aktivieren.

  Daher aktivieren oder deaktivieren Sie den Protokoll-Upload für Aurora Serverless v1 DB-Cluster, indem Sie verschiedene Protokolltypen in der DB-Cluster-Parametergruppe ein- und ausschalten. Sie ändern die Einstellungen des Clusters selbst nicht über die AWS Management Console AWS CLI, oder RDS-API. Informationen zum Aktivieren und Deaktivieren von MySQL-Protokollen für Aurora Serverless v1-Cluster finden Sie unterParametergruppen für Aurora Serverless v1.

Konsole

Sie können Aurora MySQL-Protokolle für bereitgestellte Cluster mit der Konsole in CloudWatch Logs veröffentlichen.

Veröffentlichen Sie Aurora MySQL-Protokolle mit der Konsole wie folgt:

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Aurora MySQL-DB-Cluster, für den die Protokolldaten veröffentlicht werden sollen.
4. Wählen Sie Ändern aus.
5. Wählen Sie im Abschnitt Protokollexporte die Protokolle aus, die Sie in CloudWatch Logs veröffentlichen möchten.

6. Wählen Sie Weiter und dann auf der Übersichtsseite DB-Cluster ändern.

AWS CLI

Sie können Aurora MySQL-Protokolle für bereitgestellte Cluster mit der AWS CLI veröffentlichen. Dazu führen Sie den modify-db-cluster AWS CLI Befehl mit den folgenden Optionen aus:

- `--db-cluster-identifier` – Die DB-Cluster-Kennung.
- `--cloudwatch-logs-export-configuration`— Die Konfigurationseinstellung für die Protokolltypen, die für den Export in CloudWatch Logs für den DB-Cluster aktiviert werden sollen.

Sie können Aurora-MySQL-Protokolle auch veröffentlichen, indem Sie einen der folgenden AWS CLI -Befehle ausführen:

- create-db-cluster
- restore-db-cluster-from-s3
- restore-db-cluster-from-Schnappschuss
- restore-db-cluster-to-point-in-time

Führen Sie einen dieser AWS CLI Befehle mit den folgenden Optionen aus:

- `--db-cluster-identifier` – Die DB-Cluster-Kennung.
- `--engine`— Die Datenbank-Engine.
- `--enable-cloudwatch-logs-exports`— Die Konfigurationseinstellung für die Protokolltypen, die für den Export in CloudWatch Logs für den DB-Cluster aktiviert werden sollen.

Je nachdem, welchen AWS CLI Befehl Sie ausführen, sind möglicherweise andere Optionen erforderlich.

Example

Der folgende Befehl ändert einen vorhandenen Aurora MySQL-DB-Cluster, um Protokolldateien in CloudWatch Logs zu veröffentlichen.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
```

```
    --db-cluster-identifier mydbcluster \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["error","general","slowquery","audit"]}'
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["error","general","slowquery","audit"]}'
```

Example

Der folgende Befehl erstellt einen Aurora MySQL-DB-Cluster, um Protokolldateien in CloudWatch Logs zu veröffentlichen.

Für LinuxmacOS, oderUnix:

```
aws rds create-db-cluster \
    --db-cluster-identifier mydbcluster \
    --engine aurora \
    --enable-cloudwatch-logs-exports '["error","general","slowquery","audit"]'
```

Windows:

```
aws rds create-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --engine aurora ^
    --enable-cloudwatch-logs-exports '["error","general","slowquery","audit"]'
```

RDS-API

Sie können Aurora MySQL-Protokolle für bereitgestellte Cluster mithilfe der RDS-API veröffentlichen. Hierzu führen Sie die Aktion ModifyDBCluster mit den folgenden Optionen aus:

- `DBClusterIdentifier` – Die DB-Cluster-Kennung.

- `CloudwatchLogsExportConfiguration`— Die Konfigurationseinstellung für die Protokolltypen, die für den Export in CloudWatch Logs für den DB-Cluster aktiviert werden sollen.

Sie können Aurora MySQL-Protokolle auch mit der RDS-API veröffentlichen, indem Sie eine der folgenden RDS-API-Operationen ausführen:

- CreateDBCluster
- DB S3 wurde wiederhergestellt ClusterFrom
- DB wurde wiederhergestellt ClusterFromSnapshot
- DB wurde wiederhergestellt ClusterToPointInTime

Verwenden Sie dazu die RDS-API-Operation mit den folgenden Parametern:

- `DBClusterIdentifier` – Die DB-Cluster-Kennung.
- `Engine`— Die Datenbank-Engine.
- `EnableCloudwatchLogsExports`— Die Konfigurationseinstellung für die Protokolltypen, die für den Export in Logs für den CloudWatch DB-Cluster aktiviert werden sollen.

Je nachdem, welchen AWS CLI Befehl Sie ausführen, sind möglicherweise andere Parameter erforderlich.

Überwachen von Protokollereignissen in Amazon CloudWatch

Nachdem Sie Aurora MySQL-Protokollereignisse aktiviert haben, können Sie die Ereignisse in Amazon CloudWatch Logs überwachen. Eine neue Protokollgruppe für den Aurora-DB-Cluster wird automatisch mit folgendem Präfix erstellt. Dabei repräsentiert *`cluster-name`* den DB-Clusternamen und *`log_type`* den Protokolltyp.

```
/aws/rds/cluster/cluster-name/log_type
```

Wenn Sie beispielsweise die Exportfunktion so konfigurieren, dass das Slow-Query-Protokoll für einen DB-Cluster namens `mydbcluster` eingeschlossen wird, werden die Slow-Query-Daten in der Protokollgruppe `/aws/rds/cluster/mydbcluster/slowquery` gespeichert.

Die Ereignisse aus allen Instances in Ihrem Cluster werden von einer Protokollgruppe unter Verwendung verschiedener Protokollstreams erfasst. Das Verhalten hängt davon ab, welche der folgenden Bedingungen zutrifft:

- Eine Protokollgruppe mit dem angegebenen Namen existiert.

  Aurora verwendet die vorhandene Protokollgruppe, um Protokolldaten für den Cluster zu exportieren. Um Protokollgruppen mit vordefinierten Protokollaufbewahrungszeiten, Metrikfiltern und Kundenzugriff zu erstellen, können Sie die automatisierte Kommunikation verwenden, zum Beispiel AWS CloudFormation.
- Eine Protokollgruppe mit dem angegebenen Namen existiert nicht.

  Wenn ein passender Protokolleintrag in der Protokolldatei für die Instance erkannt wird, erstellt Aurora MySQL automatisch eine neue Protokollgruppe in CloudWatch Logs. Die Protokollgruppe nutzt den standardmäßigen Aufbewahrungszeitraum für Protokolle Never Expire (Läuft nie ab).

  Um die Aufbewahrungsdauer der CloudWatch Protokolle zu ändern, verwenden Sie die Logs-Konsole AWS CLI, die oder die CloudWatch Logs-API. Weitere Informationen zur Änderung der Aufbewahrungsfristen für CloudWatch Protokolle in Logs finden Sie unter Ändern der Aufbewahrung von Protokolldaten in CloudWatch Logs.

Um in den Protokollereignissen für einen DB-Cluster nach Informationen zu suchen, verwenden Sie die CloudWatch Logs-Konsole AWS CLI, die oder die CloudWatch Logs-API. Weitere Informationen finden Sie unter Suchen und Filtern von Protokolldaten.

Amazon Aurora MySQL-Labor-Modus

Der Aurora-Labor-Modus wird verwendet, um Aurora-Funktionen zu aktivieren, die in der aktuellen Aurora-Datenbankversion vorhanden, jedoch standardmäßig deaktiviert sind. Auch wenn die Funktionen des Aurora-Labor-Modus nicht für den Einsatz in Produktions-DB-Clustern empfohlen werden, können Sie den Aurora-Labor-Modus verwenden, um diese Funktionen für DB-Cluster in Ihrer Entwicklungs- und Testumgebung zu aktivieren. Weitere Informationen über Aurora-Funktionen, die im Aurora-Labor-Modus zur Verfügung stehen, finden Sie unter Funktionen des Aurora-Labor-Modus.

Der Parameter `aurora_lab_mode` ist ein Parameter der Instance-Ebene, der sich in der Standardparametergruppe befindet. Der Parameter ist in der Standard-DB-Parametergruppe von Oracle auf `0` (deaktiviert) gesetzt. Um den Aurora-Labormodus zu aktivieren, erstellen Sie eine benutzerdefinierte Parametergruppe, setzen den Parameter `aurora_lab_mode` in der benutzerdefinierten Parametergruppe auf `1` (aktiviert) und ändern eine oder mehrere DB-Instances in Ihrem Aurora-Cluster so, dass die benutzerdefinierte Parametergruppe verwendet wird. Stellen Sie dann eine Verbindung zu dem jeweiligen Instance-Endpunkt her, um die Lab-Modus funktionen auszuprobieren. Weitere Informationen zum Ändern von DB-Parametergruppen finden Sie unter Ändern von Parametern in einer DB-Parametergruppe. Weitere Informationen zu Parametergruppen und Amazon Aurora finden Sie unter Aurora MySQL Konfigurationsparameter.

Funktionen des Aurora-Labor-Modus

In der folgenden Tabelle werden die Aurora-Funktionen aufgeführt, die derzeit im Aurora-Labor-Modus verfügbar sind. Sie müssen den Aurora-Labor-Modus aktivieren, bevor Sie diese Funktionen verwenden können.

Funktionsmerkmal	Beschreibung
Scan-Batching	Aurora MySQL Scan-Batching beschleunigt die speicherinternen, scan-orientierten Abfragen erheblich. Die Funktion steigert die Leistung von Tabellenvollscans, Indexvollscans und Indexbereichsscans durch Stapelverarbeitung.
Hash-Joins	Diese Funktion kann die Abfrageleistung verbessern, wenn Sie eine große Datenmenge mithilfe eines Equijoins verbinden müssen. Sie

Funktionsmerkmal	Beschreibung
	können diese Funktion ohne Labor-Modus in Aurora MySQL-Version 2 verwenden. Weitere Informationen zur Verwendung dieser Funktion finden Sie unter Optimierung von großen Aurora-MySQL-Join-Abfragen mit Hash-Joins.
Schnelle DDL	Mit dieser Funktion können Sie eine `ALTER TABLE` *`tbl_name`* `ADD COLUMN` *`col_name column_definition`* -Operation praktisch augenblicklich ausführen. Die Operation wird abgeschlossen, ohne dass ein Kopieren der Tabelle erforderlich wäre und ohne eine materielle Auswirkung auf andere DML-State ments zu haben. Da kein temporärer Speicher für eine Tabellenkopie benötigt wird, haben DDL-Statements praktische Vorteile, sogar für große Tabellen auf kleinen Instance-Typen. Fast DDL wird zurzeit nur für das Hinzufüge n löschbarer Spalten ohne Standardwert am Ende einer Tabelle unterstützt. Weitere Informationen zur Verwendung dieser Funktion finden Sie unter Ändern von Tabellen in Amazon Aurora mithilfe von Fast DDL.

Bewährte Methoden mit Amazon Aurora MySQL

Dieses Thema beinhaltet Informationen zu bewährten Methoden und Optionen für die Verwendung oder Migration von Daten in einem Amazon-Aurora-MySQL-DB-Cluster. Die Informationen in diesem Thema fassen einige der Richtlinien und Verfahren zusammen, die Sie unter Verwalten eines Amazon Aurora-DB-Clusters.

Inhalt

- Minimieren von InnoDB-Deadlocks
- Überwachen von InnoDB-Deadlocks

Feststellen, mit welcher DB-Instance Sie verbunden sind

Um herauszufinden, zu welcher DB-Instance in einem Aurora-MySQL-DB-Cluster eine Verbindung besteht, prüfen Sie die globale Variable `innodb_read_only` wie im folgenden Beispiel gezeigt.

```
SHOW GLOBAL VARIABLES LIKE 'innodb_read_only';
```

Die Variable `innodb_read_only` wird auf `ON` gesetzt, wenn Sie mit einer Reader-DB-Instance verbunden sind. Diese Einstellung ist `OFF`, wenn Sie mit einer Writer-DB-Instance verbunden sind, z. B. als primäre Instance in einem bereitgestellten Cluster.

Dieser Ansatz kann hilfreich sein, wenn Sie zu Ihrem Anwendungscode eine Logik hinzufügen möchten, um den Workload auszugleichen, oder sicherzustellen, dass eine Schreiboperation die richtige Verbindung verwendet.

Bewährte Verfahren für die Leistung und Skalierung von Aurora MySQL

Sie können die folgenden bewährten Verfahren anwenden, um die Leistung und Skalierbarkeit Ihrer Aurora-MySQL-Cluster zu verbessern.

Themen

- Verwendung von T-Instance-Klassen für Entwicklung und Tests
- Optimierung von mit Aurora MySQL indizierten Join-Abfragen mit asynchronem Key Prefetch
- Optimierung von großen Aurora-MySQL-Join-Abfragen mit Hash-Joins
- Verwenden von Amazon Aurora für das Skalieren von Lesevorgängen in Ihrer MySQL-Datenbank
- Optimierung von Zeitstempeloperationen

Verwendung von T-Instance-Klassen für Entwicklung und Tests

Amazon Aurora MySQL-Instances, die die DB-Instanzklassen `db.t2`, `db.t3` oder `db.t4g` verwenden, eignen sich am besten für Anwendungen, die nicht über einen längeren Zeitraum eine hohe Arbeitslast unterstützen. Die T-Instanzen sind so konzipiert, dass sie eine mäßige Basisleistung bieten und je nach Workload eine deutlich höhere Leistung erreichen können. Sie eignen sich für

Workloads, die die volle CPU-Leistung selten oder uneinheitlich verwenden, jedoch gelegentlich Spitzenlasten verarbeiten müssen. Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter Burstable Performance Instances.

Wenn Ihr Aurora-Cluster größer als 40 TB ist, sollten Sie die T-Instance-Klassen nicht verwenden. Wenn Ihre Datenbank ein großes Datenvolumen hat, kann der Speicher-Overhead für die Verwaltung von Schemaobjekten die Kapazität einer T-Instance übersteigen.

Aktivieren Sie das MySQL-Leistungsschema nicht auf Amazon Aurora MySQL T-Instances. Wenn das Leistungsschema aktiviert ist, geht der Instance möglicherweise der Speicher aus.

> **Tip**
>
> Wenn Ihre Datenbank manchmal inaktiv ist, aber zu anderen Zeiten eine erhebliche Workload aufweist, können Sie Aurora Serverless v2 als Alternative zu T-Instances verwenden. Mit Aurora Serverless v2 definieren Sie einen Kapazitätsbereich und Aurora skaliert Ihre Datenbank je nach aktueller Workload automatisch nach oben oder unten. Details zur Verwendung finden Sie unter Verwenden von Aurora Serverless v2. Die Versionen der Datenbank-Engine, die Sie mit Aurora Serverless v2 verwenden können, finden Sie unter Anforderungen und Einschränkungen für Aurora Serverless v2.

Wenn Sie eine T-Instance als DB-Instance in einem Aurora-MySQL DB-Cluster verwenden, empfehlen wir Folgendes:

- Verwenden Sie für alle Instances in Ihrem DB–Cluster dieselbe DB-Instance-Klasse. Wenn Sie zum Beispiel `db.t2.medium` für Ihre Writer-Instance verwenden, empfehlen wir Ihnen, `db.t2.medium` auch für Ihre Reader-Instances zu verwenden.
- Nehmen Sie keine speicherbezogenen Konfigurationseinstellungen vor, wie z. B. `innodb_buffer_pool_size`. Aurora verwendet einen hochgradig abgestimmten Satz von Standardwerten für Speicherpuffer auf T-Instanzen. Diese speziellen Voreinstellungen sind erforderlich, damit Aurora auf Instanzen mit begrenztem Speicherplatz läuft. Wenn Sie speicherbezogene Einstellungen auf einer T-Instance ändern, ist es viel wahrscheinlicher, dass Sie auf out-of-memory Bedingungen stoßen, auch wenn Ihre Änderung darauf abzielt, die Puffergröße zu erhöhen.

- Überwachen Sie Ihr CPU-Guthaben (`CPUCreditBalance`), um sicherzustellen, dass es auf einem akzeptablen Stand ist. CPU-Guthaben werden nämlich zu denselben Tarifen angesammelt, wie sie verbraucht werden.

  Wenn Sie Ihr CPU-Guthaben aufgebraucht haben, werden Sie sofort eine Leistungsminderung der verfügbaren CPU und erhöhte Latenzen der Lese- und Schreibvorgänge in der Instance feststellen. Diese Situation führt zu einem starken Rückgang der Gesamtperformance der Instance.

  Wenn Ihr CPU-Guthaben nicht ausreicht, empfehlen wir Ihnen, Ihre DB-Instanz so zu ändern, dass sie eine der unterstützten R DB-Instance-Klassen (Scale Compute) verwendet.

  Weitere Informationen über das Überwachen von Metriken finden Sie unter Anzeigen von Metriken in der Amazon-RDS-Konsole.

- Überwachen Sie die Replikverzögerung (`AuroraReplicaLag`) zwischen der Writer-Instance und den Reader-Instances.

  Wenn einer Reader-Instance das CPU-Guthaben vor der Writer-Instance ausgeht, kann die daraus resultierende Verzögerung dazu führen, dass die Reader-Instance häufig neu gestartet werden muss. Dieses Ergebnis tritt häufig auf, wenn eine Anwendung eine hohe Anzahl von Lesevorgängen hat, die auf die Reader-Instance verteilt sind, während die Schreib-Instance eine minimale Anzahl von Schreibvorgängen hat.

  Wenn Sie einen anhaltenden Anstieg der Verzögerung bei der Replikation feststellen, stellen Sie sicher, dass Ihr CPU-Guthaben für die Reader-Instances in Ihrem DB-Cluster nicht erschöpft ist.

  Wenn Ihr CPU-Guthaben nicht ausreicht, empfehlen wir Ihnen, Ihre DB-Instance so zu modifizieren, dass sie eine der unterstützten R DB-Instance-Klassen (scale compute) verwendet.

- Halten Sie die Anzahl an Inserts pro Transaktion unter 1 Million für DB-Cluster, bei denen die Binärprotokollierung aktiviert ist.

  Wenn der Parameter in der DB-Cluster-Parametergruppe für Ihren DB-Cluster auf einen anderen Wert als gesetzt ist`OFF`, kann es in Ihrem DB-Cluster zu Problemen kommen, wenn der DB-Cluster Transaktionen empfängt, die mehr als 1 Million einzufügende Zeilen enthalten. `binlog_format` out-of-memory Sie können den freien Speicher (`FreeableMemory`) metrisch überwachen, um festzustellen, ob Ihrem DB-Cluster der verfügbare Speicher ausgeht. Sie überprüfen dann die Metrik der Schreibvorgänge (`VolumeWriteIOPS`), um zu sehen, ob eine Writer-Instance eine große Last von Schreibvorgängen empfängt. Wenn dies der Fall ist, empfehlen wir, Ihre Anwendung zu aktualisieren, um die Anzahl von Einfügungen in einer Transaktion auf weniger

als 1 Million zu begrenzen. Alternativ können Sie Ihre Instance so modifizieren, dass sie eine der unterstützten R DB-Instance-Klassen verwendet (scale compute).

Optimierung von mit Aurora MySQL indizierten Join-Abfragen mit asynchronem Key Prefetch

Aurora MySQL kann die asynchrone Key Prefetch (AKP)-Funktion verwenden, um die Performance von Abfragen zu verbessern, die Tabellen über Indizes hinweg verknüpfen. Diese Funktion verbessert die Leistung, indem sie die Zeilen vorwegnimmt, die zum Ausführen von Abfragen benötigt werden, bei denen eine JOIN-Abfrage die Verwendung des Batched Key Access (BKA) Join-Algorithmus und der Multi-Range Read (MRR)-Optimierungsfunktionen erfordert. Weitere Informationen zu BKA und MRR finden Sie unter Block Nested-Loop und Batched Key Access Joins und Multi-Range Read Optimization in der MySQL-Dokumentation.

Um einen Vorteil aus der AKP-Funktion zu ziehen, muss eine Abfrage sowohl BKA als auch MRR verwenden. Typischerweise tritt eine solche Abfrage auf, wenn die JOIN-Klausel einer Abfrage einen Sekundärindex verwendet, aber auch einige Spalten aus dem Primärindex benötigt. Sie können beispielsweise AKP verwenden, wenn eine JOIN-Klausel einen Equijoin auf Indexwerten zwischen einer kleinen äußeren und einer großen inneren Tabelle darstellt und der Index auf der größeren Tabelle hoch selektiv ist. AKP arbeitet mit BKA und MRR zusammen, um während der Evaluierung der JOIN-Klausel einen sekundären Index-Lookup durchzuführen. AKP identifiziert die Zeilen, die während der Auswertung der JOIN-Klausel benötigt werden, um die Abfrage auszuführen. Anschließend werden die Seiten, die diese Zeilen enthalten, mit einem Hintergrund-Thread asynchron in den Speicher geladen, bevor die Abfrage ausgeführt wird.

AKP ist für Aurora MySQL Version 2.10 und höher sowie Version 3 verfügbar. Weitere Informationen zu den Aurora MySQL-Versionen erhalten Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.

Asynchrones Key Prefetch aktivieren

Sie können die AKP-Funktion aktivieren, indem Sie `aurora_use_key_prefetch`, eine MySQL-Servervariable, auf on setzen. Standardmäßig ist dieser Wert auf on festgelegt. AKP kann jedoch erst aktiviert werden, wenn Sie auch den BKA-Join-Algorithmus aktivieren und die preisbasierte MRR-Funktionalität deaktivieren. Dazu müssen Sie die folgenden Werte für `optimizer_switch` setzen, eine Variable von MySQL-Server:

- Setzen Sie `batched_key_access` auf `on`. Dieser Wert steuert die Verwendung des BKA-Join-Algorithmus. Standardmäßig ist dieser Wert auf `off` festgelegt.
- Setzen Sie `mrr_cost_based` auf `off`. Dieser Wert steuert die Nutzung der kostenbasierten MRR-Funktionalität. Standardmäßig ist dieser Wert auf `on` festgelegt.

Derzeit können Sie diese Werte nur auf Sitzungsebene festlegen. Das folgende Beispiel veranschaulicht, wie diese Werte gesetzt werden können, um AKP für die aktuelle Sitzung durch Ausführen von SET-Anweisungen zu aktivieren.

```
mysql> set @@session.aurora_use_key_prefetch=on;
mysql> set @@session.optimizer_switch='batched_key_access=on,mrr_cost_based=off';
```

Ähnlich können Sie mit SET-Anweisungen AKP und den BKA Join-Algorithmus deaktivieren und kostenbasierte MRR-Funktionalität für die aktuelle Sitzung wieder aktivieren, wie im folgenden Beispiel gezeigt.

```
mysql> set @@session.aurora_use_key_prefetch=off;
mysql> set @@session.optimizer_switch='batched_key_access=off,mrr_cost_based=on';
```

Weitere Informationen über die Optimierungsschalter batched_key_access und mrr_cost_based finden Sie unter Switchable Optimizations in der MySQL-Dokumentation.

Optimieren von Abfragen für asynchrones Key Prefetch

Sie können bestätigen, ob eine Abfrage die AKP-Funktion nutzen können soll. Verwenden Sie dazu die `EXPLAIN`-Anweisung, um die Abfrage vor der Ausführung zu profilieren. Die `EXPLAIN`-Anweisung stellt Informationen über den Ausführungsplan bereit, der für eine angegebene Abfrage verwendet werden soll.

In der Ausgabe der `EXPLAIN`-Anweisung beschreibt die Spalte `Extra` zusätzliche Informationen, die im Ausführungsplan eingeschlossen sind. Wenn das AKP-Feature auf eine in der Abfrage verwendete Tabelle zutrifft, enthält diese Spalte einen der folgenden Werte:

- `Using Key Prefetching`
- `Using join buffer (Batched Key Access with Key Prefetching)`

Das folgende Beispiel zeigt die Verwendung von `EXPLAIN`, um den Ausführungsplan für eine Abfrage anzuzeigen, die von AKP profitieren kann.

```
mysql> explain select sql_no_cache
    ->     ps_partkey,
    ->     sum(ps_supplycost * ps_availqty) as value
    -> from
    ->     partsupp,
    ->     supplier,
    ->     nation
    -> where
    ->     ps_suppkey = s_suppkey
    ->     and s_nationkey = n_nationkey
    ->     and n_name = 'ETHIOPIA'
    -> group by
    ->     ps_partkey having
    ->         sum(ps_supplycost * ps_availqty) > (
    ->             select
    ->                 sum(ps_supplycost * ps_availqty) * 0.0000003333
    ->             from
    ->                 partsupp,
    ->                 supplier,
    ->                 nation
    ->             where
    ->                 ps_suppkey = s_suppkey
    ->                 and s_nationkey = n_nationkey
    ->                 and n_name = 'ETHIOPIA'
    ->         )
    -> order by
    ->     value desc;
+----+-------------+----------+------+----------------------+--------------
+---------+-----------------------------------+------+----------
+-------------------------------------------------------------+
| id | select_type | table    | type | possible_keys        | key           | key_len
 | ref                              | rows | filtered | Extra
                            |
+----+-------------+----------+------+----------------------+--------------
+---------+-----------------------------------+------+----------
+-------------------------------------------------------------+
|  1 | PRIMARY     | nation   | ALL  | PRIMARY              | NULL          | NULL
 | NULL                             |   25 |   100.00 | Using where; Using temporary;
 Using filesort                |
```

```
|  1 | PRIMARY     | supplier | ref  | PRIMARY,i_s_nationkey | i_s_nationkey | 5
 | dbt3_scale_10.nation.n_nationkey | 2057 |   100.00 | Using index
                              |
|  1 | PRIMARY     | partsupp | ref  | i_ps_suppkey          | i_ps_suppkey  | 4
 | dbt3_scale_10.supplier.s_suppkey |   42 |   100.00 | Using join buffer (Batched Key
 Access with Key Prefetching) |
|  2 | SUBQUERY    | nation   | ALL  | PRIMARY               | NULL          | NULL
 | NULL                             |   25 |   100.00 | Using where
                              |
|  2 | SUBQUERY    | supplier | ref  | PRIMARY,i_s_nationkey | i_s_nationkey | 5
 | dbt3_scale_10.nation.n_nationkey | 2057 |   100.00 | Using index
                              |
|  2 | SUBQUERY    | partsupp | ref  | i_ps_suppkey          | i_ps_suppkey  | 4
 | dbt3_scale_10.supplier.s_suppkey |   42 |   100.00 | Using join buffer (Batched Key
 Access with Key Prefetching) |
+----+-------------+----------+------+-----------------------+---------------
+---------+-----------------------------------+------+----------
+-------------------------------------------------------------+
6 rows in set, 1 warning (0.00 sec)
```

Weitere Informationen über das `EXPLAIN`-Ausgabeformat finden Sie unter Extended EXPLAIN Output Format in der MySQL-Dokumentation.

Optimierung von großen Aurora-MySQL-Join-Abfragen mit Hash-Joins

Wenn Sie eine große Datenmenge mit Hilfe eines Equijoins verknüpfen müssen, kann ein Hash-Join die Abfrageleistung verbessern. Sie können Hash-Joins für Aurora MySQL aktivieren.

Eine Hash-Join-Spalte kann ein beliebiger komplexer Ausdruck sein. In einer Hash-Join-Spalte haben Sie folgende Möglichkeiten, Datentypen übergreifend zu vergleichen:

- Sie können alles über die Kategorie der präzisen numerischen Datentypen hinweg vergleichen, wie z. B. `int`, `bigint`, `numeric` und `bit`.
- Sie können alles über die Kategorie der ungefähren numerischen Datentypen hinweg vergleichen, wie z. B. `float` und `double`.
- Sie können Elemente über String-Typen hinweg vergleichen, wenn die String-Typen den gleichen Zeichensatz und die gleiche Sortierreihenfolge haben.
- Sie können Elemente mit Datums- und Zeitstempel-Datentypen vergleichen, wenn die Typen identisch sind.

> **Note**
>
> Sie können Datentypen verschiedener Kategorien nicht miteinander vergleichen.

Die folgenden Einschränkungen gelten für Hash-Joins für Aurora MySQL:

- Links-Rechts-Außen-Joins werden für Aurora MySQL-Version 2 nicht unterstützt, für Version 3 hingegen schon.
- Semijoins wie Subqueries werden nicht unterstützt, es sei denn, die Subqueries erfolgen zuerst.
- Mehrfach-Tabellen-Updates oder -Löschungen werden nicht unterstützt.

  > **Note**
  >
  > Einzel-Tabellen-Updates oder -Löschungen werden unterstützt.

- BLOB- und Geodatentyp-Spalten können keine Join-Spalten in einem Hash-Join sein.

Aktivieren von Hash-Joins

So aktivieren Sie Hash-Joins:

- Aurora-MySQL-Version 2 – Stellen Sie den DB-Parameter oder den DB-Cluster-Parameter `aurora_disable_hash_join` auf `0` ein. Durch Deaktivierung von `aurora_disable_hash_join` wird der Wert von `optimizer_switch` auf `hash_join=on` gesetzt.
- Aurora-MySQL-Version 3 – Stellen Sie den MySQL-Serverparameter `optimizer_switch` auf `block_nested_loop=on` ein.

Hash-Joins sind standardmäßig in Aurora-MySQL-Version 3 aktiviert und in Aurora-MySQL-Version 2 deaktiviert. Das folgende Beispiel zeigt, wie man Hash-Joins für Aurora-MySQL-Version 3 aktivieren kann. Sie können zuerst die Anweisung `select @@optimizer_switch` ausgeben, um zu sehen, welche anderen Einstellungen in der SET-Parameterzeichenfolge vorhanden sind. Das Aktualisieren einer Einstellung im Parameter `optimizer_switch` löscht oder ändert die anderen Einstellungen nicht.

```
mysql> SET optimizer_switch='block_nested_loop=on';
```

> **Note**
>
> Für Aurora-MySQL-Version 3 ist Hash-Join-Support in allen Nebenversionen verfügbar und standardmäßig aktiviert.
> Für Aurora MySQL-Version-3 ist Hash-Join-Support in allen Nebenversionen verfügbar und standardmäßig aktiviert. In Aurora-MySQL-Version 2 wird die Hash-Join-Funktion immer durch den `aurora_disable_hash_join`-Wert gesteuert.

Mit dieser Einstellung wählt der Optimierer einen Hash-Join auf der Grundlage von Kosten, Abfragemerkmalen und Ressourcenverfügbarkeit. Wenn die Kalkulation fehlerhaft ist, können Sie den Optimierer zwingen, einen bestimmten Hash-Join zu wählen. Sie erreichen dies, indem Sie `hash_join_cost_based`, eine MySQL-Servervariable, auf `off` setzen. Das folgende Beispiel zeigt, wie Sie den Optimierer zwingen können, einen Hash-Join zu wählen.

```
mysql> SET optimizer_switch='hash_join_cost_based=off';
```

> **Note**
>
> Diese Einstellung setzt die Entscheidungen des kostenbasierten Optimierers außer Kraft. Während die Einstellung für Tests und Entwicklung nützlich sein kann, empfehlen wir, sie nicht in der Produktion zu verwenden.

Optimieren von Abfragen für Hash-Joins

Um herauszufinden, ob eine Abfrage einen Hash-Join nutzen kann, verwenden Sie die `EXPLAIN`-Anweisung, um die Abfrage zuerst zu profilieren. Die `EXPLAIN`-Anweisung stellt Informationen über den Ausführungsplan bereit, der für eine angegebene Abfrage verwendet werden soll.

In der Ausgabe der `EXPLAIN`-Anweisung beschreibt die Spalte `Extra` zusätzliche Informationen, die im Ausführungsplan eingeschlossen sind. Wenn ein Hash-Join für die in der Abfrage verwendeten Tabellen gilt, enthält diese Spalte Werte, die den folgenden ähnlich sind:

- `Using where; Using join buffer (Hash Join Outer table` *`table1_name`*`)`
- `Using where; Using join buffer (Hash Join Inner table` *`table2_name`*`)`

Das folgende Beispiel zeigt die Verwendung von EXPLAIN, um den Ausführungsplan für eine Hash-Join-Abfrage anzuzeigen.

```
mysql> explain SELECT sql_no_cache * FROM hj_small, hj_big, hj_big2
    ->     WHERE hj_small.col1 = hj_big.col1 and hj_big.col1=hj_big2.col1 ORDER BY 1;
+----+-------------+----------+------+---------------+------+---------+------+------
+----------------------------------------------------------------+
| id | select_type | table    | type | possible_keys | key  | key_len | ref  | rows |
 Extra                                                          |
+----+-------------+----------+------+---------------+------+---------+------+------
+----------------------------------------------------------------+
|  1 | SIMPLE      | hj_small | ALL  | NULL          | NULL | NULL    | NULL |    6 |
 Using temporary; Using filesort                                |
|  1 | SIMPLE      | hj_big   | ALL  | NULL          | NULL | NULL    | NULL |   10 |
 Using where; Using join buffer (Hash Join Outer table hj_big)  |
|  1 | SIMPLE      | hj_big2  | ALL  | NULL          | NULL | NULL    | NULL |   15 |
 Using where; Using join buffer (Hash Join Inner table hj_big2) |
+----+-------------+----------+------+---------------+------+---------+------+------
+----------------------------------------------------------------+
3 rows in set (0.04 sec)
```

In der Ausgabe ist der `Hash Join Inner table` die Tabelle, die zum Aufbau der Hash-Tabelle verwendet wird, und der `Hash Join Outer table` ist die Tabelle, die zum Prüfen der Hash-Tabelle verwendet wird.

Weitere Informationen über das erweiterte `EXPLAIN`-Ausgabeformat finden Sie unter Extended EXPLAIN Output Format in der MySQL-Produktdokumentation.

In Aurora MySQL 2.08 und höher können Sie mithilfe von SQL-Hinweisen beeinflussen, ob eine Abfrage einen Hash-Join verwendet oder nicht und welche Tabellen für die Build- und Testseite des Joins verwendet werden sollen. Details hierzu finden Sie unter Aurora-MySQL-Hinweise.

Verwenden von Amazon Aurora für das Skalieren von Lesevorgängen in Ihrer MySQL-Datenbank

Sie können Amazon Aurora mit Ihrer MySQL-DB-Instance verwenden, um die Möglichkeiten der Skalierung von Lesevorgängen von Amazon Aurora zu nutzen und den Lese-Workload für Ihre MySQL-DB-Instance zu erweitern. Erstellen Sie einen Aurora-MySQL-DB-Cluster und machen Sie ihn zum Read Replica Ihrer MySQL-DB-Instance, um Aurora für die Skalierung von Lesevorgängen Ihrer MySQL-DB-Instance zu verwenden. Verbinden Sie sich dann mit dem Aurora-MySQL-Cluster,

um die Leseabfragen zu verarbeiten. Die Quelldatenbank kann eine RDS for MySQL-DB-Instance oder eine MySQL-Datenbank sein, die außerhalb von Amazon RDS ausgeführt wird. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora für das Skalieren von Lesevorgängen in Ihrer MySQL-Datenbank.

Optimierung von Zeitstempeloperationen

Wenn der Wert der Systemvariablen `time_zone` auf `SYSTEM` gesetzt ist, führt jeder MySQL-Funktionsaufruf, der eine Zeitzonenberechnung erfordert, einen Systembibliotheksaufruf aus. Wenn Sie SQL-Anweisungen ausführen, die solche `TIMESTAMP`-Werte mit hoher Nebenläufigkeit zurückgeben oder ändern, kann es zu einer höheren Latenz und CPU-Auslastung sowie zu Sperrkonflikten kommen. Weitere Informationen finden Sie unter time_zone in der MySQL-Dokumentation.

Wir empfehlen, den Wert des DB-Cluster-Parameters `time_zone` in `UTC` zu ändern, um dieses Verhalten zu vermeiden. Weitere Informationen finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe.

Der Parameter `time_zone` ist zwar dynamisch (er erfordert keinen Neustart des Datenbankservers), der neue Wert wird jedoch nur für neue Verbindungen verwendet. Um sicherzustellen, dass alle Verbindungen so aktualisiert werden, dass sie den neuen `time_zone`-Wert verwenden, empfehlen wir, Ihre Anwendungsverbindungen nach der Aktualisierung des DB-Cluster-Parameters wiederzuverwenden.

Bewährte Verfahren für die Hochverfügbarkeit von Aurora MySQL

Sie können die folgenden bewährten Verfahren anwenden, um die Verfügbarkeit Ihrer Aurora MySQL-Cluster zu verbessern.

Themen

- Verwenden von Amazon Aurora zur Notfallwiederherstellung Ihrer MySQL-Datenbanken
- Migrieren von MySQL zu Amazon Aurora MySQL mit reduzierter Ausfallzeit
- Vermeiden von Leistungseinbußen, automatischem Neustart und Failover für DB-Instances von Aurora MySQL

Verwenden von Amazon Aurora zur Notfallwiederherstellung Ihrer MySQL-Datenbanken

Sie können Amazon Aurora mit Ihrer MySQL-DB-Instance verwenden, um ein außerhalb liegendes Backup für eine Notfallwiederherstellung zu erstellen. Erstellen Sie einen Amazon-Aurora-DB-Cluster und legen Sie ihn als Read Replica Ihrer MySQL-DB-Instance fest, um Aurora für die Notfallwiederherstellung Ihrer MySQL-DB-Instance zu verwenden. Dies gilt für eine RDS for MySQL-DB-Instance oder eine MySQL-Datenbank, die außerhalb von Amazon RDS ausgeführt wird.

> **Important**
>
> Wenn Sie eine Replikation zwischen Ihrer MySQL-DB-Instance und einem Amazon-Aurora-MySQL-DB-Cluster einrichten, sollten Sie die Replikation prüfen, um sicherzustellen, dass sie sich in einem guten Zustand befindet, und sie bei Bedarf reparieren.

Anweisungen zum Erstellen eines Amazon-Aurora-MySQL-DB-Clusters und Festlegen als Read Replica Ihrer MySQL-DB-Instance finden Sie im Abschnitt Verwenden von Amazon Aurora für das Skalieren von Lesevorgängen in Ihrer MySQL-Datenbank.

Weitere Hinweise zu Notfallwiederherstellungsmodellen finden Sie unter So wählen Sie die beste Notfallwiederherstellungsoption für Ihren Amazon-Aurora-MySQL-Cluster aus.

Migrieren von MySQL zu Amazon Aurora MySQL mit reduzierter Ausfallzeit

Beim Importieren von Daten aus einer MySQL-Datenbank, die eine Live-Anwendung unterstützt, in einen Amazon-Aurora-MySQL-DB-Cluster möchten Sie möglicherweise die Zeit reduzieren, in der der Service während der Migration unterbrochen wird. Hierfür können Sie das Verfahren verwenden, das im Abschnitt zum Importieren von Daten in eine MySQL- oder MariaDB-DB-Instance mit reduzierter Ausfallzeit im Amazon Relational Database Service-Benutzerhandbuch dokumentiert ist. Diese Prozedur kann insbesondere dann hilfreich sein, wenn Sie mit einer sehr großen Datenbank arbeiten. Mit dieser Prozedur können Sie die Kosten des Imports reduzieren, indem Sie die Menge der Daten, die über das Netzwerk an AWS weitergeleitet werden, minimieren.

In der Prozedur sind Schritte zur Übertragung einer Kopie Ihrer Datenbank in eine Amazon EC2-Instance und zum Import der Daten in eine neue RDS for MySQL-DB-Instance aufgeführt. Da Amazon Aurora mit MySQL kompatibel ist, können Sie stattdessen einen Amazon-Aurora-DB-Cluster für die Amazon RDS-MySQL-DB-Ziel-Instance verwenden.

Vermeiden von Leistungseinbußen, automatischem Neustart und Failover für DB-Instances von Aurora MySQL

Wenn Sie hohe Workloads ausführen, die über die zugewiesenen Ressourcen Ihrer DB-Instance hinausgehen, können Sie die Ressourcen, auf denen Sie Ihre Anwendung und die Aurora-Datenbank ausführen, aufbrauchen. Um Metriken zu Ihrer Datenbank-Instance wie CPU-Auslastung, Speicherauslastung und Anzahl der verwendeten Datenbankverbindungen zu erhalten, können Sie auf die von Amazon CloudWatch, Performance Insights und Enhanced Monitoring bereitgestellten Metriken zurückgreifen. Informationen zur Überwachung Ihrer DB-Instance finden Sie unter Überwachung von Metriken in einem Amazon-Aurora-Cluster.

Wenn Ihre Workload die von Ihnen verwendeten Ressourcen aufbraucht, wird Ihre DB-Instance möglicherweise langsamer, neu gestartet oder es wird sogar ein Failover auf eine andere DB-Instance durchgeführt. Dies können Sie vermeiden, indem Sie Ihre Ressourcenauslastung überwachen, die Workload, die auf Ihrer DB-Instance ausgeführt wird, untersuchen und gegebenenfalls Optimierungen vornehmen. Wenn Optimierungen keine Verbesserungen der Instance-Metriken und keine Verringerung der Ressourcenauslastung ergeben, sollten Sie erwägen, Ihre DB-Instance hochzuskalieren, bevor diese an ihre Grenzen stößt. Weitere Hinweise zu verfügbaren DB-Instance-Klassen und ihren Spezifikationen finden Sie unter Aurora DB-Instance-Klassen.

Empfehlungen für Aurora MySQL

Die folgenden Funktionen sind in Aurora MySQL für die MySQL-Kompatibilität verfügbar. Sie haben jedoch Probleme mit der Leistung, Skalierbarkeit, Stabilität oder Kompatibilität in der Aurora-Umgebung. Wir empfehlen daher, dass Sie bei der Verwendung dieser Funktionen bestimmte Richtlinien einhalten. Wir empfehlen zum Beispiel, bestimmte Funktionen nicht für Aurora-Produktionseinsätze zu verwenden.

Themen

- Verwendung der Multithread-Replikation in Aurora MySQL
- AWS Lambda Funktionen mit nativen MySQL-Funktionen aufrufen
- Vermeiden von XA-Transaktionen mit Amazon Aurora MySQL
- Aktivieren von Fremdschlüsseln während DML-Anweisungen
- Konfigurieren, wie oft der Protokollpuffer geleert wird
- Minimieren und Beheben von Aurora-MySQL-Deadlocks

Verwendung der Multithread-Replikation in Aurora MySQL

Bei der Multithread-Replikation für binäre Protokolle liest ein SQL-Thread Ereignisse aus dem Relay-Log und stellt sie in die Warteschlange, damit SQL-Worker-Threads angewendet werden können. Die SQL-Worker-Threads werden von einem Koordinator-Thread verwaltet. Die binären Protokollereignisse werden nach Möglichkeit parallel angewendet.

Multithread-Replikation wird in Aurora MySQL Version 3 und in Aurora MySQL Version 2.12.1 und höher unterstützt.

Für Aurora MySQL-Versionen unter 3.04 verwendet Aurora standardmäßig die Single-Thread-Replikation, wenn ein Aurora MySQL-DB-Cluster als Read Replica für die binäre Protokollreplikation verwendet wird.

Frühere Versionen von Aurora MySQL Version 2 haben mehrere Probleme mit der Multithread-Replikation aus der MySQL Community Edition übernommen. Für diese Versionen empfehlen wir, die Multithread-Replikation in der Produktion nicht zu verwenden.

Wenn Sie die Multithread-Replikation verwenden, empfehlen wir, sie gründlich zu testen.

Weitere Informationen zur Verwendung der Replikation in Amazon Aurora finden Sie unter Replikation mit Amazon Aurora. Weitere Hinweise zur Multithread-Replikation in Aurora MySQL finden Sie unterReplikation von binären Protokollen mit mehreren Threads.

AWS Lambda Funktionen mit nativen MySQL-Funktionen aufrufen

Wir empfehlen, die nativen MySQL-Funktionen `lambda_sync` und `lambda_async` zu verwenden, um Lambda-Funktionen aufzurufen.

Wenn Sie die veraltete Prozedur `mysql.lambda_async` verwenden, empfehlen wir, dass Sie die Aufrufe an die Prozedur `mysql.lambda_async` in einer gespeicherten Prozedur übergeben. Sie können diese gespeicherte Prozedur aus verschiedenen Quellen aufrufen, wie z. B. Trigger oder Client-Code. Dieser Ansatz kann helfen, Probleme hinsichtlich Impedanz-Unstimmigkeiten zu vermeiden und macht es Ihren Datenbank-Programmieren einfacher Lambda-Funktionen aufzurufen.

Weitere Informationen über das Aufrufen von Lambda-Funktionen in Amazon Aurora finden Sie unter Aufrufen einer Lambda-Funktion aus einem Amazon Aurora MySQL-DB-Cluster.

Vermeiden von XA-Transaktionen mit Amazon Aurora MySQL

Wir empfehlen Ihnen, keine eXtended Architecture (XA)-Transaktionen mit Aurora MySQL zu verwenden, da diese lange Wiederherstellungszeiten verursachen können, wenn sich die XA im

Status `PREPARED` befunden hat. Wenn Sie XA-Transaktionen mit Aurora MySQL verwenden müssen, befolgen Sie diese bewährten Verfahren:

- Lassen Sie eine XA-Transaktion nicht im Status `PREPARED` offen.
- Halten Sie XA-Transaktionen so klein wie möglich.

Weitere Informationen zur Verwendung von XA-Transaktionen mit MySQL finden Sie unter XA Transactions in der MySQL-Dokumentation.

Aktivieren von Fremdschlüsseln während DML-Anweisungen

Wir empfehlen Ihnen dringend, keine DDL-Anweisungen (Data Definition Language) auszuführen, wenn die Variable `foreign_key_checks` auf `0` (aus) gesetzt ist.

Wenn Sie Zeilen einfügen oder aktualisieren müssen, die eine vorübergehende Verletzung von Fremdschlüsseln bedingen, gehen Sie wie folgt vor:

1. Setzen Sie `foreign_key_checks` auf `0`.
2. Nehmen Sie Ihre DML-Änderungen (Data Manipulation Language) vor.
3. Stellen Sie sicher, dass Ihre durchgeführten Änderungen keine Fremdschlüsselbedingungen verletzen.
4. Setzen Sie `foreign_key_checks` auf `1` (ein).

Darüber hinaus halten Sie die folgenden anderen bewährten Methoden für Fremdschlüsselbedingungen ein:

- Stellen Sie sicher, dass Ihre Client-Anwendungen die Variable `foreign_key_checks` nicht auf `0` als Teil der Variablen `init_connect` setzen.
- Wenn eine Wiederherstellung aus einer logischen Sicherung, wie beispielsweise `mysqldump`, fehlschlägt oder unvollständig ist, stellen Sie sicher, dass `foreign_key_checks` auf `1` gesetzt ist, bevor Sie innerhalb derselben Sitzung andere Operationen starten. Eine logische Sicherung setzt `foreign_key_checks` beim Start auf `0`.

Konfigurieren, wie oft der Protokollpuffer geleert wird

In der MySQL Community Edition muss der InnoDB-Protokollpuffer in einen dauerhaften Speicher geleert werden, um Transaktionen dauerhaft zu machen. Verwenden Sie den Parameter

`innodb_flush_log_at_trx_commit`, um zu konfigurieren, wie oft der Protokollpuffer geleert und auf die Festplatte übertragen wird.

Wenn Sie den Parameter `innodb_flush_log_at_trx_commit` auf den Standardwert 1 festlegen, wird der Protokollpuffer bei jedem Transaktions-Commit geleert. Diese Einstellung hilft, die Datenbank ACID-konform zu halten. Wir empfehlen, die Standardeinstellung 1 beizubehalten.

Das Ändern `innodb_flush_log_at_trx_commit` zu einem anderen Wert als dem Standardwert kann dazu beitragen, die Latenz in der Datenmanipulationssprache (Data Manipulation Language, DML) zu reduzieren, beeinträchtigt jedoch die Haltbarkeit der Protokolldatensätze. Durch diese mangelnde Haltbarkeit ist die Datenbank nicht ACID-konform. Ihre Datenbanken sollten ACID-konform sein, um das Risiko von Datenverlusten bei einem Serverneustart zu vermeiden. Weitere Informationen zu diesem Parameter finden Sie unter innodb_flush_log_at_trx_commit in der MySQL-Dokumentation.

In Aurora MySQL wird die Redo-Protokollverarbeitung auf die Speicherschicht verlagert, sodass auf der DB-Instance kein Leeren in Protokolldateien erfolgt. Wenn ein Schreibvorgang ausgeführt wird, werden Redo-Protokolle von der Writer-DB-Instance direkt an das Aurora-Cluster-Volume gesendet. Die einzigen Schreibvorgänge, die das Netzwerk passieren, sind Redo-Protokolldatensätze. Auf der Datenbankebene werden grundsätzlich keine Seiten geschrieben.

Standardmäßig wartet jeder Thread, der eine Transaktion festschreibt, auf die Bestätigung durch das Aurora-Cluster-Volume. Diese Bestätigung gibt an, dass dieser Datensatz und alle vorherigen Redo-Protokolldatensätze geschrieben wurden und das Quorum erreicht haben. Dadurch, dass die Protokolldatensätze beibehalten und das Quorum erreicht wird, ist die Transaktion dauerhaft gemacht worden, sei es durch Autocommit oder explizites Commit. Weitere Informationen zur Aurora-Speicherarchitektur finden Sie unter Amazon Aurora storage demystified (Amazon-Aurora-Speicher entmystifiziert).

Aurora MySQL leert keine Protokolle in Datendateien, wie dies bei der MySQL Community Edition der Fall ist. Sie können den Parameter `innodb_flush_log_at_trx_commit` jedoch verwenden, um Haltbarkeitsbeschränkungen beim Schreiben von Redo-Protokolldatensätzen auf das Aurora-Clustervolume zu lockern.

Für Aurora MySQL Version 2:

- `innodb_flush_log_at_trx_commit`= 0 oder 2 — Die Datenbank wartet nicht auf die Bestätigung, dass die Redo-Log-Datensätze auf das Aurora-Cluster-Volume geschrieben wurden.

- `innodb_flush_log_at_trx_commit=` 1 — Die Datenbank wartet auf die Bestätigung, dass die Redo-Log-Datensätze auf das Aurora-Cluster-Volume geschrieben wurden.

Für Aurora MySQL Version 3:

- `innodb_flush_log_at_trx_commit=` 0 — Die Datenbank wartet nicht auf die Bestätigung, dass die Redo-Log-Datensätze auf das Aurora-Cluster-Volume geschrieben wurden.
- `innodb_flush_log_at_trx_commit=` 1 oder 2 — Die Datenbank wartet auf die Bestätigung, dass die Redo-Log-Datensätze auf das Aurora-Cluster-Volume geschrieben wurden.

Um in Aurora MySQL Version 3 dasselbe nicht standardmäßige Verhalten zu erzielen, das Sie mit dem Wert 0 oder 2 in Aurora MySQL Version 2 erzielen würden, setzen Sie den Parameter daher auf 0.

Diese Einstellungen können zwar die DML-Latenz für den Client verringern, sie können im Falle eines Failovers oder Neustarts aber auch zu Datenverlust führen. Daher empfehlen wir, für den Parameter `innodb_flush_log_at_trx_commit` den Standardwert 1 beizubehalten.

Während Datenverlust sowohl bei der MySQL Community Edition als auch bei Aurora MySQL auftreten kann, unterscheidet sich das Verhalten in jeder Datenbank aufgrund ihrer unterschiedlichen Architekturen. Diese Unterschiede in der Architektur können zu unterschiedlich starkem Datenverlust führen. damit sichergestellt wird, dass Ihre Datenbank ACID-konform ist, legen Sie `innodb_flush_log_at_trx_commit` immer auf den Wert 1 fest.

> **Note**
>
> Bevor Sie in Aurora MySQL Version 3 `innodb_flush_log_at_trx_commit` zu einem anderen Wert als 1 wechseln können, müssen Sie zuerst den Wert von `innodb_trx_commit_allow_data_loss` auf 1 ändern. Auf diese Weise erkennen Sie das Risiko eines Datenverlusts an.

Minimieren und Beheben von Aurora-MySQL-Deadlocks

Bei Benutzern, die Workloads ausführen, bei denen regelmäßig Einschränkungen für eindeutige sekundäre Indizes oder Fremdschlüssel verletzt werden, kann es bei der gleichzeitigen Änderung von Datensätzen auf derselben Datenseite zu erhöhten Deadlocks und Wartezeitüberschreitungen

bei Sperren kommen. Diese Deadlocks und Zeitüberschreitungen sind auf einen Bugfix der MySQL Community Edition zurückzuführen.

Dieser Bugfix ist in den MySQL-Community-Edition-Versionen 5.7.26 und höher enthalten und wurde in die Aurora-MySQL-Versionen 2.10.3 und höher zurückportiert. Der Bugfix ist notwendig, um die Serialisierbarkeit zu erzwingen, indem zusätzliche Sperren für diese Arten von Data Manipulation Language (DML)-Operationen für Änderungen an Datensätzen in einer InnoDB-Tabelle implementiert werden. Dieses Problem wurde im Rahmen einer Untersuchung von Deadlock-Problemen aufgedeckt, die durch einen früheren Bugfix der MySQL Community Edition verursacht wurden.

Mit dem Bugfix wurde die interne Behandlung für das teilweise Rollback eines Tupel-(Zeilen-)Updates in der InnoDB-Speicher-Engine geändert. Operationen, die zu Einschränkungsverstößen bei Fremdschlüsseln oder eindeutigen Sekundärindizes führen, verursachen ein partielles Rollback. Dies beinhaltet, ist aber nicht beschränkt auf gleichzeitige `INSERT...ON DUPLICATE KEY UPDATE`-, `REPLACE INTO`,- und `INSERT IGNORE`-Anweisungen (upserts).

In diesem Zusammenhang bezieht sich partielles Rollback nicht auf das Rollback von Transaktionen auf Anwendungsebene, sondern auf ein internes InnoDB-Rollback von Änderungen an einem gruppierten Index, wenn ein Einschränkungsverstoß auftritt. Beispielsweise wird während einer Upsert-Operation ein doppelter Schlüsselwert gefunden.

In einem normalen Einfügevorgang erstellt InnoDB automatisch gruppierte und sekundäre Indexeinträge für jeden Index. Wenn InnoDB während einer Upsert-Operation einen doppelten Wert in einem eindeutigen sekundären Index erkennt, muss der eingefügte Eintrag im gruppierten Index rückgängig gemacht werden (partielles Rollback), und die Aktualisierung muss dann auf die vorhandene doppelte Zeile angewendet werden. Während dieses internen partiellen Rollback-Schritts muss InnoDB jeden Datensatz sperren, der als Teil des Vorgangs angezeigt wird. Der Bugfix gewährleistet die Serialisierbarkeit von Transaktionen, indem nach dem partiellen Rollback eine zusätzliche Sperrung eingeführt wird.

Minimieren von InnoDB-Deadlocks

Sie können die folgenden Ansätze verwenden, um die Häufigkeit von Deadlocks in Ihrer Datenbank-Instance zu reduzieren. Weitere Beispiele finden Sie in der MySQL-Dokumentation.

1. Um die Wahrscheinlichkeit von Deadlocks zu verringern, sollten Sie für Transaktionen sofort einen Commit ausführen, nachdem Sie die entsprechenden Änderungen vorgenommen haben.

Teilen Sie dazu große Transaktionen (mehrere Zeilenaktualisierungen zwischen Commits) in kleinere Transaktionen auf. Wenn Sie Zeilen stapelweise einfügen, versuchen Sie, die Größe der Stapeleinfügungen zu reduzieren, insbesondere wenn Sie die zuvor genannten Upsert-Operationen verwenden.

Um die Anzahl möglicher partieller Rollbacks zu reduzieren, können Sie einige der folgenden Ansätze ausprobieren:

a. Ersetzen Sie Batch-Einfügeoperationen durch das Einfügen einer Zeile nach der anderen. Dadurch kann die Zeit reduziert werden, in der Sperren aufgrund von Transaktionen, die möglicherweise zu Konflikten führen, aufrechterhalten bleiben.

b. Anstatt `REPLACE INTO` zu verwenden, schreiben Sie die SQL-Anweisung in eine Transaktion mit mehreren Anweisungen um, z. B. die folgende:

```
BEGIN;
DELETE conflicting rows;
INSERT new rows;
COMMIT;
```

c. Anstatt `INSERT...ON DUPLICATE KEY UPDATE` zu verwenden, schreiben Sie die SQL-Anweisung in eine Transaktion mit mehreren Anweisungen um, z. B. die folgende:

```
BEGIN;
SELECT rows that conflict on secondary indexes;
UPDATE conflicting rows;
INSERT new rows;
COMMIT;
```

2. Vermeiden Sie lang dauernde Transaktionen, ob aktiv oder inaktiv, die Sperren möglicherweise aufrechterhalten. Dazu gehören interaktive MySQL-Client-Sitzungen, die möglicherweise über einen längeren Zeitraum geöffnet sind, wenn für eine Transaktion kein Commit ausgeführt wird. Bei der Optimierung von Transaktionsgrößen oder Batch-Größen können die Auswirkungen in Abhängigkeit von einer Reihe von Faktoren wie Parallelität, Anzahl der Duplikate und Tabellenstruktur variieren. Alle Änderungen sollten auf der Grundlage Ihrer Workload implementiert und getestet werden.
3. In einigen Situationen können Deadlocks auftreten, wenn zwei Transaktionen versuchen, auf dieselben Datensätze, entweder in einer oder mehreren Tabellen, in unterschiedlicher Reihenfolge zuzugreifen. Um dies zu verhindern, können Sie die Transaktionen so ändern, dass sie in derselben Reihenfolge auf die Daten zugreifen, wodurch der Zugriff serialisiert wird. Erstellen Sie

beispielsweise eine Warteschlange mit Transaktionen, die abgeschlossen werden sollen. Dieser Ansatz kann dazu beitragen, Deadlocks zu vermeiden, wenn mehrere Transaktionen gleichzeitig stattfinden.

4. Durch Hinzufügen sorgfältig ausgewählter Indizes zu Ihren Tabellen lässt sich die Selektivität verbessern und die Notwendigkeit, auf Zeilen zuzugreifen, reduzieren, was zu weniger Sperren führt.
5. Wenn Sie auf eine Lückensperre stoßen, können Sie die Transaktionsisolationsstufe für die Sitzung oder Transaktion in `READ COMMITTED` ändern, um dies zu verhindern. Weitere Informationen zu InnoDB-Isolationsstufen und ihrem Verhalten finden Sie unter Transaktionsisolationsstufen in der MySQL-Dokumentation.

> **Note**
>
> Sie können zwar Vorkehrungen treffen, um die Wahrscheinlichkeit von Deadlocks zu verringern, Deadlocks sind jedoch ein erwartetes Datenbankverhalten und können dennoch auftreten. Anwendungen sollten über die erforderliche Logik zum Umgang mit Deadlocks verfügen, wenn diese auftreten. Implementieren Sie beispielsweise die Wiederholungs- und Back-Off-Logik in der Anwendung. Es ist am besten, die Ursache des Problems zu beheben. Wenn jedoch ein Deadlock auftritt, hat die Anwendung die Möglichkeit, zu warten und es erneut zu versuchen.

Überwachen von InnoDB-Deadlocks

Deadlocks können in MySQL auftreten, wenn Anwendungstransaktionen versuchen, Sperren auf Tabellen- und Zeilenebene so zu umgehen, dass zirkuläres Warten entsteht. Ein gelegentlicher InnoDB-Deadlock ist nicht unbedingt ein Problem, da die InnoDB-Speicher-Engine den Zustand sofort erkennt und für eine der Transaktionen automatisch ein Rollback durchführt. Wenn Sie häufig auf Deadlocks stoßen, empfehlen wir, Ihre Anwendung zu überprüfen und zu ändern, um Leistungsprobleme zu verringern und Deadlocks zu vermeiden. Wenn die Deadlock-Erkennung aktiviert ist (Standard), erkennt InnoDB automatisch Transaktions-Deadlocks und führt ein Rollback für eine oder mehrere Transaktionen durch, um den Deadlock zu durchbrechen. InnoDB versucht, kleine Transaktionen für das Rollback auszuwählen, wobei die Größe einer Transaktion durch die Anzahl der eingefügten, aktualisierten oder gelöschten Zeilen bestimmt wird.

- `SHOW ENGINE`-Anweisung – Die `SHOW ENGINE INNODB STATUS \G`-Anweisung enthält Details zum letzten Deadlock, der seit dem letzten Neustart in der Datenbank aufgetreten ist.

- MySQL-Fehlerprotokoll – Wenn Sie häufig auf Deadlocks stoßen, bei denen die Ausgabe der `SHOW ENGINE`-Anweisung unangemessen ist, können Sie den DB-Cluster-Parameter innodb_print_all_deadlocks aktivieren.

  Wenn dieser Parameter aktiviert ist, werden Informationen über alle Deadlocks in InnoDB-Benutzertransaktionen im Fehlerprotokoll von Aurora MySQL aufgezeichnet.
- CloudWatch Amazon-Metriken — Wir empfehlen Ihnen außerdem, Deadlocks anhand der CloudWatch Metrik proaktiv zu überwachen. `Deadlocks` Weitere Informationen finden Sie unter Metriken auf Instance-Ebene für Amazon Aurora.
- Amazon CloudWatch Logs — Mit CloudWatch Logs können Sie Metriken anzeigen, Protokolldaten analysieren und Alarme in Echtzeit erstellen. Weitere Informationen finden Sie unter Überwachen von Fehlern in Amazon Aurora MySQL und Amazon RDS for MySQL mithilfe von Amazon CloudWatch und Senden von Benachrichtigungen mithilfe von Amazon SNS.

  Wenn Sie CloudWatch Logs verwenden, wenn diese Option `innodb_print_all_deadlocks` aktiviert ist, können Sie Alarme so konfigurieren, dass Sie benachrichtigt werden, wenn die Anzahl der Deadlocks einen bestimmten Schwellenwert überschreitet. Wenn Sie einen Schwellenwert definieren möchten, empfehlen wir Ihnen, Ihre Trends zu beobachten und einen Wert zu verwenden, der auf Ihrer normalen Workload basiert.
- Performance Insights – Wenn Sie Performance Insights verwenden, können Sie die Metriken `innodb_deadlocks` und `innodb_lock_wait_timeout` überwachen. Weitere Informationen zu diesen Metriken, finden Sie unter Nicht-native Zähler für Aurora MySQL.

Fehlerbehebung bei der Leistung der Amazon Aurora MySQL-Datenbank

Dieses Thema konzentriert sich auf einige häufig auftretende Leistungsprobleme mit Aurora MySQL DB und darauf, wie Sie diese Probleme beheben oder Informationen sammeln können, um diese Probleme schnell zu beheben. Wir unterteilen die Datenbankleistung in zwei Kategorien:

- Serverleistung — Der gesamte Datenbankserver läuft langsamer.
- Abfrageleistung — Die Ausführung einer oder mehrerer Abfragen dauert länger.

AWS Optionen zur Überwachung

Wir empfehlen Ihnen, die folgenden AWS Überwachungsoptionen zu verwenden, um bei der Fehlerbehebung zu helfen:

- Amazon CloudWatch — Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können CloudWatch damit Metriken sammeln und verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Ressourcen und Anwendungen messen können. Weitere Informationen finden Sie unter Was ist Amazon CloudWatch? .

  Sie können alle Systemmetriken und Prozessinformationen für Ihre DB-Instances auf der einsehen AWS Management Console. Sie können Ihren Aurora MySQL-DB-Cluster so konfigurieren, dass er allgemeine, langsame Protokolldaten, Prüfdaten und Fehlerprotokolldaten in einer Protokollgruppe in Amazon CloudWatch Logs veröffentlicht. Auf diese Weise können Sie Trends einsehen, Protokolle verwalten, falls ein Host betroffen ist, und eine Ausgangsbasis für eine „normale“ Leistung erstellen, um Anomalien oder Änderungen leicht zu identifizieren. Weitere Informationen finden Sie unter Veröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs.
- Verbesserte Überwachung — Um zusätzliche CloudWatch Amazon-Metriken für eine Aurora MySQL-Datenbank zu aktivieren, aktivieren Sie Enhanced Monitoring. Wenn Sie einen Aurora-DB-Cluster erstellen oder ändern, wählen Sie Enable Enhanced Monitoring aus. Auf diese Weise kann Aurora Leistungskennzahlen veröffentlichen CloudWatch. Zu den wichtigsten verfügbaren Kennzahlen gehören CPU-Auslastung, Datenbankverbindungen, Speichernutzung und Abfragelatenz. Diese können helfen, Leistungsengpässe zu identifizieren.

Die Menge der für eine DB-Instance übertragenen Informationen ist direkt proportional zur definierten Granularität für Enhanced Monitoring. Ein kürzeres Überwachungsintervall führt zu häufigeren Berichten über Betriebssystem-Metriken und erhöht Ihre Überwachungskosten. Um die Kosten zu verwalten, legen Sie unterschiedliche Granularitäten für verschiedene Instances in Ihrem fest. AWS-Konten Die Standardgranularität bei der Erstellung einer Instanz beträgt 60 Sekunden. Weitere Informationen finden Sie unter Kosten für „Enhanced Monitoring“ (Erweiterte Überwachung).

- Performance Insights — Sie können alle Metriken für Datenbankaufrufe anzeigen. Dazu gehören DB-Sperren, Wartezeiten und die Anzahl der verarbeiteten Zeilen, die Sie alle zur Fehlerbehebung verwenden können. Wenn Sie einen Aurora-DB-Cluster erstellen oder ändern, wählen Sie Performance Insights aktivieren aus. Standardmäßig hat Performance Insights eine Datenaufbewahrungsfrist von 7 Tagen, kann jedoch angepasst werden, um längerfristige Leistungstrends zu analysieren. Für eine Aufbewahrung von mehr als 7 Tagen müssen Sie auf die kostenpflichtige Stufe umsteigen. Weitere Informationen finden Sie unter Preise für Performance Insights. Sie können den Datenaufbewahrungszeitraum für jede Aurora-DB-Instance separat festlegen. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .

Die häufigsten Gründe für Leistungsprobleme mit der Aurora MySQL-Datenbank

Sie können die folgenden Schritte verwenden, um Leistungsprobleme in Ihrer Aurora MySQL-Datenbank zu beheben. Wir listen diese Schritte in der logischen Reihenfolge der Untersuchung auf, sie sollen jedoch nicht linear ablaufen. Bei einer Entdeckung könnten mehrere Schritte übersprungen werden, was wiederum eine Reihe von Ermittlungswegen ermöglicht.

1. Arbeitslast — Machen Sie sich mit Ihrer Datenbank-Arbeitslast vertraut.
2. Protokollierung — Überprüfen Sie alle Datenbankprotokolle.
3. Abfrageleistung — Untersuchen Sie Ihre Pläne zur Abfrageausführung, um festzustellen, ob sie sich geändert haben. Codeänderungen können dazu führen, dass sich Pläne ändern.

Behebung von Workload-Problemen für Aurora MySQL-Datenbanken

Die Datenbank-Arbeitslast kann als Lese- und Schreibvorgänge betrachtet werden. Wenn Sie sich mit der „normalen“ Datenbank-Arbeitslast auskennen, können Sie Abfragen und den Datenbankserver

an die sich ändernde Nachfrage anpassen. Es gibt eine Reihe verschiedener Gründe, warum sich die Leistung ändern kann. Der erste Schritt besteht also darin, zu verstehen, was sich geändert hat.

- Gab es ein Upgrade der Haupt- oder Nebenversion?

  Ein Hauptversionsupgrade beinhaltet Änderungen am Engine-Code, insbesondere am Optimizer, die den Ausführungsplan der Abfrage ändern können. Bei der Aktualisierung von Datenbankversionen, insbesondere von Hauptversionen, ist es sehr wichtig, dass Sie die Datenbank-Arbeitslast analysieren und entsprechend optimieren. Abhängig von den Testergebnissen kann das Optimieren und Neuschreiben von Abfragen oder das Hinzufügen und Aktualisieren von Parametereinstellungen beinhalten. Wenn Sie verstehen, was die Auswirkungen verursacht, können Sie sich auf diesen speziellen Bereich konzentrieren.

  Weitere Informationen finden Sie unter Was ist neu in MySQL 8.0 und Server und in MySQL 8.0 hinzugefügte, veraltete oder entfernte Statusvariablen und -optionen in der MySQL-Dokumentation und. Vergleich von Aurora-MySQL-Version 2 und Aurora-MySQL-Version 3
- Hat die Anzahl der verarbeiteten Daten zugenommen (Zeilenanzahl)?
- Werden mehr Abfragen gleichzeitig ausgeführt?
- Gibt es Schema- oder Datenbankänderungen?
- Gab es Codefehler oder Korrekturen?

Inhalt

Metriken für Instance-Hosts

Überwachen Sie Instance-Host-Metriken wie CPU, Arbeitsspeicher und Netzwerkaktivität, um besser zu verstehen, ob sich die Arbeitslast geändert hat. Es gibt zwei Hauptkonzepte für das Verständnis von Workload-Änderungen:

- Auslastung — Die Nutzung eines Geräts, z. B. einer CPU oder einer Festplatte. Sie kann zeit- oder kapazitätsbasiert sein.
  - Zeitbasiert — Die Zeit, in der eine Ressource während eines bestimmten Beobachtungszeitraums ausgelastet ist.
  - Kapazitätsbasiert — Der Durchsatz, den ein System oder eine Komponente liefern kann, als Prozentsatz der Kapazität.
- Sättigung — Der Grad, in dem eine Ressource mehr Arbeit benötigt, als sie verarbeiten kann. Wenn die kapazitätsabhängige Nutzung 100% erreicht, kann die zusätzliche Arbeit nicht verarbeitet werden und muss in die Warteschlange gestellt werden.

CPU-Verwendung

Sie können die folgenden Tools verwenden, um die CPU-Auslastung und -Auslastung zu ermitteln:

- CloudWatch stellt die `CPUUtilization` Metrik bereit. Wenn dieser Wert 100% erreicht, ist die Instanz voll ausgelastet. Die CloudWatch Metriken werden jedoch über einen Zeitraum von 1 Minute gemittelt und es fehlt ihnen an Granularität.

  Weitere Informationen zu CloudWatch Metriken finden Sie unter. Metriken auf Instance-Ebene für Amazon Aurora
- Enhanced Monitoring stellt Metriken bereit, die vom `top` Betriebssystembefehl zurückgegeben werden. Es zeigt die durchschnittliche Auslastung und die folgenden CPU-Status mit einer Genauigkeit von 1 Sekunde an:
  - `Idle (%)`= Leerlaufzeit
  - `IRQ (%)`= Softwareunterbrechungen
  - `Nice (%)`= Gute Zeit für Prozesse mit einer schönen Priorität.
  - `Steal (%)`= Zeit, die für die Betreuung anderer Mandanten aufgewendet wurde (im Zusammenhang mit Virtualisierung)
  - `System (%)`= Systemzeit
  - `User (%)`= Benutzerzeit

- `Wait (%)`= I/O warten

Weitere Informationen zu Enhanced Monitoring-Metriken finden Sie unterBetriebssystemmetriken für Aurora.

Speicherauslastung

Wenn das System unter Speicherauslastung steht und der Ressourcenverbrauch die Obergrenze erreicht, sollten Sie ein hohes Maß an Seitenscans, Seitenauslagerungen, Auslagerungen und out-of-memory Fehlern beobachten.

Sie können die folgenden Tools verwenden, um den Speicherverbrauch und die Speicherauslastung zu ermitteln:

CloudWatch stellt die `FreeableMemory` Metrik bereit, die angibt, wie viel Speicher durch Leeren einiger Betriebssystem-Caches und den aktuell freien Speicher zurückgewonnen werden kann.

Weitere Informationen zu CloudWatch Metriken finden Sie unter. Metriken auf Instance-Ebene für Amazon Aurora

Enhanced Monitoring bietet die folgenden Messwerte, anhand derer Sie Probleme mit der Speichernutzung identifizieren können:

- `Buffers (KB)`— Die Speichermenge, die für die Pufferung von I/O-Anfragen vor dem Schreiben auf das Speichergerät verwendet wird, in Kilobyte.
- `Cached (KB)`— Die Speichermenge, die für das Zwischenspeichern dateisystembasierter I/O verwendet wird.
- `Free (KB)`— Die Menge des nicht zugewiesenen Speichers in Kilobyte.
- `Swap`— Zwischengespeichert, Kostenlos und Insgesamt.

Wenn Sie beispielsweise feststellen, dass Ihre DB-Instance `Swap` Arbeitsspeicher verwendet, ist der Gesamtspeicher für Ihren Workload größer, als Ihre Instance derzeit zur Verfügung hat. Wir empfehlen, die Größe Ihrer DB-Instance zu erhöhen oder Ihre Arbeitslast so zu optimieren, dass weniger Speicher verwendet wird.

Weitere Informationen zu Enhanced Monitoring-Metriken finden Sie unterBetriebssystemmetriken für Aurora.

Ausführlichere Informationen zur Verwendung des Leistungsschemas und des `sys` Schemas zur Bestimmung, welche Verbindungen und Komponenten Speicher verwenden, finden Sie unterBehebung von Problemen mit der Speichernutzung für Aurora MySQL-Datenbanken.

Netzwerkdurchsatz

CloudWatch bietet die folgenden Messwerte für den gesamten Netzwerkdurchsatz, jeweils gemittelt über 1 Minute:

- `NetworkReceiveThroughput`— Die Menge des Netzwerkdurchsatzes, den jede Instance im Aurora-DB-Cluster von Clients erhält.
- `NetworkTransmitThroughput`— Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Aurora-DB-Cluster an Clients gesendet wird.
- `NetworkThroughput`— Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Aurora-DB-Cluster sowohl von Clients empfangen als auch an diese übertragen wird.
- `StorageNetworkReceiveThroughput`— Die Menge des Netzwerkdurchsatzes, den jede Instance im DB-Cluster vom Aurora-Speichersubsystem erhält.
- `StorageNetworkTransmitThroughput`— Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Aurora-DB-Cluster an das Aurora-Speichersubsystem gesendet wird.
- `StorageNetworkThroughput`— Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Aurora-DB-Cluster vom Aurora-Speichersubsystem empfangen und an dieses gesendet wird.

Weitere Informationen zu CloudWatch Metriken finden Sie unterMetriken auf Instance-Ebene für Amazon Aurora.

Enhanced Monitoring stellt die `network` empfangenen (RX) und übertragenen (TX) Diagramme mit einer Genauigkeit von bis zu 1 Sekunde bereit.

Weitere Informationen zu Enhanced Monitoring-Metriken finden Sie unter. Betriebssystemmetriken für Aurora

Datenbankmetriken

Untersuchen Sie die folgenden CloudWatch Metriken auf Workload-Änderungen:

- `BlockedTransactions`— Die durchschnittliche Anzahl von Transaktionen in der Datenbank, die pro Sekunde blockiert werden.

- `BufferCacheHitRatio`— Der Prozentsatz der Anfragen, die vom Buffer Cache bedient werden.
- `CommitThroughput`— Die durchschnittliche Anzahl von Commit-Vorgängen pro Sekunde.
- `DatabaseConnections`— Die Anzahl der Client-Netzwerkverbindungen zur Datenbank-Instance.
- `Deadlocks`— Die durchschnittliche Anzahl von Deadlocks in der Datenbank pro Sekunde.
- `DMLThroughput`— Die durchschnittliche Anzahl von Einfügungen, Aktualisierungen und Löschungen pro Sekunde.
- `ResultSetCacheHitRatio`— Der Prozentsatz der Anfragen, die vom Abfrage-Cache bedient werden.
- `RollbackSegmentHistoryListLength`— Die Undo-Logs, in denen festgeschriebene Transaktionen mit mit „Löschen“ markierten Datensätzen aufgezeichnet werden.
- `RowLockTime`— Die Gesamtzeit, die für den Erwerb von Zeilensperren für InnoDB-Tabellen aufgewendet wurde.
- `SelectThroughput`— Die durchschnittliche Anzahl von ausgewählten Abfragen pro Sekunde.

Weitere Informationen zu CloudWatch Metriken finden Sie unterMetriken auf Instance-Ebene für Amazon Aurora.

Beachten Sie bei der Untersuchung der Arbeitslast die folgenden Fragen:

1. Gab es kürzlich Änderungen an der DB-Instance-Klasse, z. B. die Reduzierung der Instance-Größe von 8xlarge auf 4xlarge oder die Umstellung von db.r5 auf db.r6?
2. Können Sie einen Clone erstellen und das Problem reproduzieren, oder tritt es nur auf dieser einen Instance auf?
3. Liegt eine Erschöpfung der Serverressourcen, eine hohe CPU- oder Speicherauslastung vor? Falls ja, könnte dies bedeuten, dass zusätzliche Hardware erforderlich ist.
4. Dauern eine oder mehrere Abfragen länger?
5. Werden die Änderungen durch ein Upgrade verursacht, insbesondere durch ein Upgrade einer Hauptversion? Falls ja, vergleichen Sie die Metriken vor und nach dem Upgrade.
6. Gibt es Änderungen in der Anzahl der Reader-DB-Instances?
7. Haben Sie die allgemeine Protokollierung, die Prüfprotokollierung oder die binäre Protokollierung aktiviert? Weitere Informationen finden Sie unter Protokollierung für Aurora MySQL-Datenbanken.
8. Haben Sie Ihre Verwendung der Binärprotokollreplikation (Binlog) aktiviert, deaktiviert oder geändert?

9. Gibt es Transaktionen mit langer Laufzeit, die eine große Anzahl von Zeilensperren enthalten? Untersuchen Sie die Länge der InnoDB-Verlaufsliste (HLL) auf Hinweise auf lang andauernde Transaktionen.

   Weitere Informationen finden Sie unter Die Länge der InnoDB-Verlaufsliste wurde deutlich erhöht und im Blogbeitrag Warum läuft meine SELECT-Abfrage langsam auf meinem Amazon Aurora MySQL-DB-Cluster? .

   a. Wenn eine große HLL durch eine Schreibtransaktion verursacht wird, bedeutet dies, dass sich UNDO Protokolle ansammeln (die nicht regelmäßig bereinigt werden). Bei einer großen Schreibtransaktion kann diese Akkumulation schnell zunehmen. In MySQL UNDO ist es im SYSTEM-Tablespace gespeichert. Der SYSTEM Tablespace ist nicht verkleinerbar. Das UNDO Protokoll kann dazu führen, dass der SYSTEM Tablespace auf mehrere GB oder sogar TB anwächst. Geben Sie nach dem Löschen den zugewiesenen Speicherplatz frei, indem Sie ein logisches Backup (Dump) der Daten erstellen und das Speicherabbild anschließend in eine neue DB-Instance importieren.

   b. Wenn eine große HLL durch eine Lesetransaktion (lang andauernde Abfrage) verursacht wird, kann dies bedeuten, dass die Abfrage eine große Menge an temporärem Speicherplatz belegt. Geben Sie den temporären Speicherplatz durch einen Neustart frei. Untersuchen Sie die Performance Insights DB-Metriken auf Änderungen in Temp diesem Abschnitt, z. `created_tmp_tables` B. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .

10. Können Sie Transaktionen mit langer Laufzeit in kleinere Transaktionen aufteilen, bei denen weniger Zeilen geändert werden?

11. Gibt es Änderungen bei blockierten Transaktionen oder eine Zunahme von Deadlocks? Untersuchen Sie die Performance Insights DB-Metriken auf Änderungen der Statusvariablen im Locks Abschnitt`innodb_row_lock_time`, wie `innodb_row_lock_waits`, und `innodb_dead_locks`. Verwenden Sie Intervalle von 1 Minute oder 5 Minuten.

12. Gibt es erhöhte Wartezeiten? Untersuchen Sie Performance Insights Warteereignisse und Wartearten in Intervallen von 1 Minute oder 5 Minuten. Analysieren Sie die wichtigsten Warteereignisse und finden Sie heraus, ob sie mit Workload-Änderungen oder Datenbankkonflikten korrelieren. Weist beispielsweise auf einen Konflikt im Pufferpool `buf_pool mutex` hin. Weitere Informationen finden Sie unter Optimieren von Aurora MySQL mit Warteereignissen.

Behebung von Problemen mit der Speichernutzung für Aurora MySQL-Datenbanken

Enhanced Monitoring und Performance Insights bieten zwar CloudWatch einen guten Überblick über die Speichernutzung auf Betriebssystemebene, z. B. wie viel Speicher der Datenbankprozess verwendet, aber sie ermöglichen es Ihnen nicht, aufzuschlüsseln, welche Verbindungen oder Komponenten innerhalb der Engine diese Speicherbelegung verursachen könnten.

Um dieses Problem zu beheben, können Sie das Leistungsschema und das `sys` Schema verwenden. In Aurora MySQL Version 3 ist die Speicherinstrumentierung standardmäßig aktiviert, wenn das Performance-Schema aktiviert ist. In Aurora MySQL Version 2 ist standardmäßig nur die Speicherinstrumentierung für die Speichernutzung des Performance-Schemas aktiviert. Informationen zu Tabellen, die im Performance-Schema verfügbar sind, um die Speichernutzung nachzuverfolgen und die Performance-Schema-Speicherinstrumentierung zu aktivieren, finden Sie in der MySQL-Dokumentation unter Speicherübersichtstabellen. Weitere Informationen zur Verwendung des Performance-Schemas mit Performance Insights finden Sie unterAktivieren des Leistungsschemas für Performance Insights in Aurora MySQL.

Im Performance-Schema sind zwar detaillierte Informationen verfügbar, um die aktuelle Speicherauslastung nachzuverfolgen, aber das MySQL-Sys-Schema bietet zusätzlich zu den Performance-Schematabellen Ansichten, anhand derer Sie schnell feststellen können, wo Speicher verwendet wird.

Im `sys` Schema sind die folgenden Ansichten verfügbar, um die Speichernutzung nach Verbindung, Komponente und Abfrage nachzuverfolgen.

Anzeigen	Beschreibung
memory_by_host_by_current_bytes	Stellt Informationen zur Engine-Speichernut zung durch den Host bereit. Dies kann nützlich sein, um festzustellen, welche Anwendung sserver oder Client-Hosts Speicher verbrauch en.
memory_by_thread_by_current_bytes	Stellt Informationen zur Engine-Speichernut zung nach Thread-ID bereit. Die Thread-ID in MySQL kann eine Client-Verbindung oder ein Hintergrundthread sein. Sie können Thread-IDs MySQL-Verbindungs-IDs zuordnen, indem Sie

Anzeigen	Beschreibung
	die sys.processlist-Ansicht oder die performance_schema.threads-Tabelle verwenden.
memory_by_user_by_current_bytes	Stellt Informationen zur Engine-Speichernutzung durch den Benutzer bereit. Dies kann nützlich sein, um festzustellen, welche Benutzerkonten oder Clients Speicher verbrauchen.
memory_global_by_current_bytes	Stellt Informationen zur Engine-Speichernutzung nach Engine-Komponenten bereit. Dies kann nützlich sein, um die Speichernutzung global durch Engine-Puffer oder Komponenten zu ermitteln. Beispielsweise könnten Sie das `memory/innodb/buf_buf_pool` Ereignis für den InnoDB-Pufferpool oder das `memory/sql/Prepared_statement::main_mem_root` Ereignis für vorbereitete Anweisungen sehen.
memory_global_total	Bietet einen Überblick über die gesamte verfolgte Speicherauslastung in der Datenbank-Engine.

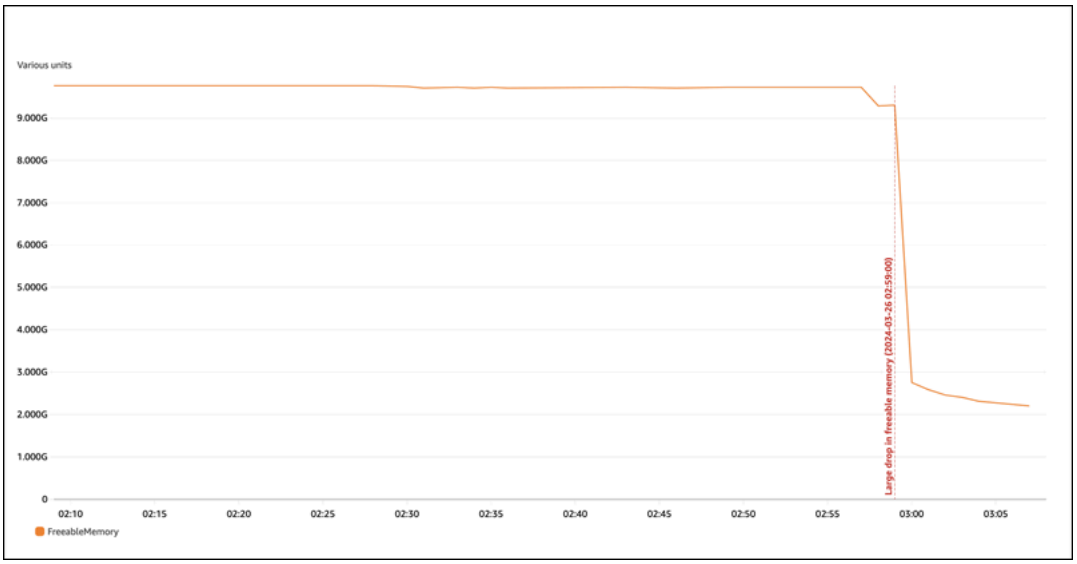
In Aurora MySQL Version 3.05 und höher können Sie die maximale Speicherauslastung auch anhand von Statement Digest in den Übersichtstabellen der Performance-Schema-Anweisungen verfolgen. Die Übersichtstabellen der Kontoauszüge enthalten normalisierte Zusammenfassungen von Kontoauszügen und aggregierte Statistiken über deren Ausführung. Anhand der `MAX_TOTAL_MEMORY` Spalte können Sie ermitteln, wie viel Speicher von Query Digest seit dem letzten Zurücksetzen der Statistiken oder seit dem Neustart der Datenbankinstanz maximal belegt wurde. Dies kann nützlich sein, um bestimmte Abfragen zu identifizieren, die möglicherweise viel Speicher verbrauchen.

> **Note**
>
> Das Leistungsschema und das `sys` Schema zeigen Ihnen die aktuelle Speicherauslastung auf dem Server und die Höchstwerte für den Speicherverbrauch pro Verbindung und Engine-Komponente. Da das Leistungsschema im Speicher gespeichert wird, werden die Informationen zurückgesetzt, wenn die DB-Instance neu gestartet wird. Um den Verlauf im Laufe der Zeit beizubehalten, empfehlen wir, den Abruf und die Speicherung dieser Daten außerhalb des Performance-Schemas zu konfigurieren.

Themen

Beispiel 1: Kontinuierlich hoher Speicherverbrauch

Wenn wir uns global ansehen `FreeableMemory` CloudWatch, können wir feststellen, dass die Speichernutzung am 26.03.2024 um 02:59 UTC stark zugenommen hat.



Das sagt uns nicht das ganze Bild. Um festzustellen, welche Komponente den meisten Speicher beansprucht, können Sie sich bei der Datenbank anmelden und Folgendes ansehen`sys.memory_global_by_current_bytes`. Diese Tabelle enthält eine Liste von Speicherereignissen, die MySQL verfolgt, zusammen mit Informationen zur Speicherzuweisung pro Ereignis. Jedes Speicherverfolgungsereignis beginnt mit`memory/%`, gefolgt von weiteren Informationen darüber, mit welcher Engine-Komponente/Funktion das Ereignis verknüpft ist.

`memory/performance_schema/%`Ist zum Beispiel für Speicherereignisse, die sich auf das Leistungsschema beziehen, `memory/innodb/%` ist für InnoDB und so weiter. Weitere Informationen zu Benennungskonventionen für Ereignisse finden Sie unter Benennungskonventionen für Performance-Schema-Instrumente in der MySQL-Dokumentation.

Anhand der folgenden Abfrage können wir den wahrscheinlichen Schuldigen ermitteln`current_alloc`, aber wir können auch viele `memory/performance_schema/%` Ereignisse erkennen.

```
mysql> SELECT * FROM sys.memory_global_by_current_bytes LIMIT 10;

+-------------------------------------------------------------------------------
+---------------+---------------+-------------------+------------+------------
+----------------+
| event_name                                                                    |
 current_count | current_alloc | current_avg_alloc | high_count | high_alloc |
 high_avg_alloc |
+-------------------------------------------------------------------------------
+---------------+---------------+-------------------+------------+------------
+----------------+
| memory/sql/Prepared_statement::main_mem_root                                  |
 512817 | 4.91 GiB      | 10.04 KiB         |     512823 | 4.91 GiB   | 10.04 KiB
 |
| memory/performance_schema/prepared_statements_instances                       |
   252 | 488.25 MiB    | 1.94 MiB          |        252 | 488.25 MiB | 1.94 MiB       |
| memory/innodb/hash0hash                                                       |
     4 | 79.07 MiB     | 19.77 MiB         |          4 | 79.07 MiB  | 19.77 MiB      |
| memory/performance_schema/events_errors_summary_by_thread_by_error            |
  1028 | 52.27 MiB     | 52.06 KiB         |       1028 | 52.27 MiB  | 52.06 KiB      |
| memory/performance_schema/events_statements_summary_by_thread_by_event_name |
     4 | 47.25 MiB     | 11.81 MiB         |          4 | 47.25 MiB  | 11.81 MiB      |
| memory/performance_schema/events_statements_summary_by_digest                |
     1 | 40.28 MiB     | 40.28 MiB         |          1 | 40.28 MiB  | 40.28 MiB      |
| memory/performance_schema/memory_summary_by_thread_by_event_name              |
     4 | 31.64 MiB     | 7.91 MiB          |          4 | 31.64 MiB  | 7.91 MiB       |
| memory/innodb/memory                                                          |
 15227 | 27.44 MiB     | 1.85 KiB          |      20619 | 33.33 MiB  | 1.66 KiB       |
| memory/sql/String::value                                                      |
 74411 | 21.85 MiB     |  307 bytes        |      76867 | 25.54 MiB  |  348 bytes     |
| memory/sql/TABLE                                                              |
  8381 | 21.03 MiB     | 2.57 KiB          |       8381 | 21.03 MiB  | 2.57 KiB       |
```

```
+-------------------------------------------------------------------------------
+---------------+---------------+------------------+------------+------------
+----------------+
10 rows in set (0.02 sec)
```

Wir haben bereits erwähnt, dass das Leistungsschema im Arbeitsspeicher gespeichert wird, was bedeutet, dass es auch in der `performance_schema` Speicherinstrumentierung nachverfolgt wird.

> **Note**
>
> Wenn Sie feststellen, dass das Leistungsschema viel Speicher beansprucht, und Sie den Speicherverbrauch einschränken möchten, können Sie die Datenbankparameter an Ihre Anforderungen anpassen. Weitere Informationen finden Sie in der MySQL-Dokumentation unter Das Performance-Schema-Speicherzuweisungsmodell.

Aus Gründen der besseren Lesbarkeit können Sie dieselbe Abfrage erneut ausführen, aber Performance-Schema-Ereignisse ausschließen. Die Ausgabe zeigt Folgendes:

- Der Hauptspeicherverbraucher ist`memory/sql/Prepared_statement::main_mem_root`.
- Aus der `current_alloc` Spalte geht hervor, dass MySQL diesem Ereignis derzeit 4,91 GiB zugewiesen hat.
- Das `high_alloc column` sagt uns, dass 4,91 GiB der Höchststand `current_alloc` seit dem letzten Reset der Statistiken oder seit dem Neustart des Servers sind. Das bedeutet, dass der `memory/sql/Prepared_statement::main_mem_root` höchste Wert erreicht ist.

```
mysql> SELECT * FROM sys.memory_global_by_current_bytes WHERE event_name NOT LIKE
 'memory/performance_schema/%' LIMIT 10;

+-----------------------------------------------+---------------+--------------
+------------------+-----------+-----------+----------------+
| event_name                                    | current_count | current_alloc |
 current_avg_alloc | high_count | high_alloc | high_avg_alloc |
+-----------------------------------------------+---------------+--------------
+------------------+-----------+-----------+----------------+
| memory/sql/Prepared_statement::main_mem_root  |        512817 | 4.91 GiB      | 10.04
 KiB         |     512823 | 4.91 GiB   | 10.04 KiB      |
| memory/innodb/hash0hash                       |             4 | 79.07 MiB     | 19.77
 MiB         |          4 | 79.07 MiB  | 19.77 MiB      |
```

```
| memory/innodb/memory                              |         17096 | 31.68 MiB     | 1.90
 KiB          |      22498 | 37.60 MiB  | 1.71 KiB       |
| memory/sql/String::value                          |        122277 | 27.94 MiB     |  239
 bytes        |     124699 | 29.47 MiB  |  247 bytes     |
| memory/sql/TABLE                                  |          9927 | 24.67 MiB     | 2.55
 KiB          |       9929 | 24.68 MiB  | 2.55 KiB       |
| memory/innodb/lock0lock                           |          8888 | 19.71 MiB     | 2.27
 KiB          |       8888 | 19.71 MiB  | 2.27 KiB       |
| memory/sql/Prepared_statement::infrastructure |        257623 | 16.24 MiB     |   66
 bytes        |     257631 | 16.24 MiB  |   66 bytes     |
| memory/mysys/KEY_CACHE                            |             3 | 16.00 MiB     | 5.33
 MiB          |          3 | 16.00 MiB  | 5.33 MiB       |
| memory/innodb/sync0arr                            |             3 | 7.03 MiB      | 2.34
 MiB          |          3 | 7.03 MiB   | 2.34 MiB       |
| memory/sql/THD::main_mem_root                     |           815 | 6.56 MiB      | 8.24
 KiB          |        849 | 7.19 MiB   | 8.67 KiB       |
+-------------------------------------------------+---------------+---------------
+------------------+-----------+-----------+----------------+
10 rows in set (0.06 sec)
```

Am Namen des Ereignisses können wir erkennen, dass dieser Speicher für vorbereitete Anweisungen verwendet wird. Wenn Sie sehen möchten, welche Verbindungen diesen Speicher verwenden, können Sie memory_by_thread_by_current_bytes überprüfen.

Im folgenden Beispiel sind jeder Verbindung ungefähr 7 MiB zugewiesen, mit einer Höchstmarke von ungefähr 6,29 MiB (). `current_max_alloc` Das ist sinnvoll, da im Beispiel 80 Tabellen und 800 Verbindungen `sysbench` mit vorbereiteten Anweisungen verwendet werden. Wenn Sie in diesem Szenario den Speicherverbrauch reduzieren möchten, können Sie die Verwendung von vorbereiteten Anweisungen durch Ihre Anwendung optimieren, um den Speicherverbrauch zu reduzieren.

```
mysql> SELECT * FROM sys.memory_by_thread_by_current_bytes;

+-----------+-------------------------------------------+-------------------
+------------------+------------------+------------------+-----------------+
| thread_id | user                                      | current_count_used |
 current_allocated | current_avg_alloc | current_max_alloc | total_allocated |
+-----------+-------------------------------------------+-------------------
+------------------+------------------+------------------+-----------------+
|        46 | rdsadmin@localhost                        |                405 | 8.47 MiB
          | 21.42 KiB         | 8.00 MiB          | 155.86 MiB      |
|        61 | reinvent@10.0.4.4                         |               1749 | 6.72 MiB
          | 3.93 KiB          | 6.29 MiB          | 14.24 MiB       |
```

```
|       101 | reinvent@10.0.4.4                        |              1845 | 6.71 MiB
          | 3.72 KiB          | 6.29 MiB          | 14.50 MiB       |
|        55 | reinvent@10.0.4.4                        |              1674 | 6.68 MiB
          | 4.09 KiB          | 6.29 MiB          | 14.13 MiB       |
|        57 | reinvent@10.0.4.4                        |              1416 | 6.66 MiB
          | 4.82 KiB          | 6.29 MiB          | 13.52 MiB       |
|       112 | reinvent@10.0.4.4                        |              1759 | 6.66 MiB
          | 3.88 KiB          | 6.29 MiB          | 14.17 MiB       |
|        66 | reinvent@10.0.4.4                        |              1428 | 6.64 MiB
          | 4.76 KiB          | 6.29 MiB          | 13.47 MiB       |
|        75 | reinvent@10.0.4.4                        |              1389 | 6.62 MiB
          | 4.88 KiB          | 6.29 MiB          | 13.40 MiB       |
|       116 | reinvent@10.0.4.4                        |              1333 | 6.61 MiB
          | 5.08 KiB          | 6.29 MiB          | 13.21 MiB       |
|        90 | reinvent@10.0.4.4                        |              1448 | 6.59 MiB
          | 4.66 KiB          | 6.29 MiB          | 13.58 MiB       |
|        98 | reinvent@10.0.4.4                        |              1440 | 6.57 MiB
          | 4.67 KiB          | 6.29 MiB          | 13.52 MiB       |
|        94 | reinvent@10.0.4.4                        |              1433 | 6.57 MiB
          | 4.69 KiB          | 6.29 MiB          | 13.49 MiB       |
|        62 | reinvent@10.0.4.4                        |              1323 | 6.55 MiB
          | 5.07 KiB          | 6.29 MiB          | 13.48 MiB       |
|        87 | reinvent@10.0.4.4                        |              1323 | 6.55 MiB
          | 5.07 KiB          | 6.29 MiB          | 13.25 MiB       |
|        99 | reinvent@10.0.4.4                        |              1346 | 6.54 MiB
          | 4.98 KiB          | 6.29 MiB          | 13.24 MiB       |
|       105 | reinvent@10.0.4.4                        |              1347 | 6.54 MiB
          | 4.97 KiB          | 6.29 MiB          | 13.34 MiB       |
|        73 | reinvent@10.0.4.4                        |              1335 | 6.54 MiB
          | 5.02 KiB          | 6.29 MiB          | 13.23 MiB       |
|        54 | reinvent@10.0.4.4                        |              1510 | 6.53 MiB
          | 4.43 KiB          | 6.29 MiB          | 13.49 MiB       |
.                                                                    .
.                                                                    .
.                                                                    .
|       812 | reinvent@10.0.4.4                        |              1259 | 6.38 MiB
          | 5.19 KiB          | 6.29 MiB          | 13.05 MiB       |
|       214 | reinvent@10.0.4.4                        |              1279 | 6.38 MiB
          | 5.10 KiB          | 6.29 MiB          | 12.90 MiB       |
|       325 | reinvent@10.0.4.4                        |              1254 | 6.38 MiB
          | 5.21 KiB          | 6.29 MiB          | 12.99 MiB       |
```

```
|       705 | reinvent@10.0.4.4                          |              1273 | 6.37 MiB
          | 5.13 KiB          | 6.29 MiB          | 13.03 MiB       |
|       530 | reinvent@10.0.4.4                          |              1268 | 6.37 MiB
          | 5.15 KiB          | 6.29 MiB          | 12.92 MiB       |
|       307 | reinvent@10.0.4.4                          |              1263 | 6.37 MiB
          | 5.17 KiB          | 6.29 MiB          | 12.87 MiB       |
|       738 | reinvent@10.0.4.4                          |              1260 | 6.37 MiB
          | 5.18 KiB          | 6.29 MiB          | 13.00 MiB       |
|       819 | reinvent@10.0.4.4                          |              1252 | 6.37 MiB
          | 5.21 KiB          | 6.29 MiB          | 13.01 MiB       |
|        31 | innodb/srv_purge_thread                    |             17810 | 3.14 MiB
          |  184 bytes        | 2.40 MiB          | 205.69 MiB      |
|        38 | rdsadmin@localhost                         |               599 | 1.76 MiB
          | 3.01 KiB          | 1.00 MiB          | 25.58 MiB       |
|         1 | sql/main                                   |              3756 | 1.32 MiB
          |  367 bytes        | 355.78 KiB        | 6.19 MiB        |
|       854 | rdsadmin@localhost                         |                46 | 1.08 MiB
          | 23.98 KiB         | 1.00 MiB          | 5.10 MiB        |
|        30 | innodb/clone_gtid_thread                   |              1596 | 573.14
 KiB        |  367 bytes        | 254.91 KiB        | 970.69 KiB      |
|        40 | rdsadmin@localhost                         |               235 | 245.19
 KiB        | 1.04 KiB          | 128.88 KiB        | 808.64 KiB      |
|       853 | rdsadmin@localhost                         |                96 | 94.63
 KiB        | 1009 bytes        | 29.73 KiB         | 422.45 KiB      |
|        36 | rdsadmin@localhost                         |                33 | 36.29
 KiB        | 1.10 KiB          | 16.08 KiB         | 74.15 MiB       |
|        33 | sql/event_scheduler                        |                 3 | 16.27
 KiB        | 5.42 KiB          | 16.04 KiB         | 16.27 KiB       |
|        35 | sql/compress_gtid_table                    |                 8 | 14.20
 KiB        | 1.77 KiB          | 8.05 KiB          | 18.62 KiB       |
|        25 | innodb/fts_optimize_thread                 |                12 | 1.86 KiB
          |  158 bytes        |  648 bytes        | 1.98 KiB        |
|        23 | innodb/srv_master_thread                   |                11 | 1.23 KiB
          |  114 bytes        |  361 bytes        | 24.40 KiB       |
|        24 | innodb/dict_stats_thread                   |                11 | 1.23 KiB
          |  114 bytes        |  361 bytes        | 1.35 KiB        |
|         5 | innodb/io_read_thread                      |                 1 |  144
 bytes        |  144 bytes        |  144 bytes        |  144 bytes      |
|         6 | innodb/io_read_thread                      |                 1 |  144
 bytes        |  144 bytes        |  144 bytes        |  144 bytes      |
|         2 | sql/aws_oscar_log_level_monitor            |                 0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|         4 | innodb/io_ibuf_thread                      |                 0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
```

```
|         7 | innodb/io_write_thread                    |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|         8 | innodb/io_write_thread                    |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|         9 | innodb/io_write_thread                    |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        10 | innodb/io_write_thread                    |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        11 | innodb/srv_lra_thread                     |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        12 | innodb/srv_akp_thread                     |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        18 | innodb/srv_lock_timeout_thread            |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |  248 bytes      |
|        19 | innodb/srv_error_monitor_thread           |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        20 | innodb/srv_monitor_thread                 |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        21 | innodb/buf_resize_thread                  |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        22 | innodb/btr_search_sys_toggle_thread       |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        32 | innodb/dict_persist_metadata_table_thread |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
|        34 | sql/signal_handler                        |                  0 |    0
 bytes        |    0 bytes        |    0 bytes        |    0 bytes      |
+-----------+-------------------------------------------+--------------------
+-------------------+------------------+------------------+-----------------+
831 rows in set (2.48 sec)
```

Wie bereits erwähnt, kann sich der Wert der Thread-ID (`thd_id`) hier auf Serverhintergrund-Threads oder Datenbankverbindungen beziehen. Wenn Sie Thread-ID-Werte Datenbankverbindungs-IDs zuordnen möchten, können Sie die `performance_schema.threads` Tabelle oder die `sys.processlist` Ansicht verwenden, wobei sich die Verbindungs-ID `conn_id` befindet.

```
mysql> SELECT thd_id,conn_id,user,db,command,state,time,last_wait FROM sys.processlist
 WHERE user='reinvent@10.0.4.4';

+--------+---------+------------------+----------+---------+----------------+------
+-----------------------------------------------+
| thd_id | conn_id | user             | db       | command | state          | time |
 last_wait                                      |
```

```
+--------+---------+-------------------+----------+---------+----------------+------
+-----------------------------------------------+
|    590 |     562 | reinvent@10.0.4.4 | sysbench | Execute | closing tables |    0 |
 wait/io/redo_log_flush                          |
|    578 |     550 | reinvent@10.0.4.4 | sysbench | Sleep   | NULL           |    0 |
 idle                                            |
|    579 |     551 | reinvent@10.0.4.4 | sysbench | Execute | closing tables |    0 |
 wait/io/redo_log_flush                          |
|    580 |     552 | reinvent@10.0.4.4 | sysbench | Execute | updating       |    0 |
 wait/io/table/sql/handler                       |
|    581 |     553 | reinvent@10.0.4.4 | sysbench | Execute | updating       |    0 |
 wait/io/table/sql/handler                       |
|    582 |     554 | reinvent@10.0.4.4 | sysbench | Sleep   | NULL           |    0 |
 idle                                            |
|    583 |     555 | reinvent@10.0.4.4 | sysbench | Sleep   | NULL           |    0 |
 idle                                            |
|    584 |     556 | reinvent@10.0.4.4 | sysbench | Execute | updating       |    0 |
 wait/io/table/sql/handler                       |
|    585 |     557 | reinvent@10.0.4.4 | sysbench | Execute | closing tables |    0 |
 wait/io/redo_log_flush                          |
|    586 |     558 | reinvent@10.0.4.4 | sysbench | Execute | updating       |    0 |
 wait/io/table/sql/handler                       |
|    587 |     559 | reinvent@10.0.4.4 | sysbench | Execute | closing tables |    0 |
 wait/io/redo_log_flush                          |
.
                                                 .
.
                                                 .
.
                                                 .
|    323 |     295 | reinvent@10.0.4.4 | sysbench | Sleep   | NULL           |    0 |
 idle                                            |
|    324 |     296 | reinvent@10.0.4.4 | sysbench | Execute | updating       |    0 |
 wait/io/table/sql/handler                       |
|    325 |     297 | reinvent@10.0.4.4 | sysbench | Execute | closing tables |    0 |
 wait/io/redo_log_flush                          |
|    326 |     298 | reinvent@10.0.4.4 | sysbench | Execute | updating       |    0 |
 wait/io/table/sql/handler                       |
|    438 |     410 | reinvent@10.0.4.4 | sysbench | Execute | System lock    |    0 |
 wait/lock/table/sql/handler                     |
|    280 |     252 | reinvent@10.0.4.4 | sysbench | Sleep   | starting       |    0 |
 wait/io/socket/sql/client_connection            |
|     98 |      70 | reinvent@10.0.4.4 | sysbench | Query   | freeing items  |    0 |
 NULL                                            |
```

```
+--------+---------+-------------------+----------+---------+---------------+------
+-----------------------------------------------+
804 rows in set (5.51 sec)
```

Jetzt beenden wir die `sysbench` Arbeitslast, wodurch die Verbindungen geschlossen und der Speicher freigegeben wird. Wenn wir die Ereignisse erneut überprüfen, können wir bestätigen, dass der Speicher freigegeben wurde, aber wir wissen `high_alloc` trotzdem, wo der Höchststand liegt. Die `high_alloc` Spalte kann sehr nützlich sein, wenn es darum geht, kurze Spitzen bei der Speichernutzung zu identifizieren, bei denen Sie die Auslastung möglicherweise nicht sofort erkennen können. In dieser Spalte wird nur der aktuell zugewiesene Speicher angezeigt. `current_alloc`

```
mysql> SELECT * FROM sys.memory_global_by_current_bytes WHERE event_name='memory/sql/
Prepared_statement::main_mem_root' LIMIT 10;

+-----------------------------------------------+--------------+--------------
+------------------+-----------+-----------+----------------+
| event_name                                    | current_count | current_alloc |
 current_avg_alloc | high_count | high_alloc | high_avg_alloc |
+-----------------------------------------------+--------------+--------------
+------------------+-----------+-----------+----------------+
| memory/sql/Prepared_statement::main_mem_root |            17 | 253.80 KiB    | 14.93
 KiB         |     512823 | 4.91 GiB   | 10.04 KiB      |
+-----------------------------------------------+--------------+--------------
+------------------+-----------+-----------+----------------+
1 row in set (0.00 sec)
```

Wenn Sie einen Reset durchführen möchten`high_alloc`, können Sie die Tabellen mit der `performance_schema` Speicherübersicht kürzen. Dadurch wird jedoch die gesamte Speicherausstattung zurückgesetzt. Weitere Informationen finden Sie unter Allgemeine Tabellenmerkmale des Performance-Schemas in der MySQL-Dokumentation.

Im folgenden Beispiel können wir sehen, dass dies nach der Kürzung zurückgesetzt `high_alloc` wird.

```
mysql> TRUNCATE `performance_schema`.`memory_summary_global_by_event_name`;
Query OK, 0 rows affected (0.00 sec)

mysql> SELECT * FROM sys.memory_global_by_current_bytes WHERE event_name='memory/sql/
Prepared_statement::main_mem_root' LIMIT 10;
```

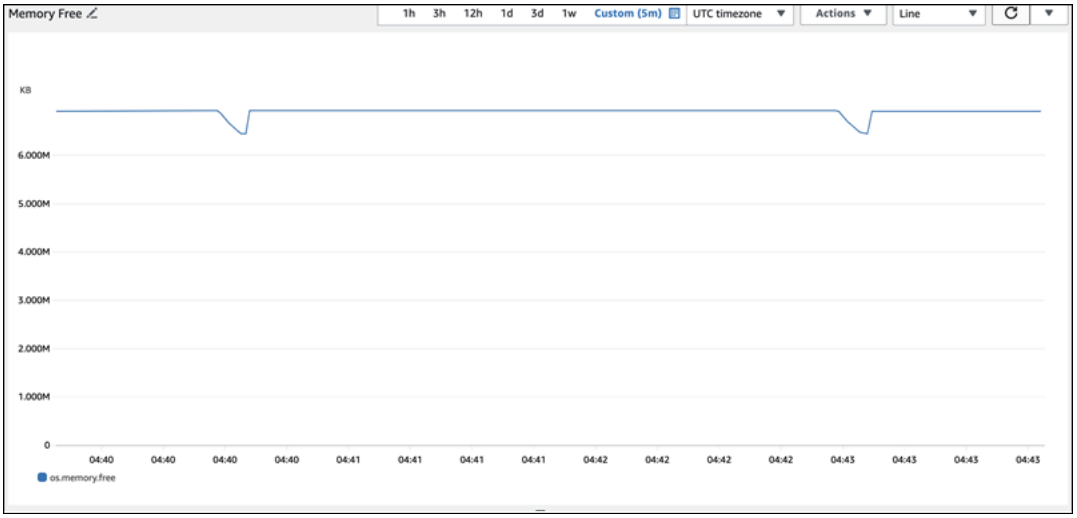
```
+-----------------------------------------------+--------------+--------------
+------------------+-----------+-----------+----------------+
| event_name                                    | current_count | current_alloc |
 current_avg_alloc | high_count | high_alloc | high_avg_alloc |
+-----------------------------------------------+--------------+--------------
+------------------+-----------+-----------+----------------+
| memory/sql/Prepared_statement::main_mem_root |            17 | 253.80 KiB    | 14.93
 KiB         |         17 | 253.80 KiB | 14.93 KiB      |
+-----------------------------------------------+--------------+--------------
+------------------+-----------+-----------+----------------+
1 row in set (0.00 sec)
```

Beispiel 2: Vorübergehende Speicherspitzen

Ein weiteres häufiges Ereignis sind kurze Spitzen bei der Speichernutzung auf einem Datenbankserver. Dabei kann es sich um periodische Einbrüche des freien Speichers handeln, `current_alloc` bei denen es schwierig ist, Fehler zu behebensys.memory_global_by_current_bytes, da der Speicher bereits freigegeben wurde.

> **Note**
>
> Wenn die Performance-Schema-Statistiken zurückgesetzt oder die Datenbankinstanz neu gestartet wurde, sind diese Informationen in `sys` oder p nicht verfügbar. `erformance_schema` Um diese Informationen beizubehalten, empfehlen wir, die Erfassung externer Metriken zu konfigurieren.

Das folgende Diagramm der `os.memory.free` Metrik in Enhanced Monitoring zeigt kurze Spitzen bei der Speichernutzung von 7 Sekunden. Mit der erweiterten Überwachung können Sie die Überwachung in Intervallen von nur 1 Sekunde durchführen. Dies ist ideal, um vorübergehende Spitzen wie diese abzufangen.



Um hier die Ursache für die Speicherauslastung besser zu diagnostizieren, können wir eine Kombination aus den Ansichten mit der Zusammenfassung des `high_alloc` `sys` Speichers und den Übersichtstabellen der Performance-Schema-Anweisungen verwenden, um zu versuchen, fehlerhafte Sitzungen und Verbindungen zu identifizieren.

Da der Speicherverbrauch derzeit nicht hoch ist, können wir in der `sys` Schemaansicht unter erwartungsgemäß keine größeren Fehler erkennen. `current_alloc`

```
mysql> SELECT * FROM sys.memory_global_by_current_bytes LIMIT 10;

+-----------------------------------------------------------------------------
+---------------+---------------+-------------------+------------+------------
+----------------+
| event_name                                                                 |
 current_count | current_alloc | current_avg_alloc | high_count | high_alloc |
 high_avg_alloc |
+-----------------------------------------------------------------------------
+---------------+---------------+-------------------+------------+------------
+----------------+
| memory/innodb/hash0hash                                                    |
     4 | 79.07 MiB     | 19.77 MiB         |          4 | 79.07 MiB  | 19.77 MiB      |
| memory/innodb/os0event                                                     |
 439372 | 60.34 MiB     |  144 bytes        |     439372 | 60.34 MiB  |  144 bytes
 |
| memory/performance_schema/events_statements_summary_by_digest              |
     1 | 40.28 MiB     | 40.28 MiB         |          1 | 40.28 MiB  | 40.28 MiB      |
| memory/mysys/KEY_CACHE                                                     |
     3 | 16.00 MiB     | 5.33 MiB          |          3 | 16.00 MiB  | 5.33 MiB       |
```

```
| memory/performance_schema/events_statements_history_long                    |
     1 | 14.34 MiB     | 14.34 MiB         |          1 | 14.34 MiB  | 14.34 MiB      |
| memory/performance_schema/events_errors_summary_by_thread_by_error          |
   257 | 13.07 MiB     | 52.06 KiB         |        257 | 13.07 MiB  | 52.06 KiB      |
| memory/performance_schema/events_statements_summary_by_thread_by_event_name |
     1 | 11.81 MiB     | 11.81 MiB         |          1 | 11.81 MiB  | 11.81 MiB      |
| memory/performance_schema/events_statements_summary_by_digest.digest_text   |
     1 | 9.77 MiB      | 9.77 MiB          |          1 | 9.77 MiB   | 9.77 MiB       |
| memory/performance_schema/events_statements_history_long.digest_text        |
     1 | 9.77 MiB      | 9.77 MiB          |          1 | 9.77 MiB   | 9.77 MiB       |
| memory/performance_schema/events_statements_history_long.sql_text           |
     1 | 9.77 MiB      | 9.77 MiB          |          1 | 9.77 MiB   | 9.77 MiB       |
+------------------------------------------------------------------------------
+---------------+---------------+------------------+------------+------------
+----------------+
10 rows in set (0.01 sec)
```

Wenn wir die Ansicht auf Sortierung nach erweiternhigh_alloc, können wir jetzt sehen, dass die memory/temptable/physical_ram Komponente hier ein sehr guter Kandidat ist. Auf seinem höchsten Stand verbrauchte es 515,00 MiB.

Wie der Name schon sagt, memory/temptable/physical_ram instrumentiert die Speichernutzung für die TEMP Speicher-Engine in MySQL, die in MySQL 8.0 eingeführt wurde. Weitere Informationen darüber, wie MySQL temporäre Tabellen verwendet, finden Sie unter Interne Verwendung temporärer Tabellen in MySQL in der MySQL-Dokumentation.

> **Note**
>
> In diesem Beispiel verwenden wir die sys.x$memory_global_by_current_bytes Ansicht.

```
mysql> SELECT event_name, format_bytes(current_alloc) AS "currently allocated",
 sys.format_bytes(high_alloc) AS "high-water mark"
FROM sys.x$memory_global_by_current_bytes ORDER BY high_alloc DESC LIMIT 10;

+------------------------------------------------------------------------------
+--------------------+-----------------+
| event_name                                                                   |
 currently allocated | high-water mark |
```

```
+-------------------------------------------------------------------------------
+--------------------+-----------------+
| memory/temptable/physical_ram                                                | 4.00
 MiB            | 515.00 MiB      |
| memory/innodb/hash0hash                                                      | 79.07
 MiB           | 79.07 MiB       |
| memory/innodb/os0event                                                       | 63.95
 MiB           | 63.95 MiB       |
| memory/performance_schema/events_statements_summary_by_digest                | 40.28
 MiB           | 40.28 MiB       |
| memory/mysys/KEY_CACHE                                                       | 16.00
 MiB           | 16.00 MiB       |
| memory/performance_schema/events_statements_history_long                     | 14.34
 MiB           | 14.34 MiB       |
| memory/performance_schema/events_errors_summary_by_thread_by_error           | 13.07
 MiB           | 13.07 MiB       |
| memory/performance_schema/events_statements_summary_by_thread_by_event_name | 11.81
 MiB           | 11.81 MiB       |
| memory/performance_schema/events_statements_summary_by_digest.digest_text   | 9.77
 MiB            | 9.77 MiB        |
| memory/performance_schema/events_statements_history_long.sql_text           | 9.77
 MiB            | 9.77 MiB        |
+-------------------------------------------------------------------------------
+--------------------+-----------------+
10 rows in set (0.00 sec)
```

In Beispiel 1: Kontinuierlich hoher Speicherverbrauch haben wir die aktuelle Speichernutzung für jede Verbindung überprüft, um festzustellen, welche Verbindung für die Nutzung des fraglichen Speichers verantwortlich ist. In diesem Beispiel ist der Speicher bereits freigegeben, sodass es nicht sinnvoll ist, den Speicherverbrauch für aktuelle Verbindungen zu überprüfen.

Um tiefer zu graben und die anstößigen Aussagen, Benutzer und Hosts zu finden, verwenden wir das Performance-Schema. Das Leistungsschema enthält mehrere Übersichtstabellen mit Aussagen, die nach verschiedenen Dimensionen wie Ereignisname, Statement Digest, Host, Thread und Benutzer unterteilt sind. Jede Ansicht ermöglicht es Ihnen, genauer zu untersuchen, wo bestimmte Anweisungen ausgeführt werden und was sie bewirken. Dieser Abschnitt konzentriert sich darauf`MAX_TOTAL_MEMORY`, aber weitere Informationen zu allen verfügbaren Spalten finden Sie in der Dokumentation mit den Übersichtstabellen für Performance-Schema-Anweisungen.

```
mysql> SHOW TABLES IN performance_schema LIKE 'events_statements_summary_%';

+-----------------------------------------------------------+
```

```
| Tables_in_performance_schema (events_statements_summary_%) |
+------------------------------------------------------------+
| events_statements_summary_by_account_by_event_name         |
| events_statements_summary_by_digest                        |
| events_statements_summary_by_host_by_event_name            |
| events_statements_summary_by_program                       |
| events_statements_summary_by_thread_by_event_name          |
| events_statements_summary_by_user_by_event_name            |
| events_statements_summary_global_by_event_name             |
+------------------------------------------------------------+
7 rows in set (0.00 sec)
```

Zuerst schauen wir `events_statements_summary_by_digest` nach`MAX_TOTAL_MEMORY`.

Daraus können wir Folgendes erkennen:

- Die Abfrage mit Digest `20676ce4a690592ff05debcffcbc26faeb76f22005e7628364d7a498769d0c4a` scheint ein guter Kandidat für diese Speichernutzung zu sein. Das `MAX_TOTAL_MEMORY` ist 537450710, was der Hochwassermarke entspricht, die wir bei der Veranstaltung in gesehen haben. `memory/temptable/physical_ram` `sys.x$memory_global_by_current_bytes`
- Es wurde viermal (`COUNT_STAR`) durchgeführt, zuerst um 2024-03-26 04:08:34.943 256 und zuletzt um 2024-03-26 04:43:06.998 310.

```
mysql> SELECT SCHEMA_NAME,DIGEST,COUNT_STAR,MAX_TOTAL_MEMORY,FIRST_SEEN,LAST_SEEN
FROM performance_schema.events_statements_summary_by_digest ORDER BY MAX_TOTAL_MEMORY
 DESC LIMIT 5;

+-------------+------------------------------------------------------------------
+------------+-----------------+---------------------------
+----------------------------+
| SCHEMA_NAME | DIGEST                                                                |
 COUNT_STAR | MAX_TOTAL_MEMORY | FIRST_SEEN                | LAST_SEEN
  |
+-------------+------------------------------------------------------------------
+------------+-----------------+---------------------------
+----------------------------+
| sysbench    | 20676ce4a690592ff05debcffcbc26faeb76f22005e7628364d7a498769d0c4a |
     4 |        537450710 | 2024-03-26 04:08:34.943256 | 2024-03-26 04:43:06.998310 |
| NULL        | f158282ea0313fefd0a4778f6e9b92fc7d1e839af59ebd8c5eea35e12732c45d |
     4 |          3636413 | 2024-03-26 04:29:32.712348 | 2024-03-26 04:36:26.269329 |
```

```
| NULL        | 0046bc5f642c586b8a9afd6ce1ab70612dc5b1fd2408fa8677f370c1b0ca3213 |
     2 |          3459965 | 2024-03-26 04:31:37.674008 | 2024-03-26 04:32:09.410718 |
| NULL        | 8924f01bba3c55324701716c7b50071a60b9ceaf17108c71fd064c20c4ab14db |
     1 |          3290981 | 2024-03-26 04:31:49.751506 | 2024-03-26 04:31:49.751506 |
| NULL        | 90142bbcb50a744fcec03a1aa336b2169761597ea06d85c7f6ab03b5a4e1d841 |
     1 |          3131729 | 2024-03-26 04:15:09.719557 | 2024-03-26 04:15:09.719557 |
+-------------+------------------------------------------------------------------
+------------+-----------------+--------------------------
+---------------------------+
5 rows in set (0.00 sec)
```

Jetzt, da wir den fraglichen Digest kennen, können wir mehr Details abrufen, z. B. den Abfragetext, den Benutzer, der ihn ausgeführt hat, und den Ort, an dem er ausgeführt wurde. Anhand des zurückgegebenen Digest-Textes können wir erkennen, dass es sich um einen Common Table Expression (CTE) handelt, der vier temporäre Tabellen erstellt und vier Tabellenscans durchführt, was sehr ineffizient ist.

```
mysql> SELECT
 SCHEMA_NAME,DIGEST_TEXT,QUERY_SAMPLE_TEXT,MAX_TOTAL_MEMORY,SUM_ROWS_SENT,SUM_ROWS_EXAMINED,SUM
FROM performance_schema.events_statements_summary_by_digest
WHERE DIGEST='20676ce4a690592ff05debcffcbc26faeb76f22005e7628364d7a498769d0c4a'\G;

*************************** 1. row ***************************
           SCHEMA_NAME: sysbench
           DIGEST_TEXT: WITH RECURSIVE `cte` ( `n` ) AS ( SELECT ? FROM `sbtest1` UNION
 ALL SELECT `id` + ? FROM `sbtest1` ) SELECT * FROM `cte`
     QUERY_SAMPLE_TEXT: WITH RECURSIVE cte (n) AS (   SELECT 1  from sbtest1 UNION ALL
  SELECT id + 1 FROM sbtest1) SELECT * FROM cte
      MAX_TOTAL_MEMORY: 537450710
         SUM_ROWS_SENT: 80000000
     SUM_ROWS_EXAMINED: 80000000
SUM_CREATED_TMP_TABLES: 4
     SUM_NO_INDEX_USED: 4
1 row in set (0.01 sec)
```

Weitere Informationen zur `events_statements_summary_by_digest` Tabelle und zu anderen Übersichtstabellen für Performance-Schema-Anweisungen finden Sie in der MySQL-Dokumentation unter Übersichtstabellen für Anweisungen.

Sie können auch eine EXPLAIN- oder EXPLAIN ANALYZE-Anweisung ausführen, um weitere Informationen zu erhalten.

> **Note**
>
> `EXPLAIN ANALYZE`kann mehr Informationen liefern als`EXPLAIN`, führt aber auch die Abfrage aus. Seien Sie also vorsichtig.

```
-- EXPLAIN
mysql> EXPLAIN WITH RECURSIVE cte (n) AS (SELECT 1  FROM sbtest1 UNION ALL SELECT id +
 1 FROM sbtest1) SELECT * FROM cte;

+----+-------------+------------+------------+-------+---------------+------+---------
+------+----------+----------+-------------+
| id | select_type | table      | partitions | type  | possible_keys | key  | key_len |
 ref  | rows     | filtered | Extra       |
+----+-------------+------------+------------+-------+---------------+------+---------
+------+----------+----------+-------------+
|  1 | PRIMARY     | <derived2> | NULL       | ALL   | NULL          | NULL | NULL    |
 NULL | 19221520 |   100.00 | NULL        |
|  2 | DERIVED     | sbtest1    | NULL       | index | NULL          | k_1  | 4       |
 NULL |  9610760 |   100.00 | Using index |
|  3 | UNION       | sbtest1    | NULL       | index | NULL          | k_1  | 4       |
 NULL |  9610760 |   100.00 | Using index |
+----+-------------+------------+------------+-------+---------------+------+---------
+------+----------+----------+-------------+
3 rows in set, 1 warning (0.00 sec)

-- EXPLAIN format=tree
mysql> EXPLAIN format=tree WITH RECURSIVE cte (n) AS (SELECT 1 FROM sbtest1 UNION ALL
 SELECT id + 1 FROM sbtest1) SELECT * FROM cte\G;

*************************** 1. row ***************************
EXPLAIN: -> Table scan on cte  (cost=4.11e+6..4.35e+6 rows=19.2e+6)
    -> Materialize union CTE cte  (cost=4.11e+6..4.11e+6 rows=19.2e+6)
        -> Index scan on sbtest1 using k_1  (cost=1.09e+6 rows=9.61e+6)
        -> Index scan on sbtest1 using k_1  (cost=1.09e+6 rows=9.61e+6)
1 row in set (0.00 sec)

-- EXPLAIN ANALYZE
mysql> EXPLAIN ANALYZE WITH RECURSIVE cte (n) AS (SELECT 1 from sbtest1 UNION ALL
 SELECT id + 1 FROM sbtest1) SELECT * FROM cte\G;

*************************** 1. row ***************************
```

```
EXPLAIN: -> Table scan on cte  (cost=4.11e+6..4.35e+6 rows=19.2e+6) (actual
 time=6666..9201 rows=20e+6 loops=1)
    -> Materialize union CTE cte  (cost=4.11e+6..4.11e+6 rows=19.2e+6) (actual
 time=6666..6666 rows=20e+6 loops=1)
       -> Covering index scan on sbtest1 using k_1  (cost=1.09e+6 rows=9.61e+6)
 (actual time=0.0365..2006 rows=10e+6 loops=1)
       -> Covering index scan on sbtest1 using k_1  (cost=1.09e+6 rows=9.61e+6)
 (actual time=0.0311..2494 rows=10e+6 loops=1)
1 row in set (10.53 sec)
```

Aber wer hat es ausgeführt? Wir können im Leistungsschema sehen, dass der `destructive_operator` Benutzer den Wert 537450710 hatte`MAX_TOTAL_MEMORY`, was wiederum den vorherigen Ergebnissen entspricht.

> **Note**
>
> Das Leistungsschema wird im Arbeitsspeicher gespeichert und sollte daher nicht als alleinige Quelle für Prüfungen verwendet werden. Wenn Sie einen Verlauf der ausgeführten Anweisungen und der Benutzer verwalten möchten, empfehlen wir, die Auditprotokollierung zu aktivieren. Wenn Sie auch Informationen zur Speichernutzung verwalten müssen, empfehlen wir, die Überwachung so zu konfigurieren, dass diese Werte exportiert und gespeichert werden.

```
mysql> SELECT USER,EVENT_NAME,COUNT_STAR,MAX_TOTAL_MEMORY FROM
 performance_schema.events_statements_summary_by_user_by_event_name
ORDER BY MAX_CONTROLLED_MEMORY DESC LIMIT 5;

+----------------------+---------------------------+------------+------------------+
| USER                 | EVENT_NAME                | COUNT_STAR | MAX_TOTAL_MEMORY |
+----------------------+---------------------------+------------+------------------+
| destructive_operator | statement/sql/select      |          4 |        537450710 |
| rdsadmin             | statement/sql/select      |       4172 |          3290981 |
| rdsadmin             | statement/sql/show_tables |          2 |          3615821 |
| rdsadmin             | statement/sql/show_fields |          2 |          3459965 |
| rdsadmin             | statement/sql/show_status |         75 |          1914976 |
+----------------------+---------------------------+------------+------------------+
5 rows in set (0.00 sec)

mysql> SELECT HOST,EVENT_NAME,COUNT_STAR,MAX_TOTAL_MEMORY FROM
 performance_schema.events_statements_summary_by_host_by_event_name
```

```
WHERE HOST != 'localhost' AND COUNT_STAR>0 ORDER BY MAX_CONTROLLED_MEMORY DESC LIMIT 5;

+------------+----------------------+------------+------------------+
| HOST       | EVENT_NAME           | COUNT_STAR | MAX_TOTAL_MEMORY |
+------------+----------------------+------------+------------------+
| 10.0.8.231 | statement/sql/select |          4 |        537450710 |
+------------+----------------------+------------+------------------+
1 row in set (0.00 sec)
```

Behebung von out-of-memory Problemen mit Aurora MySQL-Datenbanken

Mithilfe des Parameters der Instance-Ebene Aurora MySQL `aurora_oom_response` kann die DB-Instance den Arbeitsspeicher des Systems überwachen und den von verschiedenen Anweisungen und Verbindungen verbrauchten Arbeitsspeicher schätzen. Wenn dem System der Arbeitsspeicher knapp wird, kann es eine Liste von Aktionen ausführen, um zu versuchen, diesen Speicher freizugeben. Dadurch wird versucht, einen Neustart der Datenbank aufgrund von out-of-memory (OOM-) Problemen zu vermeiden. Der Parameter auf Instance-Ebene umfasst eine Reihe von kommagetrennten Aktionen, die eine DB-Instance ausführt, wenn ihr Arbeitsspeicher knapp wird. Der `aurora_oom_response` Parameter wird für die Aurora MySQL-Versionen 2 und 3 unterstützt.

Die folgenden Werte und deren Kombinationen können für den `aurora_oom_response` Parameter verwendet werden. Eine leere Zeichenfolge bedeutet, dass keine Aktion ausgeführt wird, und die Funktion wird effektiv ausgeschaltet, sodass die Datenbank anfällig für OOM-Neustarts ist.

- `decline`— Lehnt neue Abfragen ab, wenn der Arbeitsspeicher der DB-Instance knapp wird.
- `kill_connect`— Schließt Datenbankverbindungen, die viel Speicher verbrauchen, und beendet aktuelle Transaktionen und DDL-Anweisungen (Data Definition Language). Diese Antwort wird für Aurora MySQL Version 2 nicht unterstützt.

  Weitere Informationen finden Sie unter KILL-Anweisung in der MySQL-Dokumentation.
- `kill_query`— Beendet Abfragen in absteigender Reihenfolge des Speicherverbrauchs, bis der Instanzspeicher den unteren Schwellenwert überschreitet. DDL-Anweisungen werden nicht beendet.

  Weitere Informationen finden Sie unter KILL-Anweisung in der MySQL-Dokumentation.
- `print`— Druckt nur die Abfragen, die viel Speicher verbrauchen.
- `tune` – Stellt die Caches der internen Tabellen so ein, dass etwas Arbeitsspeicher für das System freigegeben wird. Aurora MySQL verringert den Speicherplatz, der für Caches verwendet wird,

z. `table_open_cache` B. `table_definition_cache` bei Speichermangel. Schließlich setzt Aurora MySQL ihre Speichernutzung wieder auf den Normalwert zurück, wenn das System nicht mehr zu wenig Arbeitsspeicher hat.

Weitere Informationen finden Sie unter table_open_cache und table_definition_cache in der MySQL-Dokumentation.

- `tune_buffer_pool`— Verringert die Größe des Pufferpools, um Speicherplatz freizugeben und ihn dem Datenbankserver zur Verarbeitung von Verbindungen zur Verfügung zu stellen. Diese Antwort wird für Aurora MySQL Version 3.06 und höher unterstützt.

  Sie müssen das Paar entweder `tune_buffer_pool` mit `kill_query` oder `kill_connect` im `aurora_oom_response` Parameterwert verbinden. Andernfalls erfolgt die Größenänderung des Pufferpools nicht, selbst wenn Sie den Wert `tune_buffer_pool` in den Parameterwert mit einbeziehen.

In Aurora MySQL-Versionen unter 3.06 gehören für DB-Instance-Klassen mit einem Arbeitsspeicher von weniger als oder gleich 4 GiB, wenn die Instance unter Speicherauslastung steht, die Standardaktionen`print`, `tunedecline`, und`kill_query`. Für DB-Instance-Klassen mit einem Speicher von mehr als 4 GiB ist der Parameterwert standardmäßig leer (deaktiviert).

In Aurora MySQL Version 3.06 und höher schließt Aurora MySQL für DB-Instance-Klassen mit einem Arbeitsspeicher von weniger als oder gleich 4 GiB auch die Verbindungen mit dem höchsten Speicherverbrauch (). `kill_connect` Für DB-Instance-Klassen mit einem Speicher von mehr als 4 GiB ist der Standardparameterwert`print`.

Wenn Sie häufig auf out-of-memory Probleme stoßen, kann die Speichernutzung mithilfe von Speicherübersichtstabellen überwacht werden, sofern diese Option aktiviert `performance_schema` ist.

Protokollierung für Aurora MySQL-Datenbanken

Aurora MySQL-Protokolle liefern wichtige Informationen über Datenbankaktivitäten und Fehler. Durch die Aktivierung dieser Protokolle können Sie Probleme identifizieren und beheben, die Datenbankleistung verstehen und Datenbankaktivitäten überprüfen. Wir empfehlen Ihnen, diese Protokolle für alle Ihre Aurora MySQL-DB-Instances zu aktivieren, um eine optimale Leistung und Verfügbarkeit der Datenbanken sicherzustellen. Die folgenden Arten der Protokollierung können aktiviert werden. Jedes Protokoll enthält spezifische Informationen, anhand derer Auswirkungen auf die Datenbankverarbeitung aufgedeckt werden können.

- Fehler — Aurora MySQL schreibt nur beim Starten, Herunterfahren und wenn Fehler auftreten, in das Fehlerprotokoll. Eine DB-Instance kann Stunden oder Tage lang laufen, ohne dass neue Einträge in das Fehlerprotokoll geschrieben werden. Wenn Sie keine neuen Einträge sehen, sind im Server keine Fehler aufgetreten, die zu einem Eintrag in das Protokoll führen würden. Die Fehlerprotokollierung ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Aurora-MySQL-Fehlerprotokolle.
- Allgemein — Das allgemeine Protokoll enthält detaillierte Informationen zur Datenbankaktivität, einschließlich aller SQL-Anweisungen, die von der Datenbank-Engine ausgeführt werden. Weitere Informationen zur Aktivierung der allgemeinen Protokollierung und zur Einstellung von Protokollierungsparametern finden Sie unter Aurora-MySQL-Protokolle für langsame Abfragen und allgemeine Protokolle und Das allgemeine Abfrageprotokoll in der MySQL-Dokumentation.

  > **Note**
  >
  > Allgemeine Protokolle können sehr umfangreich werden und Ihren Speicherplatz beanspruchen. Weitere Informationen finden Sie unter Protokollrotation und -aufbewahrung für Aurora MySQL.

- Langsame Abfrage — Das Protokoll für langsame Abfragen besteht aus SQL-Anweisungen, deren Ausführung mehr als long_query_time Sekunden in Anspruch nimmt und für deren Ausführung mindestens min_examined_row_limit-Zeilen untersucht werden müssen. Sie können das Protokoll für langsame Abfragen verwenden, um Abfragen zu finden, deren Ausführung viel Zeit in Anspruch nimmt und die daher für eine Optimierung in Frage kommen.

  Der Standardwert für `long_query_time` ist 10 Sekunden. Wir empfehlen, mit einem hohen Wert zu beginnen, um die langsamsten Abfragen zu identifizieren, und sich dann für die Feinabstimmung nach unten vorzuarbeiten.

  Sie können auch verwandte Parameter wie `log_slow_admin_statements` und `log_queries_not_using_indexes` verwenden. Vergleiche `rows_examined` mit`rows_returned`. Wenn `rows_examined` es viel größer ist als`rows_returned`, dann können diese Abfragen möglicherweise blockiert werden.

  In Aurora MySQL Version 3 können Sie aktivieren, `log_slow_extra` um weitere Informationen zu erhalten. Weitere Informationen finden Sie unter Inhalt des Slow Query-Logs in der MySQL-Dokumentation. Sie können Änderungen auch auf Sitzungsebene vornehmen, `long_query_time` um die Abfrageausführung interaktiv zu debuggen. Dies ist besonders nützlich, wenn `log_slow_extra` es global aktiviert ist.

Weitere Informationen zur Aktivierung der langsamen Abfrageprotokollierung und zur Einstellung der Protokollierungsparameter finden Sie unter Aurora-MySQL-Protokolle für langsame Abfragen und allgemeine Protokolle und Das langsame Abfrageprotokoll in der MySQL-Dokumentation.

- Audit — Das Audit-Log überwacht und protokolliert Datenbankaktivitäten. Die Auditprotokollierung für Aurora MySQL heißt Advanced Auditing. Um Advanced Auditing zu aktivieren, legen Sie bestimmte DB-Cluster-Parameter fest. Weitere Informationen finden Sie unter Verwenden von Advanced Auditing in einem Amazon Aurora MySQL DB-Cluster.
- Binär — Das Binärlog (Binlog) enthält Ereignisse, die Datenbankänderungen beschreiben, wie z. B. Tabellenerstellungsvorgänge und Änderungen an Tabellendaten. Es enthält auch Ereignisse für Anweisungen, die möglicherweise Änderungen hätten bewirken können (z. B. ein DELETE-Befehl, bei dem keine Zeilen gefunden wurden), sofern nicht die zeilenbasierte Protokollierung verwendet wird. Das Binärprotokoll enthält auch Informationen darüber, wie lange die aktualisierten Daten für jede Anweisung gedauert haben.

  Wenn Sie einen Server mit aktivierter Binärprotokollierung ausführen, wird die Leistung etwas langsamer. Die Vorteile der binären Anmeldung, mit der Sie Replikations- und Wiederherstellungsvorgänge einrichten können, überwiegen jedoch in der Regel diese geringfügige Leistungseinbuße.

  > **Note**
  >
  > Aurora MySQL benötigt keine binäre Protokollierung für Wiederherstellungsvorgänge.

  Weitere Informationen zum Aktivieren der Binärprotokollierung und zum Einstellen des Binärprotokollformats finden Sie unter Konfiguration von Aurora MySQL und Das Binärprotokoll in der MySQL-Dokumentation.

Sie können die Fehler-, allgemeinen, langsamen, Abfrage- und Auditprotokolle in Amazon CloudWatch Logs veröffentlichen. Weitere Informationen finden Sie unter Veröffentlichen von Datenbankprotokollen in Amazon CloudWatch Logs.

Ein weiteres nützliches Tool für die Zusammenfassung langsamer, allgemeiner und binärer Protokolldateien ist pt-query-digest.

Fehlerbehebung bei der Abfrageleistung für Aurora MySQL-Datenbanken

MySQL ermöglicht die Steuerung des Abfrageoptimierers durch Systemvariablen, die sich darauf auswirken, wie Abfragepläne ausgewertet werden, umschaltbare Optimierungen, Optimizer- und Indexhinweise sowie das Optimierer-Kostenmodell. Diese Datenpunkte können nicht nur beim Vergleich verschiedener MySQL-Umgebungen hilfreich sein, sondern auch, um frühere Abfrageausführungspläne mit aktuellen Ausführungsplänen zu vergleichen und die Gesamtausführung einer MySQL-Abfrage zu jedem Zeitpunkt zu verstehen.

Die Abfrageleistung hängt von vielen Faktoren ab, darunter dem Ausführungsplan, dem Tabellenschema und der Größe, Statistiken, Ressourcen, Indizes und der Parameterkonfiguration. Die Abfrageoptimierung erfordert die Identifizierung von Engpässen und die Optimierung des Ausführungspfads.

- Suchen Sie den Ausführungsplan für die Abfrage und überprüfen Sie, ob die Abfrage die entsprechenden Indizes verwendet. Sie können Ihre Abfrage optimieren, indem Sie die Details der einzelnen Pläne verwenden `EXPLAIN` und überprüfen.
- Aurora MySQL Version 3 (kompatibel mit MySQL 8.0 Community Edition) verwendet eine `EXPLAIN ANALYZE` Anweisung. Die `EXPLAIN ANALYZE` Anweisung ist ein Profilierungstool, das zeigt, wo MySQL Zeit für Ihre Anfrage aufwendet und warum. Mit`EXPLAIN ANALYZE`, Aurora MySQL plant, bereitet und führt die Abfrage aus, während gleichzeitig Zeilen gezählt und die Zeit gemessen wird, die an verschiedenen Punkten des Ausführungsplans verbracht wurde. Wenn die Abfrage abgeschlossen ist, werden der Plan und seine Messungen anstelle des Abfrageergebnisses `EXPLAIN ANALYZE` gedruckt.
- Halten Sie Ihre Schemastatistiken mithilfe der `ANALYZE` Anweisung auf dem neuesten Stand. Der Abfrageoptimierer kann aufgrund veralteter Statistiken manchmal schlechte Ausführungspläne auswählen. Dies kann aufgrund ungenauer Kardinalitätsschätzungen von Tabellen und Indizes zu einer schlechten Leistung einer Abfrage führen. `last_update`In der Spalte der Tabelle innodb_table_stats wird angezeigt, wann Ihre Schemastatistiken zuletzt aktualisiert wurden. Dies ist ein guter Indikator für „Veraldung“.
- Andere Probleme können auftreten, wie z. B. eine schiefe Verteilung von Daten, die bei der Tabellenkardinalität nicht berücksichtigt werden. Weitere Informationen finden Sie unter Schätzung der ANALYZE TABLE-Komplexität für InnoDB-Tabellen und Histogrammstatistiken in MySQL in der MySQL-Dokumentation.

Den Zeitaufwand für Abfragen verstehen

Es gibt folgende Möglichkeiten, den Zeitaufwand für Abfragen zu ermitteln:

- Profilerstellung
- Leistungsschema
- Abfrageoptimierer

Profilerstellung

Standardmäßig ist die Profilerstellung deaktiviert. Aktivieren Sie die Profilerstellung, führen Sie dann die langsame Abfrage aus und überprüfen Sie das zugehörige Profil.

```
SET profiling = 1;
Run your query.
SHOW PROFILE;
```

1. Identifizieren Sie die Phase, in der die meiste Zeit verbracht wird. Gemäß den allgemeinen Thread-Zuständen in der MySQL-Dokumentation ist das Lesen und Verarbeiten von Zeilen für eine `SELECT` Anweisung oft der am längsten laufende Zustand während der Lebensdauer einer bestimmten Abfrage. Sie können die `EXPLAIN` Anweisung verwenden, um zu verstehen, wie MySQL diese Abfrage ausführt.
2. Sehen Sie sich das Protokoll für langsame Abfragen an`rows_sent`, um eine Bewertung vorzunehmen `rows_examined` und sicherzustellen, dass die Arbeitslast in jeder Umgebung ähnlich ist. Weitere Informationen finden Sie unter Protokollierung für Aurora MySQL-Datenbanken.
3. Führen Sie den folgenden Befehl für Tabellen aus, die Teil der identifizierten Abfrage sind:

   ```
   SHOW TABLE STATUS\G;
   ```

4. Erfassen Sie die folgenden Ausgaben vor und nach der Ausführung der Abfrage in jeder Umgebung:

   ```
   SHOW GLOBAL STATUS;
   ```

5. Führen Sie die folgenden Befehle in jeder Umgebung aus, um festzustellen, ob andere Abfragen/Sitzungen die Leistung dieser Beispielabfrage beeinflussen.

```
SHOW FULL PROCESSLIST;

SHOW ENGINE INNODB STATUS\G;
```

Wenn die Ressourcen auf dem Server ausgelastet sind, wirkt sich dies manchmal auf jeden anderen Vorgang auf dem Server aus, einschließlich Abfragen. Sie können auch regelmäßig Informationen erfassen, wenn Abfragen ausgeführt werden, oder einen `cron` Job einrichten, um Informationen in sinnvollen Intervallen zu erfassen.

Leistungsschema

Das Leistungsschema bietet nützliche Informationen über die Leistung der Serverlaufzeit und hat gleichzeitig nur minimale Auswirkungen auf diese Leistung. Dies unterscheidet sich von der`information_schema`, die Schemainformationen über die DB-Instance bereitstellt. Weitere Informationen finden Sie unter Aktivieren des Leistungsschemas für Performance Insights in Aurora MySQL.

Den Trace des Optimizers abfragen

Um zu verstehen, warum ein bestimmter Abfrageplan für die Ausführung ausgewählt wurde, können Sie den `optimizer_trace` Zugriff auf den MySQL-Abfrageoptimierer einrichten.

Führen Sie einen Optimierer-Trace aus, um ausführliche Informationen zu allen Pfaden anzuzeigen, die dem Optimierer zur Verfügung stehen, und zu seiner Auswahl.

```
SET SESSION OPTIMIZER_TRACE="enabled=on";
SET optimizer_trace_offset=-5, optimizer_trace_limit=5;

-- Run your query.
SELECT * FROM table WHERE x = 1 AND y = 'A';

-- After the query completes:
SELECT * FROM information_schema.OPTIMIZER_TRACE;
SET SESSION OPTIMIZER_TRACE="enabled=off";
```

Überprüfen der Einstellungen des Abfrageoptimierers

Aurora MySQL Version 3 (kompatibel mit MySQL 8.0 Community Edition) weist im Vergleich zu Aurora MySQL Version 2 (kompatibel mit MySQL 5.7 Community Edition) viele Optimierungsänderungen auf. Wenn Sie einige benutzerdefinierte Werte für haben, empfehlen wir

Ihnenoptimizer_switch, die Unterschiede in den Standardeinstellungen zu überprüfen und optimizer_switch Werte festzulegen, die für Ihren Workload am besten geeignet sind. Wir empfehlen Ihnen außerdem, die für Aurora MySQL Version 3 verfügbaren Optionen zu testen, um zu überprüfen, wie Ihre Abfragen funktionieren.

> **Note**
>
> Aurora MySQL Version 3 verwendet den Community-Standardwert 20 für den Parameter innodb_stats_persistent_sample_pages.

Sie können den folgenden Befehl verwenden, um die Werte optimizer_switch anzuzeigen:

```
SELECT @@optimizer_switch\G;
```

Die folgende Tabelle zeigt die optimizer_switch Standardwerte für Aurora MySQL Versionen 2 und 3.

Einstellung	Aurora-MySQL-Version 2	Aurora-MySQL-Version 3
batched_key_access	aus	aus
block_nested_loop	on	on
condition_fanout_filter	on	on
derived_condition_pushdown	–	on
derived_merge	on	on
duplicateweedout	on	on
engine_condition_pushdown	on	on
firstmatch	on	on
hash_join	aus	on
hash_join_cost_based	on	–

Einstellung	Aurora-MySQL-Version 2	Aurora-MySQL-Version 3
hypergraph_optimizer	–	aus
index_condition_pushdown	on	on
index_merge	on	on
index_merge_intersection	on	on
index_merge_sort_union	on	on
index_merge_union	on	on
loosescan	on	on
materialization	on	on
mrr	on	on
mrr_cost_based	on	on
prefer_ordering_index	on	on
semijoin	on	on
skip_scan	–	on
subquery_materialization_cost_based	on	on
subquery_to_derived	–	aus
use_index_extensions	on	on
use_invisible_indexes	–	aus

Weitere Informationen finden Sie unter Switchable Optimizations (MySQL 5.7) und Switchable Optimizations (MySQL 8.0) in der MySQL-Dokumentation.

Amazon Aurora MySQL-Referenz

Diese Referenz enthält Informationen über Aurora MySQL-Parameter, Statusvariablen und allgemeine SQL-Erweiterungen oder Unterschiede zur MySQL-Datenbank-Engine der Community.

Themen

Aurora MySQL Konfigurationsparameter

Sie können Ihr Amazon-Aurora-MySQL-DB-Cluster auf dieselbe Art und Weise verwalten, wie Sie Ihre anderen Amazon-RDS-DB-Instances verwalten, und zwar indem Sie die Parameter in einer DB-Parametergruppe verwenden. Amazon Aurora unterscheidet sich von anderen DB-Engines dadurch, dass Sie über einen DB-Cluster verfügen, der mehrere DB-Instances enthält. Folglich gelten einige der Parameter, mit denen Sie Ihren Aurora MySQL-DB-Cluster verwalten, für den gesamten Cluster. Andere Parameter gelten nur für eine bestimmte DB-Instance im DB-Cluster.

Um Parameter auf Cluster-Ebene zu verwalten, verwenden Sie DB-Cluster-Parametergruppen. Um Parameter auf Instance-Ebene zu verwalten, verwenden Sie DB-Parametergruppen. Jede DB-Instance in einem Aurora MySQL-DB-Cluster ist mit der MySQL-Datenbank-Engine kompatibel. Sie wenden jedoch einige der Parameter der MySQL-Datenbank-Engine auf Cluster-Ebene an und verwalten diese Parameter mit DB-Cluster-Parametergruppen. Sie können keine Parameter auf Clusterebene in der DB-Parametergruppe für eine Instance in einem Aurora-DB-Cluster finden. Eine Liste der Parameter auf Clusterebene erscheint weiter unten in diesem Thema.

Sie können sowohl Parameter auf Cluster- als auch auf Instanzebene mit der AWS Management Console, der oder der Amazon AWS CLI RDS-API verwalten. Sie verwenden separate Befehle für die Verwaltung von Parametern auf Cluster- und Instance-Ebene. Beispielsweise können Sie mit dem CLI-Befehl modify-db-cluster-parameter-group Parameter auf Clusterebene in einer DB-Cluster-Parametergruppe verwalten. Sie können den CLI-Befehl modify-db-parameter-group verwenden,

um Parameter auf Instance-Ebene in einer DB-Parametergruppe für eine DB-Instance in einem DB-Cluster zu verwalten.

Sie können Parameter auf Cluster- und Instance-Ebene in der Konsole oder mithilfe der CLI oder der RDS-API anzeigen. Sie können beispielsweise den AWS CLI Befehl describe-db-cluster-parameters verwenden, um Parameter auf Clusterebene in einer DB-Cluster-Parametergruppe anzuzeigen. Sie können den CLI-Befehl describe-db-parameters verwenden, um Parameter auf Instance-Ebene in einer DB-Parametergruppe für eine DB-Instance in einem DB-Cluster anzuzeigen.

> **Note**
>
> Jede Standard-Parametergruppe enthält die Standardwerte für alle Parameter in der Parametergruppe. Wenn der Parameter „Engine-Standard“ für diesen Wert hat, finden Sie in der versionsspezifischen MySQL- oder PostgreSQL-Dokumentation den tatsächlichen Standardwert.
> Sofern nicht anders angegeben, gelten die in den folgenden Tabellen aufgeführten Parameter für die Aurora-MySQL-Versionen 2 und 3.

Weitere Informationen zu DB-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen. Regeln und Einschränkungen für Aurora Serverless v1-Cluster finden Sie unter Parametergruppen für Aurora Serverless v1.

Themen

- Parameter auf Cluster-Ebene
- Parameter auf Instance-Ebene
- MySQL-Parameter, die nicht auf Aurora MySQL zutreffen
- Globale Statusvariablen von Aurora MySQL
- MySQL-Statusvariablen, die nicht für Aurora MySQL gelten

Parameter auf Cluster-Ebene

In der folgenden Tabelle werden alle Parameter aufgeführt, die für das gesamte Aurora MySQL-DB-Cluster gelten.

Parametername	Anpassbar	Hinweise
aurora_binlog_read_buffer_size	Ja	Beeinflusst nur Cluster, die Binärprotokoll-Replikation (Binlog) verwenden. Hinweise zur Binärprotokoll-Replikation finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation). Aus Aurora-MySQL-Version 3 entfernt.
aurora_binlog_replication_max_yield_seconds	Ja	Beeinflusst nur Cluster, die Binärprotokoll-Replikation (Binlog) verwenden. Hinweise zur Binärprotokoll-Replikation finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).
aurora_binlog_replication_sec_index_parallel_workers	Ja	Legt die Gesamtzahl der verfügbaren parallel Threads fest, um sekundäre Indexänderungen anzuwenden, wenn Transaktionen für große Tabellen mit mehr als einem sekundären Index repliziert werden. Der Parameter ist standardmäßig auf 0 (deaktiviert) gesetzt. Dieser Parameter ist in Aurora MySQL Version 306 und höher verfügbar. Weitere Informationen finden Sie unter Optimieren der binären Protokollreplikation .
aurora_binlog_use_large_read_buffer	Ja	Beeinflusst nur Cluster, die Binärprotokoll-Replikation (Binlog) verwenden. Hinweise zur Binärprotokoll-Replikation

Parametername	Anpassbar	Hinweise
		finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation). Aus Aurora-MySQL-Version 3 entfernt.
`aurora_disable_hash_join`	Ja	Setzen Sie diesen Parameter auf `ON`, um die Hash-Join-Optimierung in Aurora MySQL Version 2.09 oder höher zu deaktivieren. Für Version 3 wird dies nicht unterstützt. Weitere Informationen finden Sie unter Arbeiten mit Parallel Query für Amazon Aurora MySQL.
`aurora_enable_replica_log_compression`	Ja	Weitere Informationen finden Sie unter Performance-Überlegungen zur Amazon Aurora MySQL-Replikation. Gilt nicht für Cluster, die Teil einer globalen Aurora-Datenbank sind. Aus Aurora-MySQL-Version 3 entfernt.
`aurora_enable_repl_bin_log_filtering`	Ja	Weitere Informationen finden Sie unter Performance-Überlegungen zur Amazon Aurora MySQL-Replikation. Gilt nicht für Cluster, die Teil einer globalen Aurora-Datenbank sind. Aus Aurora-MySQL-Version 3 entfernt.
`aurora_enable_staggered_replica_restart`	Ja	Diese Einstellung ist in Aurora MySQL Versione 3 verfügbar, wird aber nicht verwendet.

Parametername	Anpassbar	Hinweise
`aurora_enable_zdr`	Ja	Diese Einstellung ist standardmäßig in Aurora MySQL 2.10 und höher aktiviert . Weitere Informationen finden Sie unter Neustart ohne Ausfallzeit (ZDR) für Amazon Aurora MySQL.
`aurora_enhanced_binlog`	Ja	Legen Sie den Wert dieses Parameters auf 1 fest, um das erweiterte Binärprotokoll in Aurora MySQL Version 3.03.1 und höher zu aktivieren. Weitere Informationen finden Sie unter Einrichten eines erweiterten Binärprotokolls.
`aurora_jemalloc_background_thread`	Ja	Verwenden Sie diesen Parameter, um einen Hintergrund-Thread zur Durchführung von Speicherwartungsvorgängen zu aktivieren. Die zulässigen Werte sind `0` (deaktiviert) und `1` (aktiviert). Der Standardwert ist `0`. Dieser Parameter gilt für Aurora MySQL Version 3.05 und höher.
`aurora_jemalloc_dirty_decay_ms`	Ja	Verwenden Sie diesen Parameter , um freigegebenen Speicher für eine bestimmte Zeit (in Millisekunden) beizubehalten. Die Beibehaltung des Speichers ermöglicht eine schnellere Wiederverwendung. Die zulässigen Werte sind `0` bis `18446744073709551615` . Der Standardwert (`0`) gibt den gesamten Speicher als freien Speicher an das Betriebssystem zurück. Dieser Parameter gilt für Aurora MySQL Version 3.05 und höher.

Parametername	Anpassbar	Hinweise
`aurora_jemalloc_tcache_enabled`	Ja	Verwenden Sie diesen Parameter, um kleine Speicheranforderungen (bis zu 32 KiB) in einem lokalen Thread-Cache zu bearbeiten und dabei die Speicherarenen zu umgehen. Die zulässigen Werte sind `0` (deaktiviert) und 1 (aktiviert). Der Standardwert ist 1. Dieser Parameter gilt für Aurora MySQL Version 3.05 und höher.
`aurora_load_from_s3_role`	Ja	Weitere Informationen finden Sie unter Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket. Derzeit nicht in Aurora-MySQL-Version 3 verfügbar. Verwenden Sie `aws_default_s3_role` .
`aurora_mask_password_hashes_type`	Ja	Diese Einstellung ist in Aurora MySQL 2.11 und höher standardmäßig aktiviert. Verwenden Sie diese Einstellung, um Passwort-Hashes von Aurora MySQL in den allgemeinen Protokollen, den langsamen Abfrageprotokollen und den Audit-Protokollen zu maskieren . Die zulässigen Werte sind `0` und 1 (Standardeinstellung). Wenn diese Einstellung auf 1 festgelegt ist, werden Passwörter als `<secret>` protokolliert. Wenn diese Einstellung auf `0` festgelegt ist, werden Passwörter als Hash-Werte (#) protokolliert.

Parametername	Anpassbar	Hinweise
`aurora_select_into_s3_role`	Ja	Weitere Informationen finden Sie unter Speichern von Daten aus einem Amazon Aurora MySQL-DB-Cluster in Textdateien in einem Amazon S3-Bucket. Derzeit nicht in Aurora-MySQL-Version 3 verfügbar. Verwenden Sie `aws_default_s3_role` .
`authentication_kerberos_caseins_cmp`	Ja	Steuert den Benutzernamenvergleich ohne Berücksichtigung der Groß-/Kleinschreibung für das Plug-in `authentication_kerberos` . Setzen Sie den Parameter auf `true`, um den Vergleich ohne Berücksichtigung der Groß-/Kleinschreibung zu aktivieren. Standardmäßig wird der Vergleich unter Berücksichtigung der Groß-/Kleinschreibung verwendet (`false`). Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung für Aurora MySQL. Dieser Parameter ist in Aurora MySQL Version 3.03 und höher verfügbar.
`auto_increment_increment`	Ja	
`auto_increment_offset`	Ja	
`aws_default_lambda_role`	Ja	Weitere Informationen finden Sie unter Aufrufen einer Lambda-Funktion aus einem Amazon Aurora MySQL-DB-Cluster.

Parametername	Anpassbar	Hinweise
`aws_default_s3_role`	Ja	Wird beim Aufrufen der Anweisung `LOAD DATA FROM S3`, `LOAD XML FROM S3` oder `SELECT INTO OUTFILE S3` aus Ihrem DB-Cluster verwendet. Bei Aurora MySQL Version 2 wird die in diesem Parameter festgelegte IAM-Rolle verwendet, wenn keine IAM-Rolle für `aurora_load_from_s3_role` oder `aurora_select_into_s3_role` für die entsprechende Anweisung festgelegt ist. Bei Aurora-MySQL-Version 3 wird die für diesen Parameter festgelegte IAM-Rolle immer verwendet. Weitere Informationen finden Sie unter Zuweisen einer IAM-Rolle zu einem Amazon-Aurora-MySQL-DB-Cluster.
`binlog_backup`	Ja	Legen Sie den Wert dieses Parameters auf 0 fest, um das erweiterte Binärprotokoll in Aurora MySQL Version 3.03.1 und höher zu aktivieren. Sie können diesen Parameter nur deaktivieren, wenn Sie das erweiterte Binärprotokoll verwenden. Weitere Informationen finden Sie unter Einrichten eines erweiterten Binärprotokolls.

Parametername	Anpassbar	Hinweise
binlog_checksum	Ja	Die RDS-API AWS CLI und die RDS-API melden einen Wert von, None wenn dieser Parameter nicht festgelegt ist. In diesem Fall verwendet Aurora MySQL den Standardwert für die Engine, d.h. CRC32. Dies ist anders als die explizite Einstellung von NONE, die die Prüfsumme ausschaltet.
binlog-do-db	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog_format	Ja	Weitere Informationen finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).
binlog_group_commit_sync_delay	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog_group_commit_sync_no_delay_count	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog-ignore-db	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog_replication_globaldb	Ja	Legen Sie den Wert dieses Parameters auf 0 fest, um das erweiterte Binärprotokoll in Aurora MySQL Version 3.03.1 und höher zu aktivieren. Sie können diesen Parameter nur deaktivieren, wenn Sie das erweiterte Binärprotokoll verwenden. Weitere Informationen finden Sie unter Einrichten eines erweiterten Binärprotokolls.

Parametername	Anpassbar	Hinweise
binlog_row_image	Nein	
binlog_row_metadata	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog_row_value_options	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog_rows_query_log_events	Ja	
binlog_transaction_compression	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog_transaction_compression_level_zstd	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog_transaction_dependency_history_size	Ja	Dieser Parameter legt eine Obergrenze für die Anzahl der Zeilen-Hashes fest, die im Speicher abgelegt und für die Suche nach der Transaktion, die eine bestimmte Zeile zuletzt geändert hat, verwendet werden. Sobald diese Anzahl von Hashes erreicht wurde, wird der Verlauf gelöscht. Dieser Parameter gilt für Aurora-MySQL-Version 2.12 und höher sowie Version 3.
binlog_transaction_dependency_tracking	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
character-set-client-handshake	Ja	
character_set_client	Ja	

Parametername	Anpassbar	Hinweise
character_set_connection	Ja	
character_set_database	Ja	
character_set_filesystem	Ja	
character_set_results	Ja	
character_set_server	Ja	
collation_connection	Ja	
collation_server	Ja	
completion_type	Ja	
default_storage_engine	Nein	Aurora MySQL-Cluster verwenden für all Ihre Daten die InnoDB-Speicher-Engine.
enforce_gtid_consistency	Manchmal	Veränderbar in Aurora MySQL-Version 2 und höher.
event_scheduler	Ja	Zeigt den Status des Ereignisplaners an. Modifizierbar nur auf Clusterebene in Aurora-MySQL-Version 3.
gtid-mode	Manchmal	Veränderbar in Aurora MySQL-Version 2 und höher.

Parametername	Anpassbar	Hinweise
`information_schema_stats_expiry`	Ja	Die Anzahl der Sekunden, nach denen der MySQL-Datenbankserver Daten von der Speicher-Engine abruft und die Daten im Cache ersetzt. Die zulässigen Werte sind `0` bis `31536000`. Dieser Parameter gilt für Aurora MySQL Version 3.
`init_connect`	Ja	Der Befehl, der vom Server für jeden Client ausgeführt wird, der eine Verbindung herstellt. Verwenden Sie doppelte Anführungszeichen („) für Einstellungen, um Verbindungsfehler zu vermeiden, zum Beispiel: `SET optimizer_switch="hash_join =off"` Bei Aurora MySQL Version 3 gilt dieser Parameter nicht für Benutzer, die über die `CONNECTION_ADMIN` -Berechtigung verfügen. Dies schließt den Aurora-Hauptbenutzer ein. Weitere Informationen finden Sie unter Rollenbasiertes Berechtigungsmodell.
`innodb_adaptive_hash_index`	Ja	Sie können diesen Parameter auf DB-Cluster-Ebene in den Aurora-MySLQ-Versionen 2 und 3 ändern. Der Adaptive-Hash-Index wird auf Reader-DB-Instances nicht unterstützt.

Parametername	Anpassbar	Hinweise
innodb_aurora_instant_alter_column_allowed	Ja	Steuert, ob der INSTANT-Algorithmus für ALTER COLUMN-Operationen auf globaler Ebene verwendet werden kann. Die zulässigen Werte sind folgende: • 0— Der INSTANT Algorithmus ist für ALTER COLUMN Operationen (OFF) nicht zulässig. Kehrt zu anderen Algorithmen zurück. • 1— Der INSTANT Algorithmus ist für ALTER COLUMN Operationen (ON) zulässig. Dies ist der Standardwert. Weitere Informationen finden Sie unter Column Operations in der MySQL-Dokumentation. Dieser Parameter gilt für Aurora MySQL Version 3.05 und höher.
innodb_autoinc_lock_mode	Ja	
innodb_checksums	Nein	Aus Aurora-MySQL-Version 3 entfernt.
innodb_cmp_per_index_enabled	Ja	
innodb_commit_concurrency	Ja	
innodb_data_home_dir	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.

Parametername	Anpassbar	Hinweise
`innodb_deadlock_detect`	Ja	Diese Option wird verwendet, um die Deadlock-Erkennung in Aurora-MySQL-Version 2.11 und höher sowie Version 3 zu deaktivieren. Auf Systemen mit hoher Parallelität kann die Deadlock-Erkennung zu einer Verlangsamung führen, wenn zahlreiche Threads auf dieselbe Sperre warten. Weitere Informationen zu diesem Parameter finden Sie in der MySQL-Dokumentation.
`innodb_default_row_format`	Ja	Dieser Parameter definiert das Standardzeilenformat für InnoDB-Tabellen (einschließlich benutzerdefinierter temporärer InnoDB-Tabellen). Er gilt für Aurora MySQL Version 2 und 3. Mögliche Werte sind `DYNAMIC`, `COMPACT` oder `REDUNDANT`. .
`innodb_file_per_table`	Ja	Dieser Parameter wirkt sich auf die Organisation des Tabellenspeichers aus. Weitere Informationen finden Sie unter Speicherskalierung.

Parametername	Anpassbar	Hinweise
innodb_flush_log_at_trx_commit	Ja	Es wird dringend empfohlen, den Standardwert von zu verwenden1. Bevor Sie in Aurora MySQL Version 3 diesen Parameter auf einen anderen Wert als setzen können1, müssen Sie den Wert innodb_trx_commit_allow_data_loss auf setzen1. Weitere Informationen finden Sie unter Konfigurieren, wie oft der Protokollpuffer geleert wird.
innodb_ft_max_token_size	Ja	
innodb_ft_min_token_size	Ja	
innodb_ft_num_word_optimize	Ja	
innodb_ft_sort_pll_degree	Ja	
innodb_online_alter_log_max_size	Ja	
innodb_optimize_fulltext_only	Ja	
innodb_page_size	Nein	
innodb_print_all_deadlocks	Ja	Wenn dieser Parameter aktiviert ist, werden Informationen über alle InnoDB-Deadlocks im Fehlerprotokoll von Aurora MySQL aufgezeichnet. Weitere Informationen finden Sie unter Minimieren und Beheben von Aurora-MySQL-Deadlocks.

Parametername	Anpassbar	Hinweise
innodb_purge_batch_size	Ja	
innodb_purge_threads	Ja	
innodb_rollback_on_timeout	Ja	
innodb_rollback_segments	Ja	
innodb_spin_wait_delay	Ja	
innodb_strict_mode	Ja	
innodb_support_xa	Ja	Aus Aurora-MySQL-Version 3 entfernt.
innodb_sync_array_size	Ja	
innodb_sync_spin_loops	Ja	
innodb_stats_include_delete_marked	Ja	Wenn dieser Parameter aktiviert ist, bezieht InnoDB zum Löschen markierte Datensätze in die Berechnung der persistenten Optimierungsstatistiken ein. Dieser Parameter gilt für Aurora-My SQL-Version 2.12 und höher sowie Version 3.
innodb_table_locks	Ja	

Parametername	Anpassbar	Hinweise
innodb_trx_commit_allow_data_loss	Ja	Setzen Sie in Aurora MySQL Version 3 den Wert dieses Parameters auf, 1 damit Sie den Wert von ändern könneninnodb_flush_log_at_trx_commit . Der Standardwert von innodb_trx_commit_allow_data_loss ist 0. Weitere Informationen finden Sie unter Konfigurieren, wie oft der Protokollpuffer geleert wird.
innodb_undo_directory	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.
internal_tmp_disk_storage_engine	Ja	Steuert, welche In-Memory-Speicher-Engine für interne temporäre Tabellen verwendet wird. Zulässige Werte sind INNODB und MYISAM. Dieser Parameter gilt für Aurora MySQL Version 2.
internal_tmp_mem_storage_engine	Ja	Steuert, welche In-Memory-Speicher-Engine für interne temporäre Tabellen verwendet wird. Zulässige Werte sind MEMORY und TempTable . Dieser Parameter gilt für Aurora MySQL Version 3.
key_buffer_size	Ja	Schlüssel-Cache für MyISAM-Tabellen. Weitere Informationen finden Sie unter keycache->cache_lock mutex.

Parametername	Anpassbar	Hinweise
`lc_time_names`	Ja	
`log_error_suppression_list`	Ja	Gibt eine Liste von Fehlercodes an, die nicht im MySQL-Fehlerprotokoll protokolliert sind. Auf diese Weise können Sie bestimmte unkritische Fehlerbedingungen ignorieren, um Ihre Fehlerprotokolle sauber zu halten. Weitere Informationen finden Sie unter log_error_suppression_list in der MySQL-Dokumentation. Dieser Parameter gilt für Aurora MySQL Version 3.03 und höher.
`low_priority_updates`	Ja	`INSERT`-, `UPDATE`-, `DELETE`- und `LOCK TABLE WRITE`-Operationen warten, bis kein ausstehender `SELECT`-Vorgang mehr vorhanden ist. Dieser Parameter wirkt sich nur auf Speicher-Engines aus, die ausschließlich Sperren auf Tabellenebene verwenden (MyISAM, MEMORY, MERGE). Dieser Parameter gilt für Aurora-My SQL-Version 3.

Parametername	Anpassbar	Hinweise
`lower_case_table_names`	Ja (Aurora-MySQL-Version 2) Nur zur Clusterer stellung (Aurora-MySQL-Version 3)	Stellen Sie in Aurora-MySQL-Version 2.10 und höheren 2.x-Versionen sicher, dass Sie alle Reader-Instances neu starten, nachdem Sie diese Einstellung geändert und die Writer-Instance neu gestartet haben. Details hierzu finden Sie unter Neustart eines Aurora-Clusters mit Leseverfügbarkeit. In Aurora-MySQL-Version 3 wird der Wert dieses Parameters zum Zeitpunkt der Erstellung des Clusters dauerhaft festgelegt. Wenn Sie für diese Option einen nicht standardmäßigen Wert verwenden, richten Sie Ihre benutzerdefinierte Parametergruppe Aurora-MySQL-Version 3 vor dem Upgrade ein, und geben Sie die Parametergruppe während des Snapshot-Wiederherstellungsvorgangs an, der den Cluster der Version 3 erstellt. Mit einer globalen Aurora-Datenbank, die auf Aurora MySQL basiert, können Sie kein direktes Upgrade von Aurora MySQL Version 2 auf Version 3 durchführen, wenn der `lower_case_table_names` -Parameter aktiviert ist. Weitere Informationen zu den möglichen Verfahren finden Sie unter Hauptversions-Upgrades.
`master-info-repository`	Ja	Aus Aurora-MySQL-Version 3 entfernt.

Parametername	Anpassbar	Hinweise
`master_verify_checksum`	Ja	Aurora-MySQL-Version 2. Verwenden Sie `source_verify_checksum` in Aurora-MySQL-Version 3.
`max_delayed_threads`	Ja	Legt die maximale Anzahl von Threads für die Verarbeitung von `INSERT DELAYED`-Anweisungen fest. Dieser Parameter gilt für Aurora MySQL Version 3.
`max_error_count`	Ja	Die maximale Anzahl von Fehler-, Warn- und Hinweismeldungen, die für die Anzeige gespeichert werden sollen. Dieser Parameter gilt für Aurora MySQL Version 3.
`max_execution_time`	Ja	Das Timeout für die Ausführung von `SELECT` Anweisungen in Millisekunden. Der Wert kann zwischen — liegen. `0` `18446744073709551615` Wenn auf gesetzt`0`, gibt es kein Timeout. Weitere Informationen finden Sie unter max_execution_time in der MySQL-Dokumentation.
`min_examined_row_limit`	Ja	Verwenden Sie diesen Parameter, um zu verhindern, dass Abfragen, die weniger als die angegebene Anzahl von Zeilen untersuchen, protokolliert werden. Dieser Parameter gilt für Aurora-MySQL-Version 3.

Parametername	Anpassbar	Hinweise
`partial_revokes`	Nein	Dieser Parameter gilt für Aurora MySQL Version 3.
`preload_buffer_size`	Ja	Die Größe des Puffers, der beim Vorabladen von Indizes zugewiesen wird. Dieser Parameter gilt für Aurora MySQL Version 3.
`query_cache_type`	Ja	Aus Aurora-MySQL-Version 3 entfernt.

Parametername	Anpassbar	Hinweise
`read_only`	Ja	Wenn dieser Parameter aktiviert ist, erlaubt der Server nur Aktualisierungen, die von Replikat-Threads durchgeführt werden. Für Aurora MySQL Version 2 sind die folgenden Werte gültig: • `0` – `OFF` • `1` – `ON` • `{TrueIfReplica}` — `ON` für Read Replicas. Dies ist der Standardwert. • `{TrueIfClusterReplica}` — `ON` für Replikatcluster wie regionsüb ergreifende Read Replicas, sekundäre Cluster in einer globalen Aurora-Datenbank und Blue/Green-Bereitstellungen. Für Aurora MySQL Version 3 sind die folgenden Werte gültig: • `0`—`OFF`. Dies ist der Standardwert. • `1` – `ON` • `{TrueIfClusterReplica}` — `ON` für Replikatcluster wie regionsüb ergreifende Read Replicas, sekundäre Cluster in einer globalen Aurora-Datenbank und Blue/Green-Bereitstellungen. Bei Aurora MySQL Version 3 gilt dieser Parameter nicht für Benutzer, die über die `CONNECTION_ADMIN` -

Parametername	Anpassbar	Hinweise
		Berechtigung verfügen. Dies schließt den Aurora-Hauptbenutzer ein. Weitere Informationen finden Sie unter Rollenbasiertes Berechtigungsmodell.
`relay-log-space-limit`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`replica_parallel_type`	Ja	Dieser Parameter ermöglicht die parallele Ausführung aller Threads mit ausstehendem Commit, die sich bereits in der Vorbereitungsphase befinden, auf dem Replikat, ohne die Konsistenz zu verletzen. Er gilt für Aurora MySQL Version 3. In Aurora MySQL Version 3.03.* und niedriger ist der Standardwert DATABASE. In Aurora MySQL Version 3.04.* und höher ist der Standardwert LOGICAL_CLOCK.
`replica_preserve_commit_order`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`replica_transaction_retries`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.

Parametername	Anpassbar	Hinweise
`replica_type_conversions`	Ja	Dieser Parameter bestimmt die Typkonvertierungen, die für Replikate verwendet werden. Die zulässigen Werte sind `ALL_LOSSY` , `ALL_NON_LOSSY` , `ALL_SIGNED` und `ALL_UNSIGNED` . Weitere Informationen finden Sie in der MySQL-Dokumentation unter Replication with Differing Table Definitions on Source and Replica. Dieser Parameter gilt für Aurora MySQL Version 3.
`replicate-do-db`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`replicate-do-table`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`replicate-ignore-db`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`replicate-ignore-table`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`replicate-wild-do-table`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`replicate-wild-ignore-table`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`require_secure_transport`	Ja	Dieser Parameter gilt für Aurora MySQL Version 2 und 3. Weitere Informationen finden Sie unter Verwenden von TLS mit DB-Clustern von Aurora MySQL.

Parametername	Anpassbar	Hinweise
`rpl_read_size`	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
`server_audit_events`	Ja	
`server_audit_excl_users`	Ja	
`server_audit_incl_users`	Ja	
`server_audit_logging`	Ja	Anweisungen zum Hochladen der Protokolle auf Amazon CloudWatch Logs finden Sie unterVeröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs.
`server_audit_logs_upload`	Ja	Sie können Audit-Logs in CloudWatch Logs veröffentlichen, indem Sie Advanced Auditing aktivieren und diesen Parameter auf 1 setzen. Der Standardwert für den Parameter `server_audit_logs_upload` ist `0`. Weitere Informationen finden Sie unter Veröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs.
`server_id`	Nein	
`skip-character-set-client-handshake`	Ja	
`skip_name_resolve`	Nein	
`slave-skip-errors`	Ja	Gilt nur für Cluster der Aurora MySQL Version 2 mit MySQL-5.7-Kompatibilität.

Parametername	Anpassbar	Hinweise
source_verify_checksum	Ja	Aurora-MySQL-Version 3
sync_frm	Ja	Aus Aurora-MySQL-Version 3 entfernt.
thread_cache_size	Ja	Die Anzahl der Threads, die zwischeng espeichert werden sollen. Dieser Parameter gilt für Aurora MySQL Version 2 und 3.
time_zone	Ja	Standardmäßig ist die Zeitzone für einen Aurora-DB-Cluster Universal Time Coordinated (UTC). Sie können die Zeitzone für Instances in Ihrem DB-Cluster stattdessen auf die lokale Zeitzone Ihrer Anwendung festlegen. Weitere Informationen finden Sie unter Lokale Zeitzone für Amazon Aurora-DB-Cluster.
tls_version	Ja	Weitere Informationen finden Sie unter TLS-Versionen für Aurora MySQL.

Parameter auf Instance-Ebene

In der folgenden Tabelle werden alle Parameter aufgeführt, die für eine bestimmte DB-Instance in einem Aurora MySQL-DB-Cluster gelten.

Parametername	Anpassbar	Hinweise
activate_all_roles_on_login	Ja	Dieser Parameter gilt für Aurora-My SQL-Version 3.
allow-suspicious-udfs	Nein	
aurora_disable_hash_join	Ja	Setzen Sie diesen Parameter auf ON, um die Hash-Join-Optimierung in Aurora

Parametername	Anpassbar	Hinweise
		MySQL Version 2.09 oder höher zu deaktivieren. Für Version 3 wird dies nicht unterstützt. Weitere Informationen finden Sie unter Arbeiten mit Parallel Query für Amazon Aurora MySQL.
`aurora_lab_mode`	Ja	Weitere Informationen finden Sie unter Amazon Aurora MySQL-Labor-Modus. Aus Aurora-MySQL-Version 3 entfernt.
`aurora_oom_response`	Ja	Dieser Parameter wird für die Aurora-MySQL-Versionen 2 und 3 unterstützt. Weitere Informationen finden Sie unter Behebung von out-of-memory Problemen mit Aurora MySQL-Datenbanken.
`aurora_parallel_query`	Ja	Legen Sie dies auf `ON` fest, um parallele Abfragen in den Aurora-MySQL-Versionen 2.09 oder höher zu unterstützen. Der alte Parameter `aurora_pq` wird in diesen Versionen nicht verwendet. Weitere Informationen finden Sie unter Arbeiten mit Parallel Query für Amazon Aurora MySQL.
`aurora_pq`	Ja	Setzen Sie dies auf `OFF`, um parallele Abfragen für bestimmte DB-Instances in Aurora-MySQL-Versionen vor 2.09 zu deaktivieren. In den Versionen 2.09 oder höher aktivieren und deaktivieren Sie parallele Abfragen stattdessen mit `aurora_parallel_query`. Weitere Informationen finden Sie unter Arbeiten mit Parallel Query für Amazon Aurora MySQL.

Parametername	Anpassbar	Hinweise
`aurora_read_replica_read_committed`	Ja	Aktiviert die Isolationsstufe `READ COMMITTED` für Aurora Replicas und ändert das Isolationsverhalten zur Reduzierung der Bereinigungsverzögerung bei lang andauernden Abfragen. Aktivieren Sie diese Einstellung nur, wenn Sie die Verhaltensänderungen und deren Auswirkungen auf Ihre Abfrageergebnisse verstehen. Beispielsweise gehört dazu, dass diese Einstellung eine weniger strikte Isolation als der MySQL-Standard verwendet. Bei Aktivierung kann es sein, dass lang andauernde Abfragen mehr als eine Kopie derselben Zeile sehen, da Aurora die Tabellendaten umorganisiert, während die Abfrage läuft. Weitere Informationen finden Sie unter Aurora MySQL-Isolierungsstufen.
`aurora_tmptable_enable_per_table_limit`	Ja	Bestimmt, ob der der Parameter `tmp_table_size` auch die maximale Größe temporärer Tabellen im Arbeitsspeicher steuert, die von der `TempTable` -Speicher-Engine in Aurora-MySQL-Version 3.04 und höher erstellt werden. Weitere Informationen finden Sie unter Begrenzung der Größe interner temporärer Tabellen im Arbeitsspeicher.

Parametername	Anpassbar	Hinweise
aurora_use_vector_instructions	Ja	Wenn dieser Parameter aktiviert ist, verwendet Aurora MySQL optimierte Anweisungen zur Vektorverarbeitung, die von modernen CPUs bereitgestellt werden, um die Leistung bei I/O-intensiven Workloads zu verbessern. Diese Einstellung ist in Aurora MySQL Version 3.05 und höher standardmäßig aktiviert.
autocommit	Ja	
automatic_sp_privileges	Ja	
back_log	Ja	
basedir	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.
binlog_cache_size	Ja	
binlog_max_flush_queue_time	Ja	
binlog_order_commits	Ja	
binlog_stmt_cache_size	Ja	
binlog_transaction_compression	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
binlog_transaction_compression_level_zstd	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
bulk_insert_buffer_size	Ja	

Parametername	Anpassbar	Hinweise
concurrent_insert	Ja	
connect_timeout	Ja	
core-file	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.
datadir	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.
default_authentication_plugin	Nein	Dieser Parameter gilt für Aurora-MySQL-Version 3.
default_time_zone	Nein	
default_tmp_storage_engine	Ja	Die Standard-Speicher-Engine für temporäre Tabellen.
default_week_format	Ja	
delay_key_write	Ja	
delayed_insert_limit	Ja	
delayed_insert_timeout	Ja	
delayed_queue_size	Ja	
div_precision_increment	Ja	
end_markers_in_json	Ja	
eq_range_index_dive_limit	Ja	

Parametername	Anpassbar	Hinweise
event_scheduler	Manchmal	Zeigt den Status des Ereignisplaners an. Modifizierbar nur auf Clusterebene in Aurora-MySQL-Version 3.
explicit_defaults_for_timestamp	Ja	
flush	Nein	
flush_time	Ja	
ft_boolean_syntax	Nein	
ft_max_word_len	Ja	
ft_min_word_len	Ja	
ft_query_expansion_limit	Ja	
ft_stopword_file	Ja	
general_log	Ja	Anweisungen zum Hochladen der Protokolle in Logs finden Sie unterVeröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs. CloudWatch
general_log_file	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.
group_concat_max_len	Ja	
host_cache_size	Ja	

Parametername	Anpassbar	Hinweise
`init_connect`	Ja	Der Befehl, der vom Server für jeden Client ausgeführt wird, der eine Verbindung herstellt. Verwenden Sie doppelte Anführungszeichen („) für Einstellungen, um Verbindungsfehler zu vermeiden, zum Beispiel: `SET optimizer_switch="hash_join =off"` Bei Aurora MySQL Version 3 gilt dieser Parameter nicht für Benutzer, die über die `CONNECTION_ADMIN` -Berechti gung verfügen. Weitere Informati onen finden Sie unter Rollenbasiertes Berechtigungsmodell.
`innodb_adaptive_hash_index`	Ja	Sie können diesen Parameter auf DB-Instance-Ebene in Aurora MySLQ Version 2 ändern. In Aurora MySQL Version 3 kann er nur auf DB-Cluste rebene geändert werden. Der Adaptive-Hash-Index wird auf Reader-DB-Instances nicht unterstützt.
`innodb_adaptive_max_sleep_d elay`	Ja	Das Ändern dieses Parameters hat keine Auswirkung, da `innodb_th read_concurrency` für Aurora immer 0 ist.

Parametername	Anpassbar	Hinweise
innodb_aurora_max_partitions_for_range	Ja	In einigen Fällen, in denen persistente Statistiken nicht verfügbar sind, können Sie diesen Parameter verwenden, um die Leistung von Schätzungen der Zeilenanzahl in partitionierten Tabellen zu verbessern. Sie können ihn auf einen Wert zwischen 0 und 8192 festlegen, wobei der Wert die Anzahl der Partitionen bestimmt, die bei der Schätzung der Zeilenanzahl überprüft werden sollen. Der Standardwert ist 0. Dieser entspricht der Schätzung, dass alle Partitionen verwendet werden, was mit dem Standardverhalten von MySQL übereinstimmt. Dieser Parameter ist für Aurora MySQL Version 3.03.1 verfügbar.
innodb_autoextend_increment	Ja	
innodb_buffer_pool_dump_at_shutdown	Nein	
innodb_buffer_pool_dump_now	Nein	
innodb_buffer_pool_filename	Nein	
innodb_buffer_pool_load_abort	Nein	

Parametername	Anpassbar	Hinweise
innodb_buffer_pool_load_at_startup	Nein	
innodb_buffer_pool_load_now	Nein	
innodb_buffer_pool_size	Ja	Der Standardwert wird durch eine Formel dargestellt. Mehr über die Berechnung des DBInstanceClassMemory -Werts in der Formel erfahren Sie unter DB-Parameter-Formel-Variablen.
innodb_change_buffer_max_size	Nein	Aurora MySQL verwendet den InnoDB-Änderungspuffer überhaupt nicht.
innodb_compression_failure_threshold_pct	Ja	
innodb_compression_level	Ja	
innodb_compression_pad_pct_max	Ja	
innodb_concurrency_tickets	Ja	Das Ändern dieses Parameters hat keine Auswirkung, da innodb_thread_concurrency für Aurora immer 0 ist.

Parametername	Anpassbar	Hinweise
innodb_deadlock_detect	Ja	Diese Option wird verwendet, um die Deadlock-Erkennung in Aurora-MySQL-Version 2.11 und höher sowie Version 3 zu deaktivieren. Auf Systemen mit hoher Parallelität kann die Deadlock-Erkennung zu einer Verlangsamung führen, wenn zahlreiche Threads auf dieselbe Sperre warten. Weitere Informationen zu diesem Parameter finden Sie in der MySQL-Dokumentation.
innodb_file_format	Ja	Aus Aurora-MySQL-Version 3 entfernt.
innodb_flushing_avg_loops	Nein	
innodb_force_load_corrupted	Nein	
innodb_ft_aux_table	Ja	
innodb_ft_cache_size	Ja	
innodb_ft_enable_stopword	Ja	
innodb_ft_server_stopword_table	Ja	
innodb_ft_user_stopword_table	Ja	
innodb_large_prefix	Ja	Aus Aurora-MySQL-Version 3 entfernt.
innodb_lock_wait_timeout	Ja	
innodb_log_compressed_pages	Nein	

Parametername	Anpassbar	Hinweise
innodb_lru_scan_depth	Ja	
innodb_max_purge_lag	Ja	
innodb_max_purge_lag_delay	Ja	
innodb_monitor_disable	Ja	
innodb_monitor_enable	Ja	
innodb_monitor_reset	Ja	
innodb_monitor_reset_all	Ja	
innodb_old_blocks_pct	Ja	
innodb_old_blocks_time	Ja	
innodb_open_files	Ja	
innodb_print_all_deadlocks	Ja	Wenn dieser Parameter aktiviert ist, werden Informationen über alle InnoDB-Deadlocks im Fehlerprotokoll von Aurora MySQL aufgezeichnet. Weitere Informationen finden Sie unter Minimieren und Beheben von Aurora-MySQL-Deadlocks.
innodb_random_read_ahead	Ja	
innodb_read_ahead_threshold	Ja	
innodb_read_io_threads	Nein	

Parametername	Anpassbar	Hinweise
innodb_read_only	Nein	Aurora MySQL verwaltet den Schreibschutz- und Lesen/Schreiben-Status von DB-Instances basierend auf dem Typ des Clusters. Ein bereitgestellter Cluster hat beispielsweise eine Lesen/Schreiben-DB-Instance (die primäre Instance). Alle anderen Instances im Cluster sind schreibgeschützt (die Aurora-Replicas).
innodb_replication_delay	Ja	
innodb_sort_buffer_size	Ja	
innodb_stats_auto_recalc	Ja	
innodb_stats_method	Ja	
innodb_stats_on_metadata	Ja	
innodb_stats_persistent	Ja	
innodb_stats_persistent_sample_pages	Ja	
innodb_stats_transient_sample_pages	Ja	
innodb_thread_concurrency	Nein	
innodb_thread_sleep_delay	Ja	Das Ändern dieses Parameters hat keine Auswirkung, da innodb_thread_concurrency für Aurora immer 0 ist.

Parametername	Anpassbar	Hinweise
interactive_timeout	Ja	Aurora wertet den Mindestwert von interactive_timeout und wait_timeout aus. Dieses Minimum wird dann als Timeout verwendet, um alle inaktiven Sitzungen, sowohl interaktive als auch nicht interaktive, zu beenden.
internal_tmp_disk_storage_engine	Ja	Steuert, welche In-Memory-Speicher-Engine für interne temporäre Tabellen verwendet wird. Zulässige Werte sind INNODB und MYISAM. Dieser Parameter gilt für Aurora MySQL Version 2.
internal_tmp_mem_storage_engine	Ja	Steuert, welche In-Memory-Speicher-Engine für interne temporäre Tabellen verwendet wird. Zulässige Werte sind MEMORY und TempTable . Dieser Parameter gilt für Aurora MySQL Version 3.
join_buffer_size	Ja	
keep_files_on_create	Ja	
key_buffer_size	Ja	Schlüssel-Cache für MyISAM-Tabellen. Weitere Informationen finden Sie unter keycache->cache_lock mutex.
key_cache_age_threshold	Ja	
key_cache_block_size	Ja	
key_cache_division_limit	Ja	

Parametername	Anpassbar	Hinweise
`local_infile`	Ja	
`lock_wait_timeout`	Ja	
`log-bin`	Nein	Wenn die Einstellung `binlog_format` auf `STATEMENT`, `MIXED` oder `ROW` gesetzt wird, wird `log-bin` automatisch auf `ON` festgelegt. Wenn die Einstellung `binlog_format` auf `OFF` gesetzt wird, wird `log-bin` automatisch auf `OFF` gesetzt. Weitere Informationen finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).
`log_bin_trust_function_creators`	Ja	
`log_bin_use_v1_row_events`	Ja	Aus Aurora-MySQL-Version 3 entfernt.
`log_error`	Nein	
`log_error_suppression_list`	Ja	Gibt eine Liste von Fehlercodes an, die nicht im MySQL-Fehlerprotokoll protokolliert sind. Auf diese Weise können Sie bestimmte unkritische Fehlerbedingungen ignorieren, um Ihre Fehlerprotokolle sauber zu halten. Weitere Informationen finden Sie unter log_error_suppression_list in der MySQL-Dokumentation. Dieser Parameter gilt für Aurora MySQL Version 3.03 und höher.

Parametername	Anpassbar	Hinweise
log_output	Ja	
log_queries_not_using_indexes	Ja	
log_slave_updates	Nein	Aurora-MySQL-Version 2. Verwenden Sie log_replica_updates in Aurora-MySQL-Version 3.
log_replica_updates	Nein	Aurora-MySQL-Version 3
log_throttle_queries_not_using_indexes	Ja	
log_warnings	Ja	Aus Aurora-MySQL-Version 3 entfernt.
long_query_time	Ja	
low_priority_updates	Ja	INSERT-, UPDATE-, DELETE- und LOCK TABLE WRITE-Operationen warten, bis kein ausstehender SELECT-Vorgang mehr vorhanden ist. Dieser Parameter wirkt sich nur auf Speicher-Engines aus, die ausschließlich Sperren auf Tabellenebene verwenden (MyISAM, MEMORY, MERGE). Dieser Parameter gilt für Aurora MySQL Version 3.
max_allowed_packet	Ja	
max_binlog_cache_size	Ja	
max_binlog_size	Nein	
max_binlog_stmt_cache_size	Ja	

Parametername	Anpassbar	Hinweise
max_connect_errors	Ja	
max_connections	Ja	Der Standardwert wird durch eine Formel dargestellt. Mehr über die Berechnung des DBInstanceClassMemory -Werts in der Formel erfahren Sie unter DB-Parameter-Formel-Variablen. Informationen zu den Standardwerten in Abhängigkeit von der Instance-Klasse finden Sie unter Maximale Verbindungen zu einer Aurora MySQL-DB-Instance.
max_delayed_threads	Ja	Legt die maximale Anzahl von Threads für die Verarbeitung von INSERT DELAYED-Anweisungen fest. Dieser Parameter gilt für Aurora MySQL Version 3.
max_error_count	Ja	Die maximale Anzahl von Fehler-, Warn- und Hinweismeldungen, die für die Anzeige gespeichert werden sollen. Dieser Parameter gilt für Aurora MySQL Version 3.
max_execution_time	Ja	Das Timeout für die Ausführung von SELECT Anweisungen in Millisekunden. Der Wert kann zwischen — liegen. 0 18446744073709551615 Wenn auf gesetzt0, gibt es kein Timeout. Weitere Informationen finden Sie unter max_execution_time in der MySQL-Dokumentation.

Parametername	Anpassbar	Hinweise
max_heap_table_size	Ja	
max_insert_delayed_threads	Ja	
max_join_size	Ja	
max_length_for_sort_data	Ja	Aus Aurora-MySQL-Version 3 entfernt.
max_prepared_stmt_count	Ja	
max_seeks_for_key	Ja	
max_sort_length	Ja	
max_sp_recursion_depth	Ja	
max_tmp_tables	Ja	Aus Aurora-MySQL-Version 3 entfernt.
max_user_connections	Ja	
max_write_lock_count	Ja	
metadata_locks_cache_size	Ja	Aus Aurora-MySQL-Version 3 entfernt.
min_examined_row_limit	Ja	Verwenden Sie diesen Parameter, um zu verhindern, dass Abfragen, die weniger als die angegebene Anzahl von Zeilen untersuchen, protokolliert werden. Dieser Parameter gilt für Aurora MySQL Version 3.
myisam_data_pointer_size	Ja	
myisam_max_sort_file_size	Ja	
myisam_mmap_size	Ja	

Parametername	Anpassbar	Hinweise
myisam_sort_buffer_size	Ja	
myisam_stats_method	Ja	
myisam_use_mmap	Ja	
net_buffer_length	Ja	
net_read_timeout	Ja	
net_retry_count	Ja	
net_write_timeout	Ja	
old-style-user-limits	Ja	
old_passwords	Ja	Aus Aurora-MySQL-Version 3 entfernt.
optimizer_prune_level	Ja	
optimizer_search_depth	Ja	
optimizer_switch	Ja	Weitere Informationen zu Aurora MySQL-Features, die diesen Schalter verwenden, finden Sie unter Bewährte Methoden mit Amazon Aurora MySQL.
optimizer_trace	Ja	
optimizer_trace_features	Ja	
optimizer_trace_limit	Ja	
optimizer_trace_max_mem_size	Ja	
optimizer_trace_offset	Ja	

Parametername	Anpassbar	Hinweise
performance-schema-consumer-events-waits-current	Ja	
performance-schema-instrument	Ja	
performance_schema	Ja	
performance_schema_accounts_size	Ja	
performance_schema_consumer_global_instrumentation	Ja	
performance_schema_consumer_thread_instrumentation	Ja	
performance_schema_consumer_events_stages_current	Ja	
performance_schema_consumer_events_stages_history	Ja	
performance_schema_consumer_events_stages_history_long	Ja	
performance_schema_consumer_events_statements_current	Ja	
performance_schema_consumer_events_statements_history	Ja	
performance_schema_consumer_events_statements_history_long	Ja	

Parametername	Anpassbar	Hinweise
performance_schema_consumer_events_waits_history	Ja	
performance_schema_consumer_events_waits_history_long	Ja	
performance_schema_consumer_statements_digest	Ja	
performance_schema_digests_size	Ja	
performance_schema_events_stages_history_long_size	Ja	
performance_schema_events_stages_history_size	Ja	
performance_schema_events_statements_history_long_size	Ja	
performance_schema_events_statements_history_size	Ja	
performance_schema_events_transactions_history_long_size	Ja	
performance_schema_events_transactions_history_size	Ja	
performance_schema_events_waits_history_long_size	Ja	
performance_schema_events_waits_history_size	Ja	

Parametername	Anpassbar	Hinweise
performance_schema_hosts_size	Ja	
performance_schema_max_cond_classes	Ja	
performance_schema_max_cond_instances	Ja	
performance_schema_max_digest_length	Ja	
performance_schema_max_file_classes	Ja	
performance_schema_max_file_handles	Ja	
performance_schema_max_file_instances	Ja	
performance_schema_max_index_stat	Ja	
performance_schema_max_memory_classes	Ja	
performance_schema_max_metadata_locks	Ja	
performance_schema_max_mutex_classes	Ja	
performance_schema_max_mutex_instances	Ja	
performance_schema_max_prepared_statements_instances	Ja	

Parametername	Anpassbar	Hinweise
performance_schema_max_program_instances	Ja	
performance_schema_max_rwlock_classes	Ja	
performance_schema_max_rwlock_instances	Ja	
performance_schema_max_socket_classes	Ja	
performance_schema_max_socket_instances	Ja	
performance_schema_max_sql_text_length	Ja	
performance_schema_max_stage_classes	Ja	
performance_schema_max_statement_classes	Ja	
performance_schema_max_statement_stack	Ja	
performance_schema_max_table_handles	Ja	
performance_schema_max_table_instances	Ja	
performance_schema_max_table_lock_stat	Ja	
performance_schema_max_thread_classes	Ja	

Parametername	Anpassbar	Hinweise
performance_schema_max_thread_instances	Ja	
performance_schema_session_connect_attrs_size	Ja	
performance_schema_setup_actors_size	Ja	
performance_schema_setup_objects_size	Ja	
performance_schema_show_processlist	Ja	Dieser Parameter bestimmt, welche SHOW PROCESSLIST -Implementierung verwendet werden soll: • Die Standardimplementierung iteriert innerhalb des Thread-Managers über aktive Threads hinweg und hält dabei einen globalen Mutex bereit. Dies kann zu einer langsamen Leistung führen, insbesondere bei stark ausgelasteten Systemen. • Die alternative SHOW PROCESSLIST -Implementierung basiert auf der Tabelle processlist des Leistungsschemas. Diese Implementierung fragt aktive Threaddaten aus dem Leistungsschema und nicht aus dem Thread-Manager ab und benötigt keinen Mutex. Dieser Parameter gilt für Aurora-MySQL-Version 2.12 und höher sowie Version 3.

Parametername	Anpassbar	Hinweise
performance_schema_users_size	Ja	
pid_file	Nein	
plugin_dir	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.
port	Nein	Aurora MySQL verwaltet die Verbindungseigenschaften und erzwingt konsistente Einstellungen für alle DB-Instanzen in einem Cluster.
preload_buffer_size	Ja	Die Größe des Puffers, der beim Vorabladen von Indizes zugewiesen wird. Dieser Parameter gilt für Aurora MySQL Version 3.
profiling_history_size	Ja	
query_alloc_block_size	Ja	
query_cache_limit	Ja	Aus Aurora-MySQL-Version 3 entfernt.
query_cache_min_res_unit	Ja	Aus Aurora-MySQL-Version 3 entfernt.
query_cache_size	Ja	Der Standardwert wird durch eine Formel dargestellt. Mehr über die Berechnung des DBInstanceClassMemory -Werts in der Formel erfahren Sie unter DB-Parameter-Formel-Variablen. Aus Aurora-MySQL-Version 3 entfernt.

Parametername	Anpassbar	Hinweise
query_cache_type	Ja	Aus Aurora-MySQL-Version 3 entfernt.
query_cache_wlock_invalidate	Ja	Aus Aurora-MySQL-Version 3 entfernt.
query_prealloc_size	Ja	
range_alloc_block_size	Ja	
read_buffer_size	Ja	

Parametername	Anpassbar	Hinweise
`read_only`	Ja	Wenn dieser Parameter aktiviert ist, erlaubt der Server nur Aktualisierungen, die von Replikat-Threads durchgeführt werden. Für Aurora MySQL Version 2 sind die folgenden Werte gültig: • `0` – `OFF` • `1` – `ON` • `{TrueIfReplica}` — `ON` für Read Replicas. Dies ist der Standardwert. • `{TrueIfClusterReplica}` — `ON` für Instances in Replikatclustern wie regionsübergreifende Read Replicas, sekundäre Cluster in einer globalen Aurora-Datenbank und Blue-Green-Bereitstellungen. Wir empfehlen, die DB-Cluster-Paramet ergruppe in Aurora MySQL Version 2 zu verwenden, um sicherzustellen, dass der `read_only` -Parameter beim Failover auf neue Writer-Instances angewendet wird. **Note** Reader-Instances sind immer schreibgeschützt, da Aurora MySQL `innodb_read_only` für alle Reader auf `1` festlegt. Daher ist `read_only` auf Reader-Instances redundant.

Parametername	Anpassbar	Hinweise
		Auf Instance-Ebene aus Aurora MySQL Version 3 entfernt.
read_rnd_buffer_size	Ja	
relay-log	Nein	
relay_log_info_repository	Ja	Aus Aurora-MySQL-Version 3 entfernt.
relay_log_recovery	Nein	
replica_checkpoint_group	Ja	Aurora-MySQL-Version 3
replica_checkpoint_period	Ja	Aurora-MySQL-Version 3
replica_parallel_workers	Ja	Aurora-MySQL-Version 3
replica_pending_jobs_size_max	Ja	Aurora-MySQL-Version 3
replica_skip_errors	Ja	Aurora-MySQL-Version 3
replica_sql_verify_checksum	Ja	Aurora-MySQL-Version 3
safe-user-create	Ja	
secure_auth	Ja	Dieser Parameter ist in Aurora-MySQL-Version 2 immer aktiviert. Der Versuch, ihn zu deaktivieren, generiert einen Fehler. Aus Aurora-MySQL-Version 3 entfernt.
secure_file_priv	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.

Parametername	Anpassbar	Hinweise
show_create_table_verbosity	Ja	Wenn diese Variable aktiviert wird, zeigt SHOW_CREATE_TABLE das ROW_FORMAT unabhängig davon an, ob es das Standardformat ist. Dieser Parameter gilt für Aurora-MySQL-Version 2.12 und höher sowie Version 3.
skip-slave-start	Nein	
skip_external_locking	Nein	
skip_show_database	Ja	
slave_checkpoint_group	Ja	Aurora-MySQL-Version 2. Verwenden Sie replica_checkpoint_group in Aurora-MySQL-Version 3.
slave_checkpoint_period	Ja	Aurora-MySQL-Version 2. Verwenden Sie replica_checkpoint_period in Aurora-MySQL-Version 3.
slave_parallel_workers	Ja	Aurora-MySQL-Version 2. Verwenden Sie replica_parallel_workers in Aurora-MySQL-Version 3.
slave_pending_jobs_size_max	Ja	Aurora-MySQL-Version 2. Verwenden Sie replica_pending_jobs_size_max in Aurora-MySQL-Version 3.
slave_sql_verify_checksum	Ja	Aurora-MySQL-Version 2. Verwenden Sie replica_sql_verify_checksum in Aurora-MySQL-Version 3.

Parametername	Anpassbar	Hinweise
slow_launch_time	Ja	
slow_query_log	Ja	Anweisungen zum Hochladen der Protokolle in Logs finden Sie unter. CloudWatch Veröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs
slow_query_log_file	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.
socket	Nein	
sort_buffer_size	Ja	
sql_mode	Ja	
sql_select_limit	Ja	
stored_program_cache	Ja	
sync_binlog	Nein	
sync_master_info	Ja	
sync_source_info	Ja	Dieser Parameter gilt für Aurora MySQL Version 3.
sync_relay_log	Ja	Aus Aurora-MySQL-Version 3 entfernt.
sync_relay_log_info	Ja	
sysdate-is-now	Ja	
table_cache_element_entry_ttl	Nein	

Parametername	Anpassbar	Hinweise
table_definition_cache	Ja	Der Standardwert wird durch eine Formel dargestellt. Mehr über die Berechnung des DBInstanceClassMemory -Werts in der Formel erfahren Sie unter DB-Parameter-Formel-Variablen.
table_open_cache	Ja	Der Standardwert wird durch eine Formel dargestellt. Mehr über die Berechnung des DBInstanceClassMemory -Werts in der Formel erfahren Sie unter DB-Parameter-Formel-Variablen.
table_open_cache_instances	Ja	
temp-pool	Ja	Aus Aurora-MySQL-Version 3 entfernt.
temptable_max_mmap	Ja	Dieser Parameter gilt für Aurora-MySQL-Version 3. Details hierzu finden Sie unter Neues temporäres Tabellenverhalten in Aurora-MySQL-Version 3.
temptable_max_ram	Ja	Dieser Parameter gilt für Aurora-MySQL-Version 3. Details hierzu finden Sie unter Neues temporäres Tabellenverhalten in Aurora-MySQL-Version 3.
temptable_use_mmap	Ja	Dieser Parameter gilt für Aurora-MySQL-Version 3. Details hierzu finden Sie unter Neues temporäres Tabellenverhalten in Aurora-MySQL-Version 3.

Parametername	Anpassbar	Hinweise
thread_cache_size	Ja	Die Anzahl der Threads, die zwischeng espeichert werden sollen. Dieser Parameter gilt für Aurora MySQL Version 2 und 3.
thread_handling	Nein	
thread_stack	Ja	
timed_mutexes	Ja	
tmp_table_size	Ja	Definiert die maximale Größe temporäre r Tabellen, die von der MEMORY-Speicher-Engine in Aurora-MySQL-Version 3 erstellt werden. Definiert in Aurora-MySQL-Version 3.04 und höher die maximale Größe temporärer Tabellen im Arbeitssp eicher, die von der TempTable -Speicher-Engine erstellt werden, wenn aurora_tmptable_en able_per_table_lim it auf ON festgelegt ist. Weitere Informationen finden Sie unter Begrenzung der Größe interner temporärer Tabellen im Arbeitsspeicher.
tmpdir	Nein	Aurora MySQL verwendet verwaltete Instances, bei denen Sie nicht direkt auf das Archivsystem zugreifen.
transaction_alloc_block_siz e	Ja	

Parametername	Anpassbar	Hinweise
transaction_isolation	Ja	Dieser Parameter gilt für Aurora-MySQL-Version 3. Er ersetzt tx_isolation .
transaction_prealloc_size	Ja	
tx_isolation	Ja	Aus Aurora-MySQL-Version 3 entfernt. Es wird durch transaction_isolation ersetzt.
updatable_views_with_limit	Ja	
validate-password	Nein	
validate_password_dictionary_file	Nein	
validate_password_length	Nein	
validate_password_mixed_case_count	Nein	
validate_password_number_count	Nein	
validate_password_policy	Nein	
validate_password_special_char_count	Nein	
wait_timeout	Ja	Aurora wertet den Mindestwert von interactive_timeout und wait_timeout aus. Dieses Minimum wird dann als Timeout verwendet, um alle inaktiven Sitzungen, sowohl interaktive als auch nicht interaktive, zu beenden.

MySQL-Parameter, die nicht auf Aurora MySQL zutreffen

Aufgrund von Architekturunterschieden zwischen Aurora MySQL und MySQL gelten einige MySQL-Parameter nicht für Aurora MySQL.

Die folgenden MySQL-Parameter gelten nicht für Aurora MySQL. Diese Liste ist nicht umfassend.

- `activate_all_roles_on_login` – Dieser Parameter gilt nicht für Aurora-MySQL-Version 2. Er ist in Aurora-MySQL-Version 3 verfügbar.
- `big_tables`
- `bind_address`
- `character_sets_dir`
- `innodb_adaptive_flushing`
- `innodb_adaptive_flushing_lwm`
- `innodb_buffer_pool_chunk_size`
- `innodb_buffer_pool_instances`
- `innodb_change_buffering`
- `innodb_checksum_algorithm`
- `innodb_data_file_path`
- `innodb_dedicated_server`
- `innodb_doublewrite`
- `innodb_flush_log_at_timeout`: Dieser Parameter gilt nicht für Aurora MySQL. Weitere Informationen finden Sie unter Konfigurieren, wie oft der Protokollpuffer geleert wird.
- `innodb_flush_method`
- `innodb_flush_neighbors`
- `innodb_io_capacity`
- `innodb_io_capacity_max`
- `innodb_log_buffer_size`
- `innodb_log_file_size`
- `innodb_log_files_in_group`
- `innodb_log_spin_cpu_abs_lwm`
- `innodb_log_spin_cpu_pct_hwm`
- `innodb_log_writer_threads`

- innodb_max_dirty_pages_pct
- innodb_numa_interleave
- innodb_page_size
- innodb_redo_log_capacity
- innodb_redo_log_encrypt
- innodb_undo_log_encrypt
- innodb_undo_log_truncate
- innodb_undo_logs
- innodb_undo_tablespaces
- innodb_use_native_aio
- innodb_write_io_threads

Globale Statusvariablen von Aurora MySQL

Sie können die aktuellen Werte für die globalen Statusvariablen von Aurora MySQL mithilfe einer Anweisung wie den folgenden ermitteln:

```
show global status like '%aurora%';
```

In der folgenden Tabelle werden die globalen Statusvariablen beschrieben, die Aurora MySQL verwendet.

Name	Beschreibung
AuroraDb_commits	Die Gesamtzahl der Commits seit dem letzten Neustart.
AuroraDb_commit_latency	Die aggregierte Commit-Latenz seit dem letzten Neustart.
AuroraDb_ddl_stmt_duration	Die aggregierte DDL-Latenz seit dem letzten Neustart.
AuroraDb_select_stmt_duration	Die aggregierte SELECT-Anweisungslatenz seit dem letzten Neustart.

Name	Beschreibung
AuroraDb_insert_stmt_duration	Die aggregierte INSERT-Anweisungslatenz seit dem letzten Neustart.
AuroraDb_update_stmt_duration	Die aggregierte UPDATE-Anweisungslatenz seit dem letzten Neustart.
AuroraDb_delete_stmt_duration	Die aggregierte DELETE-Anweisungslatenz seit dem letzten Neustart.
Aurora_binlog_io_cache_allocated	Die Anzahl der Byte, die dem Binlog-I/O-Cache zugewiesen wurden.
Aurora_binlog_io_cache_read_requests	Die Anzahl der Leseanfragen an den Binlog-I/OCache.
Aurora_binlog_io_cache_reads	Die Anzahl der Leseanfragen, die der Binlog-I/O-Cache verarbeitet hat.
Aurora_enhanced_binlog	Gibt an, ob das erweiterte Binärprotokoll für diese DB-Instance aktiviert oder deaktiviert ist. Weitere Informationen finden Sie unter Einrichten eines erweiterten Binärprotokolls.
Aurora_external_connection_count	Die Anzahl der Datenbankverbindungen mit der DB-Instance, ausgenommen RDS-Serviceverbindungen, die für Datenbankzustandsprüfungen verwendet werden.
Aurora_fast_insert_cache_hits	Ein Zähler, der erhöht wird, wenn der zwischengespeicherte Cursor erfolgreich abgerufen und bestätigt wurde. Weitere Informationen zum Cache für schnelles Einfügen finden Sie unter Amazon Aurora MySQL-Leistungserweiterungen.

Name	Beschreibung
`Aurora_fast_insert_cache_misses`	Ein Zähler, der erhöht wird, wenn der zwischengespeicherte Cursor nicht mehr gültig ist und Aurora einen normalen Index-Durchlauf durchführt. Weitere Informationen zum Cache für schnelles Einfügen finden Sie unter Amazon Aurora MySQL-Leistungserweiterungen.
`Aurora_fts_cache_memory_used`	Die Speichermenge in Byte, die das InnoDB-Volltextsuchsystem verwendet. Diese Variable gilt für Aurora MySQL Version 3.07 und höher.
`Aurora_fwd_master_dml_stmt_count`	Die Gesamtzahl der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Diese Variable gilt für Aurora-MySQL-Version 2.
`Aurora_fwd_master_dml_stmt_duration`	Die Gesamtdauer der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Diese Variable gilt für Aurora-MySQL-Version 2.
`Aurora_fwd_master_errors_rpc_timeout`	Gibt an, wie oft eine weitergeleitete Verbindung nicht auf dem Writer hergestellt werden konnte.
`Aurora_fwd_master_errors_session_limit`	Die Anzahl der weitergeleiteten Anfragen, die aufgrund von `session full` auf dem Writer abgelehnt werden.
`Aurora_fwd_master_errors_session_timeout`	Die Angabe, wie oft eine Weiterleitungssitzung aufgrund eines Timeouts auf dem Writer beendet wird.
`Aurora_fwd_master_open_sessions`	Die Anzahl der weitergeleiteten Sitzungen auf der Writer-DB-Instance. Diese Variable gilt für Aurora-MySQL-Version 2.

Name	Beschreibung
`Aurora_fwd_master_select_stmt_count`	Die Gesamtzahl der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Diese Variable gilt für Aurora-MySQL-Version 2.
`Aurora_fwd_master_select_stmt_duration`	Die Gesamtdauer der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Diese Variable gilt für Aurora-MySQL-Version 2.
`Aurora_fwd_writer_dml_stmt_count`	Die Gesamtzahl der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Diese Variable gilt für Aurora-MySQL-Version 3.
`Aurora_fwd_writer_dml_stmt_duration`	Die Gesamtdauer der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Diese Variable gilt für Aurora-MySQL-Version 3.
`Aurora_fwd_writer_errors_rpc_timeout`	Gibt an, wie oft eine weitergeleitete Verbindung nicht auf dem Writer hergestellt werden konnte.
`Aurora_fwd_writer_errors_session_limit`	Die Anzahl der weitergeleiteten Anfragen, die aufgrund von `session full` auf dem Writer abgelehnt werden.
`Aurora_fwd_writer_errors_session_timeout`	Die Angabe, wie oft eine Weiterleitungssitzung aufgrund eines Timeouts auf dem Writer beendet wird.
`Aurora_fwd_writer_open_sessions`	Die Anzahl der weitergeleiteten Sitzungen auf der Writer-DB-Instance. Diese Variable gilt für Aurora-MySQL-Version 3.

Name	Beschreibung
`Aurora_fwd_writer_select_stmt_count`	Die Gesamtzahl der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Diese Variable gilt für Aurora-MySQL-Version 3.
`Aurora_fwd_writer_select_stmt_duration`	Die Gesamtdauer der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Diese Variable gilt für Aurora-MySQL-Version 3.
`Aurora_lockmgr_buffer_pool_memory_used`	Die Menge an Pufferpool-Speicher in Byte, die der Aurora MySQL Lock Manager verwendet.
`Aurora_lockmgr_memory_used`	Die Speichermenge in Byte, die der Aurora MySQL Lock Manager verwendet.
`Aurora_ml_actual_request_cnt`	Die aggregierte Zahl der Anfragen, die Aurora MySQL an die Machine-Learning-Services von Aurora über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg stellt. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.
`Aurora_ml_actual_response_cnt`	Die aggregierte Zahl der Antworten, die Aurora MySQL von den Machine-Learning-Services von Aurora über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg erhält. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.

Name	Beschreibung
`Aurora_ml_cache_hit_cnt`	Die aggregierte Zahl der internen Cache-Treffer, die Aurora MySQL von den Machine-Learning-Services von Aurora über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg erhält. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.
`Aurora_ml_logical_request_cnt`	Die Anzahl der logischen Anfragen, die die DB-Instance seit dem letzten Status-Reset zum Senden an die Aurora-Machine-Learning-Services ausgewertet hat. Je nachdem, ob Stapelverarbeitung verwendet wurde, kann dieser Wert höher sein als `Aurora_ml_actual_request_cnt`. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.
`Aurora_ml_logical_response_cnt`	Die aggregierte Zahl der Antworten, die Aurora MySQL von den Machine-Learning-Services von Aurora über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg erhält. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.
`Aurora_ml_retry_request_cnt`	Die Anzahl der wiederholten Anfragen, die die DB-Instance seit dem letzten Status-Reset an die Aurora-Machine-Learning-Services gesendet hat. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.

Name	Beschreibung
`Aurora_ml_single_request_cnt`	Die aggregierte Zahl der Machine-Learning-Funktionen von Aurora, die im Nicht-Batch-Modus über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg evaluiert werden. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL.
`aurora_oom_avoidance_recovery_state`	Gibt an, ob sich Aurora out-of-memory (OOM) Avoidance Recovery für diese DB-Instance im `INACTIVE` Status `ACTIVE` oder befindet.
`aurora_oom_reserved_mem_enter_kb`	Stellt den Schwellenwert für die Eingabe des `RESERVED` Status im OOM-Behandlungsmechanismus von Aurora dar. Wenn der verfügbare Speicher auf dem Server unter diesen Schwellenwert fällt, wird der Wert auf `aurora_oom_status` geändert`RESERVED`, was darauf hinweist, dass sich der Server einem kritischen Speicheraslastungsgrad nähert.
`aurora_oom_reserved_mem_exit_kb`	Stellt den Schwellenwert für das Verlassen des `RESERVED` Status im OOM-Behandlungsmechanismus von Aurora dar. Wenn der verfügbare Speicher auf dem Server über diesen Schwellenwert steigt, `aurora_oom_status` kehrt er zu zurück`NORMAL`, was bedeutet, dass der Server in einen stabileren Zustand mit ausreichenden Speicherressourcen zurückgekehrt ist.

Name	Beschreibung
aurora_oom_status	Stellt den aktuellen OOM-Status dieser DB-Instance dar. Wenn der Wert „ist“NORMAL, bedeutet dies, dass ausreichend Speicherr essourcen vorhanden sind. Ändert sich der Wert aufRESERVED, bedeutet dies, dass der Server über wenig verfügbar en Arbeitsspeicher verfügt. Die Aktionen werden auf der Grundlage der aurora_oo m_response Parameterkonfiguration ausgeführt. Weitere Informationen finden Sie unter Behebung von out-of-memory Problemen mit Aurora MySQL-Datenbanken.
Aurora_pq_bytes_returned	Die Anzahl der Bytes, die in Zusammenh ang mit Tupel-Datenstrukturen während der Parallelabfragen an den Hauptknoten übertrage n wurden. Für den Abgleich mit durch 16 348 teile Aurora_pq_pages_pushed_down .
Aurora_pq_max_concurrent_re quests	Die Höchstanzahl der Parallel Query-Sit zungen, die auf dieser Aurora-DB-Instance gleichzeitig ausgeführt werden können. Dies ist eine feste Zahl, die von der AWS DB-Instance-Klasse abhängt.
Aurora_pq_pages_pushed_down	Die Anzahl der Datenseiten (jeweils fix 16 KiB groß), auf denen Parallel Query eine netzwerkg ebundene Übertragung an den Hauptknoten verhindert hat.

Name	Beschreibung
`Aurora_pq_request_attempted`	Die Anzahl der angeforderten Parallel Query-Sitzungen. Hinter diesem Wert können pro Abfrage mehrere Sitzungen stehen. Ausschlag gebend sind SQL-Konstrukte wie Unterabfr agen und Join-Abfragen.
`Aurora_pq_request_executed`	Die Anzahl der erfolgreich ausgeführten Parallel Query-Sitzungen.
`Aurora_pq_request_failed`	Die Anzahl der Parallel Query-Sitzungen, die dem Client einen Fehler zurückgaben. Es kann vorkommen, dass eine angeforderte Parallelabfrage fehlschlägt – z. B. wegen eines Problems auf der Speicherschicht. In diesen Fällen wird der fehlgeschlagene Abfrageteil wiederholt. Dafür kommt der nicht-parallele Abfragemechanismus zum Einsatz. Wenn auch die wiederholte Abfrage fehlschlägt, wird dem Client ein Fehler zurückgegeben. Die Zähleranz eige erhöht sich.
`Aurora_pq_request_in_progress`	Die Anzahl der derzeit in Ausführung befindlic hen Parallel Query-Sitzungen. Die Zahl bezieht sich auf die angeschlossene Aurora-DB-Instance, mit der Sie verbunden sind, nicht auf das gesamte Aurora-DB-Cluster. Sie können prüfen, ob eine DB-Instance die Obergrenze für gleichzeitige Abfragen annähernd erreicht hat. Gleichen Sie dazu diesen Wert mit a `Aurora_pq_max_concurrent_re quests` .

Name	Beschreibung
`Aurora_pq_request_not_chosen`	Die Anzahl der Situationen, in denen Parallel Query nicht für die Abarbeitung einer Abfrage genutzt wurde. Dieser Wert setzt sich aus den Beiträgen mehrerer Zähler mit höherer Granularität zusammen. Die Zähleranzeige kann mit einer `EXPLAIN`-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächlich ausgeführt wird.
`Aurora_pq_request_not_chosen_below_min_rows`	Die Anzahl der Situationen, in denen die Anzahl der Tabellenzeilen der Grund für den Nichteinsatz von Parallel Query war. Die Zähleranzeige kann mit einer `EXPLAIN`-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächlich ausgeführt wird.
`Aurora_pq_request_not_chosen_column_bit`	Die Anzahl der Parallelabfrageanforderungen, die aufgrund eines nicht unterstützten Datentyps in der Liste der projizierten Spalten den nicht-parallelen Abfrageverarbeitungspfad nutzen.
`Aurora_pq_request_not_chosen_column_geometry`	Die Anzahl der Parallelabfrageanforderungen, die den nicht-parallelen Abfrageverarbeitungspfad nutzen, da die Tabelle Spalten mit dem Datentyp `GEOMETRY` enthält. Informationen zu Aurora-MySQL-Versionen, die diese Einschränkung aufheben, finden Sie unter Upgrade paralleler Abfrage-Cluster auf Aurora-MySQL-Version 3.

Name	Beschreibung
`Aurora_pq_request_not_chosen_column_lob`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle Spalten mit einem `LOB`-Datentyp enthält oder `VARCHAR`-Spalten, die aufgrund der deklarierten Länge extern gespeichert werden. Informationen zu Aurora-MySQL-Versionen, die diese Einschränkung aufheben, finden Sie unter Upgrade paralleler Abfrage-Cluster auf Aurora-MySQL-Version 3.
`Aurora_pq_request_not_chosen_column_virtual`	Die Anzahl der Parallelabfrageanforderungen, die den nicht-parallelen Abfrageverarbeitungspfad nutzen, da die Tabelle eine virtuelle Spalte enthält.
`Aurora_pq_request_not_chosen_custom_charset`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle Spalten mit einem benutzerdefinierten Zeichensatz enthält.
`Aurora_pq_request_not_chosen_fast_ddl`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle zurzeit durch eine schnelle `ALTER`-DDL-Anweisung geändert wird.
`Aurora_pq_request_not_chosen_few_pages_outside_buffer_pool`	Die Anzahl der Situationen, in denen Parallel Query nicht genutzt wurde, obwohl weniger als 95 Prozent der Tabellendaten im Bufferpool waren. Grund: Es gab zu wenig nicht gepufferte Tabellendaten. Eine Parallelabfrage lohnte sich deshalb nicht.

Name	Beschreibung
Aurora_pq_request_not_chosen_full_text_index	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle Volltextindizes enthält.
Aurora_pq_request_not_chosen_high_buffer_pool_pct	Die Anzahl der Situationen, in denen Parallel Query nicht genutzt wurde, weil ein hoher Anteil der Tabellendaten (derzeit >95 Prozent) bereits im Bufferpool war. In diesen Fällen entscheidet der Optimierer, dass das Lesen der Daten aus dem Bufferpool effizienter ist. Die Zähleranzeige kann mit einer EXPLAIN-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächlich ausgeführt wird.
Aurora_pq_request_not_chosen_index_hint	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage einen Indexhinweis enthält.
Aurora_pq_request_not_chosen_innodb_table_format	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Tabelle ein nicht unterstütztes InnoDB-Zeilenformat verwendet. Die parallele Aurora-Abfrage gilt nur für die COMPACT-, REDUNDANT - und DYNAMIC-Zeilenformate.
Aurora_pq_request_not_chosen_long_trx	Die Anzahl der Parallelabfrageanforderungen, die den nicht-parallelen Abfrageverarbeitungspfad nutzten, weil die Abfrage in einer lang laufenden Transaktion gestartet wurde. Die Zähleranzeige kann mit einer EXPLAIN-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächlich ausgeführt wird.

Name	Beschreibung
`Aurora_pq_request_not_chosen_no_where_clause`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage keine `WHERE`-Klausel enthält.
`Aurora_pq_request_not_chosen_range_scan`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage einen Bereichsscan für einen Index verwendet.
`Aurora_pq_request_not_chosen_row_length_too_long`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Gesamtlänge aller Spalten zu groß ist.
`Aurora_pq_request_not_chosen_small_table`	Die Anzahl der Situationen, in denen die Gesamtgröße der Tabelle (Zeilenanzahl und durchschnittliche Zeilenlänge) der Grund für den Nichteinsatz von Parallel Query war. Die Zähleranzeige kann mit einer `EXPLAIN`-Anweisung erhöht werden, selbst wenn die Abfrage nicht tatsächlich ausgeführt wird.
`Aurora_pq_request_not_chosen_temporary_table`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage auf temporäre Tabellen verweist, die die nicht unterstützten Tabellentypen `MyISAM` oder `memory` verwenden.

Name	Beschreibung
`Aurora_pq_request_not_chosen_tx_isolation`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage eine nicht unterstützte Transaktionsisolationsstufe verwendet. Bei DB-Leser-Instances wird die parallele Abfrage nur auf die Isolationsstufen `REPEATABLE READ` und `READ COMMITTED` angewendet.
`Aurora_pq_request_not_chosen_update_delete_stmts`	Die Anzahl der parallelen Abfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da die Abfrage Teil einer `UPDATE`- oder `DELETE`-Anweisung ist.
`Aurora_pq_request_not_chosen_unsupported_access`	Die Anzahl der Parallelabfrageanforderungen, die den nicht-parallelen Abfrageverarbeitungspfad nutzen, weil die `WHERE`-Klausel nicht den Kriterien einer Parallelabfrage gerecht wird. Dieses Ergebnis kann eintreten, wenn für die Abfrage kein datenintensiver Scan erforderlich ist oder wenn es sich bei der Abfrage um eine `DELETE`- oder `UPDATE`-Anweisung handelt.
`Aurora_pq_request_not_chosen_unsupported_storage_type`	Die Anzahl der Parallelabfrageanforderungen, die den nicht parallelen Abfrageverarbeitungspfad verwenden, da der DB-Cluster von Aurora MySQL keine unterstützte Aurora-Cluster-Speicherkonfiguration verwendet. Weitere Informationen finden Sie unter Einschränkungen. Dieser Parameter gilt für Aurora-MySQL-Version 3.04 und höher.

Name	Beschreibung
`Aurora_pq_request_throttled`	Die Anzahl der Situationen, in denen Parallel Query nicht genutzt wurde, weil die Höchstmenge gleichzeitiger Parallelabfragen bereits auf einer bestimmten Aurora-DB-Instance ausgeführt wird.
`Aurora_repl_bytes_received`	Anzahl der Byte, die seit dem letzten Neustart auf eine Reader-Datenbank-Instance von Aurora MySQL repliziert wurden. Weitere Informationen finden Sie unter Replikation mit Amazon Aurora My SQL.
`Aurora_reserved_mem_exceeded_incidents`	Gibt an, wie oft die Engine seit dem letzten Neustart die Grenzen des reservierten Speichers überschritten hat. Falls `aurora_oom_response` konfiguriert, definiert dieser Schwellenwert, wann out-of-memory (OOM-) Vermeidungsaktivitäten ausgelöst werden. Weitere Informationen zur Antwort wegen Speichermangel von Aurora MySQL finden Sie unter Behebung von out-of-memory Problemen mit Aurora MySQL-Datenbanken.
`Aurora_thread_pool_thread_count`	Die aktuelle Anzahl von Threads im Aurora-Threadpool. Weitere Informationen zum Threadpool in Aurora MySQL finden Sie unter Thread-Pool.

Name	Beschreibung
`Aurora_tmz_version`	Bezeichnet die aktuelle Version der Zeitzoneninformationen, die vom DB-Cluster verwendet werden. Die Werte folgen dem Format der Internet Assigned Numbers Authority (IANA): YYYY`suffix` , zum Beispiel `2022a` und `2023c`. Dieser Parameter gilt für Aurora-MySQL-Version 2.12 und höher sowie Version 3.04 und höher.
`Aurora_zdr_oom_threshold`	Stellt den Speicherschwellenwert in Kilobyte (KB) für eine Aurora-DB-Instance dar, um einen Neustart ohne Ausfallzeiten (Zero Downtime Restart, ZDR) einzuleiten, um sich nach potenziellen Speicherproblemen zu erholen.
`server_aurora_das_running`	Gibt an, ob Database Activity Streams (DAS) auf dieser DB-Instance aktiviert oder deaktiviert sind. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.

MySQL-Statusvariablen, die nicht für Aurora MySQL gelten

Aufgrund der architektonischen Unterschiede zwischen Aurora MySQL und MySQL gelten einige MySQL-Statusvariablen nicht für Aurora MySQL.

Die folgenden MySQL-Statusvariablen gelten nicht für Aurora MySQL. Diese Liste ist nicht umfassend.

- `innodb_buffer_pool_bytes_dirty`
- `innodb_buffer_pool_pages_dirty`
- `innodb_buffer_pool_pages_flushed`

Aurora-MySQL-Version 3 entfernt die folgenden Statusvariablen in Aurora-MySQL-Version 2:

- `AuroraDb_lockmgr_bitmaps0_in_use`
- `AuroraDb_lockmgr_bitmaps1_in_use`
- `AuroraDb_lockmgr_bitmaps_mem_used`
- `AuroraDb_thread_deadlocks`
- `available_alter_table_log_entries`
- `Aurora_lockmgr_memory_used`
- `Aurora_missing_history_on_replica_incidents`
- `Aurora_new_lock_manager_lock_release_cnt`
- `Aurora_new_lock_manager_lock_release_total_duration_micro`
- `Aurora_new_lock_manager_lock_timeout_cnt`
- `Aurora_total_op_memory`
- `Aurora_total_op_temp_space`
- `Aurora_used_alter_table_log_entries`
- `Aurora_using_new_lock_manager`
- `Aurora_volume_bytes_allocated`
- `Aurora_volume_bytes_left_extent`
- `Aurora_volume_bytes_left_total`
- `Com_alter_db_upgrade`
- `Compression`
- `External_threads_connected`
- `Innodb_available_undo_logs`
- `Last_query_cost`
- `Last_query_partial_plans`
- `Slave_heartbeat_period`
- `Slave_last_heartbeat`
- `Slave_received_heartbeats`
- `Slave_retried_transactions`
- `Slave_running`

- `Time_since_zero_connections`

Diese MySQL-Statusvariablen sind in Aurora-MySQL-Version 1 2 verfügbar, in Aurora-MySQL-Version 3 jedoch nicht:

- `Innodb_redo_log_enabled`
- `Innodb_undo_tablespaces_total`
- `Innodb_undo_tablespaces_implicit`
- `Innodb_undo_tablespaces_explicit`
- `Innodb_undo_tablespaces_active`

Aurora-MySQL-Warteereignisse

Es folgen verschiedene typische Warteereignisse für Aurora MySQL.

> **Note**
>
> Informationen zur Optimierung der Leistung von Aurora MySQL mithilfe von Warteereignissen finden Sie unter Optimieren von Aurora MySQL mit Warteereignissen.
> Informationen zu den in MySQL-Warteereignissen geltenden Namenskonventionen finden Sie unter Performance Schema Instrument Naming Conventions in der MySQL-Dokumentation.

cpu

Die Anzahl der aktiven Verbindungen, die zum Ausführen bereit sind, ist konstant höher als die Anzahl der vCPUs. Weitere Informationen finden Sie unter cpu.

io/aurora_redo_log_flush

Eine Sitzung enthält Daten für den Aurora-Speicher. Typischerweise bezieht sich dieses Warteereignis auf eine Schreib-I/O-Operation in Aurora MySQL. Weitere Informationen finden Sie unter io/aurora_redo_log_flush.

io/aurora_respond_to_client

Die Abfrageverarbeitung ist abgeschlossen und die Ergebnisse werden für die folgenden Aurora-MySQL-Version an den Anwendungs-Client zurückgegeben: 2.10.2 und höhere 2.10-

Versionen, 2.09.3 und höhere 2.09-Versionen, 2.07.7 und höhere 2.07-Versionen. Vergleichen Sie die Netzwerkbandbreite der DB-Instance-Klasse mit der Größe der zurückgegebenen Ergebnismenge. Überprüfen Sie auch clientseitige Reaktionszeiten. Wenn der Client nicht reagiert und die TCP-Pakete nicht verarbeiten kann, können Paketabfälle und TCP-Neuübertragungen auftreten. Diese Situation wirkt sich negativ auf die Netzwerkbandbreite aus. In Versionen vor 2.10.2, 2.09.3 und 2.07.7 enthält das Warteereignis fälschlicherweise die Leerlaufzeit. Um zu erfahren, wie Sie Ihre Datenbank optimieren, wenn diese Wartezeit im Vordergrund steht, lesen Sie io/aurora_respond_to_client.

io/file/csv/data

Threads schreiben in Tabellen im CSV-Format (Comma-Separated Value). Prüfen Sie die Auslastung der CSV-Tabellen. Eine typische Ursache für dieses Ereignis ist die Einstellung `log_output` auf einer Tabelle.

io/file/sql/binlog

Ein Thread wartet auf eine binäre Protokoll-Datei (binlog), die auf den Datenträger geschrieben wird.

io/redo_log_flush

Eine Sitzung enthält Daten für den Aurora-Speicher. Typischerweise bezieht sich dieses Warteereignis auf eine Schreib-I/O-Operation in Aurora MySQL. Weitere Informationen finden Sie unter io/redo_log_flush.

io/socket/sql/client_connection

Das Programm `mysqld` ist damit beschäftigt, Threads zu erstellen, um eingehende neue Client-Verbindungen zu verarbeiten. Weitere Informationen finden Sie unter io/socket/sql/client_connection.

io/table/sql/handler

Der Motor wartet auf Zugang zu einer Tabelle. Dieses Ereignis tritt unabhängig davon auf, ob die Daten im Pufferpool zwischengespeichert oder auf der Festplatte zugegriffen werden. Weitere Informationen finden Sie unter io/table/sql/handler.

lock/table/sql/handler

Dieses Warteereignis ist ein Warteereignis-Handler für Tabellensperren. Weitere Informationen zu Atom- und Molekülereignissen im Leistungsschema finden Sie unter Leistungsschema-Atom- und Molekülereignisse in der MySQL-Dokumentation.

synch/cond/innodb/row_lock_wait

Mehrere DML-Anweisungen (DML = Data Manipulation Language) greifen gleichzeitig auf dieselben Datenbankzeilen zu. Weitere Informationen finden Sie unter synch/cond/innodb/row_lock_wait.

synch/cond/innodb/row_lock_wait_cond

Mehrere DML-Anweisungen greifen gleichzeitig auf dieselben Datenbankzeilen zu. Weitere Informationen finden Sie unter synch/cond/innodb/row_lock_wait_cond.

synch/cond/sql/MDL_context::COND_wait_status

Threads warten auf eine Tabellen-Metadatensperre. Die Engine verwendet diese Art von Sperre, um den gleichzeitigen Zugriff auf ein Datenbankschema zu verwalten und die Datenkonsistenz sicherzustellen. Weitere Informationen finden Sie unter Optimizing Locking Operations in der MySQL-Dokumentation. Um zu erfahren, wie Sie Ihre Datenbank optimieren, wenn dieses Ereignis im Vordergrund steht, lesen Sie synch/cond/sql/MDL_context::COND_wait_status.

synch/cond/sql/MYSQL_BIN_LOG::COND_done

Sie haben die binäre Protokollierung aktiviert. Es kann einen hohen Commit-Durchsatz, eine große Anzahl von Transaktionen oder Replikate geben, die Binlogs lesen. Erwägen Sie, mehrzeilige Anweisungen zu verwenden oder Anweisungen in einer Transaktion zu bündeln. Verwenden Sie in Aurora globale Datenbanken anstelle der Binärprotokollreplikation oder verwenden Sie die Parameter `aurora_binlog_*`.

synch/mutex/innodb/aurora_lock_thread_slot_futex

Mehrere DML-Anweisungen greifen gleichzeitig auf dieselben Datenbankzeilen zu. Weitere Informationen finden Sie unter synch/mutex/innodb/aurora_lock_thread_slot_futex.

synch/mutex/innodb/buf_pool_mutex

Der Puffer-Pool ist nicht groß genug, um den Arbeitsdatensatz zu speichern. Oder die Workload greift auf Seiten aus einer bestimmten Tabelle zu, was zu Konflikten im Pufferpool führt. Weitere Informationen finden Sie unter synch/mutex/innodb/buf_pool_mutex.

synch/mutex/innodb/fil_system_mutex

Der Prozess wartet auf den Zugriff auf den Tablespace-Speicher-Cache. Weitere Informationen finden Sie unter synch/mutex/innodb/fil_system_mutex.

synch/mutex/innodb/trx_sys_mutex

Vorgänge überprüfen, aktualisieren, löschen oder hinzufügen Transaktions-IDs in InnoDB konsistent oder kontrolliert. Diese Vorgänge erfordern einen `trx_sys`-Mutex-Aufruf, der von der Leistungs-Schema-Instrumentierung verfolgt wird. Zu den Vorgängen gehören die Verwaltung des Transaktionssystems beim Starten oder Herunterfahren der Datenbank, Rollbacks, Rückgängig-Bereinigungen, Zeilen-Lesezugriff und Pufferpool-Lasten. Eine hohe Datenbanklast bei einer großen Anzahl von Transaktionen führt zum häufigen Auftreten dieses Wait-Ereignisses. Weitere Informationen finden Sie unter synch/mutex/innodb/trx_sys_mutex.

synch/mutex/mysys/key_cache:: cache_lock

Der `keycache->cache_lock`-Mutex steuert den Zugriff auf den Schlüsselcache für MyISAM-Tabellen. Aurora MySQL erlaubt zwar keine MyISAM-Tabellen zum Speichern persistenter Daten, diese werden jedoch zum Speichern interner temporärer Tabellen verwendet. Prüfen Sie ggf. die Statuszähler `created_tmp_tables` oder `created_tmp_disk_tables`, da in bestimmten Situationen temporäre Tabellen auf die Festplatte geschrieben werden, wenn sie nicht mehr in den Speicher passen.

synch/mutex/sql/FILE_AS_TABLE::LOCK_offsets

Die Engine erwirbt diesen Mutex beim Öffnen oder Erstellen eines Tabellen-Metadatenarchivs. Wenn dieses Warteereignis mit übermäßiger Häufigkeit auftritt, ist die Anzahl der erstellten oder geöffneten Tabellen gestiegen.

synch/mutex/sql/file_as_table:: LOCK_shim_lists

Die Engine ruft diesen Mutex ab, während sie Vorgänge wie `reset_size`, `detach_contents` oder `add_contents` an der internen Struktur durchführt, die geöffnete Tabellen verfolgt. Der Mutex synchronisiert den Zugriff auf den Listeninhalt. Wenn dieses Warteereignis mit hoher Frequenz auftritt, deutet dies auf eine plötzliche Änderung des Tabellensatzes hin, auf die zuvor zugegriffen wurde. Die Engine muss auf neue Tabellen zugreifen oder den Kontext, der sich auf zuvor aufgerufene Tabellen bezieht, loslassen.

synch/mutex/sql/LOCK_open

Die Anzahl der Tabellen, die Ihre Sitzungen öffnen, überschreitet die Größe des Tabellendefinitions-Caches oder des Caches zum Öffnen der Tabelle. Erhöhen Sie die Größe dieser Caches. Weitere Informationen finden Sie unter How MySQL Opens and Closes Tables.

synch/mutex/sql/LOCK_table_cache

Die Anzahl der Tabellen, die Ihre Sitzungen öffnen, überschreitet die Größe des Tabellendefinitions-Caches oder des Caches zum Öffnen der Tabelle. Erhöhen Sie die Größe dieser Caches. Weitere Informationen finden Sie unter How MySQL Opens and Closes Tables.

synch/mutex/sql/LOG

Bei diesem Warteereignis warten Threads auf eine Protokollsperre. Beispiel: Ein Thread wartet auf eine Sperre, um in die Slow-Query-Protokolldatei zu schreiben.

synch/mutex/sql/MYSQL_BIN_LOG::LOCK_commit

Bei diesem Warteereignis wartet ein Thread auf eine Sperre, um Daten in das Binärprotokoll schreiben zu können. Konflikte in der Binärprotokollierung können bei Datenbanken mit sehr hoher Änderungsrate auftreten. In Abhängigkeit von der MySQL-Version werden verschiedene Sperren verwendet, um Konsistenz und Haltbarkeit des Binärprotokolls zu schützen. In RDS for MySQL werden Binärprotokolle für die Replikation und für automatische Sicherungen verwendet. In Aurora MySQL werden keine Binärprotokolle für die native Replikation und für Sicherungen benötigt. Sie sind standardmäßig deaktiviert, können aber aktiviert und für die externe Replikation oder die Erfassung von Änderungsdaten genutzt werden. Weitere Informationen finden Sie unter The Binary Log in der MySQL-Dokumentation.

sync/mutex/sql/MYSQL_BIN_LOG:: LOCK_dump_thread_metrics_collection

Wenn die binäre Protokollierung aktiviert ist, erwirbt die Engine diesen Mutex, wenn sie aktive Dump-Thread-Metriken an das Engine-Fehlerprotokoll und in die interne Vorgangs-Mappe druckt.

sync/mutex/sql/MYSQL_BIN_LOG:: LOCK_inactive_binlogs_map

Wenn die binäre Protokollierung aktiviert ist, erwirbt die Engine diesen Mutex, wenn sie die Liste der Binlog-Datei hinter der neuesten hinzufügt, sie löscht oder durchsucht.

sync/mutex/sql/MYSQL_BIN_LOG:: LOCK_IO_cache

Wenn die binäre Protokollierung aktiviert ist, erwirbt die Engine diesen Mutex während der Aurora-Binlog-IO-Cache-Vorgänge: Zuweisen, Größe ändern, freigeben, schreiben, lesen, löschen und auf Cache-Informationen zugreifen. Wenn dieses Ereignis häufig auftritt, greift die Engine auf den Cache zu, in dem Binlog-Ereignisse gespeichert werden. Um Wartezeiten zu reduzieren, reduzieren Sie Commits. Versuchen Sie, mehrere Anweisungen in einer einzigen Transaktion zu gruppieren.

synch/mutex/sql/MYSQL_BIN_LOG::LOCK_log

Sie haben die binäre Protokollierung aktiviert. Möglicherweise gibt es einen hohen Commit-Durchsatz, viele Transaktionen oder Replikate, die Binlogs lesen. Erwägen Sie, mehrzeilige Anweisungen zu verwenden oder Anweisungen in einer Transaktion zu bündeln. Verwenden Sie in Aurora globale Datenbanken anstelle der Binärprotokollreplikation oder verwenden Sie die Parameter `aurora_binlog_*`.

synch/mutex/sql/Server_thread:: LOCK_sync

Der `SERVER_THREAD::LOCK_sync`-Mutex wird während des Planens, Verarbeitens oder Startens von Threads für Dateischreibvorgänge erfasst. Das übermäßige Auftreten dieses Wait-Ereignisses weist auf eine erhöhte Schreibaktivität in der Datenbank hin.

synch/mutex/sql/tableSpaces:LOCK

Die Engine ruft den `TABLESPACES:lock`-Mutex während der folgenden Tablespace-Vorgänge ab: erstellen, löschen, abschneiden und erweitern. Das übermäßige Auftreten dieses Wait-Ereignisses weist auf eine hohe Häufigkeit von Tablespace-Vorgänge hin. Ein Beispiel ist das Laden einer großen Datenmenge in die Datenbank.

synch/rwlock/innodb/dict

Bei diesem Warteereignis warten Threads auf eine rwlock, die für das InnoDB-Datenwörterbuch gesetzt ist.

synch/rwlock/innodb/dict_operation_lock

Bei diesem Warteereignis warten Threads auf Sperren, die für InnoDB-Datenwörterbuch-Operationen gesetzt sind.

synch/rwlock/innodb/dict sys RW lock

Eine hohe Anzahl gleichzeitiger Datensteuerungssprachenanweisungen (DCLs) im Datendefinitionssprachcode (DDLs) wird gleichzeitig ausgelöst. Reduzieren Sie die Abhängigkeit der Anwendung von DDLs während regulärer Anwendungsaktivitäten.

synch/rwlock/innodb/index_tree_rw_lock

Eine große Anzahl ähnlicher DML-Anweisungen (Data Manipulation Language) greift gleichzeitig auf dasselbe Datenbankobjekt zu. Versuchen Sie es mit mehrreihigen Anweisungen. Verteilen Sie die Workload auch auf verschiedene Datenbankobjekte. Implementieren Sie beispielsweise die Partitionierung.

synch/sxlock/innodb/dict_operation_lock

Eine hohe Anzahl gleichzeitiger Datensteuerungssprachenanweisungen (DCLs) im Datendefinitionssprachcode (DDLs) wird gleichzeitig ausgelöst. Reduzieren Sie die Abhängigkeit der Anwendung von DDLs während regulärer Anwendungsaktivitäten.

synch/sxlock/innodb/dict_sys_lock

Eine hohe Anzahl gleichzeitiger Datensteuerungssprachenanweisungen (DCLs) im Datendefinitionssprachcode (DDLs) wird gleichzeitig ausgelöst. Reduzieren Sie die Abhängigkeit der Anwendung von DDLs während regulärer Anwendungsaktivitäten.

synch/sxlock/innodb/hash_table_locks

Die Sitzung konnte keine Seiten im Puffer-Pool finden. Die Engine muss entweder eine Datei lesen oder die zuletzt verwendete Liste (LRU) für den Pufferpool ändern. Erwägen Sie, die Puffer-Cache-Größe zu erhöhen und die Zugriffspfade für die entsprechenden Abfragen

synch/sxlock/innodb/index_tree_rw_lock

Viele ähnliche DML-Anweisungen (DML = Data Manipulation Language) greifen gleichzeitig auf dasselbe Datenbankobjekt zu. Versuchen Sie es mit mehrreihigen Anweisungen. Verteilen Sie die Workload auch auf verschiedene Datenbankobjekte. Implementieren Sie beispielsweise die Partitionierung.

Weitere Informationen zur Fehlerbehebung bei Synchronisierungs-Warteereignissen finden Sie unter Warum zeigt meine MySQL-DB-Instance eine hohe Anzahl aktiver Sitzungen an, die auf SYNCH-Warteereignisse in Performance Insights warten?.

Aurora-MySQL-Thread-Zustände

Im Folgenden werden einige allgemeine Thread-Zustände für Aurora MySQL aufgeführt.

Berechtigungen werden überprüft

Der Thread prüft, ob der Server über die erforderlichen Berechtigungen zum Ausführen der Anweisung verfügt.

Abfrage-Cache auf Abfrage prüfen

Der Server prüft, ob die aktuelle Abfrage im Abfrage-Cache vorhanden ist.

Bereinigen

Dies ist der endgültige Status einer Verbindung, deren Arbeit abgeschlossen ist, aber vom Client nicht geschlossen wurde. Die beste Lösung besteht darin, die Verbindung explizit im Code zu schließen. Oder Sie stellen einen niedrigeren Wert für `wait_timeout` in Ihrer Parametergruppe ein.

Schließen von Tabellen

Der Thread löscht die geänderten Tabellendaten auf die Festplatte und schließt die verwendeten Tabellen. Wenn dies kein schneller Vorgang ist, überprüfen Sie die Metriken für den Verbrauch der Netzwerkbandbreite im Hinblick auf die Netzwerkbandbreite der Instance-Klasse. Überprüfen Sie außerdem, ob die Parameterwerte für die Parameter `table_open_cache` und `table_definition_cache` erlauben, dass genügend Tabellen gleichzeitig geöffnet sind, damit die Engine Tabellen nicht häufig öffnen und schließen muss. Diese Parameter beeinflussen den Speicherverbrauch der Instance.

Konvertieren von HEAP in myISAM

Die Abfrage konvertiert eine temporäre Tabelle von In-Memory in On-Disk. Diese Konvertierung ist notwendig, da die von MySQL in den Zwischenschritten der Abfrageverarbeitung erstellten temporären Tabellen für den Speicher zu groß wurden. Überprüfen Sie die Werte von `tmp_table_size` und `max_heap_table_size`. In späteren Versionen lautet dieser Threadstatusname `converting HEAP to ondisk`.

Konvertieren von HEAP in Ondisk

Der Thread konvertiert eine interne temporäre Tabelle von einer In-Memory-Tabelle in eine On-Disk-Tabelle.

in tmp-Tabelle kopieren

Der Thread verarbeitet eine `ALTER TABLE`-Anweisung. Dieser Status tritt auf, nachdem die Tabelle mit der neuen Struktur erstellt wurde, aber bevor Zeilen in sie kopiert werden. Für einen Thread in diesem Status können Sie das Leistungsschema verwenden, um Informationen über den Fortschritt des Kopiervorgangs zu erhalten.

Sortierindex erstellen

Aurora MySQL führt eine Sortierung durch, weil es keinen vorhandenen Index verwenden kann, um die `ORDER BY`- oder `GROUP BY`-Klausel einer Abfrage zu erfüllen. Weitere Informationen finden Sie unter Erstellen des Sortierindex.

Tabelle wird erstellt

Der Thread erstellt eine permanente oder temporäre Tabelle.

verzögertes Commit ok fertig

Ein asynchrones Commit in Aurora MySQL hat eine Bestätigung erhalten und ist vollständig.

verzögertes Commit ok initiiert

Der Aurora MySQL-Thread hat den asynchronen Commit-Prozess gestartet, wartet aber auf die Bestätigung. Dies ist normalerweise die echte Commit-Zeit einer Transaktion.

verzögert senden ok fertig

Ein Aurora MySQL-Worker-Thread, der an eine Verbindung gebunden ist, kann freigegeben werden, während eine Antwort an den Client gesendet wird. Der Thread kann mit anderen Arbeiten beginnen. Der Zustand `delayed send ok` bedeutet, dass die asynchrone Quittung an den Client abgeschlossen ist.

verzögert senden ok initiiert

Ein Aurora MySQL-Worker-Thread hat asynchron eine Antwort an einen Client gesendet und kann nun für andere Verbindungen arbeiten. Die Transaktion hat einen asynchronen Commit-Prozess gestartet, der noch nicht bestätigt wurde.

executing

Der Thread hat begonnen, eine Anweisung auszuführen.

Freigeben von Gegenständen

Der Thread hat einen Befehl ausgeführt. Ein gewisses Freigeben von Elementen, die in diesem Status durchgeführt wurden, beinhaltet den Abfrage-Cache. Auf diesen Zustand folgt normalerweise ein Aufräumen.

init

Dieser Zustand tritt vor der Initialisierung von `ALTER TABLE`-, `DELETE`-, `INSERT`-, `SELECT`- oder `UPDATE`-Anweisungen auf. Zu den Aktionen in diesem Status gehören das Löschen des Binärprotokolls oder des InnoDB-Protokolls und eine Bereinigung des Abfrage-Caches.

master hat alle Binlog an Slave geschickt

Der Primärknoten hat seinen Teil der Replikation abgeschlossen. Der Thread wartet darauf, dass weitere Abfragen ausgeführt werden, damit er in das Binärprotokoll (Binlog) schreiben kann.

Öffnen von Tabellen

Der Thread versucht eine Tabelle zu öffnen. Dieser Vorgang ist schnell, es sei denn, eine `ALTER TABLE`- oder `LOCK TABLE`-Anweisung muss beendet werden oder sie überschreitet den Wert von `table_open_cache`.

optimieren

Der Server führt erste Optimierungen für eine Abfrage durch.

vorbereiten

Dieser Status tritt während der Abfrageoptimierung auf.

Abfrage Ende

Dieser Status tritt nach der Verarbeitung einer Abfrage jedoch vor dem Status „Freigegebene Elemente“ auf.

Entfernen von Duplikaten

Aurora MySQL konnte einen `DISTINCT`-Vorgang in der frühen Phase einer Abfrage nicht optimieren. Aurora MySQL muss alle duplizierten Zeilen entfernen, bevor das Ergebnis an den Client gesendet wird.

Zeilen nach Update suchen

Der Thread findet alle übereinstimmenden Zeilen, bevor er sie aktualisiert. Diese Phase ist erforderlich, wenn `UPDATE` den Index ändert, den die Engine zum Auffinden der Zeilen verwendet.

Binlog-Ereignis an Slave senden

Der Thread liest ein Ereignis aus dem Binärprotokoll und sendet es an das Replikat.

Zwischengespeichertes Ergebnis an den Client senden

Der Server nimmt das Ergebnis einer Abfrage aus dem Abfrage-Cache und sendet es an den Client.

senden von Daten

Der Thread liest und verarbeitet Zeilen für eine `SELECT`-Anweisung, hat aber noch nicht damit begonnen, Daten an den Client zu senden. Der Prozess identifiziert, welche Seiten die Ergebnisse enthalten, die erforderlich sind, um die Abfrage zu erfüllen. Weitere Informationen finden Sie unter Senden von Daten.

an den Kunden senden

Der Server schreibt ein Paket an den Client. In früheren MySQL-Versionen wurde dieses Warteereignis mit `writing to net` bezeichnet.

starting

Dies ist die erste Stufe zu Beginn der Ausführung von Anweisungen.

statistics

Der Server berechnet Statistiken, um einen Abfrageausführungsplan zu entwickeln. Wenn sich ein Thread längere Zeit in diesem Zustand befindet, ist der Server wahrscheinlich festplattengebunden, während er andere Arbeiten ausführt.

Speichern von Ergebnis im Abfrage-Cache

Der Server speichert das Ergebnis einer Abfrage im Abfrage-Cache.

Systemsperre

Der Thread hat `mysql_lock_tables` aufgerufen, aber der Threadstatus wurde seit dem Aufruf nicht aktualisiert. Dieser allgemeine Zustand tritt aus vielen Gründen auf.

update

Der Thread bereitet sich darauf vor, die Tabelle zu aktualisieren.

executing

Der Thread sucht nach Zeilen und aktualisiert sie.

Benutzersperre

Der Thread hat einen `GET_LOCK`-Aufruf ausgegeben. Der Thread hat entweder eine Beratungssperre angefordert und wartet darauf oder plant, sie anzufordern.

auf weitere Updates warten

Der Primärknoten hat seinen Teil der Replikation abgeschlossen. Der Thread wartet darauf, dass weitere Abfragen ausgeführt werden, damit er in das Binärprotokoll (Binlog) schreiben kann.

Warten auf Schema-Metadatensperre

Dies ist ein Warten auf eine Metadatensperre.

auf die Sperre der gespeicherten Funktion Metadaten

Dies ist ein Warten auf eine Metadatensperre.

Warten auf Metadatensperre der gespeicherten

Dies ist ein Warten auf eine Metadatensperre.

Warten auf Tabellenintegration

Der Thread führt `FLUSH TABLES` aus und wartet darauf, dass alle Threads ihre Tabellen schließen. Oder der Thread erhielt eine Benachrichtigung, dass sich die zugrunde liegende Struktur für eine Tabelle geändert hat, daher muss er die Tabelle erneut öffnen, um die neue Struktur zu erhalten. Um die Tabelle erneut zu öffnen, muss der Thread warten, bis alle anderen Threads die Tabelle geschlossen haben. Diese Benachrichtigung erfolgt, wenn ein anderer Thread eine der folgenden Anweisungen in der Tabelle verwendet hat: `FLUSH TABLES`, `ALTER TABLE`, `RENAME TABLE`, `REPAIR TABLE`, `ANALYZE TABLE`, oder `OPTIMIZE TABLE`.

auf Tabellen-Levelsperre

Eine Sitzung hält eine Sperre für eine Tabelle, während eine andere Sitzung versucht, dieselbe Sperre für dieselbe Tabelle zu erwerben.

Warten auf Tabellen-Metadatensperre

Aurora MySQL verwendet die Sperre von Metadaten, um den gleichzeitigen Zugriff auf Datenbankobjekte zu verwalten und die Datenkonsistenz sicherzustellen. In diesem Warteereignis hält eine Sitzung eine Metadatensperre für eine Tabelle, während eine andere Sitzung versucht, dieselbe Sperre für dieselbe Tabelle zu erwerben. Wenn das Leistungsschema aktiviert ist, wird dieser Threadstatus als Warteereignis `synch/cond/sql/MDL_context::COND_wait_status` gemeldet.

Schreiben ins Netz

Der Server schreibt ein Paket in das Netzwerk. In späteren MySQL-Versionen wird dieses Warteereignis mit `Sending to client` markiert.

Aurora MySQL-Isolierungsstufen

Im Folgenden erfahren Sie, wie DB-Instances in einem Aurora MySQL-Cluster die Datenbankeigenschaft „Isolation“ implementieren. Dieses Thema erläutert, wie das Standardverhalten von Aurora MySQL einen Ausgleich zwischen strenger Konsistenz und

hoher Leistung sucht. Mithilfe dieser Informationen können Sie entscheiden, wann je nach den Eigenschaften Ihres Workloads die Standardeinstellungen geändert werden sollten.

Verfügbare Isolierungsstufen für Writer-Instances

Sie können die Isolierungsstufen `REPEATABLE READ`, `READ COMMITTED`, `READ UNCOMMITTED` und `SERIALIZABLE` für die primäre Instance eines Aurora MySQL DB-Clusters verwenden. Diese Isolierungsstufen funktionieren in Aurora MySQL genauso wie in RDS for MySQL.

Isolierungsstufe REPEATABLE READ für Reader-Instances

Standardmäßig verwenden als schreibgeschützte Aurora-Replicas konfigurierte Aurora MySQL-DB-Instances die Isolierungsstufe `REPEATABLE READ`. Diese DB-Instances ignorieren alle `SET TRANSACTION ISOLATION LEVEL`-Anweisungen und verwenden weiterhin die Isolierungsstufe `REPEATABLE READ`.

Sie können die Isolationsstufe für Reader-DB-Instances nicht mithilfe von DB-Parametern oder DB-Cluster-Parametern festlegen.

Isolierungsstufe READ COMMITTED für Reader-Instances

Wenn Ihre Anwendung schreibintensive Workloads auf der primären Instance und lang andauernde Abfragen auf den Aurora-Replicas beinhaltet, kann es zu erheblichen Bereinigungsverzögerungen kommen. Eine Bereinigungsverzögerung tritt auf, wenn die interne Garbage Collection von lang andauernden Abfragen blockiert wird. Das Symptom, das Sie sehen, ist ein hoher Wert für `history list length` in der Ausgabe des `SHOW ENGINE INNODB STATUS`-Befehls. Sie können diesen Wert anhand der `RollbackSegmentHistoryListLength`-Metrik in CloudWatch überwachen. Eine erhebliche Bereinigungsverzögerung kann die Effektivität sekundärer Indizes reduzieren und zu einer geringeren allgemeinen Abfrageleistung führen sowie Speicherplatz verschwenden.

Wenn diese Probleme bei Ihnen auftreten, können Sie mit einer Aurora MySQL-Konfigurationseinstellung auf Sitzungsebene, `aurora_read_replica_read_committed`, die Isolierungsstufe `READ COMMITTED` für Aurora-Replicas verwenden. Die Verwendung dieser Einstellung kann Verlangsamungen sowie die Verschwendung von Speicherplatz durch lang andauernde Abfragen reduzieren, während Transaktionen Ihre Tabellen modifizieren.

Wie empfehlen, dass Sie sich mit dem spezifischen Aurora MySQL-Verhalten der `READ COMMITTED`-Isolierung gut vertraut machen, bevor Sie diese Einstellung verwenden. Das Aurora-Replica `READ COMMITTED`-Verhalten entspricht dem ANSI SQL-Standard. Die Isolierung ist jedoch weniger strikt als bei dem typischen MySQL `READ COMMITTED`-Verhalten, mit dem Sie möglicherweise vertraut

sind. So kann es etwa zu abweichenden Ergebnissen einer Abfrage unter `READ COMMITTED` auf einem Aurora MySQL-Lesereplikat und für dieselbe Abfrage unter `READ COMMITTED` auf der primären Aurora MySQL-Instance oder auf RDS für MySQL kommen. Sie können die `aurora_read_replica_read_committed`-Einstellung für Anwendungsfälle wie einen umfassenden Bericht über eine sehr große Datenbank verwenden. Für kurze Abfragen mit kleinen Ergebnissätzen, bei denen es auf Präzision und Wiederholbarkeit ankommt, sollten Sie sie eher nicht verwenden.

Die `READ COMMITTED`-Isolierungsstufe ist nicht für Sitzungen innerhalb eines sekundären Clusters in einer globalen Aurora-Datenbank verfügbar, die die Schreibweiterleitungsfunktion verwenden. Informationen zur Schreibweiterleitung finden Sie unter Verwenden der Schreibweiterleitung in einer Amazon Aurora globalen Datenbank.

Verwenden von READ COMMITTED für Reader

Um die Isolierungsstufe `READ COMMITTED` für Aurora-Replicas zu aktivieren, setzen Sie die Konfigurationseinstellung `aurora_read_replica_read_committed` auf `ON`. Verwenden Sie diese Einstellung auf Sitzungsebene bei Verbindung zu einer spezifischen Aurora-Replica. Führen Sie dazu die folgenden SQL-Befehle aus:

```
set session aurora_read_replica_read_committed = ON;
set session transaction isolation level read committed;
```

Sie können diese Konfigurationseinstellung temporär verwenden, um interaktive einmalige Abfragen durchzuführen. Sie können auch eine Berichts- oder Datenanalyseanwendung ausführen, die von der Isolierungsstufe `READ COMMITTED` profitiert, wobei die Standards für andere Anwendungen unverändert bleiben.

Wenn die `aurora_read_replica_read_committed`-Einstellung aktiviert ist, geben Sie mit dem `SET TRANSACTION ISOLATION LEVEL`-Befehl die Isolierungsstufe für die jeweiligen Transaktionen an.

```
set transaction isolation level read committed;
```

Unterschiede beim Verhalten von READ COMMITTED auf Aurora-Replikaten

Die `aurora_read_replica_read_committed`-Einstellung stellt die Isolierungsstufe `READ COMMITTED` für eine Aurora-Replica zur Verfügung, mit einem Konsistenzverhalten, das für lang andauernde Transaktionen optimiert ist. Die Isolierungsstufe `READ COMMITTED` auf Aurora-Replicas

bietet eine weniger strikte Isolierung als auf primären Aurora-Instances. Aktivieren Sie daher diese Einstellung nur auf Aurora-Replicas, wenn Sie wissen, dass für Ihre Abfragen bestimmte Arten inkonsistenter Ergebnisse akzeptabel sind.

Bei Ihren Abfragen können bestimmte Arten von Anomalien auftreten, wenn die `aurora_read_replica_read_committed`-Einstellung aktiviert ist. Dabei sollten Sie besonders zwei Arten von Anomalien verstehen und in Ihrem Anwendungscode berücksichtigen. Eine nicht-wiederholbarer Lesevorgang tritt auf, wenn eine andere Transaktion ein Commit durchführt, während Ihre Abfrage läuft. Eine lang andauernde Abfrage kann an ihrem Anfang andere Daten sehen als an ihrem Ende. Eine Phantom-Lesevorgang tritt auf, wenn andere Transaktionen dazu führen, dass bestehende Zeilen umorganisiert werden, während Ihre Abfrage läuft, und dass dadurch eine oder mehrere Zeilen von Ihrer Abfrage zweimal gelesen werden.

Phantom-Lesevorgänge können in Ihren Abfragen zu inkonsistenten Zeilenanzahlen führen. Nicht-wiederholbare Lesevorgänge können auch zur Ausgabe unvollständiger oder inkonsistenter Ergebnisse führen. Nehmen Sie beispielsweise an, eine Join-Operation bezieht sich auf Tabellen, die gleichzeitig von SQL-Anweisungen wie `INSERT` oder `DELETE` modifiziert werden. In diesem Fall kann es sein, dass die Join-Abfrage eine Zeile aus einer Tabelle liest, aber nicht die entsprechende Zeile aus einer anderen Tabelle.

Der ANSI SQL-Standard lässt beide Verhaltensweisen für die Isolationsstufe `READ COMMITTED` zu. Diese Verhaltensweisen unterscheiden sich jedoch von der typischen MySQL-Implementierung von `READ COMMITTED`. Prüfen Sie daher vor der Aktivierung der `aurora_read_replica_read_committed`-Einstellung bestehenden SQL-Code darauf, ob er im Rahmen des lockereren Konsistenzmodell so funktioniert wie erwartet.

Zeilenanzahlen und andere Ergebnisse sind auf der Isolationsstufe `READ COMMITTED` bei Aktivierung dieser Einstellung möglicherweise nicht streng konsistent. Sie sollten diese Einstellung daher typischerweise nur aktivieren, wenn Sie analytische Abfragen ausführen, die große Datenmengen aggregieren und für die keine absolute Präzision erforderlich ist. Wenn Sie nicht solche lang andauernden Abfragen zusammen mit schreibintensiven Workloads verwenden, benötigen Sie die `aurora_read_replica_read_committed`-Einstellung wahrscheinlich nicht. Ohne die Kombination aus lang andauernden Abfragen und schreibintensiven Workloads sind Probleme mit der Länge der Verlaufsliste unwahrscheinlich.

Example Abfragen mit Isolationsverhalten für READ COMMITTED auf Aurora-Replicas

Das folgende Beispiel zeigt, wie `READ COMMITTED`-Abfragen auf einer Aurora-Replica möglicherweise nicht wiederholbare Ergebnisse ausgeben, wenn Transaktionen gleichzeitig die

zugehörigen Tabellen modifizieren. Die Tabelle `BIG_TABLE` enthält eine Million Zeilen vor Beginn jeder Anfrage. Andere DML- (Data Manipulation Language) Anweisungen fügen Zeilen hinzu, entfernen oder ändern sie.

Die Abfragen auf der primären Aurora-Instance bei Isolierungsstufe `READ COMMITTED` führen zu vorhersehbaren Ergebnissen. Die Overheadlast, die damit verbunden ist, den Consistent-Lesevorgang für die gesamte Dauer einer lang andauernden Abfrage aufrechtzuerhalten, kann später zum umfangreichen Garbage Collection führen.

Die Abfragen auf der Aurora-Replica bei Isolierungsstufe `READ COMMITTED` sind so optimiert, dass dieses Garbage-Collection-Overhead minimiert wird. Dies führt aber andererseits dazu, dass die Ergebnisse abweichen können, wenn die Abfragen auf Zeilen stoßen, die von Transaktionen, die während der Ausführung der Abfrage Commits durchführen, hinzugefügt, entfernt oder umorganisiert werden. Die Abfragen können diese Zeilen berücksichtigen, müssen dies aber nicht tun. Zu Demonstrationszwecken prüfen die Abfragen nur die Anzahl der Zeilen in der Tabelle mithilfe der `COUNT(*)`-Funktion.

Zeit	DML-Anweisung auf der primären Aurora-Instance	Abfrage auf der primären Aurora-Instance mit READ COMMITTED	Abfrage auf einer Aurora-Replica mit READ COMMITTED
T1	`INSERT INTO big_table SELECT * FROM other_table LIMIT 1000000; COMMIT;`		
T2		Q1: `SELECT COUNT(*) FROM big_table;`	Q2: `SELECT COUNT(*) FROM big_table;`
T3	`INSERT INTO big_table (c1, c2) VALUES (1, 'one more row'); COMMIT;`		

Zeit	DML-Anweisung auf der primären Aurora-Instance	Abfrage auf der primären Aurora-Instance mit READ COMMITTED	Abfrage auf einer Aurora-Replica mit READ COMMITTED
T4		Wenn Q1 jetzt beendet wird, ist das Ergebnis 1.000.000.	Wenn Q2 jetzt beendet wird, ist das Ergebnis 1.000.000 oder 1.000.001.
T5	`DELETE FROM big_table LIMIT 2; COMMIT;`		
T6		Wenn Q1 jetzt beendet wird, ist das Ergebnis 1.000.000.	Wenn Q2 jetzt beendet wird, ist das Ergebnis 1.000.000 , 1.000.001, 999.999 oder 999.998.
T7	`UPDATE big_table SET c2 = CONCAT(c2 ,c2,c2); COMMIT;`		
T8		Wenn Q1 jetzt beendet wird, ist das Ergebnis 1.000.000.	Wenn Q2 jetzt beendet wird, ist das Ergebnis 1.000.000 , 1.000.001, 999.999 oder möglicherweise eine höhere Zahl.
T9		Q3: `SELECT COUNT(*) FROM big_table;`	Q4: `SELECT COUNT(*) FROM big_table;`

Zeit	DML-Anweisung auf der primären Aurora-Instance	Abfrage auf der primären Aurora-Instance mit READ COMMITTED	Abfrage auf einer Aurora-Replica mit READ COMMITTED
T10		Wenn Q3 jetzt beendet wird, ist das Ergebnis 999.999.	Wenn Q4 jetzt beendet wird, ist das Ergebnis 999.999.
T11		Q5: `SELECT COUNT(*) FROM parent_table p JOIN child_table c ON (p.id = c.id) WHERE p.id = 1000;`	Q6: `SELECT COUNT(*) FROM parent_table p JOIN child_table c ON (p.id = c.id) WHERE p.id = 1000;`
T12	`INSERT INTO parent_table (id, s) VALUES (1000, 'hello'); INSERT INTO child_table (id, s) VALUES (1000, 'world'); COMMIT;`		
T13		Wenn Q5 jetzt beendet wird, ist das Ergebnis 0.	Wenn Q6 jetzt beendet wird, ist das Ergebnis 0 oder 1.

Wenn die Abfragen schnell abgeschlossen sind, bevor andere Transaktionen DML-Anweisungen und Commits durchführen, sind die Ergebnisse vorhersehbar und zwischen der primären Instance und der Aurora-Replica identisch. Sehen wir uns die Verhaltensunterschiede im Detail an, beginnend mit der ersten Abfrage.

Die Ergebnisse für Q1 sind äußerst vorhersehbar, weil `READ COMMITTED` auf der primären Instance ein starkes Konsistenzmodell ähnlich der Isolierungsstufe `REPEATABLE READ` verwendet.

Die Ergebnisse für Q2 können je nachdem, welche Transaktionen während der Ausführung der Abfrage Commits durchführen, abweichen. Nehmen wir beispielsweise an, dass andere Transaktionen DML-Anweisungen und Commits durchführen, während die Abfragen laufen. In diesem Fall kann es sein, dass die Abfrage auf der Aurora-Replica mit Isolierungsstufe `READ COMMITTED` die Änderungen berücksichtigt oder nicht. Die Zeilenanzahlen sind dabei nicht in der gleichen Weise vorhersagbar wie bei Isolierungsstufe `REPEATABLE READ`. Sie sind auch nicht so vorhersagbar wie Abfragen mit Isolierungsstufe `READ COMMITTED` auf der primären Instance oder auf einer RDS für MySQL-Instance.

Die `UPDATE`-Anweisung bei T7 ändert die Anzahl der Zeilen in der Tabelle nicht. Durch die Änderung der Länge einer Spalte mit variabler Länge kann diese Anweisung jedoch dazu führen, dass Zeilen intern umorganisiert werden. Eine lang andauernde `READ COMMITTED`-Transaktion kann zunächst die alte Version einer Zeile und später im Rahmen derselben Transaktion eine neue Version derselben Zeile sehen. Die Abfrage kann auch die alte und die neue Version der Zeile überspringen, so dass die Anzahl der Zeilen von der erwarteten abweicht.

Die Ergebnisse von Q5 und Q6 können identisch oder leicht abweichend sein. Abfrage Q6 auf der Aurora-Replica unter `READ COMMITTED` kann, muss aber nicht, die neuen Zeilen sehen, für die während der Dauer der Abfrage ein Commit durchgeführt wird. Möglicherweise sieht sie auch die Zeile aus einer, aber nicht aus der anderen Tabelle. Wenn die Join-Abfrage keine übereinstimmende Zeile in beiden Tabellen findet, gibt sie die Anzahl 0 zurück. Wenn die Abfrage beide neuen Zeilen in `PARENT_TABLE` und `CHILD_TABLE` findet, gibt sie die Anzahl 1 zurück. In einer lang andauernden Anfrage können die Lookups aus den verbundenen Tabellen zu weit auseinanderliegenden Zeitpunkten stattfinden.

> **Note**
>
> Diese Verhaltensunterschiede hängen davon ab, wann für Transaktionen Commits durchgeführt werden, und wann die Abfragen die zugrunde liegenden Tabellenzeilen abfragen. Daher sind solche Unterschiede am wahrscheinlichsten in Berichtsabfragen, die mehrere Minuten oder Stunden dauern, und die auf Aurora-Clustern durchgeführt werden, die gleichzeitig OLTP-Transaktionen ausführen. Dies sind die Arten gemischter Workloads, die am meisten von der Isolierungsstufe `READ COMMITTED` auf Aurora-Replicas profitieren.

Aurora-MySQL-Hinweise

Sie können SQL-Hinweise mit Aurora-MySQL-Abfragen verwenden, um die Leistung zu optimieren. Sie können auch Hinweise verwenden, um zu verhindern, dass Ausführungspläne für wichtige Abfragen aufgrund unvorhersehbarer Bedingungen geändert werden.

> **Tip**
>
> Um zu überprüfen, welche Auswirkungen ein Hinweis auf eine Abfrage hat, überprüfen Sie den von der `EXPLAIN`-Anweisung erzeugten Abfrageplan. Vergleichen Sie die Abfragepläne mit und ohne Hinweis.

In Aurora MySQL Version 3 können Sie alle Hinweise verwenden, die in der MySQL Community Edition 8.0 verfügbar sind. Weitere Informationen zu diesen Hinweisen finden Sie unter Optimierungshinweise im MySQL-Referenzhandbuch.

Die folgenden Hinweise sind in Aurora MySQL Version 2 verfügbar. Diese Hinweise gelten für Abfragen, bei denen die Hash-Join-Funktion in Aurora MySQL Version 2 verwendet wird, insbesondere Abfragen, bei denen die parallele Abfrageoptimierung verwendet wird.

PQ, NO_PQ

Gibt an, ob der Optimierer gezwungen werden soll, Parallelabfragen pro Tabelle oder pro Abfrage zu verwenden.

`PQ` zwingt den Optimierer, Parallelabfragen für bestimmte Tabellen oder die gesamte Abfrage (Block) zu verwenden. `NO_PQ` verhindert, dass der Optimierer Parallelabfragen für bestimmte Tabellen oder die gesamte Abfrage (Block) verwendet.

Dieser Hinweis ist in Aurora MySQL 2.11 und höher verfügbar. In den folgenden Beispielen wird gezeigt, wie Sie diesen Hinweis verwenden können.

> **Note**
>
> Die Angabe eines Tabellennamens zwingt den Optimierer, den `PQ/NO_PQ`-Hinweis nur auf diese ausgewählten Tabellen anzuwenden. Wenn kein Tabellenname angegeben ist, wird der `PQ/NO_PQ`-Hinweis für alle vom Abfrageblock betroffenen Tabellen erzwungen.

```
EXPLAIN SELECT /*+ PQ() */ f1, f2
    FROM num1 t1 WHERE f1 > 10 and f2 < 100;

EXPLAIN SELECT /*+ PQ(t1) */ f1, f2
    FROM num1 t1 WHERE f1 > 10 and f2 < 100;

EXPLAIN SELECT /*+ PQ(t1,t2) */ f1, f2
    FROM num1 t1, num1 t2 WHERE t1.f1 = t2.f21;

EXPLAIN SELECT /*+ NO_PQ() */ f1, f2
    FROM num1 t1 WHERE f1 > 10 and f2 < 100;

EXPLAIN SELECT /*+ NO_PQ(t1) */ f1, f2
    FROM num1 t1 WHERE f1 > 10 and f2 < 100;

EXPLAIN SELECT /*+ NO_PQ(t1,t2) */ f1, f2
    FROM num1 t1, num1 t2 WHERE t1.f1 = t2.f21;
```

HASH_JOIN, NO_HASH_JOIN

Aktiviert oder deaktiviert die Funktion des Parallelabfragenoptimierers, auszuwählen, ob die Hash-Join-Optimierungsmethode für eine Abfrage verwendet werden soll. `HASH_JOIN` ermöglicht es dem Optimierer, Hash-Join zu verwenden, wenn dieser Mechanismus effizienter ist. `NO_HASH_JOIN` verhindert, dass der Optimierer Hash-Join für die Abfrage verwendet. Dieser Hinweis ist in Aurora MySQL 2.08 und höher verfügbar. Er hat keine Auswirkungen in Aurora-MySQL-Version 3.

In den folgenden Beispielen wird gezeigt, wie Sie diesen Hinweis verwenden können.

```
EXPLAIN SELECT/*+ HASH_JOIN(t2) */ f1, f2
  FROM t1, t2 WHERE t1.f1 = t2.f1;

EXPLAIN SELECT /*+ NO_HASH_JOIN(t2) */ f1, f2
  FROM t1, t2 WHERE t1.f1 = t2.f1;
```

HASH_JOIN_PROBING, NO_HASH_JOIN_PROBING

Gibt in einer Hash-Join-Abfrage an, ob die angegebene Tabelle für die Testseite des Joins verwendet werden soll. Statt den gesamten Inhalt der Testtabelle zu lesen, wird über die Abfrage geprüft, ob Spaltenwerte aus der Build-Tabelle in der Testtabelle vorhanden sind. Mit `HASH_JOIN_PROBING` und `HASH_JOIN_BUILDING` können Sie angeben, wie Hash-Join-

Abfragen verarbeitet werden, ohne die Tabellen innerhalb des Abfragetextes neu zu ordnen. Dieser Hinweis ist in Aurora MySQL 2.08 und höher verfügbar. Er hat keine Auswirkungen in Aurora-MySQL-Version 3.

In den folgenden Beispielen wird gezeigt, wie Sie diesen Hinweis verwenden können. Die Angabe des `HASH_JOIN_PROBING`-Hinweises für die Tabelle `T2` hat den gleichen Effekt wie die Angabe von `NO_HASH_JOIN_PROBING` für die Tabelle `T1`.

```
EXPLAIN SELECT /*+ HASH_JOIN(t2) HASH_JOIN_PROBING(t2) */ f1, f2
  FROM t1, t2 WHERE t1.f1 = t2.f1;

EXPLAIN SELECT /*+ HASH_JOIN(t2) NO_HASH_JOIN_PROBING(t1) */ f1, f2
  FROM t1, t2 WHERE t1.f1 = t2.f1;
```

HASH_JOIN_BUILDING, NO_HASH_JOIN_BUILDING

Gibt in einer Hash-Join-Abfrage an, ob die angegebene Tabelle für die Build-Seite des Joins verwendet werden soll oder nicht. Mit der Abfrage werden alle Zeilen aus dieser Tabelle verarbeitet, um die Liste der Spaltenwerte und den Querverweis auf die andere Tabelle zu erstellen. Mit `HASH_JOIN_PROBING` und `HASH_JOIN_BUILDING` können Sie angeben, wie Hash-Join-Abfragen verarbeitet werden, ohne die Tabellen innerhalb des Abfragetextes neu zu ordnen. Dieser Hinweis ist in Aurora MySQL 2.08 und höher verfügbar. Er hat keine Auswirkungen in Aurora-MySQL-Version 3.

Im folgenden Beispiel wird gezeigt, wie Sie diesen Hinweis verwenden können. Die Angabe des `HASH_JOIN_BUILDING`-Hinweises für die Tabelle `T2` hat den gleichen Effekt wie die Angabe von `NO_HASH_JOIN_BUILDING` für die Tabelle `T1`.

```
EXPLAIN SELECT /*+ HASH_JOIN(t2) HASH_JOIN_BUILDING(t2) */ f1, f2
  FROM t1, t2 WHERE t1.f1 = t2.f1;

EXPLAIN SELECT /*+ HASH_JOIN(t2) NO_HASH_JOIN_BUILDING(t1) */ f1, f2
  FROM t1, t2 WHERE t1.f1 = t2.f1;
```

JOIN_FIXED_ORDER

Gibt an, dass Tabellen in der Abfrage basierend auf der Reihenfolge, in der sie in der Abfrage aufgelistet sind, verknüpft werden. Dieser Hinweis ist besonders nützlich bei Abfragen mit drei oder mehr Tabellen. Er ist als Ersatz für den MySQL–H9inweis gedacht und entspricht dem

MySQL-Hinweis JOIN_FIXED_ORDER. Dieser Hinweis ist in Aurora MySQL 2.08 und höher verfügbar.

Im folgenden Beispiel wird gezeigt, wie Sie diesen Hinweis verwenden können.

```
EXPLAIN SELECT /*+ JOIN_FIXED_ORDER() */ f1, f2
  FROM t1 JOIN t2 USING (id) JOIN t3 USING (id) JOIN t4 USING (id);
```

JOIN_ORDER

Gibt die Join-Reihenfolge für die Tabellen in der Abfrage an. Dieser Hinweis ist besonders nützlich bei Abfragen mit drei oder mehr Tabellen. Er entspricht dem MySQL-JOIN_ORDER-Hinweis. Dieser Hinweis ist in Aurora MySQL 2.08 und höher verfügbar.

Im folgenden Beispiel wird gezeigt, wie Sie diesen Hinweis verwenden können.

```
EXPLAIN SELECT /*+ JOIN_ORDER (t4, t2, t1, t3) */ f1, f2
  FROM t1 JOIN t2 USING (id) JOIN t3 USING (id) JOIN t4 USING (id);
```

JOIN_PREFIX

Gibt die Tabellen an, die in der Join-Reihenfolge an erster Stelle stehen sollen. Dieser Hinweis ist besonders nützlich bei Abfragen mit drei oder mehr Tabellen. Er entspricht dem MySQL-JOIN_PREFIX-Hinweis. Dieser Hinweis ist in Aurora MySQL 2.08 und höher verfügbar.

Im folgenden Beispiel wird gezeigt, wie Sie diesen Hinweis verwenden können.

```
EXPLAIN SELECT /*+ JOIN_PREFIX (t4, t2) */ f1, f2
  FROM t1 JOIN t2 USING (id) JOIN t3 USING (id) JOIN t4 USING (id);
```

JOIN_SUFFIX

Gibt die Tabellen an, die in der Join-Reihenfolge an letzter Stelle stehen sollen. Dieser Hinweis ist besonders nützlich bei Abfragen mit drei oder mehr Tabellen. Er entspricht dem MySQL-JOIN_SUFFIX-Hinweis. Dieser Hinweis ist in Aurora MySQL 2.08 und höher verfügbar.

Im folgenden Beispiel wird gezeigt, wie Sie diesen Hinweis verwenden können.

```
EXPLAIN SELECT /*+ JOIN_SUFFIX (t1) */ f1, f2
  FROM t1 JOIN t2 USING (id) JOIN t3 USING (id) JOIN t4 USING (id);
```

Informationen zur Verwendung von Hash-Join-Abfragen finden Sie unter Optimierung von großen Aurora-MySQL-Join-Abfragen mit Hash-Joins.

Von Aurora MySQL gespeicherte Prozeduren

Sie können Ihren Aurora MySQL-DB-Clusters durch Aufrufen integrierter gespeicherter Verfahren verwalten.

Themen

- Konfigurieren
- Beenden einer Sitzung oder Abfrage
- Protokollierung
- Verwalten des globalen Statusverlaufs
- Replikation

Konfigurieren

Die folgenden gespeicherten Prozeduren legen Konfigurationsparameter fest und zeigen sie an, z. B. für die Aufbewahrung binärer Protokolldateien.

Themen

- mysql.rds_set_configuration
- mysql.rds_show_configuration

mysql.rds_set_configuration

Gibt die Anzahl an Stunden an, für die die Binärprotokolle aufbewahrt werden sollen, oder die Anzahl Sekunden, um die die Replikation verzögert werden soll.

Syntax

```
CALL mysql.rds_set_configuration(name,value);
```

Parameter

Name

Der Name des festzulegenden Konfigurationsparameters

Wert

Der Wert des Konfigurationsparameters

Nutzungshinweise

Die Prozedur `mysql.rds_set_configuration` unterstützt die folgenden Konfigurationsparameter:

- binlog retention hours

Die Konfigurationsparameter werden dauerhaft gespeichert und überstehen jeden Neustart oder Failover der DB-Instance.

binlog retention hours

Der Parameter `binlog retention hours` wird verwendet, um die Anzahl der Stunden anzugeben, die Binärprotokolldateien aufbewahrt werden sollen. In der Regel werden binäre Protokolldateien von Amazon Aurora so schnell wie möglich bereinigt. Eine binäre Protokolldatei ist möglicherweise für die Replikation mit einer außerhalb von Aurora ausgeführten MySQL-Datenbank erforderlich.

Der Standardwert von `binlog retention hours` ist `NULL`. Für Aurora MySQL `NULL` bedeutet, dass binäre Protokolle faul aufgeräumt werden. Aurora-MySQL-Binärprotokolle können für einen bestimmten Zeitraum im System verbleiben, normalerweise nicht länger als einen Tag.

Um die Anzahl der Stunden zu bestimmen, für die Binärprotokolle auf einer/einem DB-Cluster aufbewahrt werden sollen, verwenden Sie die gespeicherte Prozedur `mysql.rds_set_configuration` und geben Sie, wie in dem folgenden Beispiel gezeigt, einen ausreichend großen Zeitraum für die gewünschte Replikation an.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

> **Note**
>
> Sie können den Wert `0` nicht für `binlog retention hours` verwenden.

Der maximal zulässige `binlog retention hours`-Wert für DB-Cluster von Aurora MySQL Version 2.11.0 und höher sowie Version 3 ist 2 160 (90 Tage).

Nachdem Sie den Aufbewahrungszeitraum festgelegt haben, überwachen Sie die Speichernutzung für die DB-Instance, um sicherzustellen, dass die aufbewahrten binären Protokolle nicht zu viel Speicherplatz beanspruchen.

mysql.rds_show_configuration

Die Anzahl der Stunden, während der binäre Protokolldateien aufbewahrt werden sollen.

Syntax

```
CALL mysql.rds_show_configuration;
```

Nutzungshinweise

Mit der gespeicherten Prozedur `mysql.rds_show_configuration` überprüfen Sie, wie viele Stunden Amazon RDS die binären Protokolldateien aufbewahrt werden.

Beispiele

Nachfolgend sehen Sie ein Beispiel für die Anzeige des Aufbewahrungszeitraums:

```
call mysql.rds_show_configuration;
                name                          value     description
                binlog retention hours        24        binlog retention hours specifies
 the duration in hours before binary logs are automatically deleted.
```

Beenden einer Sitzung oder Abfrage

Die folgenden gespeicherten Prozeduren beenden eine Sitzung oder Abfrage.

Themen

- mysql.rds_kill
- mysql.rds_kill_query

mysql.rds_kill

Beendet eine Verbindung zum MySQL-Server.

Syntax

```
CALL mysql.rds_kill(processID);
```

Parameter

processID

Die ID des Verbindungs-Threads, der beendet werden soll.

Nutzungshinweise

Jede Verbindung zum MySQL-Server wird in einem eigenen Thread ausgeführt. Um eine Verbindung zu beenden, verwenden Sie die Prozedur `mysql.rds_kill` und übergeben ihr als Parameter die Thread-ID der Verbindung. Die Thread-ID erhalten Sie mithilfe des MySQL-Befehls SHOW PROCESSLIST.

Beispiele

Im folgenden Beispiel wird eine Verbindung mit der Thread-ID 4243 beendet:

```
CALL mysql.rds_kill(4243);
```

mysql.rds_kill_query

Beendet eine an den MySQL-Server übermittelte Abfrage.

Syntax

```
CALL mysql.rds_kill_query(processID);
```

Parameter

processID

Die Identität des Prozesses oder Threads, der die zu beendende Abfrage ausführt.

Nutzungshinweise

Um eine an den MySQL-Server übermittelte Abfrage zu beenden, verwenden Sie die Prozedur `mysql_rds_kill_query` und übergeben die ID des Threads, der die Abfrage ausführt. Die Prozedur beendet dann die Verbindung.

Die Abfrage-ID erhalten Sie mithilfe der MySQL-Tabelle INFORMATION_SCHEMA PROCESSLIST oder des MySQL-Befehls SHOW PROCESSLIST. Der Wert in der ID-Spalte von `SHOW PROCESSLIST` oder `SELECT * FROM INFORMATION_SCHEMA.PROCESSLIST` ist die *processID*.

Beispiele

Im folgenden Beispiel wird eine Abfrage mit der Thread-ID 230040 beendet:

```
CALL mysql.rds_kill_query(230040);
```

Protokollierung

Die folgenden gespeicherten Prozeduren rotieren MySQL-Protokolle in Backup-Tabellen. Weitere Informationen finden Sie unter Aurora-MySQL-Datenbank-Protokolldateien.

Themen

- mysql.rds_rotate_general_log
- mysql.rds_rotate_slow_log

mysql.rds_rotate_general_log

Rotiert die Tabelle `mysql.general_log` in eine Sicherungstabelle.

Syntax

```
CALL mysql.rds_rotate_general_log;
```

Nutzungshinweise

Sie können die Tabelle `mysql.general_log` in eine Sicherungstabelle rotieren, indem Sie die Prozedur `mysql.rds_rotate_general_log` aufrufen. Beim Rotieren von Protokolldateien wird die aktuelle Protokolltabelle in eine Sicherungsprotokolltabelle kopiert, und die Einträge in der aktuellen Protokolltabelle werden entfernt. Sofern bereits eine Sicherungsprotokolltabelle vorhanden ist, wird diese gelöscht, bevor die aktuelle Protokolltabelle in die Sicherungsprotokolltabelle kopiert wird. Sie können die Sicherungsprotokolltabelle abfragen, wenn dies nötig ist. Die Backup-Protokolltabelle für die `mysql.general_log`-Tabelle ist als `mysql.general_log_backup` benannt.

Sie können dieses Verfahren nur ausführen, wenn der Parameter `log_output` auf `TABLE` eingestellt ist.

mysql.rds_rotate_slow_log

Rotiert die Tabelle `mysql.slow_log` in eine Sicherungstabelle.

Syntax

```
CALL mysql.rds_rotate_slow_log;
```

Nutzungshinweise

Sie können die Tabelle `mysql.slow_log` in eine Sicherungstabelle rotieren, indem Sie die Prozedur `mysql.rds_rotate_slow_log` aufrufen. Beim Rotieren von Protokolldateien wird die aktuelle Protokolltabelle in eine Sicherungsprotokolltabelle kopiert, und die Einträge in der aktuellen Protokolltabelle werden entfernt. Sofern bereits eine Sicherungsprotokolltabelle vorhanden ist, wird diese gelöscht, bevor die aktuelle Protokolltabelle in die Sicherungsprotokolltabelle kopiert wird.

Sie können die Sicherungsprotokolltabelle abfragen, wenn dies nötig ist. Die Backup-Protokolltabelle für die `mysql.slow_log`-Tabelle ist als `mysql.slow_log_backup` benannt.

Verwalten des globalen Statusverlaufs

Amazon RDS stellt einen Satz von Verfahren bereit, die Snapshots der Werte dieser Statusvariablen im Zeitverlauf erstellen und diese zusammen mit allen Änderungen seit dem letzten Snapshot in eine Tabelle schreiben. Diese Infrastruktur wird als Global Status History bezeichnet. Weitere Informationen finden Sie unter Verwalten des globalen Statusverlaufs.

Die folgenden gespeicherten Verfahren verwalten, wie die Global Status History erfasst und verwaltet wird.

Themen

- mysql.rds_collect_global_status_history
- mysql.rds_disable_gsh_collector
- mysql.rds_disable_gsh_rotation
- mysql.rds_enable_gsh_collector
- mysql.rds_enable_gsh_rotation
- mysql.rds_rotate_global_status_history
- mysql.rds_set_gsh_collector
- mysql.rds_set_gsh_rotation

mysql.rds_collect_global_status_history

Generiert einen Snapshot auf Anforderung für den globalen Statusverlauf (Global Status History, GoSH).

Syntax

```
CALL mysql.rds_collect_global_status_history;
```

mysql.rds_disable_gsh_collector

Deaktiviert die periodische Generierung von Snapshots des globalen Statusverlaufs (Global Status History, GoSH).

Syntax

```
CALL mysql.rds_disable_gsh_collector;
```

mysql.rds_disable_gsh_rotation

Schaltet die Rotation der `mysql.global_status_history`-Tabelle aus.

Syntax

```
CALL mysql.rds_disable_gsh_rotation;
```

mysql.rds_enable_gsh_collector

Aktiviert den globalen Statusverlauf (Global Status History, GoSH), um Standard-Snapshots in zeitlichen Abständen, die mithilfe von `rds_set_gsh_collector` festgelegt wurden, zu generieren.

Syntax

```
CALL mysql.rds_enable_gsh_collector;
```

mysql.rds_enable_gsh_rotation

Aktiviert die Rotation der Inhalte der Tabelle `mysql.global_status_history` zu `mysql.global_status_history_old` in zeitlichen Abständen, die durch `rds_set_gsh_rotation` angegeben werden.

Syntax

```
CALL mysql.rds_enable_gsh_rotation;
```

mysql.rds_rotate_global_status_history

Rotiert die Inhalte der Tabelle `mysql.global_status_history` bei Anforderung zu `mysql.global_status_history_old`.

Syntax

```
CALL mysql.rds_rotate_global_status_history;
```

mysql.rds_set_gsh_collector

Gibt den zeitlichen Abstand für die Generierung von aufeinander folgenden Snapshots durch den globalen Statusverlauf (Global Status History, GoSH) an.

Syntax

```
CALL mysql.rds_set_gsh_collector(intervalPeriod);
```

Parameter

intervalPeriod

Der zeitliche Abstand in Minuten für die periodische Generierung von Snapshots. Der Standardwert ist 5.

mysql.rds_set_gsh_rotation

Gibt den zeitlichen Abstand in Tagen für die periodische Rotation der Tabelle `mysql.global_status_history` an.

Syntax

```
CALL mysql.rds_set_gsh_rotation(intervalPeriod);
```

Parameter

intervalPeriod

Der zeitliche Abstand in Tagen für die periodische Tabellenrotation. Der Standardwert ist 7.

Replikation

Sie können die folgenden gespeicherten Prozeduren aufrufen, während Sie mit der primären Instance in einem Aurora MySQL-Cluster verbunden sind. Diese Verfahren steuern, wie Transaktionen aus einer externen Datenbank in Aurora MySQL oder aus Aurora MySQL in einer externen Datenbank repliziert werden. Weitere Informationen zur Verwendung der Replikation basierend auf globalen Transaktionskennungen (GTIDs) mit Aurora MySQL finden Sie unter Verwenden der GTID-basierten Replikation.

Themen

- mysql.rds_assign_gtids_to_anonymous_transactions (Aurora MySQL Version 3)
- mysql.rds_disable_session_binlog (Aurora-MySQL-Version 2)
- mysql.rds_enable_session_binlog (Aurora-MySQL-Version 2)
- mysql.rds_gtid_purged (Aurora-MySQL-Version 3)
- mysql.rds_import_binlog_ssl_material
- mysql.rds_next_master_log (Aurora-MySQL-Version 2)
- mysql.rds_next_source_log (Aurora-MySQL-Version 3)
- mysql.rds_remove_binlog_ssl_material
- mysql.rds_reset_external_master (Aurora-MySQL-Version 2)
- mysql.rds_reset_external_source (Aurora MySQL Version 3)
- mysql.rds_set_binlog_source_ssl (Aurora MySQL Version 3)
- mysql.rds_set_external_master (Aurora-MySQL-Version 2)
- mysql.rds_set_external_master_with_auto_position (Aurora-MySQL-Version 2)
- mysql.rds_set_external_source (Aurora MySQL Version 3)
- mysql.rds_set_external_source_with_auto_position (Aurora MySQL Version 3)
- mysql.rds_set_master_auto_position (Aurora-MySQL-Version 2)
- mysql.rds_set_read_only (Aurora MySQL Version 3)
- mysql.rds_set_session_binlog_format (Aurora-MySQL-Version 2)
- mysql.rds_set_source_auto_position (Aurora MySQL Version 3)
- mysql.rds_skip_transaction_with_gtid (Aurora-MySQL-Version 2 und 3)
- mysql.rds_skip_repl_error
- mysql.rds_start_replication

- mysql.rds_start_replication_until (Aurora-MySQL-Version 3)
- mysql.rds_start_replication_until_gtid (Aurora-MySQL-Version 3)
- mysql.rds_stop_replication

mysql.rds_assign_gtids_to_anonymous_transactions (Aurora MySQL Version 3)

Konfiguriert die `ASSIGN_GTIDS_TO_ANONYMOUS_TRANSACTIONS`-Option der `CHANGE REPLICATION SOURCE TO`-Anweisung. Dadurch weist der Replikationskanal replizierten Transaktionen, die keine haben, eine GTID zu. Auf diese Weise können Sie die Binärprotokollreplikation von einer Quelle aus, die keine GTID-basierte Replikation verwendet, zu einem Replikat, durchführen, das dies tut. Weitere Informationen finden Sie unter CHANGE REPLICATION SOURCE TO Statement und Replikation von einer Quelle ohne GTIDs zu einer Replik mit GTIDs im MySQL-Referenzhandbuch.

Syntax

```
CALL mysql.rds_assign_gtids_to_anonymous_transactions(gtid_option);
```

Parameter

`gtid_option`

Zeichenfolgenwert Die erlaubten Werte sind `OFF`, `LOCAL`, oder eine angegebene UUID.

Nutzungshinweise

Dieses Vorgehen hat die gleiche Wirkung wie das Absetzen der Anweisung `CHANGE REPLICATION SOURCE TO ASSIGN_GTIDS_TO_ANONYMOUS_TRANSACTIONS =` *`gtid_option`* in Community MySQL.

GTID muss auf `ON` gesetzt werden, damit *`gtid_option`* auf `LOCAL` oder eine bestimmte UUID gesetzt wird.

Der Standardwert ist `OFF`, was bedeutet, dass die Funktion nicht verwendet wird.

`LOCAL` weist eine GTID einschließlich der eigenen UUID des Replikats (der `server_uuid`-Einstellung) zu.

Das Übergeben eines Parameters, bei dem es sich um eine UUID handelt, weist eine GTID zu, die die angegebene UUID enthält, z. B. die `server_uuid`-Einstellung für den Replikationsquellserver.

Beispiele

So deaktivieren Sie diese Funktion:

```
mysql> call mysql.rds_assign_gtids_to_anonymous_transactions('OFF');
+-------------------------------------------------------------+
| Message  |
+-------------------------------------------------------------+
| ASSIGN_GTIDS_TO_ANONYMOUS_TRANSACTIONS has been set to: OFF |
+-------------------------------------------------------------+
1 row in set (0.07 sec)
```

So verwenden Sie die eigene UUID des Replikats:

```
mysql> call mysql.rds_assign_gtids_to_anonymous_transactions('LOCAL');
+------------------------------------------------------------+
| Message  |
+------------------------------------------------------------+
| ASSIGN_GTIDS_TO_ANONYMOUS_TRANSACTIONS has been set to: LOCAL |
+------------------------------------------------------------+
1 row in set (0.07 sec)
```

So verwenden Sie eine angegebene UUID:

```
mysql> call mysql.rds_assign_gtids_to_anonymous_transactions('317a4760-
f3dd-3b74-8e45-0615ed29de0e');
+-----------------------------------------------------------------------------------------------
+
| Message |
+-----------------------------------------------------------------------------------------------
+
| ASSIGN_GTIDS_TO_ANONYMOUS_TRANSACTIONS has been set to: 317a4760-
f3dd-3b74-8e45-0615ed29de0e |
+-----------------------------------------------------------------------------------------------
+
1 row in set (0.07 sec)
```

mysql.rds_disable_session_binlog (Aurora-MySQL-Version 2)

Deaktiviert die binäre Protokollierung für die aktuelle Sitzung, indem die Variable `sql_log_bin` auf `OFF` festgelegt wird.

Syntax

```
CALL mysql.rds_disable_session_binlog;
```

Parameter

None

Nutzungshinweise

Sie rufen dieses gespeicherte Verfahren für einen Aurora MySQL-DB-Cluster auf, während Sie mit der primären Instance verbunden sind.

Für Aurora wird dieses Verfahren für Aurora-MySQL-Version 2.12 und höher und MySQL-5.7-kompatible Versionen unterstützt.

> **Note**
>
> In Aurora MySQL Version 3 können Sie den folgenden Befehl verwenden, um die binäre Protokollierung für die aktuelle Sitzung zu deaktivieren, sofern Sie die entsprechenden `SESSION_VARIABLES_ADMIN` Rechte haben:
>
> ```
> SET SESSION sql_log_bin = OFF;
> ```

mysql.rds_enable_session_binlog (Aurora-MySQL-Version 2)

Aktiviert die binäre Protokollierung für die aktuelle Sitzung, indem die Variable `sql_log_bin` auf `ON` festgelegt wird.

Syntax

```
CALL mysql.rds_enable_session_binlog;
```

Parameter

None

Nutzungshinweise

Sie rufen dieses gespeicherte Verfahren für einen Aurora MySQL-DB-Cluster auf, während Sie mit der primären Instance verbunden sind.

Für Aurora wird dieses Verfahren für Aurora-MySQL-Version 2.12 und höher und MySQL-5.7-kompatible Versionen unterstützt.

> **Note**
>
> In Aurora MySQL Version 3 können Sie den folgenden Befehl verwenden, um die binäre Protokollierung für die aktuelle Sitzung zu aktivieren, sofern Sie die entsprechenden `SESSION_VARIABLES_ADMIN` Rechte haben:
>
> ```
> SET SESSION sql_log_bin = ON;
> ```

mysql.rds_gtid_purged (Aurora-MySQL-Version 3)

Legt den globalen Wert der Systemvariablen `gtid_purged` auf einen bestimmten Satz von globalen Transaktionskennungen (GTID) fest. Die Systemvariable `gtid_purged` ist ein GTID-Satz, der aus den GTIDs aller Transaktionen besteht, für die auf dem Server ein Commit ausgeführt wurde, die jedoch in keiner binären Logdatei auf dem Server vorhanden sind.

Es gibt zwei Möglichkeiten, den Wert `gtid_purged` festzulegen, um Kompatibilität mit MySQL 8.0 zu ermöglichen:

- Ersetzen Sie den Wert `gtid_purged` durch Ihren angegebenen GTID-Set.
- Fügen Sie Ihren angegebenen GTID-Satz an den GTID-Satz an, den `gtid_purged` bereits enthält.

Syntax

So ersetzen Sie den Wert `gtid_purged` durch Ihren angegebenen GTID-Satz:

```
CALL mysql.rds_gtid_purged (gtid_set);
```

So fügen Sie den Wert `gtid_purged` Ihrem angegebenen GTID-Satz an:

```
CALL mysql.rds_gtid_purged (+gtid_set);
```

Parameter

gtid_set

Der Wert *gtid_set* muss eine Obermenge des aktuellen Werts gtid_purged sein und darf sich nicht mit gtid_subtract(gtid_executed,gtid_purged) überschneiden. Das heißt, der neue GTID-Satz muss alle GTIDs enthalten, die bereits in gtid_purged enthalten waren, und darf keine GTIDs in gtid_executed enthalten, die noch nicht gelöscht wurden. Der Parameter *gtid_set* darf auch keine GTIDs enthalten, die sich im globalen gtid_owned-Satz befinden, die GTIDs für Transaktionen, die gerade auf dem Server verarbeitet werden.

Nutzungshinweise

Die Prozedur mysql.rds_gtid_purged muss vom Hauptbenutzer ausgeführt werden.

Diese Prozedur wird für Aurora-MySQL-Version 3.04 und höher unterstützt.

Beispiele

Im folgenden Beispiel wird die GTID 3E11FA47-71CA-11E1-9E33-C80AA9429562:23 der globalen Variable gtid_purged zugewiesen.

```
CALL mysql.rds_gtid_purged('3E11FA47-71CA-11E1-9E33-C80AA9429562:23');
```

mysql.rds_import_binlog_ssl_material

Importiert das Zertifizierungsstellenzertifikat, das Clientzertifikat und den Clientschlüssel in eine/einen Aurora-MySQL-DB-Cluster. Die Informationen werden für die SSL-Kommunikation und die verschlüsselte Replikation benötigt.

> **Note**
>
> Derzeit wird dieses Verfahren für folgende Aurora-MySQL 2-Versionen unterstützt: 2.09.2, 2.10.0, 2.10.1 und 2.11.0; sowie Version 3: 3.01.1 und höher.

Syntax

```
CALL mysql.rds_import_binlog_ssl_material (
  ssl_material
);
```

Parameter

ssl_material

JSON-Nutzlast mit dem Inhalt der folgenden PEM-Dateien für einen MySQL-Client:

- „ssl_ca“: „*Zertifizierungsstellenzertifikat*“
- „ssl_cert“: „*Clientzertifikat*“
- „ssl_key“: „*Clientschlüssel*“

Nutzungshinweise

Bereiten Sie die verschlüsselte Replikation vor, bevor Sie diese Schritte durchführen:

- Wenn SSL auf dem externen Server mit der MySQL-Quelldatenbankinstance nicht aktiviert ist und Sie keinen Clientschlüssel und kein Clientzertifikat vorbereitet haben, aktivieren Sie SSL auf dem MySQL-Datenbankserver und generieren Sie den Clientschlüssel und das Clientzertifikat.
- Wenn SSL auf der externen Quelldatenbankinstance aktiviert ist, geben Sie einen Clientschlüssel und ein Clientzertifikat für das Aurora MySQL-DB-Cluster an. Wenn Sie diese Werte nicht haben, erstellen Sie ein einen neuen Schlüssel und ein neues Zertifikat für das Aurora MySQL-DB-Cluster. Sie benötigen zur Signierung des Clientzertifikats den Zertifizierungsstellenschlüssel, den Sie zum Konfigurieren von SSL auf der externen MySQL-Quelldatenbankinstance verwendet haben.

Weitere Informationen finden Sie unter Creating SSL Certificates and Keys Using openssl in der MySQL-Dokumentation.

> **Important**
>
> Führen Sie nach dem Vorbereiten der verschlüsselten Replikation die folgenden Schritte über eine SSL-Verbindung durch. Der Clientschlüssel darf nicht über eine unsichere Verbindung übertragen werden.

Bei diesem Vorgang werden SSL-Informationen aus einer externen MySQL-Datenbank in ein Aurora MySQL-DB-Cluster importiert. Die SSL-Informationen für das Aurora MySQL-DB-Cluster befinden sich in PEM-Dateien. Während der verschlüsselten Replikation dient das Aurora MySQL-DB-Cluster als Client für den MySQL-Datenbankserver. Die Zertifikate und Schlüssel für den Aurora MySQL-Client befinden sich in Dateien im PEM-Format.

Sie können die Informationen aus diesen Dateien in den Parameter `ssl_material` in der richtigen JSON-Nutzlast kopieren. Um die verschlüsselte Replikation zu unterstützen, importieren Sie diese SSL-Informationen in das Aurora MySQL-DB-Cluster.

Die JSON-Nutzlast muss das folgende Format aufweisen.

```
'{"ssl_ca":"-----BEGIN CERTIFICATE-----
ssl_ca_pem_body_code
-----END CERTIFICATE-----\n","ssl_cert":"-----BEGIN CERTIFICATE-----
ssl_cert_pem_body_code
-----END CERTIFICATE-----\n","ssl_key":"-----BEGIN RSA PRIVATE KEY-----
ssl_key_pem_body_code
-----END RSA PRIVATE KEY-----\n"}'
```

Beispiele

Im folgenden Beispiel werden SSL-Informationen in eine Aurora MySQL importiert. Der Code in den PEM-Dateien ist in der Regel länger als in diesem Beispiel.

```
call mysql.rds_import_binlog_ssl_material(
'{"ssl_ca":"-----BEGIN CERTIFICATE-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END CERTIFICATE-----\n","ssl_cert":"-----BEGIN CERTIFICATE-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END CERTIFICATE-----\n","ssl_key":"-----BEGIN RSA PRIVATE KEY-----
```

```
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END RSA PRIVATE KEY-----\n"}');
```

mysql.rds_next_master_log (Aurora-MySQL-Version 2)

Ändert die Protokollposition der Quelldatenbankinstance in den Anfang des nächsten Binärprotokolls auf der Quelldatenbankinstance. Verwenden Sie diese Prozedur nur dann, wenn Sie für ein Lesereplikat bei der Replikation einen I/O-Fehler mit der Fehlernummer 1236 erhalten.

Syntax

```
CALL mysql.rds_next_master_log(
curr_master_log
);
```

Parameter

curr_master_log

Der Index der aktuellen Master-Protokolldatei. Der Index ist im Dateinamen codiert. Eine aktuelle Datei mit dem Namen `mysql-bin-changelog.012345` hat beispielsweise den Index 12345. Um den Namen der aktuellen Master-Protokolldatei zu ermitteln, führen Sie den Befehl `SHOW REPLICA STATUS` aus. Sie finden den Namen anschließend im Feld `Master_Log_File`.

> **Note**
>
> Frühere Versionen von MySQL verwenden `SHOW SLAVE STATUS` anstelle von `SHOW REPLICA STATUS`. Wenn Sie vor 8.0.23 eine MySQL-Version verwenden, verwenden Si `SHOW SLAVE STATUS`.

Nutzungshinweise

Die Prozedur `mysql.rds_next_master_log` muss vom Hauptbenutzer ausgeführt werden.

> **Warning**
>
> `mysql.rds_next_master_log` sollte nur dann aufgerufen werden, wenn die Replikation nach einem Failover einer als Replikationsquelle fungierenden Multi-AZ-DB-Instance fehlschlägt und das Feld `Last_IO_Errno` im von `SHOW REPLICA STATUS` zurückgegebenen Ergebnis einen I/O-Fehler mit der Nummer 1236 meldet.
> Ein Aufruf von `mysql.rds_next_master_log` kann zu Datenverlust im Lesereplikat führen, falls Transaktionen in der Quell-Instance nicht in das binäre Protokoll auf der Festplatte geschrieben wurden, bevor das Failover-Ereignis auftrat.

Beispiele

Angenommen, die Replikation schlägt auf einer - Aurora-MySQL-Read Replica fehl. Die Ausführung von `SHOW REPLICA STATUS\G` für das Lesereplikat gibt das folgende Ergebnis zurück:

```
*************************** 1. row ***************************
             Replica_IO_State:
                  Source_Host: myhost.XXXXXXXXXXXXXX.rr-rrrr-1.rds.amazonaws.com
                  Source_User: MasterUser
                  Source_Port: 3306
                Connect_Retry: 10
              Source_Log_File: mysql-bin-changelog.012345
          Read_Source_Log_Pos: 1219393
               Relay_Log_File: relaylog.012340
                Relay_Log_Pos: 30223388
        Relay_Source_Log_File: mysql-bin-changelog.012345
           Replica_IO_Running: No
          Replica_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 0
                   Last_Error:
                 Skip_Counter: 0
          Exec_Source_Log_Pos: 30223232
              Relay_Log_Space: 5248928866
              Until_Condition: None
```

```
               Until_Log_File:
                Until_Log_Pos: 0
           Source_SSL_Allowed: No
           Source_SSL_CA_File:
           Source_SSL_CA_Path:
              Source_SSL_Cert:
            Source_SSL_Cipher:
               Source_SSL_Key:
       Seconds_Behind_Master: NULL
Source_SSL_Verify_Server_Cert: No
               Last_IO_Errno: 1236
               Last_IO_Error: Got fatal error 1236 from master when reading data from
 binary log: 'Client requested master to start replication from impossible position;
 the first event 'mysql-bin-changelog.013406' at 1219393, the last event read from
 '/rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4, the last byte read from '/
rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4.'
              Last_SQL_Errno: 0
              Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Source_Server_Id: 67285976
```

Den Angeben im Feld `Last_IO_Errno` ist zu entnehmen, dass die Instance eine I/O-Fehlermeldung mit der Nummer 1236 erhalten hat. Dem Feld `Master_Log_File` ist zudem zu entnehmen, dass die betroffene Protokolldatei den Namen `mysql-bin-changelog.012345` aufweist und ihr Index folglich `12345` lautet. Zur Behebung des Fehlers können Sie dann `mysql.rds_next_master_log` mit dem folgenden Parameter aufrufen:

```
CALL mysql.rds_next_master_log(12345);
```

> **Note**
>
> Frühere Versionen von MySQL verwenden `SHOW SLAVE STATUS` anstelle von `SHOW REPLICA STATUS`. Wenn Sie vor 8.0.23 eine MySQL-Version verwenden, verwenden Si `SHOW SLAVE STATUS`.

mysql.rds_next_source_log (Aurora-MySQL-Version 3)

Ändert die Protokollposition der Quelldatenbankinstance in den Anfang des nächsten Binärprotokolls auf der Quelldatenbankinstance. Verwenden Sie diese Prozedur nur dann, wenn Sie für ein Lesereplikat bei der Replikation einen I/O-Fehler mit der Fehlernummer 1236 erhalten.

Syntax

```
CALL mysql.rds_next_source_log(
curr_source_log
);
```

Parameter

curr_source_log

Der Index der aktuellen Quell-Protokolldatei. Der Index ist im Dateinamen codiert. Eine aktuelle Datei mit dem Namen `mysql-bin-changelog.012345` hat beispielsweise den Index 12345. Um den Namen der aktuellen Quell-Protokolldatei zu ermitteln, führen Sie den Befehl `SHOW REPLICA STATUS` aus. Sie finden den Namen anschließend im Feld `Source_Log_File`.

Nutzungshinweise

Die Prozedur `mysql.rds_next_source_log` muss vom Hauptbenutzer ausgeführt werden.

> **Warning**
>
> `mysql.rds_next_source_log` sollte nur dann aufgerufen werden, wenn die Replikation nach einem Failover einer als Replikationsquelle fungierenden Multi-AZ-DB-Instance fehlschlägt und das Feld `Last_IO_Errno` im von `SHOW REPLICA STATUS` zurückgegebenen Ergebnis einen I/O-Fehler mit der Nummer 1236 meldet.
> Ein Aufruf von `mysql.rds_next_source_log` kann zu Datenverlust im Lesereplikat führen, falls Transaktionen in der Quell-Instance nicht in das binäre Protokoll auf der Festplatte geschrieben wurden, bevor das Failover-Ereignis auftrat.

Beispiele

Angenommen, die Replikation für eine Aurora–MySQL-Read Replica schlägt fehl. Die Ausführung von `SHOW REPLICA STATUS\G` für das Lesereplikat gibt das folgende Ergebnis zurück:

```
*************************** 1. row ***************************
             Replica_IO_State:
                  Source_Host: myhost.XXXXXXXXXXXXXX.rr-rrrr-1.rds.amazonaws.com
                  Source_User: MasterUser
```

```
                  Source_Port: 3306
                 Connect_Retry: 10
               Source_Log_File: mysql-bin-changelog.012345
           Read_Source_Log_Pos: 1219393
                Relay_Log_File: relaylog.012340
                 Relay_Log_Pos: 30223388
         Relay_Source_Log_File: mysql-bin-changelog.012345
            Replica_IO_Running: No
           Replica_SQL_Running: Yes
               Replicate_Do_DB:
           Replicate_Ignore_DB:
            Replicate_Do_Table:
        Replicate_Ignore_Table:
       Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 0
                   Last_Error:
                 Skip_Counter: 0
           Exec_Source_Log_Pos: 30223232
               Relay_Log_Space: 5248928866
               Until_Condition: None
                Until_Log_File:
                 Until_Log_Pos: 0
            Source_SSL_Allowed: No
            Source_SSL_CA_File:
            Source_SSL_CA_Path:
               Source_SSL_Cert:
             Source_SSL_Cipher:
                Source_SSL_Key:
         Seconds_Behind_Source: NULL
Source_SSL_Verify_Server_Cert: No
                 Last_IO_Errno: 1236
                 Last_IO_Error: Got fatal error 1236 from source when reading data from
 binary log: 'Client requested source to start replication from impossible position;
 the first event 'mysql-bin-changelog.013406' at 1219393, the last event read from
 '/rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4, the last byte read from '/
rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4.'
                Last_SQL_Errno: 0
                Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Source_Server_Id: 67285976
```

Den Angeben im Feld `Last_IO_Errno` ist zu entnehmen, dass die Instance eine I/O-Fehlermeldung mit der Nummer 1236 erhalten hat. Dem Feld `Source_Log_File` ist zudem zu entnehmen, dass die betroffene Protokolldatei den Namen `mysql-bin-changelog.012345` aufweist und ihr Index folglich `12345` lautet. Zur Behebung des Fehlers können Sie dann `mysql.rds_next_source_log` mit dem folgenden Parameter aufrufen:

```
CALL mysql.rds_next_source_log(12345);
```

mysql.rds_remove_binlog_ssl_material

Entfernt das Zertifizierungsstellenzertifikat, das Clientzertifikat und den Clientschlüssel für SSL-Kommunikation und verschlüsselte Replikation. Diese Informationen werden mit importier mysql.rds_import_binlog_ssl_material.

Syntax

```
CALL mysql.rds_remove_binlog_ssl_material;
```

mysql.rds_reset_external_master (Aurora-MySQL-Version 2)

Rekonfiguriert eine Aurora-MySQL-DB-Instance, sodass sie keine Read Replica einer Instance von MySQL außerhalb von Amazon RDS ist.

> **Important**
>
> Um diese Prozedur auszuführen, muss `autocommit` aktiviert sein. Um dies zu aktivieren, setzen Sie den `autocommit`-Parameter auf 1. Weitere Informationen zum Ändern von Parametern finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.

Syntax

```
CALL mysql.rds_reset_external_master;
```

Nutzungshinweise

Die Prozedur `mysql.rds_reset_external_master` muss vom Hauptbenutzer ausgeführt werden. Diese Prozedur muss auf der MySQL-DB-Instance ausgeführt werden, die nicht mehr Lesereplikat einer außerhalb von Amazon RDS ausgeführten MySQL-Instance sein soll.

> **Note**
>
> Wir bieten diese gespeicherten Prozeduren hauptsächlich an, um die Replikation mit MySQL-Instances zu ermöglichen, die außerhalb von Amazon RDS ausgeführt werden. Wir empfehlen die Verwendung von Aurora Replicas, um die Replikation innerhalb eines DB-Clusters von Aurora MySQL zu verwalten, wenn dies möglich ist. Informationen zur Verwaltung der Replikation in DB-Clustern von Aurora MySQL finden Sie unter Verwendung von Aurora-Replicas.

Weitere Informationen zur Verwendung der Replikation für den Import von Daten aus einer außerhalb von Aurora MySQL ausgeführten Instance finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).

mysql.rds_reset_external_source (Aurora MySQL Version 3)

Rekonfiguriert eine Aurora-MySQL-DB-Instance, sodass sie keine Read Replica einer Instance von MySQL außerhalb von Amazon RDS ist.

> **Important**
>
> Um diese Prozedur auszuführen, muss `autocommit` aktiviert sein. Um dies zu aktivieren, setzen Sie den `autocommit`-Parameter auf 1. Weitere Informationen zum Ändern von Parametern finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.

Syntax

```
CALL mysql.rds_reset_external_source;
```

Nutzungshinweise

Die Prozedur `mysql.rds_reset_external_source` muss vom Hauptbenutzer ausgeführt werden. Diese Prozedur muss auf der MySQL-DB-Instance ausgeführt werden, die nicht mehr Lesereplikat einer außerhalb von Amazon RDS ausgeführten MySQL-Instance sein soll.

> **Note**
>
> Wir bieten diese gespeicherten Prozeduren hauptsächlich an, um die Replikation mit MySQL-Instances zu ermöglichen, die außerhalb von Amazon RDS ausgeführt werden. Wir empfehlen die Verwendung von Aurora Replicas, um die Replikation innerhalb eines DB-Clusters von Aurora MySQL zu verwalten, wenn dies möglich ist. Informationen zur Verwaltung der Replikation in DB-Clustern von Aurora MySQL finden Sie unter Verwendung von Aurora-Replicas.

mysql.rds_set_binlog_source_ssl (Aurora MySQL Version 3)

Aktiviert die SOURCE_SSL Verschlüsselung für die Binlog-Replikation. Weitere Informationen finden Sie unter CHANGE REPLICATION SOURCE TO statement in der MySQL-Dokumentation.

Syntax

```
CALL mysql.rds_set_binlog_source_ssl(mode);
```

Parameter

Modus

Ein Wert, der angibt, ob die SOURCE_SSL Verschlüsselung aktiviert ist:

- 0— Die SOURCE_SSL Verschlüsselung ist deaktiviert. Der Standardwert ist 0.
- 1— SOURCE_SSL Verschlüsselung ist aktiviert. Sie können die Verschlüsselung mit SSL oder TLS konfigurieren.

Nutzungshinweise

Dieses Verfahren wird für Aurora MySQL Version 3.06 und höher unterstützt.

mysql.rds_set_external_master (Aurora-MySQL-Version 2)

Konfiguriert eine Aurora-MySQL-Instance für die Verwendung als Read Replica einer außerhalb von Amazon RDS ausgeführten MySQL-Instance.

Das `mysql.rds_set_external_master`-Verfahren ist veraltet und wird in einer künftigen Version entfernt. Verwenden Sie stattdessen `mysql.rds_set_external_source`.

> **Important**
>
> Um diese Prozedur auszuführen, muss `autocommit` aktiviert sein. Um dies zu aktivieren, setzen Sie den `autocommit`-Parameter auf 1. Weitere Informationen zum Ändern von Parametern finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.

Syntax

```
CALL mysql.rds_set_external_master (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
);
```

Parameter

host_name

Der Hostname bzw. die IP-Adresse der außerhalb von Amazon RDS ausgeführten MySQL-Instance, die als Quelldatenbank-Instance festgelegt werden soll.

host_port

Der Port, der von der außerhalb von Amazon RDS ausgeführten MySQL-Instance verwendet wird, die als Quelldatenbank-Instance konfiguriert werden soll. Wenn Ihre Netzwerkkonfiguration die Replikation über Secure Shell (SSH)-Ports einschließt, welche die Portnummer konvertiert, geben Sie für diesen Parameter die von SSH offengelegte Portnummer an.

replication_user_name

Die ID eines Benutzers mit den Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` auf der MySQL-Instance, die extern zu Amazon RDS ausgeführt wird. Es wird empfohlen, ein Benutzerkonto bereitzustellen, das ausschließlich für die Replikation mit der externen Instance genutzt wird.

replication_user_password

Das zu dem in `replication_user_name` angegebenen User-ID gehörige Passwort.

mysql_binary_log_file_name

Der Name des Binärprotokolls auf der Quelldatenbank-Instance, die die Replikationsinformationen enthält.

mysql_binary_log_file_location

Die Position in der binären Protokolldatei `mysql_binary_log_file_name`, ab der bei der Replikation die Replikationsinformationen gelesen werden.

Sie können den Namen und den Speicherort der Binlog-Datei ermitteln, indem Sie `SHOW MASTER STATUS`auf der Quelldatenbankinstanz starten.

ssl_encryption

Ein Wert, der angibt, ob die SSL-Verschlüsselung (Secure Socket Layer) für die Replikationsverbindung verwendet wird. 1 = SSL-Verschlüsselung, 0 = keine Verschlüsselung. Der Standardwert ist 0.

> **Note**
>
> Die Option `MASTER_SSL_VERIFY_SERVER_CERT` wird nicht unterstützt. Diese Option ist auf 0 gesetzt, was bedeutet, dass die Verbindung verschlüsselt ist, aber die Zertifikate nicht überprüft werden.

Nutzungshinweise

Die Prozedur `mysql.rds_set_external_master` muss vom Hauptbenutzer ausgeführt werden. Diese Prozedur muss auf der MySQL-DB-Instance ausgeführt werden, die als Lesereplikat einer außerhalb von Amazon RDS ausgeführten MySQL-Instance konfiguriert werden soll.

Vor der Ausführung von `mysql.rds_set_external_master` müssen Sie zuerst die außerhalb von Amazon RDS ausgeführte MySQL-Instance für die Verwendung als Quelldatenbank-Instance konfigurieren. Um eine Verbindung zu der außerhalb von Amazon RDS ausgeführten MySQL-Instance herzustellen, müssen Sie Werte für `replication_user_name` und `replication_user_password` bereitstellen, die auf einen Replikationsbenutzer verweisen, der

über die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` für die externe MySQL-Instance verfügt.

So konfigurieren Sie eine externe Instance von MySQL als Quelldatenbank-Instance

1. Verbinden Sie sich mithilfe eines MySQL-Clients Ihrer Wahl mit der externen MySQL-Instance und erstellen Sie ein Benutzerkonto, das für die Replikation verwendet werden soll. Im Folgenden wird ein Beispiel gezeigt.

   MySQL 5.7

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

   MySQL 8.0

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED WITH mysql_native_password BY
    'password';
   ```

   > **Note**
   >
   > Geben Sie aus Sicherheitsgründen ein anderes Passwort als hier angegeben an.

2. Erteilen Sie innerhalb der externen MySQL-Instance Ihrem Replikationsbenutzer die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE`. Im folgenden Beispiel werden dem Benutzer 'repl_user' für Ihre Domäne die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` für alle Datenbanken erteilt.

   MySQL 5.7

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
    IDENTIFIED BY 'password';
   ```

   MySQL 8.0

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
   ```

Um die verschlüsselte Replikation zu verwenden, konfigurieren Sie die Quelldatenbank-Instance für die Verwendung von SSL-Verbindungen. Importieren Sie außerdem mit der Prozedur

mysql.rds_import_binlog_ssl_material das Zertifizierungsstellenzertifikat, das Clientzertifikat und den Clientschlüssel in die DB-Instance bzw. das DB-Cluster.

> **Note**
>
> Wir bieten diese gespeicherten Prozeduren hauptsächlich an, um die Replikation mit MySQL-Instances zu ermöglichen, die außerhalb von Amazon RDS ausgeführt werden. Wir empfehlen die Verwendung von Aurora Replicas, um die Replikation innerhalb eines DB-Clusters von Aurora MySQL zu verwalten, wenn dies möglich ist. Informationen zur Verwaltung der Replikation in DB-Clustern von Aurora MySQL finden Sie unter Verwendung von Aurora-Replicas.

Nachdem Sie `mysql.rds_set_external_master` aufgerufen haben, um eine Amazon RDS-DB-Instance als Lesereplikat zu konfigurieren, können Sie mysql.rds_start_replication für das Lesereplikat aufrufen, um die Replikation zu starten Zudem haben Sie die Möglichkeit, mit einem Aufruf von mysql.rds_reset_external_master (Aurora-MySQL-Version 2) die Lesereplikat-Konfiguration zu entfernen.

Beim Aufrufen von `mysql.rds_set_external_master` werden von Amazon RDS Uhrzeit, Benutzer und eine Aktion von `set master` in den Tabellen `mysql.rds_history` und `mysql.rds_replication_status` protokolliert.

Beispiele

Bei Ausführung innerhalb einer MySQL-DB-Instance konfiguriert das folgende Beispiel diese DB-Instance für die Verwendung als Lesereplikat einer außerhalb von Amazon RDS ausgeführten MySQL-Instance.

```
call mysql.rds_set_external_master(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'password',
  'mysql-bin-changelog.0777',
  120,
  0);
```

mysql.rds_set_external_master_with_auto_position (Aurora-MySQL-Version 2)

Konfiguriert eine primäre Instance von Aurora MySQL, um eine eingehende Replikation von einer externen MySQL-Instance zu akzeptieren. Diese Prozedur konfiguriert auch die auf globalen Transaktionskennungen (GTIDs) basierende Replikation.

Dieses Verfahren konfiguriert nicht die verzögerte Replikation, da Aurora MySQL die verzögerte Replikation nicht unterstützt.

Syntax

```
CALL mysql.rds_set_external_master_with_auto_position (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , ssl_encryption
);
```

Parameter

host_name

Der Hostname bzw. die IP-Adresse der außerhalb von Aurora ausgeführten MySQL-Instance, die als Replikationsmaster festgelegt werden soll.

host_port

Der Port, der von der außerhalb von Aurora ausgeführten MySQL-Instance verwendet wird, die als Replikations-Master konfiguriert werden soll. I Wenn Ihre Netzwerkkonfiguration die Replikation über Secure Shell (SSH)-Ports einschließt, welche die Portnummer konvertiert, geben Sie für diesen Parameter die von SSH offengelegte Portnummer an.

replication_user_name

Die ID eines Benutzers mit den Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` auf der MySQL-Instance, die extern zu Aurora ausgeführt wird. Es wird empfohlen, ein Benutzerkonto bereitzustellen, das ausschließlich für die Replikation mit der externen Instance genutzt wird.

replication_user_password

Das zu dem in `replication_user_name` angegebenen User-ID gehörige Passwort.

ssl_encryption

Diese Option ist derzeit nicht implementiert. Der Standardwert ist 0.

Nutzungshinweise

Sie rufen dieses gespeicherte Verfahren für einen Aurora MySQL-DB-Cluster auf, während Sie mit der primären Instance verbunden sind.

Die Prozedur `mysql.rds_set_external_master_with_auto_position` muss vom Hauptbenutzer ausgeführt werden. Der Master-Benutzer führt diese Verfahren auf der primären Instance eines Aurora MySQL-DB-Clusters durch, der als Replikationsziel fungiert. Dies kann das Replikationsziel einer externen MySQL-DB-Instance oder eines Aurora MySQL-DB-Clusters sein.

Diese Prozedur wird für Aurora-MySQL-Version 2 unterstützt. Verwenden Sie für Aurora-MySQL-Version 3 stattdessen das Verfahren mysql.rds_set_external_source_with_auto_position (Aurora MySQL Version 3).

Konfigurieren Sie die externe MySQL-DB-Instance vor der Ausführung von `mysql.rds_set_external_master_with_auto_position` als Replikationsmaster. Um sich mit der externen MySQL-Instance zu verbinden, geben Sie Werte für `replication_user_name` und `replication_user_password` an. Diese Werte müssen einen Replikationsbenutzer mit den Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` auf der externen MySQL-Instance angeben.

So konfigurieren Sie eine externe MySQL-Instance als Replikationsmaster

1. Verbinden Sie sich mithilfe eines MySQL-Clients Ihrer Wahl mit der externen MySQL-Instance und erstellen Sie ein Benutzerkonto, das für die Replikation verwendet werden soll. Im Folgenden wird ein Beispiel gezeigt.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
   ```

2. Erteilen Sie Ihrem Replikationsbenutzer auf der externen MySQL-Instance die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE`. Im folgenden Beispiel werden dem Benutzer `REPLICATION CLIENT` für Ihre Domäne die Berechtigungen `REPLICATION SLAVE` und `'repl_user'` für alle Datenbanken erteilt.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
   ```

```
IDENTIFIED BY 'SomePassW0rd'
```

Wenn Sie `mysql.rds_set_external_master_with_auto_position` aufrufen, zeichnet Amazon RDS bestimmte Informationen auf. Diese Informationen umfassen die Zeit, den Benutzer und eine Aktion von `"set master"` in den Tabellen `mysql.rds_history` und `mysql.rds_replication_status`.

Wenn Sie eine bestimmte GTID-basierte Transaktion überspringen möchten, von der Sie wissen, dass sie ein Problem verursacht, können Sie die gespeicherte Prozedur mysql.rds_skip_transaction_with_gtid verwenden. Weitere Informationen über das Arbeiten mit der GTID-basierten Replikation finden Sie unter Verwenden der GTID-basierten Replikation.

Beispiele

Wenn die folgende Beispielkonfiguration auf einer primären Instance von Aurora ausgeführt wird, wird der Aurora-Cluster so konfiguriert, dass er als Lesereplikat einer Instance von MySQL dient, die extern von Aurora ausgeführt wird.

```
call mysql.rds_set_external_master_with_auto_position(
  'Externaldb.some.com',
  3306,
  'repl_user'@'mydomain.com',
  'SomePassW0rd');
```

mysql.rds_set_external_source (Aurora MySQL Version 3)

Konfiguriert eine DB-Instance von Aurora MySQL für die Verwendung als Lesereplikat einer außerhalb von Amazon RDS ausgeführten MySQL-Instance.

> **Important**
>
> Um diese Prozedur auszuführen, muss `autocommit` aktiviert sein. Um dies zu aktivieren, setzen Sie den `autocommit`-Parameter auf 1. Weitere Informationen zum Ändern von Parametern finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.

Syntax

```
CALL mysql.rds_set_external_source (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
);
```

Parameter

host_name

Der Hostname bzw. die IP-Adresse der außerhalb von Amazon RDS ausgeführten MySQL-Instance, die als Quelldatenbank-Instance festgelegt werden soll.

host_port

Der Port, der von der außerhalb von Amazon RDS ausgeführten MySQL-Instance verwendet wird, die als Quelldatenbank-Instance konfiguriert werden soll. Wenn Ihre Netzwerkkonfiguration die Replikation über Secure Shell (SSH)-Ports einschließt, welche die Portnummer konvertiert, geben Sie für diesen Parameter die von SSH offengelegte Portnummer an.

replication_user_name

Die ID eines Benutzers mit den Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` auf der MySQL-Instance, die extern zu Amazon RDS ausgeführt wird. Es wird empfohlen, ein Benutzerkonto bereitzustellen, das ausschließlich für die Replikation mit der externen Instance genutzt wird.

replication_user_password

Das zu dem in `replication_user_name` angegebenen User-ID gehörige Passwort.

mysql_binary_log_file_name

Der Name des Binärprotokolls auf der Quelldatenbank-Instance, die die Replikationsinformationen enthält.

mysql_binary_log_file_location

Die Position in der binären Protokolldatei `mysql_binary_log_file_name`, ab der bei der Replikation die Replikationsinformationen gelesen werden.

Sie können den Namen und den Speicherort der Binlog-Datei ermitteln, indem Sie `SHOW MASTER STATUS`auf der Quelldatenbankinstanz starten.

`ssl_encryption`

Ein Wert, der angibt, ob die SSL-Verschlüsselung (Secure Socket Layer) für die Replikationsverbindung verwendet wird. 1 = SSL-Verschlüsselung, 0 = keine Verschlüsselung. Der Standardwert ist 0.

> **Note**
>
> Sie müssen ein benutzerdefiniertes SSL-Zertifikat importiert haben, mit dem mysql.rds_import_binlog_ssl_material Sie diese Option aktivieren können. Wenn Sie kein benutzerdefiniertes SSL-Zertifikat importiert haben, setzen Sie diesen Parameter auf 0 und verwenden Sie ihn, um SSL für die binäre Protokollreplikation mysql.rds_set_binlog_source_ssl (Aurora MySQL Version 3) zu aktivieren.
> Die Option `MASTER_SSL_VERIFY_SERVER_CERT` wird nicht unterstützt. Diese Option ist auf 0 gesetzt, was bedeutet, dass die Verbindung verschlüsselt ist, aber die Zertifikate nicht überprüft werden.

Nutzungshinweise

Die Prozedur `mysql.rds_set_external_source` muss vom Hauptbenutzer ausgeführt werden. Diese Prozedur muss auf der DB-Instance von Aurora MySQL ausgeführt werden, die als Lesereplikat einer außerhalb von Amazon RDS ausgeführten MySQL-Instance konfiguriert werden soll.

Vor der Ausführung von `mysql.rds_set_external_source` müssen Sie zuerst die außerhalb von Amazon RDS ausgeführte MySQL-Instance für die Verwendung als Quelldatenbank-Instance konfigurieren. Um eine Verbindung zu der außerhalb von Amazon RDS ausgeführten MySQL-Instance herzustellen, müssen Sie Werte für `replication_user_name` und `replication_user_password` bereitstellen, die auf einen Replikationsbenutzer verweisen, der über die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` für die externe MySQL-Instance verfügt.

So konfigurieren Sie eine externe Instance von MySQL als Quelldatenbank-Instance

1. Verbinden Sie sich mithilfe eines MySQL-Clients Ihrer Wahl mit der externen MySQL-Instance und erstellen Sie ein Benutzerkonto, das für die Replikation verwendet werden soll. Im Folgenden wird ein Beispiel gezeigt.

   MySQL 5.7

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

   MySQL 8.0

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED WITH mysql_native_password BY
    'password';
   ```

   > **Note**
   >
   > Geben Sie aus Sicherheitsgründen ein anderes Passwort als hier angegeben an.

2. Erteilen Sie innerhalb der externen MySQL-Instance Ihrem Replikationsbenutzer die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE`. Im folgenden Beispiel werden dem Benutzer 'repl_user' für Ihre Domäne die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` für alle Datenbanken erteilt.

   MySQL 5.7

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
    IDENTIFIED BY 'password';
   ```

   MySQL 8.0

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
   ```

Um die verschlüsselte Replikation zu verwenden, konfigurieren Sie die Quelldatenbank-Instance für die Verwendung von SSL-Verbindungen. Importieren Sie außerdem mit der Prozedur mysql.rds_import_binlog_ssl_material das Zertifizierungsstellenzertifikat, das Clientzertifikat und den Clientschlüssel in die DB-Instance bzw. den DB-Cluster.

> **Note**
>
> Wir bieten diese gespeicherten Prozeduren hauptsächlich an, um die Replikation mit MySQL-Instances zu ermöglichen, die außerhalb von Amazon RDS ausgeführt werden. Wir empfehlen die Verwendung von Aurora Replicas, um die Replikation innerhalb eines DB-Clusters von Aurora MySQL zu verwalten, wenn dies möglich ist. Informationen zur Verwaltung der Replikation in DB-Clustern von Aurora MySQL finden Sie unter Verwendung von Aurora-Replicas.

Nachdem Sie `mysql.rds_set_external_source` aufgerufen haben, um eine DB-Instance von Aurora MySQL als Lesereplikat zu konfigurieren, können Sie mysql.rds_start_replication für das Lesereplikat aufrufen, um die Replikation zu starten. Zudem haben Sie die Möglichkeit, mit einem Aufruf von mysql.rds_reset_external_source die Lesereplikat-Konfiguration zu entfernen.

Beim Aufrufen von `mysql.rds_set_external_source` werden von Amazon RDS Uhrzeit, Benutzer und eine Aktion von `set master` in den Tabellen `mysql.rds_history` und `mysql.rds_replication_status` protokolliert.

Beispiele

Bei Ausführung innerhalb einer DB-Instance von Aurora MySQL konfiguriert das folgende Beispiel diese DB-Instance für die Verwendung als Lesereplikat einer außerhalb von Amazon RDS ausgeführten MySQL-Instance.

```
call mysql.rds_set_external_source(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'password',
  'mysql-bin-changelog.0777',
  120,
  0);
```

mysql.rds_set_external_source_with_auto_position (Aurora MySQL Version 3)

Konfiguriert eine primäre Instance von Aurora MySQL, um eine eingehende Replikation von einer externen MySQL-Instance zu akzeptieren. Diese Prozedur konfiguriert auch die auf globalen Transaktionskennungen (GTIDs) basierende Replikation.

Syntax

```
CALL mysql.rds_set_external_source_with_auto_position (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , ssl_encryption
);
```

Parameter

host_name

Der Hostname bzw. die IP-Adresse der außerhalb von Aurora ausgeführten MySQL-Instance, die als Replikationsquelle festgelegt werden soll.

host_port

Der Port, der von der außerhalb von Aurora ausgeführten MySQL-Instance verwendet wird, die als Replikations-Quelle konfiguriert werden soll. Wenn Ihre Netzwerkkonfiguration die Replikation über Secure Shell (SSH)-Ports einschließt, welche die Portnummer konvertiert, geben Sie für diesen Parameter die von SSH offengelegte Portnummer an.

replication_user_name

Die ID eines Benutzers mit den Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` auf der MySQL-Instance, die extern zu Aurora ausgeführt wird. Es wird empfohlen, ein Benutzerkonto bereitzustellen, das ausschließlich für die Replikation mit der externen Instance genutzt wird.

replication_user_password

Das zu dem in `replication_user_name` angegebenen User-ID gehörige Passwort.

ssl_encryption

Diese Option ist derzeit nicht implementiert. Der Standardwert ist 0.

> **Note**
>
> Wird verwendetmysql.rds_set_binlog_source_ssl (Aurora MySQL Version 3), um SSL für die binäre Protokollreplikation zu aktivieren.

Nutzungshinweise

Sie rufen dieses gespeicherte Verfahren für einen Aurora MySQL-DB-Cluster auf, während Sie mit der primären Instance verbunden sind.

Der Administrator muss das `mysql.rds_set_external_source_with_auto_position`-Verfahren ausführen. Der Administrator-Benutzer führt diese Verfahren auf der primären Instance eines Aurora MySQL-DB-Clusters durch, der als Replikationsziel fungiert. Dies kann das Replikationsziel einer externen MySQL-DB-Instance oder eines Aurora MySQL-DB-Clusters sein.

Zurzeit wird diese Prozedur für Aurora MySQL Version 3 unterstützt. Dieses Verfahren konfiguriert nicht die verzögerte Replikation, da Aurora MySQL die verzögerte Replikation nicht unterstützt.

Konfigurieren Sie die externe MySQL-DB-Instance vor der Ausführung von `mysql.rds_set_external_source_with_auto_position` als Replikationsquelle. Um sich mit der externen MySQL-Instance zu verbinden, geben Sie Werte für `replication_user_name` und `replication_user_password` an. Diese Werte müssen einen Replikationsbenutzer mit den Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE` auf der externen MySQL-Instance angeben.

So konfigurieren Sie eine externe MySQL-Instance als Replikationsquelle

1. Verbinden Sie sich mithilfe eines MySQL-Clients Ihrer Wahl mit der externen MySQL-Instance und erstellen Sie ein Benutzerkonto, das für die Replikation verwendet werden soll. Im Folgenden wird ein Beispiel gezeigt.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
   ```

2. Erteilen Sie Ihrem Replikationsbenutzer auf der externen MySQL-Instance die Berechtigungen `REPLICATION CLIENT` und `REPLICATION SLAVE`. Im folgenden Beispiel werden dem Benutzer `REPLICATION CLIENT` für Ihre Domäne die Berechtigungen `REPLICATION SLAVE` und `'repl_user'` für alle Datenbanken erteilt.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
   IDENTIFIED BY 'SomePassW0rd'
   ```

Wenn Sie `mysql.rds_set_external_source_with_auto_position` aufrufen, zeichnet Amazon RDS bestimmte Informationen auf. Diese Informationen umfassen die Zeit, den

Benutzer und eine Aktion von `"set master"` in den Tabellen `mysql.rds_history` und `mysql.rds_replication_status`.

Wenn Sie eine bestimmte GTID-basierte Transaktion überspringen möchten, von der Sie wissen, dass sie ein Problem verursacht, können Sie die gespeicherte Prozedur mysql.rds_skip_transaction_with_gtid verwenden. Weitere Informationen über das Arbeiten mit der GTID-basierten Replikation finden Sie unter Verwenden der GTID-basierten Replikation.

Beispiele

Wenn die folgende Beispielkonfiguration auf einer primären Instance von Aurora ausgeführt wird, wird der Aurora-Cluster so konfiguriert, dass er als Lesereplikat einer Instance von MySQL dient, die extern von Aurora ausgeführt wird.

```
call mysql.rds_set_external_source_with_auto_position(
  'Externaldb.some.com',
  3306,
  'repl_user'@'mydomain.com',
  'SomePassW0rd');
```

mysql.rds_set_master_auto_position (Aurora-MySQL-Version 2)

Legt den Replikationsmodus als auf Binärprotokolldateipositionen oder globalen Transaktionskennungen (GTIDs) basierend fest.

Syntax

```
CALL mysql.rds_set_master_auto_position (
auto_position_mode
);
```

Parameter

auto_position_mode

Ein Wert, der angibt, ob die Replikation auf Basis der Protokolldateiposition oder der GTID verwendet werden soll:

- `0` – Verwendung der auf der Binärprotokolldateiposition basierenden Replikationsmethode. Der Standardwert ist `0`.
- 1 – Verwendung der auf GTID basierenden Replikationsmethode.

Nutzungshinweise

Die Prozedur `mysql.rds_set_master_auto_position` muss vom Hauptbenutzer ausgeführt werden.

Diese Prozedur wird für Aurora-MySQL-Version 2 unterstützt.

mysql.rds_set_read_only (Aurora MySQL Version 3)

Schaltet `read_only` den Modus global für die DB-Instance ein oder aus.

Syntax

```
CALL mysql.rds_set_read_only(mode);
```

Parameter

`Modus`

Ein Wert, der angibt, ob der `read_only` Modus für die DB-Instance global aktiviert oder deaktiviert ist:

- `0`—`OFF`. Die Standardeinstellung ist`0`.
- `1` – `ON`

Nutzungshinweise

Die `mysql.rds_set_read_only` gespeicherte Prozedur ändert nur den `read_only` Parameter. Der `innodb_read_only` Parameter kann auf Reader-DB-Instances nicht geändert werden.

Die `read_only` Parameteränderung bleibt beim Neustart nicht bestehen. Um dauerhafte Änderungen vorzunehmen`read_only`, müssen Sie den `read_only` DB-Cluster-Parameter verwenden.

Dieses Verfahren wird für Aurora MySQL Version 3.06 und höher unterstützt.

mysql.rds_set_session_binlog_format (Aurora-MySQL-Version 2)

Legt das binäre Protokollformat für die aktuelle Sitzung fest.

Syntax

```
CALL mysql.rds_set_session_binlog_format(format);
```

Parameter

format

Ein Wert, der das binäre Protokollformat für die aktuelle Sitzung angibt:

- `STATEMENT` – Die Replikationsquelle schreibt Ereignisse auf der Grundlage von SQL-Anweisungen in das Binärprotokoll.
- `ROW` – Die Replikationsquelle schreibt Ereignisse in das Binärprotokoll, die auf Änderungen an einzelnen Tabellenzeilen hinweisen.
- `MIXED` – Die Protokollierung basiert in der Regel auf SQL-Anweisungen, wechselt jedoch unter bestimmten Bedingungen zu Zeilen. Weitere Informationen finden Sie unter Mixed Binary Logging Format (Gemischtes Binärprotokollformat) in der MySQL-Dokumentation.

Nutzungshinweise

Sie rufen dieses gespeicherte Verfahren für einen Aurora MySQL-DB-Cluster auf, während Sie mit der primären Instance verbunden sind.

Wenn Sie diese gespeicherte Prozedur verwenden möchten, müssen Sie die Binärprotokollierung für die aktuelle Sitzung konfiguriert haben.

Für Aurora wird dieses Verfahren für Aurora-MySQL-Version 2.12 und höher und MySQL-5.7-kompatible Versionen unterstützt.

mysql.rds_set_source_auto_position (Aurora MySQL Version 3)

Legt den Replikationsmodus als auf Binärprotokolldateipositionen oder globalen Transaktionskennungen (GTIDs) basierend fest.

Syntax

```
CALL mysql.rds_set_source_auto_position (auto_position_mode);
```

Parameter

auto_position_mode

Ein Wert, der angibt, ob die Replikation auf Basis der Protokolldateiposition oder der GTID verwendet werden soll:

- `0` – Verwendung der auf der Binärprotokolldateiposition basierenden Replikationsmethode. Der Standardwert ist `0`.
- 1 – Verwendung der auf GTID basierenden Replikationsmethode.

Nutzungshinweise

Sie rufen dieses gespeicherte Verfahren für einen Aurora MySQL-DB-Cluster auf, während Sie mit der primären Instance verbunden sind.

Der Administrator muss das `mysql.rds_set_source_auto_position`-Verfahren ausführen.

mysql.rds_skip_transaction_with_gtid (Aurora-MySQL-Version 2 und 3)

Überspringt die Replikation einer Transaktion mit der angegebenen globalen Transaktionskennung (GTID) auf einer primären Instance von Aurora.

Sie können dieses Verfahren für die Notfallwiederherstellung verwenden, wenn eine bestimmte GTID-Transaktion bekanntermaßen ein Problem verursacht. Verwenden Sie diese gespeicherte Prozedur, um die problematische Transaktion zu überspringen. Problematisch sind beispielsweise Transaktionen, die die Replikation deaktivieren, wichtige Daten löschen oder dafür sorgen, dass die DB-Instance nicht mehr verfügbar ist.

Syntax

```
CALL mysql.rds_skip_transaction_with_gtid (
gtid_to_skip
);
```

Parameter

`gtid_to_skip`

Die GTID der zu überspringenden Replikationstransaktion.

Nutzungshinweise

Die Prozedur `mysql.rds_skip_transaction_with_gtid` muss vom Hauptbenutzer ausgeführt werden.

Diese Prozedur wird für Aurora-MySQL-Version 2 und 3 unterstützt.

Beispiele

Im folgenden Beispiel wird die Replikation der Transaktion mit der GTID übersprunge `3E11FA47-71CA-11E1-9E33-C80AA9429562:23`.

```
CALL mysql.rds_skip_transaction_with_gtid('3E11FA47-71CA-11E1-9E33-C80AA9429562:23');
```

mysql.rds_skip_repl_error

Ignoriert und löscht einen Replikationsfehler in einem MySQL-DB-Lesereplikat.

Syntax

```
CALL mysql.rds_skip_repl_error;
```

Nutzungshinweise

Der Hauptbenutzer muss die Prozedur `mysql.rds_skip_repl_error` auf einem Lesereplikat ausführen. Weitere Informationen zu dieser Prozedur finden Sie unter Überspringen des aktuellen Replikationsfehlers.

Führen Sie den MySQL-Befehl `SHOW REPLICA STATUS\G` aus, um festzustellen, ob Fehler aufgetreten sind. Wenn ein Replikationsfehler nicht als kritisch eingestuft, ist, können Sie `mysql.rds_skip_repl_error` ausführen, um den Fehler zu überspringen. Wenn mehrere Fehler aufgetreten sind, löscht `mysql.rds_skip_repl_error` den ersten Fehler und weist darauf hin, dass weitere Fehlermeldungen anhängig sind. In diesem Fall können Sie mithilfe von `SHOW REPLICA STATUS\G` die angemessene Vorgehensweise bei der Handhabung des nächsten Fehlers ermitteln. Informationen zu den zurückgegebenen Werten finden Sie unter SHOW REPLICA STATUS-Anweisung in der MySQL-Dokumentation.

> **Note**
>
> Frühere Versionen von MySQL verwenden `SHOW SLAVE STATUS` anstelle von `SHOW REPLICA STATUS`. Wenn Sie vor 8.0.23 eine MySQL-Version verwenden, verwenden Si `SHOW SLAVE STATUS`.

Weitere Informationen zur Handhabung von Replikationsfehlern mit Aurora MySQL finden Sie unter Diagnose und Lösung eines Fehlers bei einer MySQL Read Replica.

Fehler „Replication stopped (Replikation gestoppt)“

Wenn Sie die Prozedur `mysql.rds_skip_repl_error` aufrufen, wird möglicherweise eine Fehlermeldung angezeigt, die besagt, dass das Replikat ausgefallen oder deaktiviert ist.

Diese Fehlermeldung wird angezeigt, wenn Sie die Prozedur auf der primären Instance statt auf dem Lesereplikat ausführen. Sie müssen diese Prozedur auf dem Lesereplikat ausführen, damit sie funktioniert.

Diese Fehlermeldung wird möglicherweise auch angezeigt, wenn Sie die Prozedur zwar auf dem Lesereplikat ausführen, die Replikation jedoch nicht neu gestartet werden kann.

Wenn Sie eine größere Anzahl von Fehlern überspringen müssen, kann die Dauer der Replikationsverzögerung den standardmäßigen Aufbewahrungszeitraum für binäre Protokolldateien (binlog) überschreiten. In diesem Fall kann es zu einem schwerwiegenden Fehler kommen, weil Binärprotokolldateien bereinigt werden, bevor ihr Inhalt in das Lesereplikat repliziert wurde. Diese Bereinigung führt zur Beendigung der Replikation, und Sie können den Befehl `mysql.rds_skip_repl_error` nicht mehr aufrufen, um Replikationsfehler zu überspringen und zu ignorieren.

Sie können dieses Problem verringern, indem Sie die Anzahl der Stunden erhöhen, die die Binärprotokolldateien auf Ihrer Quelldatenbankinstance aufbewahrt werden. Nachdem Sie die Aufbewahrungsdauer für binäre Protokolldateien verlängert haben, können Sie die Replikation neu starten und nach Bedarf den Befehl `mysql.rds_skip_repl_error` aufrufen.

Verwenden Sie zur Festlegung der Aufbewahrungszeit für Binärprotokolldateien die Prozedur mysql.rds_set_configuration und legen Sie einen Konfigurationsparameter für `'binlog retention hours'` zusammen mit der Stundenanzahl für die Aufbewahrung der Binärprotokolldateien im DB-Cluster fest. Beim folgenden Beispiel wird die Aufbewahrungszeit für binäre Protokolle auf 48 Stunden festgelegt.

```
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

mysql.rds_start_replication

Startet die Replikation von einer/einem Aurora-MySQL-DB-Cluster.

> **Note**
>
> Sie können die gespeicherte Prozedur mysql.rds_start_replication_until (Aurora-MySQL-Version 3) oder mysql.rds_start_replication_until_gtid (Aurora-MySQL-Version 3) verwenden, um die Replikation von einer Aurora-MySQL-DB-Instance zu initiieren und die Replikation an der angegebenen Position der Binärprotokolldatei zu stoppen.

Syntax

```
CALL mysql.rds_start_replication;
```

Nutzungshinweise

Die Prozedur `mysql.rds_start_replication` muss vom Hauptbenutzer ausgeführt werden.

Zum Import von Daten aus einer außerhalb von Amazon RDS ausgeführten MySQL-Instance, rufen Sie `mysql.rds_start_replication` für das Lesereplikat auf, um den Replikationsvorgang zu starten, nachdem Sie `mysql.rds_set_external_master`oder `mysql.rds_set_external_source` aufgerufen haben, um die Replikation zu konfigurieren. Weitere Informationen finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).

Zum Export von Daten in eine außerhalb von Amazon RDS ausgeführte MySQL-Instance rufen Sie `mysql.rds_start_replication` und `mysql.rds_stop_replication` für das Lesereplikat auf, um Replikationsaktionen wie das Bereinigen von Binärprotokollen zu steuern. Weitere Informationen finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).

Darüber hinaus können Sie `mysql.rds_start_replication` für das Lesereplikat aufrufen, um einen zuvor durch einen Aufruf von `mysql.rds_stop_replication` gestoppten Replikationsprozess wieder zu starten. Weitere Informationen finden Sie unter Fehler „Replication stopped (Replikation gestoppt)“.

mysql.rds_start_replication_until (Aurora-MySQL-Version 3)

Initiiert die Replikation von einem Aurora-MySQL-DB-Cluster und stoppt die Replikation an der angegebenen Position in der Binärprotokolldatei.

Syntax

```
CALL mysql.rds_start_replication_until (
replication_log_file
  , replication_stop_point
);
```

Parameter

replication_log_file

Der Name des Binärprotokolls auf der Quelldatenbank-Instance, die die Replikationsinformationen enthält.

replication_stop_point

Die Position im `replication_log_file`-Binärprotokoll, an der die Replikation stoppt.

Nutzungshinweise

Die Prozedur `mysql.rds_start_replication_until` muss vom Hauptbenutzer ausgeführt werden.

Diese Prozedur wird für Aurora-MySQL-Version 3.04 und höher unterstützt.

Die `mysql.rds_start_replication_until` gespeicherte Prozedur wird für die verwaltete Replikation nicht unterstützt. Sie umfasst Folgendes:

- Replizieren von Amazon-Aurora-MySQL-DB-Clustern über AWS-Regionen hinweg
- Migrieren von Daten aus einer RDS-für-MySQL-DB-Instance zu einem Amazon-Aurora-MySQL-DB-Cluster mittels einer Aurora Read Replica (Lesereplikat)

Der für den Parameter `replication_log_file` angegebene Dateiname muss mit dem Binlogdateinamen der Quelldatenbankinstance übereinstimmen.

Wenn der Parameter `replication_stop_point`eine Stoppposition angibt, die in der Vergangenheit liegt, wird die Replikation sofort gestoppt.

Beispiele

Das folgende Beispiel initiiert die Replikation und repliziert die Änderungen, bis die Position `120` in der Binärprotokolldatei `mysql-bin-changelog.000777` erreicht wird.

```
call mysql.rds_start_replication_until(
  'mysql-bin-changelog.000777',
  120);
```

mysql.rds_start_replication_until_gtid (Aurora-MySQL-Version 3)

Initiiert die Replikation von einer/einem Aurora-MySQL-DB-Cluster und stoppt die Replikation unmittelbar nach der angegebenen globalen Transaktionskennung (GTID).

Syntax

```
CALL mysql.rds_start_replication_until_gtid(gtid);
```

Parameter

`gtid`

Die GTID, nach der die Replikation stoppen soll.

Nutzungshinweise

Die Prozedur `mysql.rds_start_replication_until_gtid` muss vom Hauptbenutzer ausgeführt werden.

Diese Prozedur wird für Aurora-MySQL-Version 3.04 und höher unterstützt.

Die `mysql.rds_start_replication_until_gtid` gespeicherte Prozedur wird für die verwaltete Replikation nicht unterstützt. Dazu gehören:

- Replizieren von Amazon-Aurora-MySQL-DB-Clustern über AWS-Regionen hinweg
- Migrieren von Daten aus einer RDS-für-MySQL-DB-Instance zu einem Amazon-Aurora-MySQL-DB-Cluster mittels einer Aurora Read Replica (Lesereplikat)

Wenn der Parameter `gtid` eine Transaktion angibt, die bereits von dem Replikat ausgeführt wurde, wird die Replikation sofort gestoppt.

Beispiele

Das folgende Beispiel initiiert die Replikation und repliziert die Änderungen, bis die GTID erreicht wir `3E11FA47-71CA-11E1-9E33-C80AA9429562:23`.

```
call mysql.rds_start_replication_until_gtid('3E11FA47-71CA-11E1-9E33-C80AA9429562:23');
```

mysql.rds_stop_replication

Stoppt die Replikation von einer MySQL-DB-Instance.

Syntax

```
CALL mysql.rds_stop_replication;
```

Nutzungshinweise

Die Prozedur `mysql.rds_stop_replication` muss vom Hauptbenutzer ausgeführt werden.

Wenn Sie die Replikation für den Import von Daten aus einer außerhalb von Amazon RDS ausgeführten MySQL-Instance konfigurieren, stoppen Sie mit einem Aufruf von `mysql.rds_stop_replication` für das Lesereplikat den Replikationsvorgang nach Abschluss des Imports. Weitere Informationen finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).

Wenn Sie die Replikation für den Export von Daten in eine außerhalb von Amazon RDS ausgeführte MySQL-Instance konfigurieren, rufen Sie `mysql.rds_start_replication` und `mysql.rds_stop_replication` für das Lesereplikat auf, um Replikationsaktionen wie das Bereinigen von Binärprotokollen zu steuern. Weitere Informationen finden Sie unter Replizieren zwischen Aurora und MySQL oder zwischen Aurora und einem anderen Aurora-DB-Cluster (binäre Protokollreplikation).

Die `mysql.rds_stop_replication` gespeicherte Prozedur wird für die verwaltete Replikation nicht unterstützt. Dazu gehören:

- Replizieren von Amazon-Aurora-MySQL-DB-Clustern über AWS-Regionen hinweg
- Migrieren von Daten aus einer RDS-für-MySQL-DB-Instance zu einem Amazon-Aurora-MySQL-DB-Cluster mittels einer Aurora Read Replica (Lesereplikat)

Aurora-MySQL-spezifische information_schema-Tabellen

Aurora MySQL verfügt über bestimmte `information_schema`-Tabellen, die für Aurora spezifisch sind.

information_schema.aurora_global_db_instance_status

Die Tabelle `information_schema.aurora_global_db_instance_status` enthält Informationen über den Status aller DB-Instances in den primären und sekundären DB-Clustern einer globalen Datenbank. Die Spalten, die Sie verwenden können, sind in der folgenden Tabelle aufgeführt. Die übrigen Spalten sind nur für den internen Gebrauch von Aurora bestimmt.

> **Note**
>
> Diese Informationsschematabelle ist nur mit globalen Aurora-MySQL-Datenbanken ab Version 3.04.0 verfügbar.

Spalte	Datentyp	Beschreibung
SERVER_ID	varchar(100)	Die ID der DB-Instance.
SESSION_ID	varchar(100)	Eindeutiger Bezeichner für die aktuelle Sitzung. Der Wert `MASTER_SESSION_ID` bezeichnet die (primäre) Writer-DB-Instance.
AWS_REGION	varchar(100)	Die AWS-Region, in der diese globale DB-Instance ausgeführt wird. Eine Liste der Regionen finden Sie unter Verfügbarkeit in Regionen.
DURABLE_LSN	bigint unsigned	Die Log-Sequenznummer (LSN), die dauerhaft gespeichert wurde. Eine Log-Sequenznummer (LSN) ist

Spalte	Datentyp	Beschreibung
		eine eindeutige fortlaufende Nummer, die einen Datensatz im Datenbank-Transakt ionsprotokoll identifiziert. LSNs werden so angeordnet, dass eine größere LSN eine spätere Transaktion darstellt.
HIGHEST_LSN_RCVD	bigint unsigned	Die höchste LSN, die die DB-Instance von der Writer-DB-Instance empfangen hat.
OLDEST_READ_VIEW_T RX_ID	bigint unsigned	Die ID der ältesten Transakti on, zu der die Writer-DB-Instance Daten löschen kann.
OLDEST_READ_VIEW_LSN	bigint unsigned	Die älteste LSN, die von der DB-Instance zum Lesen aus dem Speicher verwendet wird.
VISIBILITY_LAG_IN_MSEC	float(10,0) unsigned	Für Reader im primären DB-Cluster, wie weit diese DB-Instance der Writer-DB -Instance in Millisekunden hinterherhinkt. Für Reader in einem sekundären DB-Cluste r, wie weit diese DB-Instance dem sekundären Volume in Millisekunden hinterherhinkt.

information_schema.aurora_global_db_status

Die Tabelle `information_schema.aurora_global_db_status` enthält Informationen über verschiedene Aspekte der globalen Aurora-Datenbankverzögerung an, insbesondere die Verzögerung des zugrunde liegenden Aurora-Speichers (sogenannte Haltbarkeitsverzögerung) und die Verzögerung zwischen dem Recovery Point Objective (RPO). Die Spalten, die Sie verwenden

können, sind in der folgenden Tabelle aufgeführt. Die übrigen Spalten sind nur für den internen Gebrauch von Aurora bestimmt.

> **Note**
>
> Diese Informationsschematabelle ist nur mit globalen Aurora-MySQL-Datenbanken ab Version 3.04.0 verfügbar.

Spalte	Datentyp	Beschreibung
AWS_REGION	varchar(100)	Die AWS-Region, in der diese globale DB-Instance ausgeführt wird. Eine Liste der Regionen finden Sie unter Verfügbarkeit in Regionen.
HIGHEST_LSN_WRITTEN	bigint unsigned	Die höchste Log-Sequenznummer (LSN), die derzeit auf diesem DB-Cluster vorhanden ist. Eine Log-Sequenznummer (LSN) ist eine eindeutige fortlaufende Nummer, die einen Datensatz im Datenbank-Transaktionsprotokoll identifiziert. LSNs werden so angeordnet, dass eine größere LSN eine spätere Transaktion darstellt.
DURABILITY_LAG_IN_MILLISECONDS	float(10,0) unsigned	Die Differenz der Zeitstempelwerte zwischen `HIGHEST_LSN_WRITTEN` in einem sekundären DB-Cluster und `HIGHEST_LSN_WRITTEN` im primären DB-Cluster. Der Wert ist immer 0 im

Spalte	Datentyp	Beschreibung
		primären DB-Cluster der globalen Aurora-Datenbank.
RPO_LAG_IN_MILLISECONDS	float(10,0) unsigned	Die Recovery Point Objective (RPO)-Verzögerung. Die RPO-Verzögerung ist die Zeit, die benötigt wird, bis die letzte Benutzertransaktion COMMIT auf einem sekundären DB-Cluster gespeichert wird, nachdem sie auf dem primären DB-Cluster einer globalen Aurora-Datenbank abgelegt wurde. Der Wert ist immer 0 im primären DB-Cluster der globalen Aurora-Datenbank. Einfach ausgedrückt berechnet diese Metrik das Recovery Point Objective für jeden DB-Cluster voon Aurora MySQL in der globalen Aurora-Datenbank, d. h., wie viele Daten bei einem Ausfall verloren gehen könnten. Wie die Verzögerung wird auch RPO zeitlich gemessen.

Spalte	Datentyp	Beschreibung
LAST_LAG_CALCULATION_TIMESTAMP	datetime	Der Zeitstempel, der angibt, wann die Werte für `DURABILITY_LAG_IN_MILLISECONDS` und `RPO_LAG_IN_MILLISECONDS` zuletzt berechnet wurden. Ein Zeitwert wie `1970-01-01 00:00:00+00` bedeutet, dass dies der primäre DB-Cluster ist.
OLDEST_READ_VIEW_TRX_ID	bigint unsigned	Die ID der ältesten Transaktion, zu der die Writer-DB-Instance Daten löschen kann.

information_schema.replica_host_status

Die Tabelle `information_schema.replica_host_status` enthält Replikationsinformationen. Die Spalten, die Sie verwenden können, sind in der folgenden Tabelle aufgeführt. Die übrigen Spalten sind nur für den internen Gebrauch von Aurora bestimmt.

Spalte	Datentyp	Beschreibung
CPU	double	Die prozentuale CPU-Auslastung des Replikat-Hosts.
IS_CURRENT	tinyint	Gibt an, ob das Replikat aktuell ist.
LAST_UPDATE_TIMESTAMP	datetime(6)	Zeitpunkt, an dem die letzte Aktualisierung stattfand. Wird verwendet, um festzustellen, ob ein Datensatz veraltet ist.

Spalte	Datentyp	Beschreibung
REPLICA_LAG_IN_MILLISECONDS	double	Die Replikatverzögerung in Millisekunden.
SERVER_ID	varchar(100)	Die ID des Datenbankservers.
SESSION_ID	varchar(100)	Die ID der Datenbanksitzung. Wird verwendet, um festzustellen, ob es sich bei einer DB-Instance um eine Writer- oder Reader-Instance handelt.

> **Note**
>
> Wenn eine Replikat-Instance in Verzug gerät, sind die aus ihrer `information_schema.replica_host_status`-Tabelle abgefragten Informationen möglicherweise veraltet. In diesem Fall empfehlen wir, stattdessen eine Abfrage von der Writer-Instance aus durchzuführen.
> Die Tabelle `mysql.ro_replica_status` enthält zwar ähnliche Informationen, wir raten Ihnen jedoch davon ab, diese zu verwenden.

information_schema.aurora_forwarding_processlist

Die Tabelle `information_schema.aurora_forwarding_processlist` enthält Informationen über Prozesse, die an der Schreibweiterleitung beteiligt sind.

Der Inhalt dieser Tabelle ist nur auf der Writer-DB-Instance für einen DB-Cluster sichtbar, bei dem die globale oder clusterinterne Schreibweiterleitung aktiviert ist. Auf Reader-DB-Instances wird ein leerer Ergebnissatz zurückgegeben.

Feld	Datentyp	Beschreibung
ID	bigint	Der Bezeichner der Verbindung auf der Writer-DB-Instance. Dieser Bezeichner ist derselbe Wert, der in der Spalte `Id` der `SHOW PROCESSLIST` -Anweisung angezeigt wird,

Feld	Datentyp	Beschreibung
		und wird von der Funktion `CONNECTION_ID()` innerhalb des Threads zurückgegeben.
USER	varchar(32)	Der MySQL-Benutzer, der die Anweisung erstellt hat.
HOST	varchar(255)	Der MySQL-Client, der die Anweisung erstellt hat. Für weitergeleitete Anweisungen zeigt dieses Feld die Hostadresse des Anwendungsclients an, der die Verbindung auf der weiterleitenden Reader-DB-Instance hergestellt hat.
DB	varchar(64)	Die Standarddatenbank für den Thread.
COMMAND	varchar(16)	Die Art des Befehls, den der Thread im Namen des Clients ausführt, oder `Sleep`, wenn die Sitzung inaktiv ist. Eine Beschreibung der Thread-Befehle finden Sie unter Thread Command Values (Thread-Befehlswerte) in der MySQL-Dokumentation .
TIME	int	Die Zeit in Sekunden, in der sich der Thread in seinem aktuellen Status befand.
STATE	varchar(64)	Eine Aktion, ein Ereignis oder ein Status, der angibt, welche Aktionen der Thread ausführt. Eine Beschreibung der Statuswerte finden Sie unter General Thread Status (Allgemeine Thread-Status) in der MySQL-Dokumentation.
INFO	longtext	Die Anweisung, die der Thread ausführt, oder `NULL`, wenn er keine Anweisung ausführt. Bei der Anweisung kann es sich um die an den Server gesendete oder um eine innerste Anweisung handeln, wenn die Anweisung andere Anweisungen ausführt.
IS_FORWARDED	bigint	Gibt an, ob der Thread von einer Reader-DB-Instance weitergeleitet wird.

Feld	Datentyp	Beschreibung
REPLICA_SESSION_ID	bigint	Die Verbindungs-ID in der Aurora Replica. Dieser Bezeichner ist derselbe Wert, der in der Spalte `Id` der `SHOW PROCESSLIST` -Anweisung auf der weiterleitenden Reader-DB-Instance von Aurora angezeigt wird.
REPLICA_INSTANCE_IDENTIFIER	varchar(64)	Die ID der DB-Instance des weiterleitenden Threads.
REPLICA_CLUSTER_NAME	varchar(64)	Die ID des DB-Clusters des weiterleitenden Threads. Für die In-Cluster-Schreibweiterleitung ist diese ID derselbe DB-Cluster wie die Writer-DB-Instance.
REPLICA_REGION	varchar(64)	Die AWS-Region, aus der der weiterleitende Thread stammt. Für die In-Cluster-Schreibweiterleitung ist diese Region dieselbe AWS-Region wie die Writer-DB-Instance.

Datenbank-Engine-Updates für Amazon Aurora MySQL

Amazon Aurora veröffentlicht regelmäßig Updates. Updates werden auf Aurora-DB-Cluster während des Wartungszeitraums angewendet. Zu welchem Zeitpunkt Updates angewandt werden, hängt von den Einstellungen für die Region und den Wartungszeitraum für das DB-Cluster sowie vom Typ des Updates ab.

Amazon Aurora Aurora-Versionen werden im Laufe mehrerer Tage für alle AWS Regionen verfügbar gemacht. Einige Regionen zeigen möglicherweise vorübergehend eine Engine-Version an, die in einer anderen Region noch nicht verfügbar ist.

Updates werden auf alle Instances in einem DB-Cluster gleichzeitig angewendet. Ein Update erfordert einen Neustart einer Datenbank auf allen Instances in einem DB-Cluster. Daher dauert es 20 bis 30 Sekunden, bis Sie wieder mit der Verwendung Ihrer DB-Cluster fortfahren können. Sie können die Einstellungen für den Wartungszeitraum in der anzeigen und ändern AWS Management Console.

Weitere Informationen zu den Aurora-MySQL-Versionen, die von Amazon Aurora unterstützt werden, finden Sie in den Versionshinweisen für Aurora MySQL.

Im Folgenden erfahren Sie, wie Sie die richtige Aurora MySQL-Version für Ihren Cluster auswählen, wie Sie die Version beim Erstellen oder Aktualisieren eines Clusters angeben, und wie Sie mit minimaler Unterbrechung einen Cluster von einer Version auf eine andere aktualisieren können.

Themen

Aurora MySQL-Versionsnummern und Sonderversionen

Obwohl Aurora MySQL-kompatible Edition mit den MySQL-Datenbank-Engines kompatibel ist, enthält Aurora MySQL Funktionen und Fehlerbehebungen, die spezifisch für bestimmte Aurora MySQL-

Versionen sind. Anwendungsentwickler können die Aurora MySQL-Version in ihren Anwendungen mithilfe von SQL überprüfen. Datenbankadministratoren können beim Erstellen oder Aktualisieren von Aurora MySQL-DB-Clustern und DB-Instances Aurora MySQL-Versionen überprüfen und angeben.

Themen

Überprüfen oder Spezifizieren von Aurora MySQL-Engine-Versionen über AWS

Wenn Sie Verwaltungsaufgaben mit der AWS Management Console, oder RDS-API ausführen AWS CLI, geben Sie die Aurora MySQL-Version in einem beschreibenden alphanumerischen Format an.

Seit Aurora-MySQL-Version 2 wird für Aurora-Engine-Versionen die folgende Syntax verwendet.

```
mysql-major-version.mysql_aurora.aurora-mysql-version
```

Der *mysql-major-version*--Anteil ist `5.7` oder `8.0`. Dieser Wert stellt die Version des Clientprotokolls und die allgemeine Ebene der MySQL-Funktionsunterstützung für die entsprechende Aurora MySQL-Version dar.

aurora-mysql-version ist ein gepunkteter Wert mit drei Teilen: der Aurora MySQL-Hauptversion, der Aurora MySQL-Nebenversion und der Patch-Ebene. Die Hauptversion ist `2` oder `3`. Diese Werte stellen Aurora MySQL dar, das mit MySQL 5.7 bzw. 8.0 kompatibel ist. Die Unterversion stellt die Funktionsversion innerhalb der 2.x- oder 3.x-Serie dar. Die Patch-Ebene beginnt bei `0` für jede Nebenversion und stellt die Reihe der nachfolgenden Fehlerbehebungen dar, die für die Nebenversion gelten. Gelegentlich wird eine neue Funktion in eine Nebenversion integriert, aber nicht sofort sichtbar gemacht. In diesen Fällen wird die Funktion einer Optimierung unterzogen und in einem späteren Patch-Stufe veröffentlicht.

Alle 2.x Aurora MySQL Engine-Versionen sind vollkommen kompatibel mit dem Community MySQL 5.7.12. Alle Versionen der Aurora-MySQL-Engine 3.x sind mit MySQL ab Version 8.0.23 drahtkompatibel. Sie können auf Versionshinweise einer bestimmten 3.x-Version zurückgreifen, um die entsprechende MySQL-kompatible Version zu finden.

Zum Beispiel sind die Engine-Versionen für Aurora MySQL 3.02.0 und 2.11.2 die folgenden.

```
8.0.mysql_aurora.3.02.0
5.7.mysql_aurora.2.11.2
```

> **Note**
>
> Es gibt keine one-to-one Entsprechung zwischen Community-MySQL-Versionen und den Aurora MySQL 2.x-Versionen. Für Aurora-MySQL-Version 3 gibt es ein direkteres Mapping. Um zu überprüfen, welche Fehlerbehebungen und neuen Funktionen in einer bestimmten Aurora-MySQL-Version enthalten sind, lesen Sie Aktualisierungen der Datenbank-Engine für Amazon-Aurora-MySQL-Version 3 und Aktualisierungen der Datenbank-Engine für Amazon-Aurora-MySQL-Version 2 in den Versionshinweisen für Aurora MySQL. Eine chronologische Liste der neuen Funktionen und Releases finden Sie unter Dokumentverlauf. Informationen zum Überprüfen der Mindestversion, die für eine sicherheitsbezogene Fehlerbehebung erforderlich ist, finden Sie unter In Aurora MySQL behobene Sicherheitsschwachstellen in den Versionshinweisen für Aurora MySQL.

In einigen AWS CLI Befehlen und RDS-API-Vorgängen geben Sie die Version der Aurora MySQL-Engine an. Beispielsweise geben Sie die `--engine-version` Option an, wenn Sie die AWS CLI Befehle create-db-clusterund ausführen modify-db-cluster. Sie geben den Parameter `EngineVersion` an, wenn Sie die RDS-API-Operationen CreateDBCluster und ModifyDBCluster ausführen.

In Aurora MySQL Version 2 und höher beinhaltet die Engine-Version in der AWS Management Console auch die Aurora-Version. Beim Upgraden des Clusters ändert sich der angezeigte Wert. Diese Änderung hilft Ihnen, die genauen Aurora MySQL-Versionen anzugeben und zu überprüfen, ohne dass Sie eine Verbindung zum Cluster herstellen oder SQL-Befehle ausführen müssen.

> **Tip**
>
> Bei Aurora-Clustern AWS CloudFormation, die über verwaltet werden, kann diese Änderung der `EngineVersion` Einstellung Aktionen von auslösen AWS CloudFormation. Informationen darüber, wie mit Änderungen AWS CloudFormation an der `EngineVersion` Einstellung umgegangen wird, finden Sie in der AWS CloudFormation Dokumentation.

Überprüfen von Aurora MySQL-Versionen mit SQL

Die Aurora-Versionsnummern, die Sie in Ihrer Anwendung mit SQL-Abfragen abrufen können, verwenden das Format *<major version>*.*<minor version>*.*<patch version>*. Sie können diese Versionsnummer für jede DB-Instance in Ihrem Aurora MySQL-Cluster abrufen, indem Sie die `AURORA_VERSION`-Systemvariable abfragen. Verwenden Sie eine der folgenden Abfragen, um diese Versionsnummer zu erhalten.

```
select aurora_version();
select @@aurora_version;
```

Diese Abfragen erzeugen eine Ausgabe ähnlich der folgenden.

```
mysql> select aurora_version(), @@aurora_version;
+------------------+------------------+
| aurora_version() | @@aurora_version |
+------------------+------------------+
| 2.11.1           | 2.11.1           |
+------------------+------------------+
```

Die Versionsnummern, die von der Konsole, CLI und der RDS-API mit den unter Überprüfen oder Spezifizieren von Aurora MySQL-Engine-Versionen über AWS beschriebenen Techniken zurückgegeben werden, sind in der Regel aussagekräftiger.

Aurora MySQL Long-Term Support- (LTS, Langzeit-Support) Versionen

Jede neue Aurora MySQL-Version bleibt für eine bestimmte Zeit zum Erstellen oder Aktualisieren eines DB-Clusters verfügbar. Nach diesem Zeitraum müssen Sie alle Cluster aktualisieren, die diese Version verwenden. Sie können Ihren Cluster vor Ablauf des Supportzeitraums manuell aktualisieren, oder Aurora kann ihn automatisch für Sie aktualisieren, wenn die Aurora MySQL-Version nicht mehr unterstützt wird.

Aurora bezeichnet bestimmte Aurora MySQL-Versionen als „Long-term Support“ (LTS, Langzeitsupport)-Versionen. DB-Cluster, die LTS-Versionen verwenden, können länger dieselbe Version nutzen und weniger Upgradezyklen durchlaufen als Cluster, die Nicht-LTS-Versionen verwenden. Aurora unterstützt jede LTS-Version mindestens drei Jahr lang, nachdem diese Veröffentlichung verfügbar ist. Wenn ein DB-Cluster mit einer LTS-Version ein Upgrade benötigt, aktualisiert Aurora ihn auf die nächste LTS-Version. Auf diese Weise muss lange Zeit kein erneutes Upgrade für den Cluster durchgeführt werden.

Während der Lebensdauer einer Aurora MySQL-LTS-Version sorgen neue Patchlevels für Korrekturen bei wichtigen Problemen. Die Patchlevels enthalten keine neuen Funktionen. Sie können wählen, ob Sie solche Patches auf DB-Cluster anwenden möchten, die die LTS-Version ausführen. Für bestimmte kritische Korrekturen kann Amazon innerhalb derselben LTS-Version ein verwaltetes Upgrade auf einen Patchlevel durchführen. Solche verwalteten Upgrades werden automatisch innerhalb des Wartungsfensters des Clusters durchgeführt.

Wir empfehlen, dass Sie für die meisten Ihrer Aurora MySQL-Cluster auf die neueste Version upgraden, anstatt die LTS-Version zu verwenden. Auf diese Weise wird Aurora als Managed verwalteter Service genutzt und Sie erhalten Zugriff auf die neuesten Funktionen und Bugfixes. Die LTS-Releases sind für Cluster mit folgenden Merkmalen gedacht:

- Sie können sich, abgesehen von seltenen Fällen, keine Upgrade-Ausfallzeiten Ihrer Aurora MySQL-Anwendung für kritische Patches leisten.
- Der Testzyklus für den Cluster und die zugehörigen Anwendungen dauert bei einer Aktualisierung der Aurora MySQL-Datenbank-Engine sehr lange.
- Die Datenbankversion für Ihren Aurora MySQL-Cluster enthält alle Funktionen der DB-Engine und Bugfixes, die Ihre Anwendung benötigt.

Die aktuelle LTS-Version für Aurora MySQL ist folgende:

- Aurora MySQL Version 3.04.*. Weitere Informationen zur LTS-Version finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL Version 3 in den Versionshinweisen für Aurora MySQL.

> **Note**
>
> Wir empfehlen, den `AutoMinorVersionUpgrade` Parameter für LTS-Versionen nicht auf zu setzen `true` (oder die automatische Aktualisierung kleinerer Versionen in der zu aktivieren AWS Management Console). Dies könnte dazu führen, dass Ihr DB-Cluster auf eine Nicht-LTS-Version wie 3.05.2 aktualisiert wird.

Aurora MySQL Betaversionen

Bei einer Aurora MySQL-Betaversion handelt es sich um ein frühes Sicherheitsupdate, das nur in einer begrenzten Anzahl von Versionen verfügbar ist. AWS-Regionen Diese Fixes werden später mit der nächsten Patch-Version in allen Regionen umfassender eingesetzt.

Die Nummerierung für eine Beta-Version ähnelt der einer Aurora MySQL-Nebenversion, jedoch mit einer zusätzlichen vierten Ziffer, zum Beispiel 2.12.0.1 oder 3.05.0.1.

Weitere Informationen finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL Version 2 und Datenbank-Engine-Updates für Amazon Aurora MySQL Version 3 in den Versionshinweisen für Aurora MySQL.

Vorbereitung auf das Ende des Standardsupports für Amazon Aurora MySQL-Compatible Edition Version 2

Die Amazon Aurora MySQL-Compatible Edition Version 2 (mit MySQL 5.7-Kompatibilität) wird voraussichtlich am 31. Oktober 2024 das Ende des Standardsupports erreichen. Wir empfehlen, dass Sie alle Cluster, auf denen Aurora MySQL Version 2 ausgeführt wird, auf die Standardversion von Aurora MySQL 3 (mit MySQL 8.0-Kompatibilität) oder höher aktualisieren, bevor Aurora MySQL Version 2 das Ende des Standard-Supportzeitraums erreicht. Am 31. Oktober 2024 registriert Amazon RDS Ihre Datenbanken automatisch bei Amazon RDS Extended Support. Wenn Sie Amazon Aurora MySQL Version 2 (mit MySQL 5.7-Kompatibilität) in einem Cluster der Aurora Serverless Version 1 ausführen, gilt dies nicht für Sie. Wenn Sie Ihre Cluster der Aurora Serverless Version 1 auf Aurora MySQL Version 3 aktualisieren möchten, finden Sie weitere Informationen unterUpgrade-Pfad für Aurora Serverless v1 DB-Cluster.

Die nächsten end-of-support Termine für Aurora-Hauptversionen finden Sie unterAmazon-Aurora-Versionen.

Wenn Sie Cluster haben, auf denen Aurora MySQL Version 2 ausgeführt wird, erhalten Sie regelmäßig Benachrichtigungen mit den neuesten Informationen zur Durchführung eines Upgrades, sobald wir uns dem Ende des Standard-Supportdatums nähern. Wir werden diese Seite regelmäßig mit den neuesten Informationen aktualisieren.

Zeitplan für das Ende des Standard-Supports

1. Jetzt bis zum 31. Oktober 2024 – Sie können jederzeit Upgrades von Aurora-MySQL-Clustern der Version 2 (mit MySQL 5.7-Kompatibilität) auf Aurora MySQL Version 3 (mit MySQL 8.0-Kompatibilität) starten.

2. 31. Oktober 2024 — An diesem Tag endet der Standardsupport für Aurora MySQL Version 2 und Amazon RDS registriert Ihre Cluster automatisch bei Amazon RDS Extended Support.

Wir werden Sie automatisch für RDS Extended Support registrieren. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Extended Support.

Suche nach Clustern, die von diesem end-of-life Prozess betroffen sind

Gehen Sie wie folgt vor, um Cluster zu finden, die von diesem end-of-life Prozess betroffen sind.

> **Important**
>
> Stellen Sie sicher, dass Sie diese Anweisungen an jedem AWS-Region Ort ausführen AWS-Konto , an dem sich Ihre Ressourcen befinden.

Konsole

So finden Sie einen Aurora-MySQL-Cluster der Version 2

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Geben Sie im Feld Nach Datenbanken filtern 5.7 ein.
4. Suchen Sie in der Engine-Spalte nach Aurora MySQL.

AWS CLI

Rufen Sie den describe-db-clustersBefehl auf, um mithilfe von nach Clustern zu suchen AWS CLI, die von diesem end-of-life Prozess betroffen sind. Sie können das folgende Beispielskript verwenden.

Example

```
aws rds describe-db-clusters --include-share --query 'DBClusters[?(Engine==`aurora-
mysql` && contains(EngineVersion,`5.7.mysql_aurora`))].{EngineVersion:EngineVersion,
 DBClusterIdentifier:DBClusterIdentifier, EngineMode:EngineMode}' --output table
 --region us-east-1
```

```
+-------------------------------------------------------------+
|                      DescribeDBClusters                     |
+---------------------+---------------+-------------------------+
|         DBCI        |      EM       |          EV             |
+---------------------+---------------+-------------------------+
|    aurora-mysql2    |  provisioned  | 5.7.mysql_aurora.2.11.3 |
| aurora-serverlessv1 |   serverless  | 5.7.mysql_aurora.2.11.3 |
+---------------------+---------------+-------------------------+
```

RDS-API

Um Aurora-MySQL-DB-Cluster zu finden, auf denen Aurora MySQL Version 2 ausgeführt wird, verwenden Sie den RDS-DescribeDBClusters-API-Vorgang mit folgenden erforderlichen Parametern:

- `DescribeDBClusters`
  - Filters.Filter.N
    - Name
      - engine
    - Values.Value.N
      - ['aurora']

Amazon RDS Extended Support

Sie können Amazon RDS Extended Support bis zum Ende des Supports, dem 31. Oktober 2024, kostenlos über die Community MySQL 5.7 nutzen. Am 31. Oktober 2024 registriert Amazon RDS Ihre Datenbanken automatisch bei RDS Extended Support for Aurora MySQL Version 2. RDS Extended Support for Aurora ist ein kostenpflichtiger Service, der bis zum Ende des RDS Extended Support im Februar 2027 bis zum Ende des RDS Extended Support bis zum Ende des RDS Extended Support bis zu 28 zusätzliche Monate Support für Aurora MySQL Version 2 bietet. RDS Extended Support wird nur für die Aurora-MySQL-Nebenversionen 2.11 und 2.12 angeboten. Wenn Sie Amazon Aurora MySQL Version 2 nach dem Ende des Standard-Supports verwenden möchten, planen Sie, Ihre Datenbanken vor dem 31. Oktober 2024 auf einer dieser Nebenversionen auszuführen.

Weitere Informationen zum RDS Extended Support, z. B. zu Gebühren und anderen Überlegungen, finden Sie unterVerwenden von Amazon RDS Extended Support.

Durchführen eines Upgrades

Das Upgrade zwischen Hauptversionen erfordert umfangreichere Planung und Tests als für eine Nebenversion. Der Prozess kann beträchtliche Zeit in Anspruch nehmen. Wir möchten das Upgrade als dreistufigen Prozess mit Aktivitäten vor dem Upgrade, für das Upgrade und nach dem Upgrade betrachten.

Vor dem Upgrade:

Wir empfehlen, vor der Aktualisierung die Anwendungskompatibilität, die Leistung, Wartungsverfahren und ähnliche Dinge für den aktualisierten Cluster zu prüfen, um sicherzustellen, dass Ihre Anwendungen nach der Aktualisierung wie erwartet funktionieren werden. Im Folgenden finden Sie fünf Empfehlungen, die Ihnen zu einem besseren Upgrade-Komfort verhelfen sollen.

- Zunächst ist es wichtig zu verstehenFunktionsweise des Aurora MySQL direkten Upgrade der Hauptversion.
- Erkunden Sie als Nächstes die Upgrade-Techniken, die wann verfügbar sindUpgrade von Aurora MySQL Version 2 auf Version 3.
- Um Ihnen bei der Entscheidung über den richtigen Zeitpunkt und die richtige Vorgehensweise für ein Upgrade zu helfen, können Sie sich mit den Unterschieden zwischen Aurora MySQL Version 3 und Ihrer aktuellen Umgebung vertraut machenVergleich von Aurora-MySQL-Version 2 und Aurora-MySQL-Version 3.
- Nachdem Sie sich für die Option entschieden haben, die praktisch ist und am besten funktioniert, versuchen Sie es mit einem simulierten In-Place-Upgrade auf einem geklonten Cluster. Planen eines Hauptversionsupgrades für einen Aurora MySQL-Cluster Der Pre-Checker kann ausgeführt werden und feststellen, ob die Datenbank erfolgreich aktualisiert werden kann und ob es nach dem Upgrade Probleme mit der Anwendungsinkompatibilität gibt, ebenso wie Leistung, Wartungsverfahren und ähnliche Überlegungen.

  Lesen Sie die Blogbeiträge zur Upgrade-Checkliste, Teil 1 und Teil 2.
- Nicht alle Arten oder Versionen von Aurora MySQL Clustern können den integrierten Upgrade-Mechanismus verwenden. Weitere Informationen finden Sie unter Aurora MySQL Upgrade-Vorgang für die Hauptversion.

Wenn Sie Fragen oder Bedenken haben, steht Ihnen das AWS Support-Team in den Community-Foren und im Premium-Support zur Verfügung.

Durchführen der Aktualisierung:

Sie können eine der folgenden Upgrade-Techniken verwenden. Wie lange Ihr System ausfällt, hängt von der gewählten Technik ab.

- Blaue/grüne Bereitstellungen — In Situationen, in denen die Reduzierung von Anwendungsausfällen oberste Priorität hat, können Sie Amazon RDS Blue/Green Deployments verwenden, um das Hauptversions-Upgrade in bereitgestellten Amazon Aurora Aurora-DB-Clustern durchzuführen. Mit einer Blau/Grün-Bereitstellung wird eine Staging-Umgebung erstellt, die die Produktionsumgebung kopiert. Sie können bestimmte Änderungen am Aurora-DB-Cluster in der grünen (Staging-)Umgebung vornehmen, ohne die Produktions-Workloads zu beeinträchtigen. Die Umstellung dauert in der Regel weniger als eine Minute, ohne dass Daten verloren gehen. Weitere Informationen finden Sie unter Übersicht über Blau/Grün-Bereitstellungen von Amazon RDS für Aurora. Dadurch werden Ausfallzeiten minimiert. Sie müssen jedoch während der Durchführung des Upgrades zusätzliche Ressourcen einsetzen.
- Direkte Upgrades — Sie können ein direktes Upgrade durchführen, bei dem Aurora automatisch eine Vorabprüfung für Sie durchführt, den Cluster offline nimmt, Ihren Cluster sichert, das Upgrade durchführt und Ihren Cluster wieder online stellt. Ein direktes Upgrade der Hauptversion kann mit wenigen Klicks durchgeführt werden und erfordert keine weitere Koordination oder Failover mit anderen Clustern, ist jedoch mit Ausfallzeiten verbunden. Weitere Informationen finden Sie unter Erläuterung der Durchführung eines direkten Upgrades.
- Snapshot-Wiederherstellung — Sie können Ihren Aurora MySQL Version 2-Cluster aktualisieren, indem Sie von einem Aurora MySQL Version 2-Snapshot auf einen Aurora MySQL Version 3-Cluster wiederherstellen. Um dies zu tun, sollten Sie den Prozess zum Erstellen eines Snapshots und zum Wiederherstellen von diesem befolgen. Dieser Vorgang beinhaltet eine Datenbankunterbrechung, da Sie die Wiederherstellung aus einem Snapshot durchführen.

Nach dem Upgrade:

Nach dem Upgrade müssen Sie Ihr System (Anwendung und Datenbank) genau überwachen und gegebenenfalls Feinabstimmungen vornehmen. Wenn Sie die Schritte vor dem Upgrade genau befolgen, werden die erforderlichen Änderungen auf ein Minimum reduziert. Weitere Informationen finden Sie unter Fehlerbehebung bei der Leistung der Amazon Aurora MySQL-Datenbank.

Um mehr über die Methoden, die Planung, das Testen und die Fehlerbehebung von Aurora MySQL-Hauptversions-Upgrades zu erfahren, lesen Sie bitte sorgfältigAktualisieren der Hauptversion eines DB-Clusters von Amazon Aurora MySQL, einschließlichProblembehandlung für Aurora MySQL direkte Upgrades. Beachten Sie außerdem, dass einige Instance-Typen für Aurora MySQL Version 3 nicht unterstützt werden. Weitere Informationen finden Sie unter Aurora DB-Instance-Klassen.

Upgrade-Pfad für Aurora Serverless v1 DB-Cluster

Das Upgrade zwischen Hauptversionen erfordert umfangreichere Planung und Tests als für eine Nebenversion. Der Prozess kann beträchtliche Zeit in Anspruch nehmen. Wir möchten das Upgrade als dreistufigen Prozess mit Aktivitäten vor dem Upgrade, für das Upgrade und nach dem Upgrade betrachten.

Aurora MySQL Version 2 (mit MySQL 5.7-Kompatibilität) wird weiterhin Standardunterstützung für Aurora Serverless v1 Cluster erhalten.

Wenn Sie ein Upgrade zu Amazon Aurora MySQL 3 (mit MySQL-8.0-Kompatibilität) durchführen und weiterhin Aurora Serverless ausführen möchten, können Sie Amazon Aurora Serverless v2 verwenden. Informationen zu den Unterschieden zwischen Aurora Serverless v1 und Aurora Serverless v2 finden Sie unterAurora Serverless v2 und Aurora Serverless v1 im Vergleich.

Upgrade aufAurora Serverless v2: Sie können einen Aurora Serverless v1 Cluster auf aktualisierenAurora Serverless v2. Weitere Informationen finden Sie unter Aktualisieren eines Aurora Serverless v1-Clusters auf Aurora Serverless v2.

Vorbereitung auf das Lebenszyzklusende der Amazon Aurora MySQL-kompatible Edition Version 1

Amazon-Aurora-MySQL-kompatible Edition Version 1 (mit MySQL 5.6-Kompatibilität) soll am 28. Februar 2023 das Lebenszyzklusende erreichen. Amazon rät, dass Sie alle (bereitgestellten) Cluster (und Aurora Serverless) mit Aurora MySQL Version 1 auf Aurora MySQL Version 2 (mit MySQL 5.7-Kompatibilität) oder Aurora MySQL Version 3 (mit MySQL 8.0 Kompatibilität) aktualisieren. Tun Sie dies, bevor Aurora-MySQL-Version 1 das Ende ihres Supportzeitraums erreicht.

Für Aurora-bereitgestellte DB-Cluster können Sie Upgrades von Aurora MySQL Version 1 auf Aurora MySQL Version 2 mit verschiedenen Methoden durchführen. Eine Anleitung zum Direkt-Upgrade-Mechanismus finden Sie unter Erläuterung der Durchführung eines direkten Upgrades. Eine weitere Möglichkeit, das Upgrade abzuschließen, besteht darin, einen Snapshot eines Aurora-MySQL-Version-1-Clusters zu erstellen und den Snapshot in einem Aurora-MySQL-Version-2-Cluster wiederherzustellen. Oder Sie können einen mehrstufigen Prozess verfolgen, bei dem die alten und neuen Cluster nebeneinander ausgeführt werden. Weitere Einzelheiten zu den einzelnen Methoden finden Sie unter Aktualisieren der Hauptversion eines DB-Clusters von Amazon Aurora MySQL.

Für DB-Cluster von Aurora Serverless v1 können Sie ein direktes Upgrade von Aurora-MySQL-Version 1 auf Aurora-MySQL-Version 2 durchführen. Weitere Einzelheiten zu dieser Methode finden Sie unter Ändern eines Aurora Serverless v1-DB-Clusters.

Für Aurora-bereitgestellte DB-Cluster können Sie Upgrades von Aurora-MySQL-Version 1 auf Aurora-MySQL-Version 3 mithilfe eines zweistufigen Upgrade-Prozesses durchführen:

1. Führen Sie ein Upgrade von Aurora-MySQL-Version 1 auf Aurora-MySQL-Version 2 unter Verwendung der zuvor beschriebenen Methoden durch.
2. Aktualisieren Sie von Aurora-MySQL-Version 2 auf Aurora-MySQL-Version 3 mit den gleichen Methoden wie von Version 1 auf Version 2. Weitere Informationen finden Sie unter Upgrade von Aurora MySQL Version 2 auf Version 3. Beachten Sie den Funktionsunterschiede zwischen Aurora MySQL Version 2 und 3.

Die Datumsangaben zum Ende des Lebenszyklus für Aurora-Hauptversionen finden Sie in Amazon-Aurora-Versionen. Amazon aktualisiert automatisch alle Cluster, die Sie vor dem Ende des Lebenszyklus nicht selbst aktualisieren. Nach dem Ende des Lebenszyklus erfolgen diese automatischen Upgrades auf die nachfolgende Hauptversion während eines geplanten Wartungsfensters für Cluster.

Im Folgenden finden Sie zusätzliche Meilensteine für das Upgrade von Aurora-MySQL-Cluster der Version 1 (bereitgestellt und Aurora Serverless), die das Ende des Lebenszyklus erreichen. Für alle ist die Startzeit 00:00 Uhr (UTC).

1. Jetzt bis zum 28. Februar 2023 – Sie können jederzeit Upgrades von Aurora-MySQL-Cluster der Version 1 (mit MySQL 5.6-Kompatibilität) auf Aurora MySQL Version 2 (mit MySQL 5.7-Kompatibilität) starten. Von Aurora-MySQL-Version 2 aus können Sie ein weiteres Upgrade auf Aurora-MySQL-Version 3 (mit MySQL 8.0-Kompatibilität) für von Aurora bereitgestellte DB-Cluster durchführen.
2. 16. Januar 2023 – Ab diesem Zeitpunkt können Sie keine neuen Cluster oder Instances von Aurora MySQL Version 1 über die AWS Management Console oder die AWS Command Line Interface (AWS CLI) erstellen. Sie können einer globalen Aurora-Datenbank auch keine neuen sekundären Regionen hinzufügen. Dies kann sich auf Ihre Fähigkeit auswirken, sich nach einem ungeplanten Ausfall wie in Wiederherstellen einer globalen Amazon Aurora-Datenbank nach einem ungeplanten Ausfall beschrieben zu erholen, da Sie die Schritte 5 und 6 nach dieser Zeit nicht ausführen können. Sie können auch kein neues regionsübergreifendes Lesereplikat erstellen,

auf dem Aurora MySQL Version 1 ausgeführt wird. Für bestehende Aurora-MySQL-Cluster der Version 1 können Sie bis zum 28. Februar 2023 immer noch Folgendes tun:

- Wiederherstellen eines Snapshots eines Clusters von Aurora-MySQL-Version 1 auf die Version des ursprünglichen Snapshot-Clusters.
- Lesereplikate hinzufügen (gilt nicht für Aurora Serverless-DB-Cluster).
- Ändern der Instance-Konfiguration.
- Durchführen einer Point-in-Time-Wiederherstellung.
- Erstellen von Klonen bestehender Cluster der Version 1.
- Erstellen eines neuen regionsübergreifendes Lesereplikats, auf dem Aurora-MySQL-Version 2 oder höher ausgeführt wird.

3. 28. Februar 2023 – Nach dieser Zeit planen wir, Aurora-MySQL-Cluster der Version 1 innerhalb eines darauf folgenden geplanten Wartungsfensters automatisch auf die Standardversion von Aurora-MySQL-Version 2 zu aktualisieren. Das Wiederherstellen von Aurora-MySQL-Version-1-DB-Snapshots führt zu einem automatischen Upgrade des wiederhergestellten Clusters auf die Standardversion von Aurora MySQL Version 2 zu diesem Zeitpunkt.

Das Upgrade zwischen Hauptversionen erfordert umfangreichere Planung und Tests als für eine Nebenversion. Der Prozess kann beträchtliche Zeit in Anspruch nehmen.

In Situationen, in denen die Reduzierung von Ausfallzeiten oberste Priorität hat, können Sie auch Blau/Grün-Bereitstellungen verwenden, um das Hauptversions-Upgrade in bereitgestellten DB-Clustern von Amazon Aurora durchzuführen. Mit einer Blau/Grün-Bereitstellung wird eine Staging-Umgebung erstellt, die die Produktionsumgebung kopiert. Sie können Änderungen am Aurora-DB-Cluster in der grünen (Staging-) Umgebung vornehmen, ohne die Produktions-Workloads zu beeinträchtigen. Die Umstellung dauert in der Regel weniger als eine Minute, ohne dass Daten verloren gehen und Anwendungsänderungen erforderlich sind. Weitere Informationen finden Sie unter Übersicht über Blau/Grün-Bereitstellungen von Amazon RDS für Aurora.

Nachdem das Upgrade abgeschlossen ist, müssen Sie möglicherweise auch Follow-up-Arbeiten ausführen. Beispielsweise müssen Sie möglicherweise aufgrund von Unterschieden in der SQL-Kompatibilität, der Funktionsweise bestimmter MySQL-bezogener Funktionen oder Parametereinstellungen zwischen der alten und der neuen Version nachverfolgen.

Um mehr über die Methoden, die Planung, das Testen und die Fehlerbehebung von Aurora-MySQL-Hauptversions-Upgrades zu erfahren, lesen Sie unbedingt Aktualisieren der Hauptversion eines DB-Clusters von Amazon Aurora MySQL .

Finden von Clustern, die von diesem Lebenszyklusende-Prozess betroffen sind

Gehen Sie wie folgt vor, um Cluster zu finden, die von diesem Lebenszyklusende-Prozess betroffen sind.

> **Important**
>
> Stellen Sie sicher, dass Sie diese Anweisungen in jeder AWS-Region und für jedes AWS-Konto ausführen, in der sich Ihre Ressourcen befinden.

Konsole

Suchen Sie einen Aurora-MySQL-Cluster der Version 1 wie folgt:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Geben Sie im Feld Nach Datenbanken filtern 5.6 ein.
4. Suchen Sie in der Engine-Spalte nach Aurora MySQL.

AWS CLI

Um unter Verwendung von AWS CLI Cluster zu finden, die von diesem Lebenszyklusende-Prozess betroffen sind, rufen Sie den describe-db-clusters-Befehl auf. Sie können das folgende Beispielskript verwenden.

Example

```
aws rds describe-db-clusters --include-share --query 'DBClusters[?Engine==`aurora`].
{EV:EngineVersion, DBCI:DBClusterIdentifier, EM:EngineMode}' --output table --region
 us-east-1

        +-----------------------------------------+
        |            DescribeDBClusters           |
        +---------------+--------------+----------+
        |     DBCI      |     EM       |    EV    |
        +---------------+--------------+----------+
        |  my-database-1|  serverless  |  5.6.10a |
        +---------------+--------------+----------+
```

RDS-API

Um Aurora-MySQL-DB-Cluster zu finden, auf denen Aurora MySQL Version 1 ausgeführt wird, verwenden Sie den RDS-DescribeDBClusters-API-Vorgang mit folgenden erforderlichen Parametern:

- `DescribeDBClusters`
  - Filters.Filter.N
    - Name
      - engine
    - Values.Value.N
      - ['aurora']

Upgrade von Amazon Aurora MySQL-DB-Clustern

Sie können einen Aurora MySQL-DB-Cluster aktualisieren, um Fehlerbehebungen oder neue Aurora MySQL-Funktionen zu erhalten oder zu einer völlig neuen Version der zugrunde liegenden Datenbank-Engine zu wechseln. Die folgenden Abschnitte zeigen wie.

> **Note**
>
> Die Art des Upgrades, das Sie durchführen, hängt davon ab, wie viel Ausfallzeit Sie sich für Ihren Cluster leisten können, wie viele Verifizierungstests Sie durchführen möchten, wie wichtig die spezifischen Fehlerbehebungen oder neuen Funktionen für Ihren Anwendungsfall sind und ob Sie vorhaben häufig kleine Upgrades oder gelegentliche Upgrades durchführen, die mehrere Zwischenversionen überspringen. Für jedes Upgrade können Sie die Hauptversion, die Nebenversion und die Patch-Ebene für Ihren Cluster ändern. Wenn Sie mit der Unterscheidung zwischen Aurora MySQL-Hauptversionen, Nebenversionen und Patch-Ebenen nicht vertraut sind, können Sie die Hintergrundinformationen unter lese Aurora MySQL-Versionsnummern und Sonderversionen.

> **Tip**
>
> Sie können die für ein DB-Cluster-Upgrade erforderlichen Ausfallzeiten minimieren, indem Sie eine Blau/Grün-Bereitstellung verwenden. Weitere Informationen finden

Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

Themen

- Upgrade der Nebenversion oder der Patch-Ebene eines Aurora MySQL-DB-Clusters
- Aktualisieren der Hauptversion eines DB-Clusters von Amazon Aurora MySQL

Upgrade der Nebenversion oder der Patch-Ebene eines Aurora MySQL-DB-Clusters

Sie können die folgenden Methoden verwenden, um die Nebenversion eines DB-Clusters zu aktualisieren oder einen DB-Cluster zu patchen:

- Upgrade von Aurora MySQL durch Ändern der Engine-Version (für Aurora-MySQL-Version 2) und 3
- Aktivieren von automatischen Upgrades zwischen Aurora MySQL-Nebenversionen

Informationen dazu, wie Patches ohne Ausfallzeiten Unterbrechungen während des Upgrade-Vorgangs reduzieren können, finden Sie unter Verwendung von Zero-Downtime-Patching (Patchen ohne Ausfallzeiten).

Vor der Durchführung eines kleineren Versionsupgrades

Wir empfehlen Ihnen, die folgenden Aktionen durchzuführen, um die Ausfallzeit während eines Upgrades einer Nebenversion zu reduzieren:

- Die Wartung des Aurora-DB-Clusters sollte in Zeiten mit geringem Datenverkehr durchgeführt werden. Verwenden Sie Performance Insights, um diese Zeiträume zu identifizieren und die Wartungsfenster korrekt zu konfigurieren. Weitere Informationen zu Performance Insights finden Sie unter Überwachen der DB-Auslastung mit Performance Insights auf Amazon RDS. Weitere Informationen zum Wartungsfenster für DB-Cluster finden Sie unterAnpassen des bevorzugten DB-Cluster-Wartungsfensters.
- Verwenden Sie als AWS bewährte Methode SDKs, die exponentielles Backoff und Jitter unterstützen. Weitere Informationen finden Sie unter Exponentieller Backoff und Jitter.

Vorabprüfungen für kleinere Versionsupgrades für Aurora MySQL

Wenn Sie ein Upgrade auf eine kleinere Version starten, führt Amazon Aurora automatisch Vorabprüfungen durch.

Diese Vorabprüfungen müssen durchgeführt werden. Sie können nicht ausgelassen werden. Die Vorabprüfungen bieten folgende Vorteile:

- Sie können ungeplante Ausfallzeiten während des Upgrades vermeiden.
- Wenn es Inkompatibilitäten gibt, verhindert Amazon Aurora das Upgrade und stellt Ihnen ein Protokoll zur Verfügung, in dem Sie mehr darüber erfahren können. Anschließend können Sie das Protokoll verwenden, um Ihre Datenbank auf das Upgrade vorzubereiten, indem Sie die Inkompatibilitäten reduzieren. Ausführliche Informationen zum Entfernen von Inkompatibilitäten finden Sie unter Vorbereiten Ihrer Installation für das Upgrade in der MySQL-Dokumentation.

Die Vorabprüfungen werden ausgeführt, bevor die DB-Instance aufgrund des Upgrades angehalten wird. Sie verursachen also keine Ausfallzeiten. Wenn bei den Vorprüfungen eine Inkompatibilität festgestellt wird, bricht Aurora das Upgrade automatisch ab, bevor die DB-Instance gestoppt wird. Aurora generiert auch ein Ereignis für die Inkompatibilität. Weitere Informationen zu Amazon Aurora Aurora-Veranstaltungen finden Sie unterArbeiten mit Amazon-RDS-Ereignisbenachrichtigungen.

Aurora zeichnet detaillierte Informationen zu jeder Inkompatibilität in der Protokolldatei `PrePatchCompatibility.log` auf. In den meisten Fällen enthalten die Protokolleinträge einen Link zur MySQL-Dokumentation mit Informationen zur Lösung des Inkompatibilitätsproblems. Weitere Informationen zum Anzeigen von Protokolldateien finden Sie unter Anzeigen und Auflisten von Datenbank-Protokolldateien.

Aufgrund der Art der Vorabprüfungen werden die Objekte in Ihrer Datenbank geprüft. Diese Analyse verbraucht Ressourcen und verlängert die Zeit, die für die Durchführung des Upgrades benötigt wird.

Upgrade von Aurora MySQL durch Ändern der Engine-Version

Durch das Upgrade der Nebenversion eines Aurora MySQL-DB-Clusters werden zusätzliche Korrekturen und neue Funktionen auf einen vorhandenen Cluster angewendet.

Diese Art von Upgrade gilt für Aurora MySQL-Cluster, bei denen die Originalversion und die aktualisierte Version beide dieselbe Aurora MySQL-Hauptversion haben, entweder 2 oder 3. Der Prozess ist schnell und unkompliziert, da er keine Konvertierung für die Aurora-MySQL-Metadaten oder Reorganisation Ihrer Tabellendaten erfordert.

Sie führen diese Art von Upgrade durch, indem Sie die Engine-Version des DB-Clusters mithilfe der AWS Management Console AWS CLI, oder der RDS-API ändern. Wenn auf Ihrem Cluster beispielsweise Aurora MySQL 2.x ausgeführt wird, wählen Sie eine höhere 2.x-Version.

Wenn Sie ein kleineres Upgrade für eine globale Aurora-Datenbank durchführen, aktualisieren Sie alle sekundären Cluster, bevor Sie den primären Cluster aktualisieren.

> **Note**
>
> Gehen Sie wie folgt vor, um ein Unterversion-Upgrade auf Aurora-MySQL-Version 3.03.* oder höher bzw. Version 2.12* durchzuführen:
>
> 1. Entfernen Sie alle sekundären Regionen aus dem globalen Cluster. Führen Sie die Schritte unter Entfernen eines Clusters aus einer Amazon Aurora Global Database aus.
> 2. Aktualisieren Sie die Engine-Version der primären Region auf Version 3.03.* oder höher bzw. Version 2.12.*, falls zutreffend. Führen Sie die Schritte unter To modify the engine version of a DB cluster aus.
> 3. Fügen Sie dem globalen Cluster sekundäre Regionen hinzu. Führen Sie die Schritte unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank aus.

So ändern Sie die Engine-Version eines DB-Clusters:

- Über die Konsole – Ändern Sie die Eigenschaften Ihres Clusters. Ändern Sie im Fenster DB-Cluster ändern die Aurora-MySQL-Engine-Version im Feld DB-Engine-Version. Wenn Sie mit dem allgemeinen Verfahren zum Ändern eines Clusters nicht vertraut sind, folgen Sie den Anweisungen unter Ändern des DB-Clusters über die Konsole, die CLI und die API.
- Verwenden Sie den Befehl AWS CLI— Rufen Sie den AWS CLI Befehl modify-db-cluster auf und geben Sie den Namen Ihres DB-Clusters für die Option und die Engine-Version für die `--db-cluster-identifier` Option an. `--engine-version`

  Um beispielsweise auf Aurora MySQL Version 2.12.1 zu aktualisieren, setzen Sie die `--engine-version` Option auf. `5.7.mysql_aurora.2.12.1` Geben Sie die Option `--apply-immediately` an, um die Engine-Version für Ihren DB-Cluster sofort zu aktualisieren.
- Über die RDS-API Rufen Sie die API-Operation ModifyDBCluster auf und geben Sie den Namen Ihres DB-Clusters für den Parameter `DBClusterIdentifier` sowie die Engine-Version für den Parameter `EngineVersion` an. Legen Sie den Parameter `ApplyImmediately` auf `true` fest, um die Engine-Version für Ihren DB-Cluster sofort zu aktualisieren.

Aktivieren von automatischen Upgrades zwischen Aurora MySQL-Nebenversionen

Für einen DB-Cluster von Amazon Aurora MySQL können Sie angeben, dass Aurora den DB-Cluster automatisch auf neue Nebenversionen aktualisiert. Sie tun dies, indem Sie die `AutoMinorVersionUpgrade` Eigenschaft (Automatisches Upgrade der Nebenversion in AWS Management Console) des DB-Clusters festlegen.

Automatische Aktualisierungen erfolgen während des Wartungsfensters. Wenn die einzelnen DB-Instances im DB-Cluster andere Wartungsfenster haben als das Cluster-Wartungsfenster, hat das Cluster-Wartungsfenster Vorrang.

Das automatische Nebenversions-Upgrade gilt nicht für die folgenden Aurora MySQL-Clustertypen:

- Cluster, die Teil einer globalen Aurora-Datenbank sind
- Cluster, die über regionsübergreifende Replikate verfügen

Die Ausfalldauer hängt vom Workload, der Cluster-Größe, der Menge der binären Protokolldaten und davon ab, ob Aurora die Funktion „Patching ohne Ausfallzeiten“ (Zero Downtime Patching, ZDP) verwenden kann. Aurora startet den Datenbankcluster neu, sodass Sie möglicherweise eine kurze Zeit nicht verfügbar sind, bevor Sie Ihren Cluster wieder verwenden. Insbesondere wirkt sich die Menge der Binärprotokolldaten auf die Wiederherstellungszeit aus. Die DB-Instance verarbeitet die binären Protokolldaten während der Wiederherstellung. Somit erhöht eine hohe Menge an binären Protokolldaten die Wiederherstellungszeit.

> **Note**
>
> Aurora führt automatische Upgrades nur durch, wenn die `AutoMinorVersionUpgrade` Einstellung für alle DB-Instances in Ihrem DB-Cluster aktiviert ist. Informationen darüber, wie Sie sie einrichten und wie sie funktioniert, wenn sie auf Cluster- und Instance-Ebene angewendet wird, finden Sie unter Automatische Nebenversions-Upgrades für Aurora-DB-Cluster.
>
> Wenn dann ein Upgrade-Pfad für die Instances des DB-Clusters auf eine untergeordnete DB-Engine-Version existiert, die auf „true“ `AutoUpgrade` gesetzt ist, wird das Upgrade durchgeführt. Die `AutoUpgrade` Einstellung ist dynamisch und wird von RDS festgelegt. Automatische Nebenversions-Upgrades werden auf die standardmäßige Nebenversion durchgeführt.

Sie können einen CLI-Befehl wie den folgenden verwenden, um den Status der Einstellung `AutoMinorVersionUpgrade` für alle DB-Instances in Ihren Aurora-MySQL-Clustern zu überprüfen.

```
aws rds describe-db-instances \
  --query '*[].
{DBClusterIdentifier:DBClusterIdentifier,DBInstanceIdentifier:DBInstanceIdentifier,AutoMinorVer
```

Die Ausgabe dieses Befehls sieht etwa so aus:

```
[
  {
      "DBInstanceIdentifier": "db-t2-medium-instance",
      "DBClusterIdentifier": "cluster-57-2020-06-03-6411",
      "AutoMinorVersionUpgrade": true
  },
  {
      "DBInstanceIdentifier": "db-t2-small-original-size",
      "DBClusterIdentifier": "cluster-57-2020-06-03-6411",
      "AutoMinorVersionUpgrade": false
  },
  {
      "DBInstanceIdentifier": "instance-2020-05-01-2332",
      "DBClusterIdentifier": "cluster-57-2020-05-01-4615",
      "AutoMinorVersionUpgrade": true
  },
... output omitted ...
```

In diesem Beispiel ist die Einstellung Automatisches Nebenversions-Upgrade aktivieren für den DB-Cluster `cluster-57-2020-06-03-6411` deaktiviert, da sie für eine der DB-Instances im Cluster deaktiviert ist.

Verwendung von Zero-Downtime-Patching (Patchen ohne Ausfallzeiten)

Das Durchführen von Upgrades für Aurora MySQL DB-Cluster beinhaltet die Möglichkeit eines Ausfalls, wenn die Datenbank heruntergefahren wird und während sie aktualisiert wird. Wenn Sie das Upgrade starten, während die Datenbank ausgelastet ist, verlieren Sie standardmäßig alle Verbindungen und Transaktionen, die der DB-Cluster verarbeitet. Wenn Sie warten, bis die Datenbank im Leerlauf ist, um das Upgrade durchzuführen, müssen Sie möglicherweise lange warten.

Beim Feature des Patchens ohne Ausfallzeiten (ZDP – Zero-Downtime Patching) wird versucht, Client-Verbindungen auf Best-Effort-Basis vor der Aurora MySQL-Aktualisierung zu bewahren. Wenn das ZDP erfolgreich abgeschlossen wird, werden Anwendungssitzungen bewahrt und die Datenbank-Engine wird während der laufenden Aktualisierung neu gestartet. Der Neustart der Datenbank-Engine kann zu einem Abfall des Durchsatzes von eingen Sekunden bis 1 Minute führen.

ZDP gilt nicht für Folgendes:

- Patches und Upgrades für das Betriebssystem
- Hauptversions-Upgrades

ZDP ist für alle unterstützten Aurora MySQL-Versionen und DB-Instance-Klassen verfügbar.

ZDP wird für Aurora Serverless v1- oder globale Aurora-Datenbanken nicht unterstützt.

> **Note**
>
> Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter Verwendung von T-Instance-Klassen für Entwicklung und Tests.

Sie können Metriken wichtiger Attribute während des ZDP im MySQL-Fehlerprotokoll sehen. Sie können auch Informationen darüber sehen, wann Aurora MySQL ZDP verwendet oder nicht verwendet und zwar auf der Seite Ereignisse der AWS Management Console.

In Aurora MySQL Version 2.10 und höher sowie Version 3 kann Aurora einen Patch ohne Ausfallzeiten ausführen, unabhängig davon, ob die binäre Protokollreplikation aktiviert ist. Wenn die binäre Protokollreplikation aktiviert ist, löscht Aurora MySQL während eines ZDP-Vorgangs automatisch die Verbindung zum Binärprotokollziel. Aurora MySQL stellt automatisch eine Verbindung zum binlog-Ziel her und setzt die Replikation fort, nachdem der Neustart abgeschlossen ist.

Das ZDP arbeitet auch in Kombination mit den Neustartverbesserungen in Aurora MySQL 2.10 und höher. Durch das Patchen der Writer-DB-Instance werden die Leser automatisch gleichzeitig gepatcht. Aurora stellt nach dem Ausführen des Patches die Verbindungen sowohl auf den Writer- als auch der Reader-DB-Instances wieder Vor Aurora MySQL 2.10 gilt das ZDP nur für die Writer-DB-Instance eines Clusters.

ZDP kann unter den folgenden Bedingungen möglicherweise nicht erfolgreich abgeschlossen werden:

- Wenn langandauernde Abfragen oder Transaktionen ausgeführt werden. Wenn Aurora in diesem Fall ZDP durchführen kann, werden alle offenen Transaktionen abgebrochen.
- Es werden Temporäre Tabellen oder Tabellensperren verwendet, beispielsweise während Anweisungen für die Datendefinitionssprache (DDL) ausgeführt werden. Wenn Aurora in diesem Fall ZDP durchführen kann, werden alle offenen Transaktionen abgebrochen.
- Wenn ausstehende Parameteränderungen vorhanden sind.

Wenn sich kein passendes Zeitfenster für die Durchführung von ZDP finden lässt, weil eine dieser Bedingungen vorliegt, wird das Patchen im normalen Modus ausgeführt.

> **Note**
>
> Bei Aurora MySQL Version 2 unter 2.11.0 und Version 3 unter 3.04.0 wird das ZDP möglicherweise nicht erfolgreich abgeschlossen, wenn offene Secure Socket Layer (SSL)- oder Transport Layer Security (TLS)-Verbindungen vorhanden sind.

Obwohl Verbindungen nach einem erfolgreichen ZDP-Vorgang intakt bleiben, werden einige Variablen und Funktionen neu initialisiert. Die folgenden Arten von Informationen werden durch einen Neustart, der durch Patchen ohne Ausfallzeiten verursacht wird, nicht beibehalten:

- Globale Variablen Aurora stellt Sitzungsvariablen wieder her, stellt jedoch nach dem Neustart keine globalen Variablen wieder her.
- Statusvariablen. Insbesondere wird der vom Engine-Status gemeldete Betriebszeit-Wert nach einem Neustart zurückgesetzt, der die ZDR- oder ZDP-Mechanismen verwendet.
- `LAST_INSERT_ID`.
- In-Memory-`auto_increment`-Status für Tabellen. Der Status des automatischen In-Memory-Inkrements wird neu initialisiert. Weitere Informationen zu automatischen Inkrementwerten finden Sie im MySQL-Referenzhandbuch.
- Diagnoseinformationen aus `INFORMATION_SCHEMA`- und `PERFORMANCE_SCHEMA`-Tabellen. Diese Diagnoseinformationen erscheinen auch in der Ausgabe von Befehlen wie `SHOW PROFILE` und `SHOW PROFILES`.

Die folgenden Aktivitäten im Zusammenhang mit einem Neustart ohne Ausfallzeiten werden auf der Seite Ereignisse gemeldet:

- Es wird versucht, die Datenbank ohne Ausfallzeiten zu aktualisieren.
- Der Versuch, die Datenbank ohne Ausfallzeiten zu aktualisieren, ist beendet. Die Veranstaltung berichtet, wie lange der Prozess gedauert hat. Das Ereignis meldet auch, wie viele Verbindungen während des Neustarts beibehalten wurden und wie viele Verbindungen gelöscht wurden. Sie können das Datenbankfehlerprotokoll einsehen, um weitere Details darüber zu erfahren, was während des Neustarts passiert ist.

Alternatives Blau/Grün-Upgradeverfahren

In einigen Situationen ist es Ihre oberste Priorität, eine sofortige Umstellung vom alten auf einen aktualisierten Cluster durchzuführen. In solchen Situationen können Sie einen mehrstufigen Prozess verwenden, der die alten und neuen Cluster ausführt. side-by-side Hier replizieren Sie Daten vom alten auf den neuen Cluster, bis der neuen Cluster zur Übernahme bereit ist. Details hierzu finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

Aktualisieren der Hauptversion eines DB-Clusters von Amazon Aurora MySQL

In einer Aurora MySQL-Versionsnummer wie 2.12.1 steht die 2 für die Hauptversion. Aurora-MySQL-Version 2 ist mit MySQL 5.7 kompatibel. Aurora-MySQL-Version 3 ist mit MySQL 8.0 kompatibel.

Das Upgrade zwischen Hauptversionen erfordert umfangreichere Planung und Tests als für eine Nebenversion. Der Prozess kann beträchtliche Zeit in Anspruch nehmen. Nachdem das Upgrade abgeschlossen ist, müssen Sie möglicherweise auch Follow-up-Arbeiten ausführen. Dies kann beispielsweise aufgrund von Unterschieden in der SQL-Kompatibilität oder der Funktionsweise bestimmter Funktionen im Zusammenhang mit MySQL nötig sein. Oder es kann aufgrund unterschiedlicher Parametereinstellungen zwischen der alten und der neuen Version erforderlich sein.

Inhalt

Upgrade von Aurora MySQL Version 2 auf Version 3

Wenn Sie einen mit MySQL 5.7 kompatiblen Cluster auf einen mit MySQL 8.0 kompatiblen Cluster aktualisieren möchten, führen Sie einen Upgrade-Prozess auf dem Cluster selbst aus. Diese Art von Upgrade ist ein direktes Upgrade im Gegensatz zu Upgrades, die Sie durch die Erstellung eines neuen Clusters durchführen. Diese Technik behält den gleichen Endpunkt und andere Eigenschaften des Clusters bei. Das Upgrade ist relativ schnell, da nicht alle Ihre Daten auf ein neues Cluster-Volume kopiert werden müssen. Diese Stabilität hilft, Konfigurationsänderungen in Ihren Anwendungen zu minimieren. Sie trägt auch dazu bei, die Anzahl der Tests für den aktualisierten Cluster zu reduzieren. Das liegt daran, dass die Anzahl der DB-Instances und ihrer Instance-Klassen gleich bleibt.

Der direkte Upgrade-Mechanismus umfasst das Herunterfahren Ihres DB-Clusters, während der Vorgang ausgeführt wird. Aurora führt ein sauberes Herunterfahren durch und schließt ausstehende Vorgänge wie Transaktions-Rollback und Rückgängig-Bereinigung ab. Weitere Informationen finden Sie unter Funktionsweise des Aurora MySQL direkten Upgrade der Hauptversion.

Die direkte Upgrade-Methode ist praktisch, da sie einfach durchzuführen ist und Konfigurationsänderungen an zugehörigen Anwendungen minimiert. Beispielsweise behält ein

direktes Upgrade die Endpunkte und die Gruppe von DB-Instances für Ihren Cluster bei. Die für ein direktes Upgrade benötigte Zeit kann jedoch je nach den Eigenschaften Ihres Schemas und der Auslastung des Clusters variieren. Je nach den Anforderungen Ihres Clusters können Sie also zwischen den folgenden Upgrade-Techniken wählen:

- Direktes Upgrade
- Einsatz in Blau/Grün
- Snapshot-Wiederherstellung

> **Note**
>
> Wenn Sie die AWS CLI oder RDS-API für die Upgrade-Methode zur Snapshot-Wiederherstellung verwenden, müssen Sie einen nachfolgenden Vorgang ausführen, um eine Writer-DB-Instance im wiederhergestellten DB-Cluster zu erstellen.

Allgemeine Informationen zu Aurora-MySQL-Version 3 und den neuen Funktionen finden Sie unter Aurora mit MySQL Version 3 ist kompatibel mit MySQL 8.0.

Einzelheiten zur Planung eines Upgrades finden Sie unter Planen eines Hauptversionsupgrades für einen Aurora MySQL-Cluster und Erläuterung der Durchführung eines direkten Upgrades.

Planen eines Hauptversionsupgrades für einen Aurora MySQL-Cluster

Um Ihnen bei der Entscheidung über den richtigen Zeitpunkt und die richtige Vorgehensweise für ein Upgrade zu helfen, können Sie sich mit den Unterschieden zwischen Aurora MySQL Version 3 und Ihrer aktuellen Umgebung vertraut machen:

- Wenn Sie von RDS for MySQL 8.0 oder MySQL 8.0 Community Edition konvertieren, finden Sie weitere Informationen unterVergleich von Aurora-MySQL-Version 3 und MySQL 8.0 Community Edition.
- Wenn Sie ein Upgrade von Aurora MySQL Version 2, RDS for MySQL 5.7 oder Community MySQL 5.7 durchführen, finden Sie weitere Informationen unterVergleich von Aurora-MySQL-Version 2 und Aurora-MySQL-Version 3.
- Erstellen Sie neue MySQL 8.0-kompatible Versionen beliebiger benutzerdefinierter Parametergruppen. Wenden Sie alle erforderlichen benutzerdefinierten Parameterwerte auf die neuen Parametergruppen an. Konsultieren Sie Parameteränderungen für Aurora MySQL Version 3, um mehr über Parameteränderungen zu erfahren.

- Überprüfen Sie das Datenbankschema und die Objektdefinitionen für Aurora-MySQL-Version 2 auf die Verwendung neuer reservierter Schlüsselwörter, die in der MySQL 8.0 Community Edition eingeführt wurden. Führen Sie diesen Schritt vor dem Upgrade aus. Weitere Informationen finden Sie unter MySQL 8.0 Neue Schlüsselwörter und reservierte Wörter in der MySQL-Dokumentation.

Weitere MySQL-Spezifische Upgrades und Tipps finden Sie auch unterÄnderungen in MySQL 8.0imMySQL-Referenzhandbuchaus. Sie können beispielsweise den Befehl `mysqlcheck --check-upgrade` verwenden, um Ihre bestehenden Aurora-MySQL-Datenbanken zu analysieren und potenzielle Upgrade-Probleme zu identifizieren.

> **Note**
>
> Wir empfehlen die Verwendung größerer DB-Instance-Klassen beim Upgrade auf Aurora-MySQL-Version 3 mit dem direkten Upgrade oder der Snapshot-Wiederherstellungsmethode. Beispiele sind db.r5.24xlarge und db.r6g.16xlarge. Dadurch kann der Upgrade-Prozess schneller abgeschlossen werden, da der Großteil der verfügbaren CPU-Kapazität auf der DB-Instance genutzt wird. Sie können zu der gewünschten DB-Instance-Klasse wechseln, nachdem das Upgrade der Hauptversion abgeschlossen ist.

Nachdem Sie das Upgrade selbst abgeschlossen haben, können Sie die Verfahren nach dem Upgrade unter Bereinigung nach dem Upgrade für Aurora MySQL Version 3 befolgen. Testen Sie abschließend die Funktionalität und Leistung Ihrer Anwendung.

Wenn Sie von RDS aus MySQL oder Community-MySQL konvertieren, folgen Sie dem unter erläuterten MigrationsverfahrenMigrieren von Daten zu einem Amazon Aurora MySQL-DB-Cluster. In einigen Fällen können Sie die Binärprotokollreplikation verwenden, um Ihre Daten im Rahmen der Migration mit einem Aurora MySQL-Cluster der Version 3 zu synchronisieren. In diesem Fall muss auf dem Quellsystem eine Version ausgeführt werden, die mit Ihrem Ziel-DB-Cluster kompatibel ist.

Damit sichergestellt wird, dass Ihre Anwendungen und Verwaltungsverfahren nach dem Upgrade eines Clusters zwischen Hauptversionen reibungslos funktionieren, führen Sie einige Vorausplanungen und Vorbereitungen durch. Informationen darüber, welche Arten von Verwaltungscode für Ihre AWS CLI Skripts oder auf der RDS-API basierenden Anwendungen aktualisiert werden müssen, finden Sie unter. Wie sich direkte Upgrades auf die Parametergruppen für einen Cluster auswirken Lesen Sie auch Änderungen an Cluster-Eigenschaften zwischen Aurora-MySQL-Versionen.

Informationen zu den Problemen, die während des Upgrades auftreten können, finden Sie unter. Problembehandlung für Aurora MySQL direkte Upgrades Bei Problemen, die dazu führen können, dass das Upgrade sehr lange dauert, können Sie diese Bedingungen im Voraus testen und korrigieren.

> **Note**
>
> Bei einem direkten Upgrade muss Ihr DB-Cluster heruntergefahren werden, während der Vorgang stattfindet. Aurora MySQL führt einen sauberen Shutdown durch und schließt ausstehende Operationen wie das Löschen rückgängig machen ab. Ein Upgrade kann lange dauern, wenn viele Undo-Datensätze gelöscht werden müssen. Wir empfehlen, das Upgrade erst durchzuführen, wenn die Länge der Verlaufsliste (HLL) niedrig ist. Ein allgemein akzeptabler Wert für die HLL ist 100.000 oder weniger. Weitere Informationen finden Sie in diesem Blogbeitrag.

Simulieren Sie das Upgrade, indem Sie Ihren DB-Cluster klonen

Sie können die Anwendungskompatibilität, die Leistung, die Wartungsverfahren und ähnliche Überlegungen für den aktualisierten Cluster überprüfen. Zu diesem Zweck können Sie vor dem eigentlichen Upgrade eine Simulation des Upgrades durchführen. Diese Technik kann besonders für Produktionscluster nützlich sein. Hier ist es wichtig, Ausfallzeiten zu minimieren und den aktualisierten Cluster einsatzbereit zu haben, sobald das Upgrade abgeschlossen ist.

Gehen Sie dazu wie folgt vor:

1. Erstellen Sie einen Klon des ursprünglichen Clusters. Folgen Sie dem Verfahren unter Klonen eines Volumes für einen Amazon-Aurora-DB-Cluster.
2. Richten Sie einen ähnlichen Satz von Writer- und Reader-DB-Instances wie im ursprünglichen Cluster ein.
3. Führen Sie ein direktes Upgrade des geklonten Clusters durch. Folgen Sie dem Verfahren unter Erläuterung der Durchführung eines direkten Upgrades.

   Starten Sie das Upgrade sofort nach dem Erstellen des Klons. Auf diese Weise ist das Cluster-Volume immer noch identisch mit dem Zustand des ursprünglichen Clusters. Wenn der Klon vor dem Upgrade im Leerlauf ist, führt Aurora Datenbankbereinigungsprozesse im Hintergrund durch. In diesem Fall ist das Upgrade des Klons keine genaue Simulation für das Upgrade des ursprünglichen Clusters.

4. Sie können die Anwendungskompatibilität, Performance, Administrationsprozeduren usw. mit dem geklonten Cluster testen.
5. Wenn Probleme auftreten, passen Sie Ihre Upgrade-Pläne an, um sie zu beheben. Passen Sie beispielsweise jeden Anwendungscode so an, dass er mit dem Funktionsumfang der höheren Version kompatibel ist. Sie können abschätzen, wie lange das Upgrade wahrscheinlich auf der Grundlage der Datenmenge in Ihrem Cluster dauern wird. Sie können das Upgrade auch für eine Zeit planen, in der der Cluster nicht ausgelastet ist.
6. Nachdem Sie sich vergewissert haben, dass Ihre Anwendungen und Workload mit dem Testcluster ordnungsgemäß funktionieren, können Sie das direkte Upgrade für Ihren Produktionscluster durchführen.
7. Minimieren Sie möglichst die Gesamtausfallzeit Ihres Clusters während des Upgrades einer Hauptversion. Stellen Sie dazu sicher, dass die Workload auf dem Cluster zum Zeitpunkt des Upgrades niedrig oder Null ist. Stellen Sie insbesondere sicher, dass beim Start des Upgrades keine länger laufenden Transaktionen durchgeführt werden.

Verwenden Sie die blau-grüne Upgrade-Technik

Sie können auch eine blaue/grüne Bereitstellung erstellen, in der die alten und neuen Cluster ausgeführt werden. side-by-side Hier replizieren Sie Daten vom alten auf den neuen Cluster, bis der neuen Cluster zur Übernahme bereit ist. Details hierzu finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

Vorabprüfungen für wichtige Versionsupgrades für Aurora MySQL

MySQL 8.0 ist in vielen Punkten nicht mit MySQL 5.7 kompatibel. Diese Inkompatibilitäten können bei einem Upgrade von Aurora MySQL Version 2 auf Version 3 zu Problemen führen. Möglicherweise sind einige Vorbereitungen für Ihre Datenbank erforderlich, damit das Upgrade erfolgreich ist.

Wenn Sie ein Upgrade von Aurora MySQL Version 2 auf Version 3 starten, führt Amazon Aurora automatisch Vorabprüfungen durch, um diese Inkompatibilitäten zu erkennen.

Diese Vorabprüfungen müssen durchgeführt werden. Sie können nicht ausgelassen werden. Die Vorabprüfungen bieten folgende Vorteile:

- Sie können ungeplante Ausfallzeiten während des Upgrades vermeiden.
- Wenn es Inkompatibilitäten gibt, verhindert Amazon Aurora das Upgrade und stellt Ihnen ein Protokoll zur Verfügung, in dem Sie mehr darüber erfahren können. Anschließend können Sie das Protokoll verwenden, um Ihre Datenbank auf das Upgrade auf Version 3 vorzubereiten, indem Sie

die Inkompatibilitäten reduzieren. Detaillierte Informationen zum Entfernen von Inkompatibilitäten finden Sie unter Vorbereiten Ihrer Installation auf ein Upgrade in der MySQL-Dokumentation und unter Upgrade auf MySQL 8.0? Dies müssen Sie wissen ... im MySQL Server Blog.

Weitere Informationen zum Upgrade auf MySQL 8.0 finden Sie unter Upgrade von MySQL in der MySQL-Dokumentation.

Zu den Vorabprüfungen gehören einige, die in MySQL enthalten sind, und einige, die speziell vom Aurora-Team erstellt wurden. Informationen zu den von MySQL bereitgestellten Vorabprüfungen finden Sie unter Upgrade Checker-Dienstprogramm.

Die Vorabprüfungen werden ausgeführt, bevor die DB-Instance aufgrund des Upgrades angehalten wird. Sie verursachen also keine Ausfallzeiten. Wenn bei den Vorprüfungen eine Inkompatibilität festgestellt wird, bricht Aurora das Upgrade automatisch ab, bevor die DB-Instance gestoppt wird. Aurora generiert auch ein Ereignis für die Inkompatibilität. Weitere Informationen zu Amazon Aurora Aurora-Veranstaltungen finden Sie unterArbeiten mit Amazon-RDS-Ereignisbenachrichtigungen.

Aurora zeichnet detaillierte Informationen zu jeder Inkompatibilität in der Protokolldatei `PrePatchCompatibility.log` auf. In den meisten Fällen enthalten die Protokolleinträge einen Link zur MySQL-Dokumentation mit Informationen zur Lösung des Inkompatibilitätsproblems. Weitere Informationen zum Anzeigen von Protokolldateien finden Sie unter Anzeigen und Auflisten von Datenbank-Protokolldateien.

Aufgrund der Art der Vorabprüfungen werden die Objekte in Ihrer Datenbank geprüft. Diese Analyse verbraucht Ressourcen und verlängert die Zeit, die für die Durchführung des Upgrades benötigt wird.

Community-MySQL-Upgrade-Vorprüfungen

Im Folgenden finden Sie eine allgemeine Liste der Inkompatibilitäten zwischen MySQL 5.7 und 8.0:

- Ihr MySQL 5.7-kompatibler DB-Cluster darf keine Funktionen verwenden, die in MySQL 8.0 nicht unterstützt werden.

  Weitere Informationen finden Sie unter In MySQL 8.0 entfernte Funktionen in der MySQL-Dokumentation.
- Es darf keine Verletzungen von Schlüsselwörtern oder reservierten Wörtern geben. Einige Schlüsselwörter sind in MySQL 8.0 möglicherweise reserviert, die zuvor nicht reserviert waren.

  Weitere Informationen finden Sie unter Schlüsselwörter und reservierte Wörter in der MySQL-Dokumentation.

- Um die Unicode-Unterstützung zu verbessern, sollten Sie die Konvertierung von Objekten, die den `utf8mb3`-Zeichensatz verwenden, in Objekte in Betracht ziehen, die den `utf8mb4`-Zeichensatz verwenden. Der `utf8mb3`-Zeichensatz ist veraltet. Sie sollten darüber hinaus anstelle von `utf8mb4` die Verwendung von `utf8` für Zeichensatzverweise in Betracht ziehen, da `utf8` zurzeit ein Alias für den `utf8mb3`-Zeichensatz ist.

  Weitere Informationen finden Sie unter Der utf8mb3-Zeichensatz (UTF-8-Unicode-Kodierung mit 3 Bytes) in der MySQL-Dokumentation.
- Es darf keine InnoDB-Tabellen mit einem nicht standardmäßigen Zeilenformat geben.
- Es dürfen keine Attribute vom Typ `display` Länge `ZEROFILL` oder Länge vorhanden sein.
- Es darf keine partitionierte Tabelle mit einer Speicher-Engine geben, für die es keine native Partitionierungsunterstützung gibt.
- Es darf keine Tabellen in der MySQL 5.7 `mysql`-Systemdatenbank geben, die denselben Namen wie eine Tabelle haben, die vom MySQL 8.0-Daten-Dictionary verwendet wird.
- Es darf keine Tabellen geben, die veraltete Datentypen oder Funktionen verwenden.
- Es darf keine Namen für Fremdschlüsseleinschränkungen mit mehr als 64 Zeichen geben.
- Es dürfen keine veralteten SQL-Modi in Ihrer `sql_mode`-Systemvariableneinstellung definiert sein.
- Es dürfen keine Tabellen oder gespeicherten Prozeduren mit einzelnen Elementen `ENUM` oder `SET` Spaltenelementen mit einer Länge von mehr als 255 Zeichen vorhanden sein.
- Es darf keine Tabellenpartitionen geben, die sich in gemeinsam genutzten InnoDB-Tablespaces befinden.
- Die Pfade der Tablespace-Datendateien dürfen keine Zirkelverweise enthalten.
- Es dürfen keine Abfragen und gespeicherten Programmdefinitionen vorhanden sein, die Klauseln `ASC` oder `DESC` Kennzeichner verwenden. `GROUP BY`
- Es dürfen keine Systemvariablen entfernt werden, und Systemvariablen müssen die neuen Standardwerte für MySQL 8.0 verwenden.
- Es dürfen keine Werte für Datum, Uhrzeit oder Zeitstempel mit Null (`0`) vorhanden sein.
- Es dürfen keine Schemainkonsistenzen vorliegen, die auf das Entfernen oder Korrumpieren von Dateien zurückzuführen sind.
- Es darf keine Tabellennamen geben, die die `FTS` Zeichenfolge enthalten.
- Es darf keine InnoDB-Tabellen geben, die zu einer anderen Engine gehören.
- Es darf keine Tabellen- oder Schemanamen geben, die für MySQL 5.7 ungültig sind.

Weitere Informationen zum Upgrade auf MySQL 8.0 finden Sie unter Upgrade von MySQL in der MySQL-Dokumentation.

Vorabprüfungen für das Aurora MySQL-Upgrade

Aurora MySQL hat seine eigenen spezifischen Anforderungen beim Upgrade von Version 2 auf Version 3:

- In Ansichten, Routinen, Triggern und `QUERY_CACHE` Ereignissen darf keine veraltete SQL-Syntax wie`SQL_CACHE`,, und vorkommen. `SQL_NO_CACHE`
- In keiner Tabelle ohne den Index darf eine `FTS_DOC_ID` Spalte vorhanden sein. `FTS`
- Es darf keine Diskrepanz der Spaltendefinition zwischen dem InnoDB-Datenwörterbuch und der tatsächlichen Tabellendefinition geben.
- Alle Datenbank- und Tabellennamen müssen in Kleinbuchstaben geschrieben werden, wenn der `lower_case_table_names` Parameter auf gesetzt ist. `1`
- Ereignisse und Trigger dürfen keinen fehlenden oder leeren Definer oder einen ungültigen Erstellungskontext haben.
- Alle Triggernamen in einer Datenbank müssen eindeutig sein.
- DDL-Wiederherstellung und Fast DDL werden in Aurora MySQL Version 3 nicht unterstützt. Datenbanken dürfen keine Artefakte enthalten, die sich auf diese Funktionen beziehen.
- Tabellen mit dem `COMPACT` Zeilenformat `REDUNDANT` oder dürfen keine Indizes haben, die größer als 767 Byte sind.
- Die Präfixlänge von Indizes, die für `tiny` Textspalten definiert sind, darf 255 Byte nicht überschreiten. Mit dem `utf8mb4` Zeichensatz wird dadurch die unterstützte Präfixlänge auf 63 Zeichen begrenzt.

  Eine größere Präfixlänge war in MySQL 5.7 unter Verwendung des `innodb_large_prefix` Parameters zulässig. Dieser Parameter ist in MySQL 8.0 veraltet.
- Die Tabelle darf keine Inkonsistenzen der InnoDB-Metadaten enthalten. `mysql.host`
- In den Systemtabellen darf es keine Diskrepanz zwischen den Spaltendatentypen geben.
- In dem `prepared` Bundesstaat dürfen keine XA-Transaktionen stattfinden.
- Spaltennamen in Ansichten dürfen nicht länger als 64 Zeichen sein.
- Sonderzeichen in gespeicherten Prozeduren dürfen nicht inkonsistent sein.
- Tabellen dürfen keine inkonsistenten Datendateipfade aufweisen.

Aurora MySQL Upgrade-Vorgang für die Hauptversion

Nicht alle Arten oder Versionen von Aurora MySQL Clustern können den integrierten Upgrade-Mechanismus verwenden. Sie können den geeigneten Upgrade-Pfad für jeden Aurora MySQL-Cluster finden, indem Sie die folgende Tabelle konsultieren.

Typ des Aurora MySQL-DB-Clusters	Kann ein direktes Upgrade verwende werden?	Aktion
Aurora MySQL bereitgestellter Cluster, 2.0 oder höher	Ja	Das direkte Upgrade wird für 5.7-kompatible Aurora-MySQL-Cluster unterstützt. Informationen zum Upgrade auf Aurora-MySQL-Version 3 finden Sie unter Planen eines Hauptversionsupgrades für einen Aurora MySQL-Cluster und Erläuterung der Durchführung eines direkten Upgrades.
Von Aurora MySQL bereitgestellter Cluster, 3.01.0 oder höher	N/A	Verwenden Sie ein Upgrade-Verfahren für Nebenversionen, um ein Upgrade zwischen Versionen von Aurora-MySQL-Version 3 durchzuführen.
Aurora Serverless v1-Cluster	N/A	Derzeit Aurora Serverless v1 wird Aurora MySQL nur in Version 2 unterstützt.
Aurora Serverless v2-Cluster	N/A	Zurzeit wird Aurora Serverless v2 für Aurora MySQL nur auf Version 3 unterstützt.
Cluster in einer Aurora globalen Datenbank	Ja	Wenn Sie Aurora-MySQL-Version 2 zu Version 3 aktualisieren möchten, folgen Sie den Anweisungen für ein direktes Upgrade für Cluster in einer globalen Aurora-Datenbank. Führen Sie das Upgrade auf dem globalen Cluster durch. Aurora aktualisiert den primären Cluster und alle sekundären Cluster in der globalen Datenbank gleichzeitig.

Typ des Aurora MySQL-DB-Clusters	Kann ein direktes Upgrade verwende werden?	Aktion
		Wenn Sie die AWS CLI oder RDS-API verwenden, rufen Sie den `modify-global-cluster` Befehl oder die `ModifyGlobalCluster` Operation anstelle von `modify-db-cluster` oder auf`ModifyDBCluster` . Sie können kein direktes Upgrade von Aurora-My SQL-Version 2 zu Version 3 durchführen, wenn der `lower_case_table_names` -Parameter aktiviert ist. Weitere Informationen finden Sie unter Hauptversions-Upgrades.
Paralleler Abfrage-Cluster	Ja	Sie können ein direktes Upgrade durchführen. In diesem Fall wählen Sie 2.09.1 oder höher für die Aurora MySQL Version.
Cluster, der das Ziel der binären Protokollreplikation ist	Vielleicht	Wenn die binäre Protokollreplikation von einem Aurora-MySQL-Cluster stammt, können Sie ein direktes Upgrade durchführen. Sie können das Upgrade nicht durchführen, wenn die binäre Protokollreplikation von einer RDS-for-MySQL- oder einer On-Premises MySQL-DB-Instance stammt. In diesem Fall können Sie ein Upgrade mit dem Snapshot-Wiederherstellungs mechanismus durchführen.

Typ des Aurora MySQL-DB-Clusters	Kann ein direktes Upgrade verwende werden?	Aktion
Cluster mit Null DB-Instan ces	Nein	Mit der AWS CLI oder der RDS-API können Sie einen Aurora MySQL-Cluster ohne angehängte DB-Instan ces erstellen. Auf die gleiche Weise können Sie auch alle DB-Instances aus einem Aurora MySQL-Cluster entfernen, während die Daten im Cluster-Volume intakt bleiben. Während ein Cluster keine DB-Instances hat, können Sie kein direktes Upgrade durchführen. Der Upgrade-Mechanismus erfordert eine Writer-In stance im Cluster, um Conversions für die Systemtab ellen, Datendateien usw. durchzuführen. Verwenden Sie in diesem Fall die AWS CLI oder die RDS-API, um eine Writer-Instance für den Cluster zu erstellen. Dann können Sie ein direktes Upgrade durchführen.
Cluster mit aktivierter Rückverfolgung	Ja	Sie können ein direktes Upgrade für einen Aurora MySQL Cluster durchführen, der die Funktion Rückverfo lgung verwendet. Nach dem Upgrade können Sie den Cluster jedoch nicht auf einen Zeitpunkt vor dem Upgrade zurückverfolgen.

Funktionsweise des Aurora MySQL direkten Upgrade der Hauptversion

Aurora MySQL führt das Upgrade einer Hauptversion als mehrstufigen Prozess durch. Sie können den aktuellen Status eines Upgrades überprüfen. Einige der Upgrade-Schritte enthalten auch Fortschrittsinformationen. Beim Start jeder Phase, zeichnet Aurora MySQL ein Ereignis auf. Sie können Ereignisse so untersuchen, wenn sie auf der Seite Ereignisse in der RDS-Konsole auftreten. Weitere Informationen zur Arbeit mit -Ereignissen finden Sie unter Arbeiten mit Amazon-RDS-Ereignisbenachrichtigungen.

> **Important**
>
> Sobald der Prozess beginnt, wird er ausgeführt, bis das Upgrade erfolgreich ist oder fehlschlägt. Sie können das Upgrade nicht abbrechen, während es läuft. Wenn das Upgrade fehlschlägt, setzt Aurora alle Änderungen zurück und Ihr Cluster hat die gleiche Engine-Version, Metadaten usw. wie zuvor.

Der Upgrade-Prozess besteht aus drei Schritten:

1. Aurora führt vor Beginn des Upgrade-Vorgangs eine Reihe von Vorprüfungen durch. Ihr Cluster läuft weiter, während Aurora diese Prüfungen durchführt. Zum Beispiel kann der Cluster keine XA-Transaktionen im vorbereiteten Zustand haben oder irgendwelche DDL-Anweisungen (Data Definition Language) verarbeiten. Beispielsweise müssen Sie möglicherweise Anwendungen herunterfahren, die bestimmte Arten von SQL-Anweisungen einreichen. Oder Sie könnten einfach warten, bis bestimmte lang andauernde Anweisungen beendet sind. Versuchen Sie dann erneut das Upgrade durchzuführen. Einige Prüfungen testen auf Bedingungen, die das Upgrade nicht verhindern, aber dazu führen können, dass das Upgrade möglicherweise länger dauert.

   Wenn Aurora feststellt, dass die erforderlichen Bedingungen nicht erfüllt sind, ändern Sie die in den Ereignisdetails angegebenen Bedingungen. Befolgen Sie die Anweisungen unter Problembehandlung für Aurora MySQL direkte Upgrades. Wenn Aurora Bedingungen erkennt, die ein langsames Upgrade verursachen könnten, planen Sie ein, das Upgrade über einen längeren Zeitraum zu überwachen.
2. Aurora nimmt Ihren Cluster offline. Aurora führt dann ähnliche Tests wie in der vorherigen Phase durch, um zu bestätigen, dass während des Shutdown-Vorgangs keine neuen Probleme aufgetreten sind. Wenn Aurora zu diesem Zeitpunkt Bedingungen erkennt, die das Upgrade verhindern würden, bricht Aurora das Upgrade ab und bringt den Cluster wieder online. Bestätigen Sie in diesem Fall, wenn die Bedingungen nicht mehr gelten, und starten Sie das Upgrade erneut.
3. Aurora erstellt einen Snapshot Ihres Cluster-Volumes. Stellen Sie sich vor, Sie stellen nach Abschluss des Upgrades Kompatibilitäts- oder andere Probleme fest. Oder angenommen, Sie möchten Tests sowohl mit den ursprünglichen als auch mit den aktualisierten Clustern durchführen. In solchen Fällen können Sie aus diesem Snapshot den Cluster wiederherstellen, um einen neuen Cluster mit der ursprünglichen Engine-Version und den ursprünglichen Daten zu erstellen.

> **Tip**
>
> Dieser Snapshot ist ein manueller Snapshot. Aurora kann den Snapshot jedoch erstellen und den Upgrade-Prozess fortsetzen, auch wenn Sie Ihr Limit für manuelle Snapshots erreicht haben. Dieser Snapshot bleibt dauerhaft (falls erforderlich) erhalten, bis Sie ihn löschen. Nachdem Sie alle Tests nach dem Upgrade abgeschlossen haben, können Sie diesen Snapshot löschen, um die Speicherkosten zu minimieren.

4. Aurora klont Ihr Cluster-Volume. Das Klonen ist ein schneller Vorgang, bei dem die tatsächlichen Tabellendaten nicht kopiert werden müssen. Wenn Aurora während des Upgrades ein Problem feststellt, werden die Originaldaten des geklonten Cluster-Volumes zurückgesetzt und der Cluster wieder online gebracht. Das temporär geklonte Volume während des Upgrades unterliegt nicht dem üblichen Limit für die Anzahl der Klone für ein einzelnes Cluster-Volume.
5. Aurora führt ein sauberes Herunterfahren für die Writer-DB-Instance durch. Während des sauberen Herunterfahrens werden Fortschrittsereignisse alle 15 Minuten für die folgenden Vorgänge aufgezeichnet. Sie können Ereignisse so untersuchen, wenn sie auf der Seite Ereignisse in der RDS-Konsole auftreten.
   - Aurora bereinigt die Undo-Datensätze für alte Versionen von Zeilen.
   - Aurora setzt alle nicht festgeschriebenen Transaktionen zurück.
6. Aurora aktualisiert die Engine-Version auf der Writer-DB-Instance:
   - Aurora installiert die Binärdatei für die neue Engine-Version auf der Writer-DB-Instance.
   - Aurora verwendet die Writer-DB-Instance, um Ihre Daten auf das mit MySQL 5.7-kompatible Format zu aktualisieren. In dieser Phase ändert Aurora die Systemtabellen und führt andere Konvertierungen durch, die sich auf die Daten in Ihrem Cluster-Volume auswirken. Insbesondere Aurora aktualisiert die Partitions-Metadaten in den Systemtabellen, um mit dem Partitionsformat MySQL 5.7 kompatibel zu sein. Diese Phase kann lange dauern, wenn die Tabellen in Ihrem Cluster eine große Anzahl von Partitionen haben.

     Wenn während dieser Phase Fehler auftreten, finden Sie die Details in den MySQL-Fehlerprotokollen. Wenn diese Phase nach dem Start der Upgradevorgang aus irgendeinem Grund fehlschlägt, stellt Aurora die Originaldaten aus dem geklonten Cluster-Volume wieder her.
7. Aurora aktualisiert die Engine-Version auf den Reader-DB-Instances.
8. Der Upgrade-Vorgang ist abgeschlossen. Aurora zeichnet ein letztes Ereignis auf, um anzuzeigen, dass der Upgrade-Prozess erfolgreich abgeschlossen wurde. Jetzt läuft Ihr DB-Cluster mit der neuen Hauptversion.

Blau/Grün-Bereitstellungen

In einigen Situationen ist es Ihre oberste Priorität, eine sofortige Umstellung vom alten auf einen aktualisierten Cluster durchzuführen. In solchen Situationen können Sie einen mehrstufigen Prozess verwenden, bei dem der alte und der neue Cluster side-by-side ausgeführt werden. Hier replizieren Sie Daten vom alten auf den neuen Cluster, bis der neuen Cluster zur Übernahme bereit ist. Details hierzu finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

Erläuterung der Durchführung eines direkten Upgrades

Sehen Sie sich die Hintergrundinformationen unter Funktionsweise des Aurora MySQL direkten Upgrade der Hauptversion an.

Führen Sie alle Planungen und Tests vor dem Upgrade durch, wie unter beschrieben. Planen eines Hauptversionsupgrades für einen Aurora MySQL-Cluster

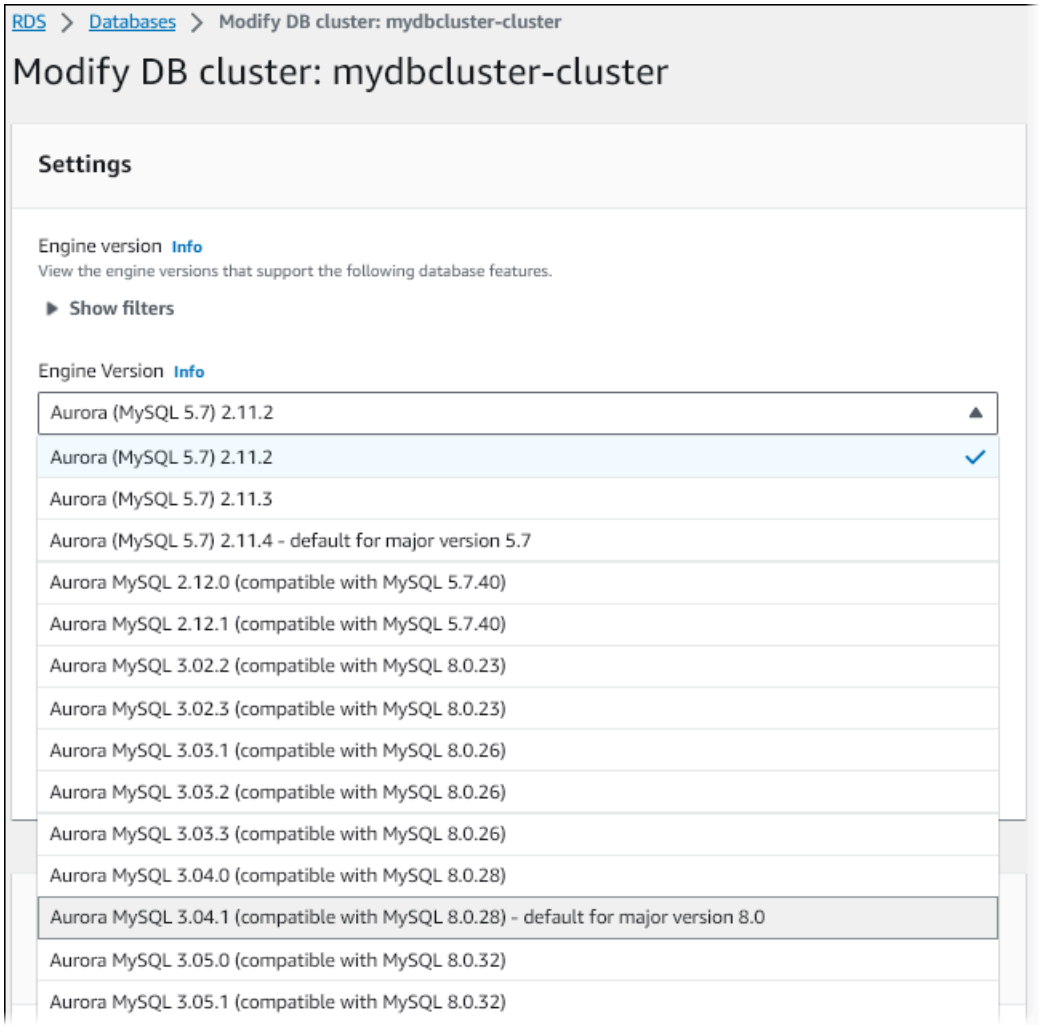
Konsole

Im folgenden Beispiel wird der `mydbcluster-cluster` DB-Cluster auf Aurora MySQL Version 3.04.1 aktualisiert.

Aktualisieren der Hauptversion eines Aurora MySQL-DB-Clusters

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wenn Sie eine benutzerdefinierte Parametergruppe für den ursprünglichen DB-Cluster verwendet haben, erstellen Sie eine entsprechende Parametergruppe, die mit der neuen Hauptversion kompatibel ist. Nehmen Sie alle erforderlichen Anpassungen an den Konfigurationsparametern in dieser neuen Parametergruppe vor. Weitere Informationen finden Sie unter Wie sich direkte Upgrades auf die Parametergruppen für einen Cluster auswirken.
3. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
4. Wählen Sie den DB-Cluster aus, den Sie ändern möchten.
5. Wählen Sie Ändern aus.
6. Wählen Sie unter Version eine neue Aurora-MySQL-Hauptversion aus.

   Wir empfehlen im Allgemeinen, die neueste Nebenversion der Hauptversion zu verwenden. Hier wählen wir die aktuelle Standardversion.



7. Klicken Sie auf Weiter.
8. Geben Sie auf der nächsten Seite an, wann das Upgrade durchgeführt werden soll. Wählen Sie During the next scheduled maintenance window (Während des nächsten geplanten Wartungsfensters) oder Sofort aus.
9. (Optional) Überprüfen Sie während des Upgrades regelmäßig die Seite Ereignisse in der RDS-Konsole. Auf diese Weise können Sie den Fortschritt des Upgrades überwachen und etwaige Probleme erkennen. Wenn das Upgrade auf Probleme stößt, lesen Sie Problembehandlung für Aurora MySQL direkte Upgrades für zu ergreifende Schritte.
10. Wenn Sie zu Beginn dieses Vorgangs eine neue Parametergruppe erstellt haben, ordnen Sie die benutzerdefinierte Parametergruppe Ihrem aktualisierten Cluster zu. Weitere Informationen finden Sie unter Wie sich direkte Upgrades auf die Parametergruppen für einen Cluster auswirken.

> **Note**
>
> Wenn Sie diesen Schritt ausführen, müssen Sie den Cluster erneut neu starten, um die neue Parametergruppe anzuwenden.

11. (Optional) Löschen Sie nach dem Upgrade den manuellen Snapshot, den Aurora zu Beginn des Upgrades erstellt hat.

AWS CLI

Um die Hauptversion eines Aurora MySQL-DB-Clusters zu aktualisieren, verwenden Sie den Befehl AWS CLI modify-db-cluster mit den folgenden erforderlichen Parametern:

- `--db-cluster-identifier`
- `--engine-version`
- `--allow-major-version-upgrade`
- `--apply-immediately` oder `--no-apply-immediately`

Wenn Ihr Cluster benutzerdefinierte Parametergruppen verwendet, schließen Sie auch eine oder beide der folgenden Optionen ein:

- `--db-cluster-parameter-group-name`, wenn der Cluster eine benutzerdefinierte Cluster-Parametergruppe verwendet
- `--db-instance-parameter-group-name`, falls Instances im Cluster eine benutzerdefinierte DB-Parametergruppe verwenden

Im folgenden Beispiel wird der `sample-cluster` DB-Cluster auf Aurora MySQL Version 3.04.1 aktualisiert. Das Upgrade erfolgt sofort, anstatt auf das nächste Wartungsfenster zu warten.

Example

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
          --db-cluster-identifier sample-cluster \
          --engine-version 8.0.mysql_aurora.3.04.1 \
          --allow-major-version-upgrade \
```

```
          --apply-immediately
```

Windows:

```
aws rds modify-db-cluster ^
          --db-cluster-identifier sample-cluster ^
          --engine-version 8.0.mysql_aurora.3.04.1 ^
          --allow-major-version-upgrade ^
          --apply-immediately
```

Sie können andere CLI-Befehle mit kombinieren`modify-db-cluster`, um einen automatisierten end-to-end Prozess für die Durchführung und Überprüfung von Upgrades zu erstellen. Weitere Informationen und Beispiele finden Sie unter Aurora MySQL direktes Upgrade.

> **Note**
>
> Wenn Ihr Cluster Teil einer Aurora globalen Datenbank ist, unterscheidet sich das Verfahren des direkten Upgrades geringfügig. Sie rufen die Befehlsoperation modify-global-cluster statt `modify-db-cluster` auf. Weitere Informationen finden Sie unter In-Situ-Hauptversions-Upgrades für globale Datenbanken.

RDS-API

Verwenden Sie zum Aktualisieren der Hauptversion eines DB-Clusters von Aurora MySQL die RDS-API-Operation ModifyDBCluster mit den folgenden erforderlichen Parametern:

- `DBClusterIdentifier`
- `Engine`
- `EngineVersion`
- `AllowMajorVersionUpgrade`
- `ApplyImmediately` (festgelegt auf `true` oder `false`)

> **Note**
>
> Wenn Ihr Cluster Teil einer Aurora globalen Datenbank ist, unterscheidet sich das Verfahren des direkten Upgrades geringfügig. Stattdessen rufen Sie den ModifyGlobalCluster-Vorgang

auf. `ModifyDBCluster` Weitere Informationen finden Sie unter In-Situ-Hauptversions-Upgrades für globale Datenbanken.

Wie sich direkte Upgrades auf die Parametergruppen für einen Cluster auswirken

Aurora-Parametergruppen haben verschiedene Sätze von Konfigurationseinstellungen für Cluster, die mit MySQL 5.7 oder 8.0 kompatibel sind. Wenn Sie ein direktes Upgrade durchführen, müssen der aktualisierte Cluster und alle seine Instances die entsprechenden Cluster- und Instance-Parametergruppen verwenden:

Ihr Cluster und Ihre Instances verwenden möglicherweise die standardmäßigen 5.7-kompatiblen Parametergruppen. In diesem Fall beginnen der aktualisierte Cluster und die Instance mit den standardmäßigen 8.0-kompatiblen Parametergruppen. Wenn Ihr Cluster und Ihre Instances benutzerdefinierte Parametergruppen verwenden, müssen Sie entsprechende oder 8.0-kompatible Parametergruppen erstellen. Diese müssen während des Upgrade-Vorgangs angegeben werden.

Note

Für die meisten Parametereinstellungen können Sie die benutzerdefinierte Parametergruppe an zwei Stellen auswählen. Und zwar können Sie sie auswählen, wenn Sie den Cluster erstellen oder wenn Sie die Parametergruppe später dem Cluster zuordnen.
Wenn Sie jedoch eine nicht standardmäßige Einstellung für den Parameter `lower_case_table_names` verwenden, müssen Sie die benutzerdefinierte Parametergruppe mit dieser Einstellung im Voraus einrichten. Geben Sie dann die Parametergruppe an, wenn Sie die Snapshot-Wiederherstellung zum Erstellen des Clusters durchführen. Änderungen des `lower_case_table_names`-Parameters haben keine Auswirkung, nachdem der Cluster erstellt wurde.
Wir empfehlen Ihnen, die gleiche Einstellung für `lower_case_table_names` zu verwenden, wenn Sie ein Upgrade von Aurora MySQL Version 2 auf Version 3 durchführen.
Bei einer auf Aurora MySQL basierenden globalen Aurora-Datenbank, können Sie kein direktes Upgrade von Aurora-MySQL-Version 2 auf Version 3 durchführen, wenn der Parameter `lower_case_table_names` aktiviert ist. Weitere Informationen zu den möglichen Verfahren finden Sie unter Hauptversions-Upgrades.

> **Important**
>
> Wenn Sie während des Upgrade-Vorgangs eine benutzerdefinierte Parametergruppe angeben, müssen Sie den Cluster nach Abschluss des Upgrades unbedingt manuell neu starten. Danach nutzt der Cluster Ihre benutzerdefinierten Parametereinstellungen.

Änderungen an Cluster-Eigenschaften zwischen Aurora-MySQL-Versionen

Wenn Sie von Aurora-MySQL-Version 2 zu Version 3 aktualisieren, stellen Sie sicher, dass Sie alle Anwendungen oder Skripts ändern, die Sie zum Einrichten oder Verwalten von Clustern und DB-Instances von Aurora MySQL verwenden.

Ändern Sie außerdem Ihren Code, der Parametergruppen manipuliert, um der Tatsache Rechnung zu tragen, dass die Standardnamen der Parametergruppen für 5.7- und 8.0-kompatible Cluster unterschiedlich sind. Die entsprechenden Parametergruppennamen für Aurora-MySQL-Version 2 und 3-Cluster sind `default.aurora-mysql5.7` und `default.aurora-mysql8.0`.

Beispielsweise haben Sie möglicherweise Code wie den folgenden, der vor einem Upgrade für Ihren Cluster gilt.

```
# Check the default parameter values for MySQL 5.7-compatible clusters.
aws rds describe-db-parameters --db-parameter-group-name default.aurora-mysql5.7 --
region us-east-1
```

Ändern Sie nach dem Upgrade der Hauptversion des Clusters diesen Code wie folgt.

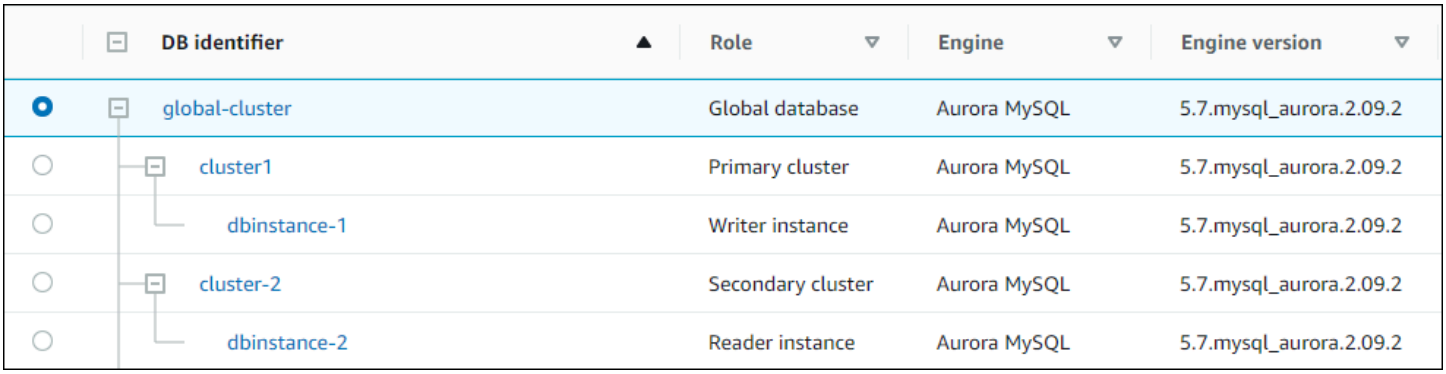
```
# Check the default parameter values for MySQL 8.0-compatible clusters.
aws rds describe-db-parameters --db-parameter-group-name default.aurora-mysql8.0 --
region us-east-1
```

In-Situ-Hauptversions-Upgrades für globale Datenbanken

Bei einer globalen Aurora-Datenbank aktualisieren Sie den globalen Datenbank-Cluster. Aurora aktualisiert automatisch alle Cluster gleichzeitig und stellt sicher, dass sie alle dieselbe Engine-Version ausführen. Diese Anforderung liegt darin begründet, dass Änderungen an Systemtabellen, Datendateiformaten usw. automatisch auf alle sekundären Cluster repliziert werden.

Folgen Sie den Anweisungen in Funktionsweise des Aurora MySQL direkten Upgrade der Hauptversion. Wenn Sie angeben, was aktualisiert werden soll, stellen Sie sicher, dass Sie den globalen Datenbank-Cluster anstelle eines der darin enthaltenen Cluster auswählen.

Wenn Sie das verwenden AWS Management Console, wählen Sie das Element mit der Rolle Globale Datenbank.



DB identifier	Role	Engine	Engine version
global-cluster	Global database	Aurora MySQL	5.7.mysql_aurora.2.09.2
cluster1	Primary cluster	Aurora MySQL	5.7.mysql_aurora.2.09.2
dbinstance-1	Writer instance	Aurora MySQL	5.7.mysql_aurora.2.09.2
cluster-2	Secondary cluster	Aurora MySQL	5.7.mysql_aurora.2.09.2
dbinstance-2	Reader instance	Aurora MySQL	5.7.mysql_aurora.2.09.2

Wenn Sie die AWS CLI oder die RDS-API verwenden, starten Sie den Upgrade-Vorgang, indem Sie den Befehl modify-global-cluster oder den Cluster-Vorgang aufrufen. ModifyGlobal Verwenden Sie diese anstelle von `modify-db-cluster` oder `ModifyDBCluster`.

> **Note**
>
> Sie können keine benutzerdefinierte Parametergruppe für den globalen Datenbank-Cluster angeben, während Sie ein größeres Versions-Upgrade dieser globalen Aurora-Datenbank durchführen. Erstellen Sie Ihre benutzerdefinierten Parametergruppen in jeder Region des globalen Clusters. Wenden Sie sie nach dem Upgrade manuell auf die regionalen Cluster an.

Um die Hauptversion eines globalen Aurora MySQL-Datenbank-Clusters mithilfe von zu aktualisieren AWS CLI, verwenden Sie den Befehl modify-global-cluster mit den folgenden erforderlichen Parametern:

- `--global-cluster-identifier`
- `--engine aurora-mysql`
- `--engine-version`
- `--allow-major-version-upgrade`

Im folgenden Beispiel wird der globale Datenbank-Cluster auf Aurora-MySQL-Version 2.10.2 aktualisiert.

Example

Für, oder: Linux macOS Unix

```
aws rds modify-global-cluster \
          --global-cluster-identifier global_cluster_identifier \
          --engine aurora-mysql \
          --engine-version 5.7.mysql_aurora.2.10.2 \
          --allow-major-version-upgrade
```

Windows:

```
aws rds modify-global-cluster ^
          --global-cluster-identifier global_cluster_identifier ^
          --engine aurora-mysql ^
          --engine-version 5.7.mysql_aurora.2.10.2 ^
          --allow-major-version-upgrade
```

Überlegungen zurückverfolgen

Wenn für den von Ihnen aktualisierten Cluster die Rückverfolgungsfunktion aktiviert war, können Sie den aktualisierten Cluster nicht auf einen Zeitpunkt vor dem Upgrade zurückverfolgen.

Aurora MySQL direktes Upgrade

Die folgenden Linux-Beispiele zeigen, wie Sie die allgemeinen Schritte des Verfahrens für ein direktes Upgrade mit dem durchführen können AWS CLI.

In diesem ersten Beispiel wird ein Aurora-DB-Cluster erstellt, auf dem eine 2.x-Version von Aurora MySQL ausgeführt wird. Der Cluster enthält eine Writer-DB-Instance und eine Reader-DB-Instance Der Befehl `wait db-instance-available` pausiert, bis die Writer-DB-Instanz verfügbar ist. Das ist der Punkt, an dem der Cluster für ein Upgrade bereit ist.

```
aws rds create-db-cluster --db-cluster-identifier mynewdbcluster --engine aurora-mysql
 \
  --db-cluster-version 5.7.mysql_aurora.2.10.2
...
```

```
aws rds create-db-instance --db-instance-identifier mynewdbcluster-instance1 \
  --db-cluster-identifier mynewdbcluster --db-instance-class db.t4g.medium --engine
 aurora-mysql
...
aws rds wait db-instance-available --db-instance-identifier mynewdbcluster-instance1
```

Die Aurora MySQL 3.x-Versionen, auf die Sie den Cluster aktualisieren können, hängen von der 2.x-Version ab, auf der der Cluster derzeit ausgeführt wird, und davon, AWS-Region wo sich der Cluster befindet. Der erste Befehl mit `--output text` zeigt nur die verfügbare Zielversion an. Der zweite Befehl zeigt die vollständige JSON-Ausgabe der Antwort an. Diese Antwort enthält Details wie den `aurora-mysql`-Wert, den Sie für den `engine`-Parameter verwenden. Sie können auch sehen, dass ein Upgrade auf 3.02.0 ein Hauptversions-Upgrade darstellt.

```
aws rds describe-db-clusters --db-cluster-identifier mynewdbcluster \
  --query '*[].{EngineVersion:EngineVersion}' --output text
5.7.mysql_aurora.2.10.2

aws rds describe-db-engine-versions --engine aurora-mysql --engine-version
 5.7.mysql_aurora.2.10.2 \
  --query '*[].[ValidUpgradeTarget]'
...
{
    "Engine": "aurora-mysql",
    "EngineVersion": "8.0.mysql_aurora.3.02.0",
    "Description": "Aurora MySQL 3.02.0 (compatible with MySQL 8.0.23)",
    "AutoUpgrade": false,
    "IsMajorVersionUpgrade": true,
    "SupportedEngineModes": [
        "provisioned"
    ],
    "SupportsParallelQuery": true,
    "SupportsGlobalDatabases": true,
    "SupportsBabelfish": false
},
...
```

Dieses Beispiel zeigt, dass Aurora das Upgrade nicht durchführt, wenn Sie eine Zielversionsnummer eingeben, die kein gültiges Upgrade-Ziel für den Cluster ist. Aurora führt auch kein Hauptversions-Upgrade durch, es sei denn, Sie geben den Parameter `--allow-major-version-upgrade` an. Auf diese Weise können Sie nicht versehentlich ein Upgrade durchführen, das umfangreiche Tests und Änderungen an Ihrem Anwendungscode erfordert.

```
aws rds modify-db-cluster --db-cluster-identifier mynewdbcluster \
  --engine-version 5.7.mysql_aurora.2.09.2 --apply-immediately
An error occurred (InvalidParameterCombination) when calling the ModifyDBCluster
 operation: Cannot find upgrade target from 5.7.mysql_aurora.2.10.2 with requested
 version 5.7.mysql_aurora.2.09.2.

aws rds modify-db-cluster --db-cluster-identifier mynewdbcluster \
  --engine-version 8.0.mysql_aurora.3.02.0 --region us-east-1 --apply-immediately
An error occurred (InvalidParameterCombination) when calling the ModifyDBCluster
 operation: The AllowMajorVersionUpgrade flag must be present when upgrading to a new
 major version.

aws rds modify-db-cluster --db-cluster-identifier mynewdbcluster \
  --engine-version 8.0.mysql_aurora.3.02.0 --apply-immediately --allow-major-version-
upgrade
{
  "DBClusterIdentifier": "mynewdbcluster",
  "Status": "available",
  "Engine": "aurora-mysql",
  "EngineVersion": "5.7.mysql_aurora.2.10.2"
}
```

Es dauert einige Augenblicke, bis sich der Status des Clusters und der zugehörigen DB-Instances auf änder `upgrading`. Die Versionsnummern für die Cluster- und DB-Instances ändern sich erst, wenn das Upgrade abgeschlossen ist. Auch hier können Sie den `wait db-instance-available`-Befehl verwenden, damit die Writer-DB-Instance wartet, bis das Upgrade abgeschlossen ist, bevor Sie fortfahren.

```
aws rds describe-db-clusters --db-cluster-identifier mynewdbcluster \
  --query '*[].[Status,EngineVersion]' --output text
upgrading 5.7.mysql_aurora.2.10.2

aws rds describe-db-instances --db-instance-identifier mynewdbcluster-instance1 \
  --query '*[].
{DBInstanceIdentifier:DBInstanceIdentifier,DBInstanceStatus:DBInstanceStatus} | [0]'
{
    "DBInstanceIdentifier": "mynewdbcluster-instance1",
    "DBInstanceStatus": "upgrading"
}

aws rds wait db-instance-available --db-instance-identifier mynewdbcluster-instance1
```

Zu diesem Zeitpunkt entspricht die Versionsnummer für den Cluster der Nummer, die für das Upgrade angegeben wurde.

```
aws rds describe-db-clusters --db-cluster-identifier mynewdbcluster \
  --query '*[].[EngineVersion]' --output text

8.0.mysql_aurora.3.02.0
```

Das vorhergehende Beispiel führte ein sofortiges Upgrade durch Angabe des `--apply-immediately`-Parameters durch. Damit das Upgrade zu einem geeigneten Zeitpunkt durchgeführt wird, zu dem nicht zu erwarten ist, dass der Cluster ausgelastet ist, können Sie den Parameter `--no-apply-immediately` festlegen. Dadurch wird das Upgrade während des nächsten Wartungsfensters für den Cluster gestartet. Das Wartungsfenster definiert den Zeitraum, in dem Wartungsvorgänge beginnen können. Ein lang andauernder Vorgang kann während des Wartungsfensters möglicherweise nicht beendet werden. Daher müssen Sie kein größeres Wartungsfenster definieren, selbst wenn Sie davon ausgehen, dass das Upgrade sehr lange dauern kann.

Im folgenden Beispiel wird ein Cluster aktualisiert, auf dem ursprünglich Aurora-MySQL-Version 2.10.2 ausgeführt wurde. In der Ausgabe `describe-db-engine-versions` stellen die Werte `False` und `True` die Eigenschaft `IsMajorVersionUpgrade` dar. Ab Version 2.10.2 können Sie auf andere 2.*-Versionen aktualisieren. Diese Upgrades gelten nicht als Hauptversions-Upgrades und erfordern daher kein direktes Upgrade. Ein direktes Upgrade ist nur für die 3.*-Versionen verfügbar, die in der Liste aufgeführt sind.

```
aws rds describe-db-clusters --db-cluster-identifier mynewdbcluster \
  --query '*[].{EngineVersion:EngineVersion}' --output text
5.7.mysql_aurora.2.10.2

aws rds describe-db-engine-versions --engine aurora-mysql --engine-version
 5.7.mysql_aurora.2.10.2 \
  --query '*[].[ValidUpgradeTarget]|[0][0]|[*].[EngineVersion,IsMajorVersionUpgrade]'
 --output text

5.7.mysql_aurora.2.10.3 False
5.7.mysql_aurora.2.11.0 False
5.7.mysql_aurora.2.11.1 False
8.0.mysql_aurora.3.01.1 True
8.0.mysql_aurora.3.02.0 True
8.0.mysql_aurora.3.02.2 True
```

```
aws rds modify-db-cluster --db-cluster-identifier mynewdbcluster \
  --engine-version 8.0.mysql_aurora.3.02.0 --no-apply-immediately --allow-major-
version-upgrade
...
```

Wenn ein Cluster ohne ein festgelegtes Wartungsfenster erstellt wird, wählt Aurora einen zufälligen Wochentag aus. In diesem Fall wird der Befehl `modify-db-cluster` an einem Montag gesendet. Daher ändern wir das Wartungsfenster auf Dienstagmorgen. Alle Zeiten sind in der UTC-Zeitzone dargestellt. Das Fenster `tue:10:00-tue:10:30` entspricht 2:00 - 2:30 Uhr Pacific Time. Die Änderung des Wartungsfensters wird sofort wirksam.

```
aws rds describe-db-clusters --db-cluster-identifier mynewdbcluster --query '*[].
[PreferredMaintenanceWindow]'
[
    [
        "sat:08:20-sat:08:50"
    ]
]

aws rds modify-db-cluster --db-cluster-identifier mynewdbcluster --preferred-
maintenance-window tue:10:00-tue:10:30"
aws rds describe-db-clusters --db-cluster-identifier mynewdbcluster --query '*[].
[PreferredMaintenanceWindow]'
[
    [
        "tue:10:00-tue:10:30"
    ]
]
```

Das folgende Beispiel zeigt, wie ein Bericht über die durch das Upgrade generierten Ereignisse abgerufen wird. Das Argument `--duration` gibt die Anzahl der Minuten an, die für den Abruf der Ereignisinformationen erforderlich sind. Dieses Argument ist erforderlich, da standardmäßig `describe-events` nur Ereignisse der letzten Stunde zurückgegeben werden.

```
aws rds describe-events --source-type db-cluster --source-identifier mynewdbcluster --
duration 20160
{
    "Events": [
        {
```

```
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "DB cluster created",
            "EventCategories": [
                "creation"
            ],
            "Date": "2022-11-17T01:24:11.093000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        },
        {
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "Upgrade in progress: Performing online pre-upgrade checks.",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2022-11-18T22:57:08.450000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        },
        {
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "Upgrade in progress: Performing offline pre-upgrade checks.",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2022-11-18T22:57:59.519000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        },
        {
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "Upgrade in progress: Creating pre-upgrade snapshot [preupgrade-
mynewdbcluster-5-7-mysql-aurora-2-10-2-to-8-0-mysql-aurora-3-02-0-2022-11-18-22-55].",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2022-11-18T23:00:22.318000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        },
        {
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "Upgrade in progress: Cloning volume.",
```

```
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2022-11-18T23:01:45.428000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        },
        {
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "Upgrade in progress: Purging undo records for old row versions.
Records remaining: 164",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2022-11-18T23:02:25.141000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        },
        {
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "Upgrade in progress: Purging undo records for old row versions.
Records remaining: 164",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2022-11-18T23:06:23.036000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        },
        {
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "Upgrade in progress: Upgrading database objects.",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2022-11-18T23:06:48.208000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        },
        {
            "SourceIdentifier": "mynewdbcluster",
            "SourceType": "db-cluster",
            "Message": "Database cluster major version has been upgraded",
            "EventCategories": [
                "maintenance"
```

```
            ],
            "Date": "2022-11-18T23:10:28.999000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mynewdbcluster"
        }
    ]
}
```

Finden Sie die Gründe für Upgrade-Fehler

Im vorherigen Tutorial war das Upgrade von Aurora MySQL Version 2 auf Version 3 erfolgreich. Wenn das Upgrade jedoch fehlgeschlagen wäre, würden Sie wissen wollen, warum.

Sie können damit beginnen, den `describe-events` AWS CLI Befehl zu verwenden, um sich die DB-Cluster-Ereignisse anzusehen. Dieses Beispiel zeigt die Ereignisse der letzten 10 Stunden. `mydbcluster`

```
aws rds describe-events \
    --source-type db-cluster \
    --source-identifier mydbcluster \
    --duration 600
```

In diesem Fall ist bei der Upgrade-Vorabprüfung ein Fehler aufgetreten.

```
{
    "Events": [
        {
            "SourceIdentifier": "mydbcluster",
            "SourceType": "db-cluster",
            "Message": "Database cluster engine version upgrade started.",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2024-04-11T13:23:22.846000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mydbcluster"
        },
        {
            "SourceIdentifier": "mydbcluster",
            "SourceType": "db-cluster",
            "Message": "Database cluster is in a state that cannot be upgraded: Upgrade
 prechecks failed. For more details, see the
             upgrade-prechecks.log file. For more information on troubleshooting the
 cause of the upgrade failure, see
```

```
             https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/
AuroraMySQL.Updates.MajorVersionUpgrade.html#AuroraMySQL.Upgrading.Troubleshooting.",
            "EventCategories": [
                "maintenance"
            ],
            "Date": "2024-04-11T13:23:24.373000+00:00",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:mydbcluster"
        }
    ]
}
```

Um die genaue Ursache des Problems zu diagnostizieren, untersuchen Sie die Datenbankprotokolle für die Writer-DB-Instance. Wenn ein Upgrade auf Aurora MySQL Version 3 fehlschlägt, enthält die Writer-Instanz eine Protokolldatei mit dem Namen`upgrade-prechecks.log`. Dieses Beispiel zeigt, wie Sie das Vorhandensein dieses Protokolls erkennen und es dann zur Untersuchung in eine lokale Datei herunterladen.

```
aws rds describe-db-log-files --db-instance-identifier mydbcluster-instance \
    --query '*[].[LogFileName]' --output text

error/mysql-error-running.log
error/mysql-error-running.log.2024-04-11.20
error/mysql-error-running.log.2024-04-11.21
error/mysql-error.log
external/mysql-external.log
upgrade-prechecks.log

aws rds download-db-log-file-portion --db-instance-identifier mydbcluster-instance \
    --log-file-name upgrade-prechecks.log \
    --starting-token 0 \
    --output text >upgrade_prechecks.log
```

Die `upgrade-prechecks.log`-Datei befindet sich im JSON-Format. Wir laden sie mit der Option `--output text` herunter, um JSON-Output nicht in einem anderen JSON-Wrapper zu kodieren. Für Upgrades auf Aurora-MySQL-Version 3 enthält dieses Protokoll immer bestimmte Informations- und Warnmeldungen. Es enthält nur Fehlermeldungen, wenn das Upgrade fehlschlägt. Wenn das Upgrade erfolgreich ist, wird die Protokolldatei überhaupt nicht erstellt.

Um alle Fehler zusammenzufassen und die zugehörigen Objekt- und Beschreibungsfelder anzuzeigen, können Sie den Befehl für `grep -A 2 '"level": "Error"'` den Inhalt der `upgrade-prechecks.log` Datei ausführen. Dadurch werden jede Fehlerzeile und die beiden

Zeilen danach angezeigt. Diese enthalten den Namen des entsprechenden Datenbankobjekts und Anleitungen zur Behebung des Problems.

```
$ cat upgrade-prechecks.log | grep -A 2 '"level": "Error"'

"level": "Error",
"dbObject": "problematic_upgrade.dangling_fulltext_index",
"description": "Table `problematic_upgrade.dangling_fulltext_index` contains dangling
 FULLTEXT index. Kindly recreate the table before upgrade."
```

In diesem Beispiel können Sie den folgenden SQL-Befehl für die fehlerhafte Tabelle ausführen, um zu versuchen, das Problem zu beheben, oder Sie können die Tabelle ohne den fehlerhaften Index neu erstellen.

```
OPTIMIZE TABLE problematic_upgrade.dangling_fulltext_index;
```

Versuchen Sie dann erneut, das Upgrade durchzuführen.

Problembehandlung für Aurora MySQL direkte Upgrades

Verwenden Sie die folgenden Tipps, um Probleme mit direkten Aurora-MySQL-Upgrades zu beheben. Diese Tipps gelten nicht für Aurora Serverless-DB-Cluster.

Grund für das abgebrochene oder langsame direkte Upgrade	Auswirkung	Lösung, die den Abschluss eines direkten Upgrades im Wartungsfenster ermöglicht
Das zugehörige regionsübergreifende Aurora-Replikat wurde noch nicht gepatcht	Aurora bricht das Upgrade ab.	Aktualisieren Sie das Aurora Cross-Region-Replikat und versuchen Sie es erneut.
Der Cluster hat XA-Transaktionen im vorbereiteten Zustand	Aurora bricht das Upgrade ab.	Bestätigen Sie alle vorbereiteten XA-Transaktionen oder setzen Sie sie zurück.
Der Cluster verarbeitet alle DDL-Anweisungen (Data Definition Language)	Aurora bricht das Upgrade ab.	Erwägen Sie, zu warten und das Upgrade durchzuführen, nachdem alle DDL-Anweisungen abgeschlossen sind.

Grund für das abgebrochene oder langsame direkte Upgrade	Auswirkung	Lösung, die den Abschluss eines direkten Upgrades im Wartungsfenster ermöglicht
Der Cluster hat für viele Zeilen nicht festgeschriebene Änderungen	Das Upgrade könnte eine lange Zeit dauern.	Der Upgrade-Prozess setzt die nicht festgeschriebenen Änderungen zurück. Der Indikator für diese Bedingung ist der Wert von `TRX_ROWS_MODIFIED` in der `INFORMATION_SCHEMA.INNODB_TRX` -Tabelle. Erwägen Sie, das Upgrade erst durchzuführen, nachdem alle großen Transaktionen festgeschrieben oder zurückgesetzt wurden.

Grund für das abgebrochene oder langsame direkte Upgrade	Auswirkung	Lösung, die den Abschluss eines direkten Upgrades im Wartungsfenster ermöglicht
Der Cluster hat eine hohe Anzahl von Undo-Datensätzen	Das Upgrade könnte eine lange Zeit dauern.	Selbst wenn sich die nicht festgeschrieben Transaktionen nicht auf eine große Anzahl von Zeilen auswirken, können sie eine große Datenmenge beinhalten. Beispielsweise könnten Sie große BLOBs einfügen. Aurora erkennt oder generiert ein Ereignis für diese Art von Transaktionsaktivität nicht automatisch. Der Indikator für diesen Zustand ist die Länge der Verlaufsliste (HLL). Der Upgrade-Prozess setzt die nicht festgeschriebenen Änderungen zurück. Sie können die HLL in der Ausgabe des `SHOW ENGINE INNODB STATUS` SQL-Befehls oder direkt mit der folgenden SQL-Abfrage überprüfen: `SELECT count FROM information_schema .innodb_metrics WHERE name = 'trx_rseg_history_len';` Sie können die `RollbackSegmentHistoryListLength` Metrik auch in Amazon CloudWatch überwachen. Erwägen Sie, das Upgrade erst durchzuführen, wenn die HLL kleiner ist.

Grund für das abgebrochene oder langsame direkte Upgrade	Auswirkung	Lösung, die den Abschluss eines direkten Upgrades im Wartungsfenster ermöglicht
Der Cluster ist dabei, eine große binäre Protokoll-Transaktion festzuschreiben	Das Upgrade könnte eine lange Zeit dauern.	Der Upgrade-Prozess wartet, bis die binären Protokolländerungen angewendet werden. In diesem Zeitraum können mehr Transaktionen oder DDL-Anweisungen gestartet werden, was den Upgrade-Prozess weiter verlangsamt. Planen Sie den Upgrade-Prozess, wenn der Cluster nicht mit der Generierung von Änderungen der binären Protokollreplikation beschäftigt Aurora erkennt oder generiert ein Ereignis für diese Bedingung nicht automatisch.

Grund für das abgebrochene oder langsame direkte Upgrade	Auswirkung	Lösung, die den Abschluss eines direkten Upgrades im Wartungsfenster ermöglicht
Schemainkonsistenzen, die auf das Entfernen oder die Beschädigung von Dateien zurückzuführen sind	Aurora bricht das Upgrade ab.	Ändern Sie die Standard-Speicher-Engine für temporäre Tabellen von MyISAM auf InnoDB. Führen Sie die folgenden Schritte aus: 1. Ändern Sie den DB-Parameter `default_tmp_storage_engine` in `InnoDB`. 2. Starten Sie den DB-Cluster neu. 3. Vergewissern Sie sich nach dem Neustart, dass der DB-Parameter `default_tmp_storage_engine` auf `InnoDB` festgelegt ist. Verwenden Sie den folgenden Befehl: `show global variables like 'default_tmp_storage_engine';` 4. Stellen Sie sicher, dass Sie keine temporären Tabellen erstellen, die die MyISAM-Speicher-Engine verwenden. Wir empfehlen, dass Sie jeden Datenbank-Workload unterbrechen und keine neuen Datenbankverbindungen herstellen, da Sie bald ein Upgrade durchführen werden. 5. Versuchen Sie erneut, das direkte Upgrade durchzuführen.

<table>
<tr><th>Grund für das abgebrochene oder langsame direkte Upgrade</th><th>Auswirkung</th><th>Lösung, die den Abschluss eines direkten Upgrades im Wartungsfenster ermöglicht</th></tr>
<tr><td>Der Hauptbenutzer wurde gelöscht</td><td>Aurora bricht das Upgrade ab.</td><td>

⚠ Important

Löschen Sie den Masterbenutzer nicht.

Sollten Sie jedoch aus irgendeinem Grund den Masterbenutzer löschen, stellen Sie ihn mithilfe der folgenden SQL-Befehle wieder her:

```
CREATE USER 'master_username '@'%'
 IDENTIFIED BY ' master_user_passwo
rd ' REQUIRE NONE PASSWORD EXPIRE
 DEFAULT ACCOUNT UNLOCK;

GRANT SELECT, INSERT, UPDATE, DELETE,
 CREATE, DROP, RELOAD, PROCESS,
 REFERENCES, INDEX, ALTER, SHOW
 DATABASES, CREATE TEMPORARY TABLES,
LOCK TABLES, EXECUTE, REPLICATION
 SLAVE, REPLICATION CLIENT, CREATE
 VIEW, SHOW VIEW, CREATE ROUTINE, ALTER
 ROUTINE, CREATE USER, EVENT,
TRIGGER, LOAD FROM S3, SELECT INTO
 S3, INVOKE LAMBDA, INVOKE SAGEMAKER
, INVOKE COMPREHEND ON *.* TO
 'master_username '@'%' WITH GRANT
 OPTION;
```

</td></tr>
</table>

Weitere Informationen zur Behebung von Problemen, die dazu führen, dass Upgrade-Vorabprüfungen fehlschlagen, finden Sie in den folgenden Blogs:

- Upgrade-Checkliste für Amazon Aurora MySQL Version 2 (mit MySQL 5.7-Kompatibilität) auf Version 3 (mit MySQL 8.0-Kompatibilität), Teil 1

- Upgrade-Checkliste für Amazon Aurora MySQL Version 2 (mit MySQL 5.7-Kompatibilität) auf Version 3 (mit MySQL 8.0-Kompatibilität), Teil 2

Sie können die folgenden Schritte verwenden, um eigene Überprüfungen für einige der Bedingungen in der vorherigen Tabelle durchzuführen. Auf diese Weise können Sie das Upgrade für einen Zeitpunkt planen, an dem Sie wissen, dass sich die Datenbank in einem Zustand befindet, in dem das Upgrade erfolgreich und schnell abgeschlossen werden kann.

- Sie können nach offenen XA-Transaktionen suchen, indem Sie die `XA RECOVER`-Anweisung ausführen. Sie können dann die XA-Transaktionen festschreiben oder zurücksetzen, bevor Sie mit dem Upgrade beginnen.
- Sie können nach DDL-Anweisungen suchen, indem Sie eine `SHOW PROCESSLIST` Anweisung ausführen und in der Ausgabe nach `CREATE`, `DROP`, `ALTER`, `RENAME` und `TRUNCATE` Anweisungen suchen. Warten Sie bis alle DDL-Anweisungen fertig sind, bevor Sie mit dem Upgrade beginnen.
- Sie können die Gesamtzahl der nicht festgeschriebenen Zeilen überprüfen, indem Sie die `INFORMATION_SCHEMA.INNODB_TRX`-Tabelle abfragen. Die Tabelle enthält eine Zeile für jede Transaktion. Die `TRX_ROWS_MODIFIED` Spalte enthält die Anzahl der Zeilen, die von der Transaktion geändert oder eingefügt wurden.
- Sie können die Länge der InnoDB-Verlaufsliste überprüfen, indem Sie die `SHOW ENGINE INNODB STATUS SQL`-Anweisung ausführen und nach `History list length` in der Ausgabe suchen. Sie können den Wert auch direkt überprüfen, indem Sie die folgende Abfrage ausführen:

  ```
  SELECT count FROM information_schema.innodb_metrics WHERE name =
   'trx_rseg_history_len';
  ```

  Die Länge der Verlaufsliste entspricht der Menge der Undo-Daten, die von der Datenbank gespeichert werden, um die Multi-Versions-Concurrency Control (MVCC) zu implementieren.

Bereinigung nach dem Upgrade für Aurora MySQL Version 3

Nachdem Sie ein Upgrade von Aurora-MySQL-Clustern der 2 auf Aurora-MySQL-Version 3 abgeschlossen haben, können Sie diese anderen Bereinigungsaktionen ausführen:

- Erstellen Sie neue MySQL 8.0-kompatible Versionen beliebiger benutzerdefinierter Parametergruppen. Wenden Sie alle erforderlichen benutzerdefinierten Parameterwerte auf die neuen Parametergruppen an.

- Aktualisieren Sie alle CloudWatch Alarme, Setup-Skripts usw., um die neuen Namen für alle Metriken zu verwenden, deren Namen von inklusiven Sprachänderungen betroffen waren. Eine Liste der -Metriken finden Sie unter Inklusive Sprachänderungen für Aurora MySQL Version 3.
- Aktualisieren Sie alle AWS CloudFormation Vorlagen so, dass sie die neuen Namen für alle Konfigurationsparameter verwenden, deren Namen von inklusiven Sprachänderungen betroffen waren. Eine vollständige Liste der Parameter finden Sie unter Inklusive Sprachänderungen für Aurora MySQL Version 3.

SPATIAL-Index

Überprüfen Sie nach dem Upgrade auf Aurora MySQL Version 3, ob Sie Objekte und Indizes im Zusammenhang mit räumlichen Indizes löschen oder neu erstellen müssen. Vor MySQL 8.0 konnte Aurora räumliche Abfragen mithilfe von Indizes optimieren, die keinen räumlichen Ressourcenbezeichner (SRID) enthielten. Aurora MySQL Version 3 verwendet nur räumliche Indizes, die SRIDs enthalten. Während eines Upgrades legt Aurora automatisch alle räumlichen Indizes ohne SRIDs ab und gibt Warnmeldungen im Datenbankprotokoll aus. Wenn Sie solche Warnmeldungen beobachten, erstellen Sie nach dem Upgrade neue räumliche Indizes mit SRIDs. Weitere Informationen zu Änderungen an räumlichen Funktionen und Datentypen in MySQL 8.0 finden Sie unter Änderungen in MySQL 8.0 im MySQL-Referenzhandbuch.

Datenbank-Engine-Updates und Fixes für Amazon Aurora MySQL

Die folgenden Informationen finden Sie in den Versionshinweisen für Amazon Aurora MySQL-Compatible Edition:

- Datenbank-Engine-Updates für Amazon Aurora MySQL Version 3
- Datenbank-Engine-Updates für Amazon Aurora MySQL Version 2
- Datenbank-Engine-Updates für Amazon Aurora MySQL Version 1 (veraltet)
- MySQL-Fehler, die durch Updates der Aurora MySQL-Datenbank-Engine behoben wurden
- Sicherheitslücken in Amazon Aurora MySQL behoben

Arbeiten mit Amazon Aurora PostgreSQL

Amazon Aurora PostgreSQL ist eine vollständig verwaltete, PostgreSQL-kompatible und ACID-kompatible relationale Datenbank-Engine, die die Geschwindigkeit, Zuverlässigkeit und Verwaltbarkeit von Amazon Aurora mit der Einfachheit und Kosteneffizienz von Open-Source-Datenbanken kombiniert. Aurora PostgreSQL ist ein Drop-In-Ersatz für PostgreSQL und macht es einfach und kostengünstig, Ihre neuen und bestehenden PostgreSQL-Implementierungen einzurichten, zu betreiben und zu skalieren, sodass Sie sich auf Ihr Unternehmen und Ihre Anwendungen konzentrieren können. Weitere Informationen über Aurora finden Sie unter Was ist Amazon Aurora?.

Zusätzlich zu den Vorteilen von Aurora bietet Aurora PostgreSQL einen bequemen Migrationspfad von Amazon RDS zu Aurora mit Migrationstools auf Knopfdruck, die Ihre vorhandenen Anwendungen von RDS für PostgreSQL in Aurora PostgreSQL konvertieren. Routinemäßige Datenbankaufgaben wie Bereitstellung, Patching, Backup, Wiederherstellung, Fehlererkennung und Reparatur sind mit Aurora PostgreSQL ebenfalls einfach zu verwalten.

Aurora PostgreSQL kann mit vielen Industriestandards arbeiten. Sie können beispielsweise Aurora PostgreSQL-Datenbanken verwenden, um HIPAA-konforme Anwendungen zu erstellen und Gesundheitsdaten einschließlich geschützter Gesundheitsdaten (Protected Health Information, PHI) entsprechend einem mit AWS abgeschlossenen Business Associate Agreement (BAA) zu speichern.

Aurora PostgreSQL ist mit FedRAMP HIGH konform. Weitere Informationen zu AWS und Compliance-Bemühungen finden Sie unter Im Rahmen des Compliance-Programms zugelassene AWS-Services.

Themen

- Verwenden von Babelfish for Aurora PostgreSQL
- Verwalten von Amazon Aurora PostgreSQL
- Optimierung mit Warteereignissen für Aurora PostgreSQL
- Optimierung von Aurora PostgreSQL mit proaktiven Einblicken von Amazon DevOps Guru
- Bewährte Methoden mit Amazon Aurora PostgreSQL
- Replikation mit Amazon Aurora PostgreSQL
- Verwendung von Aurora PostgreSQL als Wissensdatenbank für Amazon Bedrock
- Integrieren von Amazon Aurora PostgreSQL in anderen AWS-Services
- Überwachen von Abfrageausführungsplänen für Aurora PostgreSQL
- Verwalten von Abfrageausführungsplänen für Aurora PostgreSQL
- Arbeiten mit Erweiterungen und Fremddaten-Wrappern
- Arbeiten mit Trusted Language Extensions für PostgreSQL
- Amazon-Aurora-PostgreSQL-Referenz
- Amazon Aurora PostgreSQL-Aktualisierungen

Arbeiten mit Database Preview Environment

Die PostgreSQL-Community veröffentlicht jährlich eine neue Hauptversion von PostgreSQL. Ebenso stellt Amazon Aurora PostgreSQL-Hauptversionen als Vorschauversionen zur Verfügung. Auf diese Weise können Sie DB-Cluster mit der Vorschauversion erstellen und ihre Funktionen in der Datenbank-Vorschauumgebung testen.

DB-Cluster von Aurora PostgreSQL in der Database Preview-Umgebung ähneln funktionell anderen DB-Clustern von Aurora PostgreSQL. Sie können eine Vorschauversion jedoch nicht für die Produktion einsetzen.

Beachten Sie folgende wichtige Einschränkungen:

- Alle DB-Instances und DB-Cluster werden 60 Tage nach ihrer Erstellung zusammen mit allen Backups und Snapshots gelöscht.
- Sie können eine DB-Instance nur in einer virtuellen privaten Cloud (VPC) erstellen, die auf dem Service Amazon VPC basiert.
- Sie können einen Snapshot einer DB-Instance nicht in eine Produktionsumgebung kopieren.

Die folgenden Optionen werden von der Vorschauversion unterstützt.

- Sie können DB-Instances nur mit den Instance-Typen r5, r6g, r6i, r7g, x2g, t3 und t4g erstellen. Weitere Informationen zu Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.
- Sie können Single-AZ- und Multi-AZ-Bereitstellungen verwenden.
- Sie können die standardmäßigen PostgreSQL-Dump- und -Ladefunktionen verwenden, um Datenbanken aus der Database Preview-Umgebung zu exportieren oder in diese zu importieren.

Unterstützte DB-Instance-Klassentypen

Amazon Aurora PostgreSQL unterstützt die folgenden DB-Instance-Klassen in der Vorschauregion:

Speicheroptimierte Klassen

- db.r5 – arbeitsspeicheroptimierte Instance-Klassen
- db.r6g – arbeitsspeicheroptimierte Instance-Klassen mit AWS Graviton2-Prozessoren
- db.r6i – arbeitsspeicheroptimierte Instance-Klassen
- db.x2g – arbeitsspeicheroptimierte Instance-Klassen mit AWS Graviton2-Prozessoren

> **Note**
>
> Weitere Informationen zur Liste der Instance-Klassen finden Sie unter DB-Instance-Klassenarten.

Burstable-Klassen

- db.t3.medium
- db.t3.large
- db.t4g.medium
- db.t4g.large

Nicht unterstützte Funktionen in der Vorschauumgebung

Die folgenden Funktionen sind in der Vorschauumgebung nicht verfügbar:

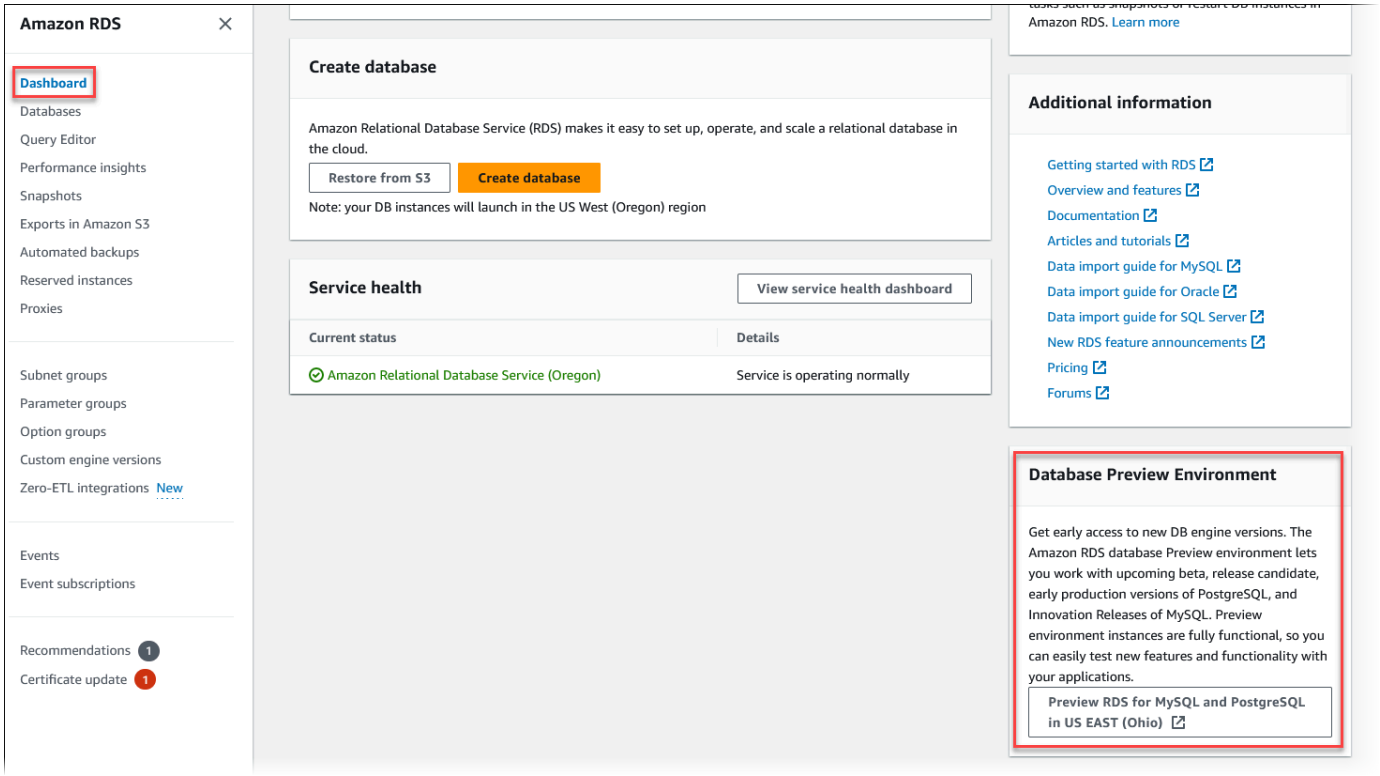
- Aurora Serverless v1 und v2
- Hauptversions-Upgrades (MVU)
- In der Vorschauregion werden keine neuen Nebenversionen veröffentlicht
- RDS für PostgreSQL zu Aurora PostgreSQL eingehende Replikation
- Blau/Grün-Bereitstellung von Amazon RDS
- Regionsübergreifende Snapshot-Kopie
- Globale Aurora-Datenbank
- Datenbankaktivitäts-Streams (DAS), RDS Proxy und AWS DMS
- Auto Scaling von Lesereplikaten
- AWS Bedrock
- RDS-Export
- Performance Insights
- Globale Schreibweiterleitung
- Optimierte Lesevorgänge
- Babelfish
- Benutzerdefinierte Endpunkte
- Snapshot-Kopie

Erstellen eines neuen DB-Clusters in der Vorschauumgebung

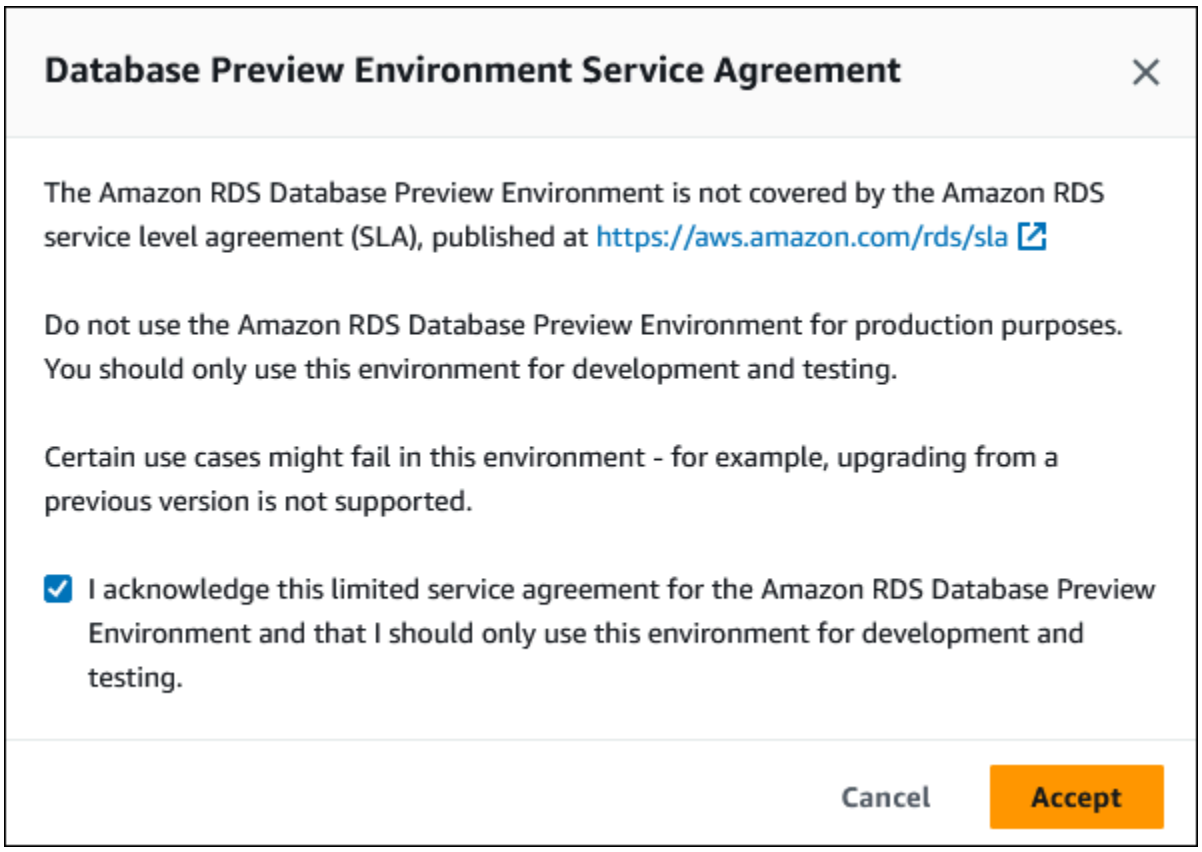
Gehen Sie wie folgt vor, um einen DB-Cluster in der Vorschauumgebung zu erstellen.

So erstellen Sie einen DB-Cluster in der Vorschauumgebung

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Dashboard aus.
3. Suchen Sie auf Dashboard-Seite nach Database Preview Environment (Datenbank-Preview-Umgebung), wie in der folgenden Abbildung gezeigt.



Sie können auch direkt zu Database Preview Environment (Datenbank-Preview-Umgebung) navigieren. Bevor Sie fortfahren können, müssen Sie die Einschränkungen bestätigen und akzeptieren.



4. Um den Aurora-PostgreSQL-DB-Cluster zu erstellen, folgen Sie demselben Verfahren wie beim Erstellen eines beliebigen Aurora-DB-Clusters. Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Verwenden Sie den folgenden EndpunktAWS CLI, um eine Instance in der Datenbank-Vorschauumgebung mithilfe der Aurora-API oder der zu erstellen.

```
rds-preview.us-east-2.amazonaws.com
```

PostgreSQL Version 16 in der Datenbank-Vorschauumgebung

⚠ Dies ist eine Vorschau der Dokumentation für Aurora PostgreSQL Version 16. Änderungen sind vorbehalten.

PostgreSQL Version 16.0 ist jetzt in der Datenbank-Vorschauumgebung in Amazon RDS verfügbar. PostgreSQL Version 16 enthält mehrere Verbesserungen, die in der folgenden PostgreSQL-Dokumentation beschrieben werden:

- PostgreSQL 16 Released

Weitere Informationen zur Database Preview-Umgebung finden Sie unter Arbeiten mit Database Preview Environment. Wählen Sie https://console.aws.amazon.com/rds-preview/ aus, um von der Konsole aus auf die Vorschauumgebung zuzugreifen.

> **Note**
>
> Es wird nicht empfohlen, PostgreSQL Version 16.0 in der Database Preview-Umgebung zu verwenden, da Aurora PostgreSQL Version 16.1 jetzt allgemein verfügbar ist. Weitere Informationen finden Sie unter Updates für Amazon Aurora PostgreSQL.

Sicherheit in Amazon Aurora PostgreSQL

Eine allgemeine Übersicht über die Aurora-Sicherheit finden Sie unter Sicherheit in Amazon Aurora. Sie können die Sicherheit für Amazon Aurora PostgreSQL auf mehreren Ebenen verwalten:

- Um zu steuern, wer Verwaltungsaktionen in Amazon RDS für Aurora-DB-Cluster und PostgreSQL-DB-Instances ausführen darf, verwenden Sie AWS Identity and Access Management (IAM). IAM übernimmt die Authentifizierung der Benutzeridentität, bevor der Benutzer auf den Service zugreifen kann. Außerdem übernimmt IAM auch die Autorisierung, d. h., ob der Benutzer für die Vorgänge berechtigt ist, die er versucht auszuführen. Die IAM-Datenbankauthentifizierung ist eine zusätzliche Authentifizierungsmethode, die Sie beim Erstellen Ihres Aurora-PostgreSQL-DB-Clusters auswählen können. Weitere Informationen finden Sie unter Identity and Access Management für Amazon Aurora.

  Wenn Sie IAM mit Ihrem Aurora-PostgreSQL-DB-Cluster verwenden, melden Sie sich bei der AWS Management Console zuerst mit Ihren IAM-Anmeldeinformationen an, bevor Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/ aufrufen.
- Stellen Sie sicher, dass Sie Aurora-DB-Cluster in einer Virtual Private Cloud (VPC) basierend auf dem Amazon-VPC-Service erstellen. Mithilfe einer VPC-Sicherheitsgruppe können Sie steuern, welche Geräte und Amazon EC2-Instances Verbindungen zum Endpunkt und Port der DB-Instance für Aurora-DB-Cluster in einer VPC herstellen können. Sie können diese Endpunkt-

und Portverbindungen mithilfe von Secure Sockets Layer (SSL) herstellen. Zusätzlich können Firewall-Regeln in Ihrem Unternehmen steuern, ob in Ihrem Unternehmen verwendete Geräte Verbindungen mit einer DB-Instance herstellen dürfen. Weitere Informationen zu VPCs finden Sie unter Amazon VPCs und Amazon Aurora.

Die unterstützte VPC-Tenancy hängt von der DB-Instance-Klasse ab, die von Ihren Aurora-PostgreSQL-DB-Clustern verwendet wird. Mit `default`-VPC-Tenancy, läuft der DB-Cluster auf gemeinsam genutzter Hardware. Mit `dedicated`-VPC-Tenancy läuft der DB-Cluster auf einer dedizierten Hardware-Instance. Die DB-Instance-Klassen mit Spitzenlastleistung unterstützen nur die Standard-VPC-Tenancy. Die DB-Instance-Klassen mit Spitzenlastleistung umfassen die DB-Instance-Klassen db.t3 und db.t4g. Alle anderen Aurora-PostgreSQL-DB-Instance-Klassen unterstützen sowohl die Standard- als auch die dedizierte VPC-Tenancy.

Weitere Informationen zu Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen. Weitere Informationen über die `default`- und `dedicated`-VPC-Tenancy finden Sie unter Dedicated Instances im Amazon Elastic Compute Cloud-Benutzerhandbuch.

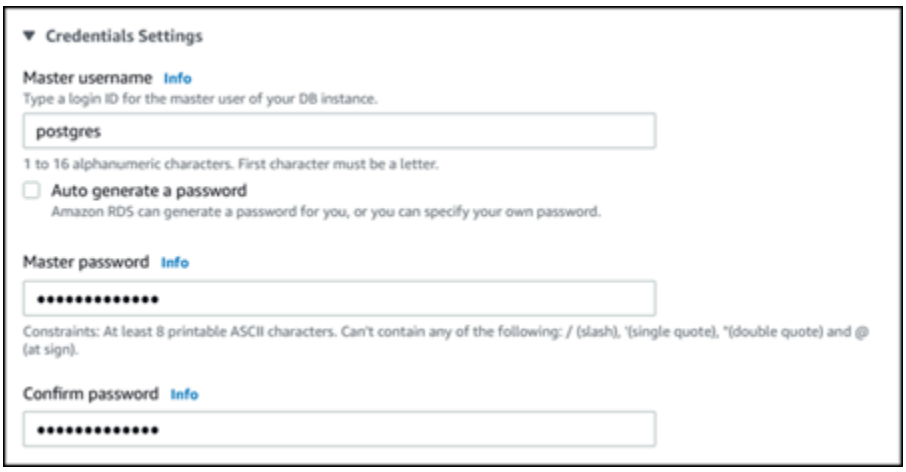
- Wenn Sie den PostgreSQL-Datenbanken, die auf Ihrem Amazon-Aurora-DB-Cluster ausgeführt werden, Berechtigungen erteilen möchten, können Sie den gleichen allgemeinen Ansatz wie bei eigenständigen Instances von PostgreSQL verwenden. Befehle wie `CREATE ROLE`, `ALTER ROLE`, `GRANT` und `REVOKE` funktionieren genau wie auf On-Premises-Datenbanken. Gleiches gilt für das direkte Ändern von Datenbanken, Schemas und Tabellen.

  PostgreSQL verwaltet Berechtigungen mithilfe von Rollen. Die Rolle `rds_superuser` ist die Rolle mit den meisten Berechtigungen in einem Aurora-PostgreSQL-DB-Cluster. Diese Rolle wird automatisch erstellt und dem Benutzer gewährt, der den DB-Cluster erstellt (das Hauptbenutzerkonto, standardmäßig `postgres`). Weitere Informationen hierzu finden Sie unter Grundlegendes zu PostgreSQL-Rollen und -Berechtigungen.

Alle verfügbaren Aurora-PostgreSQL-Versionen, einschließlich Version 10, 11, 12, 13, 14 und höher, unterstützen den Salted Challenge Response Authentication Mechanism (SCRAM) für Passwörter als Alternative zu Message Digest (MD5). Wir empfehlen Ihnen, SCRAM zu verwenden, da dies sicherer ist als MD5. Weitere Informationen einschließlich Migration von Passwörtern für Datenbankbenutzer von MD5 nach SCRAM finden Sie unter Verwenden von SCRAM für die PostgreSQL-Passwortverschlüsselung.

Grundlegendes zu PostgreSQL-Rollen und -Berechtigungen

Wenn Sie einen DB-Cluster von Aurora PostgreSQL eine DB- mit erstellen AWS Management Console, wird gleichzeitig ein Administratorkonto erstellt. Der Name lautet standardmäßig `postgres`, wie im folgenden Screenshot gezeigt:



Sie können einen anderen Namen auswählen, anstatt den Standard (`postgres`) beizubehalten. In diesem Fall muss der von Ihnen gewählte Name mit einem Buchstaben beginnen und zwischen 1 und 16 alphanumerische Zeichen umfassen. Der Einfachheit halber verwenden wir für das Hauptbenutzerkonto den Standardwert (`postgres`) in diesem Handbuch.

Wenn Sie die `create-db-cluster` AWS CLI anstelle der verwenden AWS Management Console, erstellen Sie den Benutzernamen, indem Sie ihn mit dem `master-username` Parameter übergeben. Weitere Informationen finden Sie unter Schritt 2: Erstellen eines DB-Clusters von Aurora PostgreSQL.

Unabhängig davon, ob Sie die AWS CLI, AWS Management Consoledie oder die Amazon-RDS-API verwenden und ob Sie den `postgres` Standardnamen verwenden oder einen anderen Namen auswählen, ist dieses erste Datenbankbenutzerkonto Mitglied der `rds_superuser` Gruppe und verfügt über -`rds_superuser`Berechtigungen.

Themen

- Die Rolle „rds_superuser“ verstehen
- Steuern des Benutzerzugriffs auf die PostgreSQL−Datenbank
- Delegieren und Steuern der Benutzerpasswortverwaltung
- Verwenden von SCRAM für die PostgreSQL-Passwortverschlüsselung

Die Rolle „rds_superuser“ verstehen

In PostgreSQL kann eine Rolle einen Benutzer, eine Gruppe oder einen Satz bestimmter Berechtigungen definieren, die einer Gruppe oder einem Benutzer für verschiedene Objekte in der Datenbank gewährt werden. PostgreSQL-Befehle für `CREATE USER` und `CREATE GROUP` wurden durch den allgemeineren Befehl `CREATE ROLE` mit bestimmten Eigenschaften zur Unterscheidung von Datenbankbenutzern ersetzt. Einen Datenbankbenutzer kann man sich als Rolle mit der LOGIN-Berechtigung vorstellen.

> **Note**
>
> Die Befehle `CREATE USER` und `CREATE GROUP` können weiterhin verwendet werden. Weitere Informationen dazu finden Sie im Abschnitt Datenbankrollen der PostgreSQL-Dokumentation.

Der `postgres`-Benutzer ist der Datenbankbenutzer mit den meisten Berechtigungen auf Ihrem Aurora-PostgreSQL-DB-Cluster. Er verfügt über die Eigenschaften, die durch die folgende `CREATE ROLE`-Anweisung definiert sind.

```
CREATE ROLE postgres WITH LOGIN NOSUPERUSER INHERIT CREATEDB CREATEROLE NOREPLICATION
 VALID UNTIL 'infinity'
```

Die Eigenschaften `NOSUPERUSER`, `NOREPLICATION`, `INHERIT` und `VALID UNTIL 'infinity'` sind die Standardoptionen für CREATE ROLE, sofern nicht anders angegeben.

Standardmäßig verfügt `postgres` über Berechtigungen, die der `rds_superuser`-Rolle gewährt wurden, und über Berechtigungen zum Erstellen von Rollen und Datenbanken. Die `rds_superuser`-Rolle erlaubt dem `postgres`-Benutzer, folgende Aktionen auszuführen:

- Erweiterungen für die Verwendung mit Aurora PostgreSQL. Weitere Informationen finden Sie unter Arbeiten mit Erweiterungen und Fremddaten-Wrappern.
- Rollen für Benutzer erstellen und Benutzern Berechtigungen gewähren. Weitere Informationen dazu finden Sie im Abschnitt CREATE ROLE und GRANT der PostgreSQL-Dokumentation.
- Datenbanken erstellen. Weitere Informationen finden Sie im Abschnitt CREATE DATABASE der PostgreSQL-Dokumentation.
- Gewähren Sie `rds_superuser`-Berechtigungen anderen Benutzerrollen, die nicht über diese Berechtigungen verfügen, und widerrufen Sie diese Berechtigungen bei Bedarf. Es wird

empfohlen, diese Rolle nur denjenigen Benutzern zu gewähren, die Superuser-Aufgaben ausführen. Mit anderen Worten, Sie können diese Rolle Datenbankadministratoren (DBAs) oder Systemadministratoren erteilen.

- Die `rds_replication`-Rolle Datenbankbenutzern gewähren (oder entziehen), die nicht über die `rds_superuser`-Rolle verfügen.
- Die `rds_password`-Rolle Datenbankbenutzern gewähren (oder entziehen), die nicht über die `rds_superuser`-Rolle verfügen.
- Statusinformationen über alle Datenbankverbindungen über die Ansicht `pg_stat_activity` abrufen. Bei Bedarf kann `rds_superuser` alle Verbindungen mit `pg_terminate_backend` oder `pg_cancel_backend` stoppen.

In der `CREATE ROLE postgres...`-Anweisung können Sie sehen, dass die `postgres`-Benutzerrolle PostgreSQL ausdrücklich `superuser`-Berechtigungen verweigert. Aurora PostgreSQL ist ein verwalteter Service, sodass Sie nicht auf das Host-Betriebssystem zugreifen können und keine Verbindung mit dem `superuser`-PostgreSQL-Konto herstellen können. Viele der Aufgaben, die `superuser`-Zugriff auf einem eigenständigem PostgreSQL erfordern, werden von Aurora automatisch verwaltet.

Weitere Informationen zum Gewähren von Berechtigungen finden Sie unter GRANT in der PostgreSQL-Dokumentation.

Die `rds_superuser`-Rolle ist eine von mehreren vordefinierten Rollen in einem Aurora-PostgreSQL-DB-Cluster.

> **Note**
>
> In PostgreSQL 13 und früheren Versionen werden vordefinierte Rollen als Standardrollen bezeichnet.

In der folgenden Liste finden Sie einige der anderen vordefinierten Rollen, die automatisch für einen neuen Aurora-PostgreSQL-DB-Cluster erstellt werden. Vordefinierte Rollen und ihre Berechtigungen können nicht geändert werden. Sie können Berechtigungen für diese vordefinierten Rollen nicht löschen, umbenennen oder ändern. Jeder entsprechende Versuch führt zu einem Fehler.

- rds_passwort – Eine Rolle, die Passwörter ändern und Passwortbeschränkungen für Datenbankbenutzer einrichten kann. Die `rds_superuser` Rolle wird standardmäßig mit dieser

Rolle gewährt und kann die Rolle Datenbankbenutzern gewähren. Weitere Informationen finden Sie unter Steuern des Benutzerzugriffs auf die PostgreSQL−Datenbank.

- Bei Versionen von RDS für PostgreSQL vor 14 kann die `rds_password` Rolle Passwörter ändern und Passwortbeschränkungen für Datenbankbenutzer und Benutzer mit `rds_superuser` Rolle einrichten. Ab RDS für PostgreSQL Version 14 und höher kann die `rds_password` Rolle Passwörter ändern und Passwortbeschränkungen nur für Datenbankbenutzer einrichten. Nur Benutzer mit -`rds_superuser`Rolle können diese Aktionen für andere Benutzer mit -`rds_superuser`Rolle ausführen.

- rdsadmin – Eine Rolle, die erstellt wurde, um viele der Verwaltungsaufgaben zu erledigen, die der Administrator mit `superuser`-Berechtigungen für eine eigenständige PostgreSQL-Datenbank ausführt. Diese Rolle wird intern von Aurora PostgreSQL für viele Verwaltungsaufgaben verwendet.

Wenn Sie alle vordefinierten Rollen anzeigen möchten, können Sie eine Verbindung mit der primären Instance Ihres Aurora-PostgreSQL-DB-Clusters herstellen und den Metabefehl `psql \du` verwenden. Die Ausgabe sieht wie folgt aus:

```
List of roles
  Role name   |      Attributes                    |      Member of
--------------+------------------------------------+-----------------------------------
postgres      | Create role, Create DB            +| {rds_superuser}
              | Password valid until infinity      |
rds_superuser | Cannot login                       | {pg_monitor,pg_signal_backend,
              |                                   +|   rds_replication,rds_password}
...
```

In der Ausgabe sehen Sie, dass `rds_superuser` keine Datenbankbenutzerrolle ist (sie kann sich nicht anmelden), aber über die Berechtigungen vieler anderer Rollen verfügt. Sie können auch sehen, dass dieser Datenbankbenutzer `postgres` Mitglied der `rds_superuser`-Rolle ist. Wie bereits erwähnt, ist `postgres` der Standardwert auf der Seite Create database (Datenbank erstellen) der Amazon-RDS-Konsole. Wenn Sie einen anderen Namen gewählt haben, wird dieser Name stattdessen in der Rollenliste angezeigt.

> **Note**
>
> Aurora-PostgreSQL-Versionen 15.2 und 14.7 führten ein restriktives Verhalten der `rds_superuser`-Rolle ein. Einem Aurora PostgreSQL-Benutzer muss die `CONNECT`-Berechtigung für die entsprechende Datenbank zugewiesen werden, um eine Verbindung herzustellen, auch wenn dem Benutzer die `rds_superuser`-Rolle zugewiesen ist. Vor den

Versionen 14.7 und 15.2 von Aurora PostgreSQL konnte ein Benutzer eine Verbindung zu jeder Datenbank und Systemtabelle herstellen, wenn dem Benutzer die `rds_superuser`-Rolle zugewiesen war. Dieses restriktive Verhalten steht im Einklang mit den Verpflichtungen von AWS und Amazon Aurora zur kontinuierlichen Verbesserung der Sicherheit.
Bitte aktualisieren Sie die entsprechende Logik in Ihren Anwendungen, falls die oben genannte Erweiterung Auswirkungen hat.

Steuern des Benutzerzugriffs auf die PostgreSQL−Datenbank

Neue Datenbanken in PostgreSQL werden immer mit Standardberechtigungen im `public`-Schema der Datenbank erstellt, mit dem alle Datenbankbenutzer und -rollen Objekte erstellen können. Diese Berechtigungen ermöglichen es Datenbankbenutzern, eine Verbindung mit der Datenbank herzustellen und während der Verbindung temporäre Tabellen zu erstellen.

Es wird empfohlen, diese `public`-Standardberechtigungen zu widerrufen, um den Benutzerzugriff auf die Datenbank-Instances, die Sie auf Ihrem Primärknoten des Aurora-PostgreSQL-DB-Clusters erstellen, besser kontrollieren können. Danach erteilen Sie Datenbankbenutzern auf einer detaillierteren Basis spezifische Berechtigungen, wie im Folgenden gezeigt.

So richten Sie Rollen und Berechtigungen für eine neue Datenbank-Instance ein

Angenommen, Sie richten eine Datenbank für einen neu erstellten Aurora-PostgreSQL-DB-Cluster ein, die von mehreren Forschenden verwendet wird, die alle Lese-/Schreibzugriff auf die Datenbank benötigen.

1. Verwenden Sie `psql` (oder pgAdmin) zum Herstellen einer Verbindung mit dem primären Aurora-PostgreSQL-DB-Cluster:

   ```
   psql --host=your-cluster-instance-1.666666666666.aws-region.rds.amazonaws.com --
   port=5432 --username=postgres --password
   ```

   Geben Sie bei der Aufforderung Ihr Passwort ein. Der `psql`-Client verbindet und zeigt die standardmäßige administrative Verbindungsdatenbank `postgres=>` als Eingabeaufforderung an.
2. Gehen Sie wie folgt vor, um zu verhindern, dass Datenbankbenutzer Objekte im `public`-Schema erstellen:

   ```
   postgres=> REVOKE CREATE ON SCHEMA public FROM PUBLIC;
   ```

```
REVOKE
```

3. Als Nächstes erstellen Sie eine neue Datenbank-Instance:

```
postgres=> CREATE DATABASE lab_db;
CREATE DATABASE
```

4. Widerrufen Sie alle Berechtigungen aus dem PUBLIC-Schema in dieser neuen Datenbank.

```
postgres=> REVOKE ALL ON DATABASE lab_db FROM public;
REVOKE
```

5. Erstellen Sie eine Rolle für Datenbankbenutzer.

```
postgres=> CREATE ROLE lab_tech;
CREATE ROLE
```

6. Geben Sie Datenbankbenutzern mit dieser Rolle die Möglichkeit, eine Verbindung mit der Datenbank herzustellen.

```
postgres=> GRANT CONNECT ON DATABASE lab_db TO lab_tech;
GRANT
```

7. Gewähren Sie allen Benutzern mit der `lab_tech`-Rolle alle Berechtigungen für diese Datenbank.

```
postgres=> GRANT ALL PRIVILEGES ON DATABASE lab_db TO lab_tech;
GRANT
```

8. Erstellen Sie Datenbankbenutzer wie folgt:

```
postgres=> CREATE ROLE lab_user1 LOGIN PASSWORD 'change_me';
CREATE ROLE
postgres=> CREATE ROLE lab_user2 LOGIN PASSWORD 'change_me';
CREATE ROLE
```

9. Gewähren Sie diesen beiden Benutzern die Berechtigungen, die mit der lab_tech-Rolle verknüpft sind:

```
postgres=> GRANT lab_tech TO lab_user1;
GRANT ROLE
postgres=> GRANT lab_tech TO lab_user2;
```

```
GRANT ROLE
```

An dieser Stelle können `lab_user1` und `lab_user2` eine Verbindung mit der `lab_db`-Datenbank herstellen. Dieses Beispiel folgt nicht den bewährten Methoden für den Unternehmensgebrauch, darunter das Erstellen mehrerer Datenbank-Instances, verschiedener Schemas und das Erteilen eingeschränkter Berechtigungen. Umfassende Informationen und zusätzliche Szenarien finden Sie unter Verwalten von PostgreSQL-Benutzern und -Rollen.

Weitere Informationen zu Berechtigungen in PostgreSQL-Datenbanken finden Sie unter dem Befehl GRANT in der PostgreSQL-Dokumentation.

Delegieren und Steuern der Benutzerpasswortverwaltung

Als DBA sollten Sie ggf. die Verwaltung von Benutzerpasswörtern delegieren. Oder Sie möchten verhindern, dass Datenbankbenutzer ihre Passwörter ändern oder Passwortbeschränkungen wie die Lebensdauer des Passworts neu konfigurieren. Um sicherzustellen, dass nur die von Ihnen ausgewählten Datenbankbenutzer Passworteinstellungen ändern können, können Sie die Funktion zur eingeschränkten Passwortverwaltung aktivieren. Wenn Sie diese Funktion aktivieren, können nur die Datenbankbenutzer, denen die `rds_password`-Rolle gewährt wurde, Passwörter verwalten.

> **Note**
>
> Um die eingeschränkte Passwortverwaltung nutzen zu können, muss Ihr DB-Cluster von Aurora PostgreSQL Amazon Aurora PostgreSQL 10.6 oder höher ausführen.

Standardmäßig lautet diese Funktion `off`, wie im Folgenden gezeigt:

```
postgres=> SHOW rds.restrict_password_commands;
  rds.restrict_password_commands
--------------------------------
 off
(1 row)
```

Zum Aktivieren dieser Funktion verwenden Sie eine benutzerdefinierte Parametergruppe und ändern die Einstellung für `rds.restrict_password_commands` in 1. Stellen Sie sicher, dass Sie Ihre primäre DB-Instance von Aurora PostgreSQL neu starten, damit die Einstellung wirksam wird.

Wenn diese Funktion aktiv ist, werden für die folgenden SQL-Befehle `rds_password`-Berechtigungen benötigt:

```
CREATE ROLE myrole WITH PASSWORD 'mypassword';
CREATE ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2023-01-01';
ALTER ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2023-01-01';
ALTER ROLE myrole WITH PASSWORD 'mypassword';
ALTER ROLE myrole VALID UNTIL '2023-01-01';
ALTER ROLE myrole RENAME TO myrole2;
```

Das Umbenennen einer Rolle (`ALTER ROLE myrole RENAME TO newname`) ist auch eingeschränkt, wenn das Passwort den MD5-Hashing-Algorithmus verwendet.

Wenn diese Funktion aktiv ist, generiert jeder Versuch, einen dieser SQL-Befehle ohne die `rds_password`-Rollenberechtigungen auszuführen, den folgenden Fehler:

```
ERROR: must be a member of rds_password to alter passwords
```

Wir empfehlen, dass Sie die `rds_password`-Berechtigung nur wenigen Rollen zuweisen, die Sie ausschließlich für die Passwortverwaltung verwenden. Wenn Sie `rds_password`-Berechtigungen für Datenbankbenutzer erteilen, die keine `rds_superuser`-Berechtigungen haben, müssen Sie ihnen auch das `CREATEROLE`-Attribut erteilen.

Stellen Sie sicher, dass Sie die Passwortanforderungen wie Ablaufdatum und erforderliche Komplexität auf Kundenseite überprüfen. Wenn Sie Ihr eigenes clientseitiges Dienstprogramm für passwortbezogene Änderungen verwenden, muss das Dienstprogramm Mitglied von `rds_password` sein und über `CREATE ROLE`-Berechtigungen verfügen.

Verwenden von SCRAM für die PostgreSQL-Passwortverschlüsselung

Der Salted Challenge Response Authentication Mechanism (SCRAM) ist eine Alternative zum standardmäßigen Message Digest (MD5)-Algorithmus von PostgreSQL zum Verschlüsseln von Passwörtern. Der SCRAM-Authentifizierungsmechanismus gilt als sicherer als MD5. Weitere Informationen zu diesen beiden verschiedenen Ansätzen zur Sicherung von Passwörtern finden Sie unter Passwortauthentifizierung in der PostgreSQL-Dokumentation.

Wir empfehlen, SCRAM anstelle von MD5 als Passwortverschlüsselungsschema für den Aurora-PostgreSQL-DB-Cluster zu verwenden. Ab der Veröffentlichung von Aurora PostgreSQL 14 wird SCRAM in allen verfügbaren Aurora-PostgreSQL-Versionen unterstützt, einschließlich der Versionen

10, 11, 12, 13 und 14. Es ist ein kryptografischer Challenge-Response-Mechanismus, der den scram–sha-256-Algorithmus zur Passwortauthentifizierung und -verschlüsselung nutzt.

Möglicherweise müssen Sie Bibliotheken aktualisieren, damit Ihre Clientanwendungen SCRAM unterstützen können. JDBC-Versionen vor 42.2.0 unterstützen SCRAM beispielsweise nicht. Weitere Informationen finden Sie unter PostgreSQL-JDBC-Treiber in der Dokumentation zu PostgreSQL-JDBC-Treibern. Für eine Liste anderer PostgreSQL-Treiber und SCRAM-Unterstützung siehe die Treiberliste in der PostgreSQL-Dokumentation.

> **Note**
>
> Aurora PostgreSQL Version 14 und höhere Versionen unterstützen scram-sha-256 standardmäßig zur Passwortverschlüsselung für neue DB-Cluster. Das heißt, für die standardmäßige DB-Cluster-Parametergruppe (`default.aurora-postgresql14`) ist der `password_encryption`-Wert auf scram-sha-256 festgelegt.

Einrichten des Aurora-PostgreSQL-DB-Clusters, sodass SCRAM erforderlich ist

Bei Aurora PostgreSQL 14.3 und höheren Versionen können Sie verlangen, dass der Aurora-PostgreSQL-DB-Cluster nur Passwörter akzeptiert, die den scram-sha-256-Algorithmus verwenden.

> **Important**
>
> Wenn Sie bei vorhandenen RDS-Proxys mit PostgreSQL-Datenbanken die Datenbankauthentifizierung so ändern, dass nur `SCRAM` verwendet wird, ist der Proxy für bis zu 60 Sekunden nicht verfügbar. Um das Problem zu vermeiden, führen Sie einen der folgenden Schritte aus:
>
> - Stellen Sie sicher, dass die Datenbank sowohl die `SCRAM`- als auch die `MD5`-Authentifizierung zulässt.
> - Wenn Sie nur die `SCRAM`-Authentifizierung verwenden möchten, erstellen Sie einen neuen Proxy, migrieren Sie Ihren Anwendungsdatenverkehr auf den neuen Proxy und löschen Sie dann den zuvor mit der Datenbank verknüpften Proxy.

Bevor Sie Änderungen an Ihrem System vornehmen, vergewissern Sie sich, dass Sie den folgenden Prozess komplett verstehen:

- Sammeln Sie Informationen über alle Rollen und Passwortverschlüsselung für alle Datenbankbenutzer.
- Überprüfen Sie die Parametereinstellungen für Ihren Aurora-PostgreSQL-DB-Cluster für die Parameter, die die Passwortverschlüsselung steuern.
- Wenn Ihr Aurora-PostgreSQL-DB-Cluster eine Standardparametergruppe verwendet, müssen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe erstellen und sie auf Ihren Aurora-PostgreSQL-DB-Cluster anwenden, damit Sie bei Bedarf Parameter ändern können. Wenn Ihr Aurora-PostgreSQL-DB-Cluster eine benutzerdefinierte Parametergruppe verwendet, können Sie die erforderlichen Parameter bei Bedarf später im Prozess ändern.
- Ändern Sie den Parameter `password_encryption` in `scram-sha-256`.
- Informieren Sie alle Datenbankbenutzer, dass sie ihre Passwörter aktualisieren müssen. Wiederholen Sie diesen Schritt für Ihr `postgres`-Konto. Die neuen Passwörter werden mit dem scram-sha-256-Algorithmus verschlüsselt und gespeichert.
- Stellen Sie sicher, dass alle Passwörter mit diesem Verschlüsselungstyp verschlüsselt sind.
- Wenn alle Passwörter scram-sha-256 verwenden, können Sie den `rds.accepted_password_auth_method`-Parameter von `md5+scram` in `scram-sha-256` ändern.

> **Warning**
>
> Nachdem Sie `rds.accepted_password_auth_method` nur in scram-sha-256 geändert haben, können Benutzer (Rollen) mit `md5`-verschlüsselten Passwörtern keine Verbindung herstellen.

Vorbereiten der SCRAM-Anforderung für Ihren Aurora-PostgreSQL-DB-Cluster

Bevor Sie Änderungen an Ihrem Aurora-PostgreSQL-DB-Cluster, vornehmen, überprüfen Sie alle vorhandenen Datenbankbenutzerkonten. Überprüfen Sie auch die Art der Verschlüsselung, die für Passwörter verwendet wird. Sie können für diese Aufgaben die `rds_tools`-Erweiterung verwenden. Diese Erweiterung wird in Aurora PostgreSQL 13.1 und höheren Versionen unterstützt.

So erhalten Sie eine Liste der Datenbankbenutzer (Rollen) und Passwortverschlüsselungsmethoden

1. Verwenden Sie `psql` zum Herstellen einer Verbindung mit der primären Instance Ihres Aurora-PostgreSQL-DB-Clusters , wie im Folgenden gezeigt.

```
psql --host=cluster-name-instance-1.111122223333.aws-region.rds.amazonaws.com --
port=5432 --username=postgres --password
```

2. Installieren Sie die `rds_tools`-Erweiterung.

```
postgres=> CREATE EXTENSION rds_tools;
CREATE EXTENSION
```

3. Rufen Sie eine Auflistung der Rollen und Verschlüsselungsmethoden ab.

```
postgres=> SELECT * FROM
      rds_tools.role_password_encryption_type();
```

Die Ausgabe entspricht weitgehend der folgenden.

```
       rolname        | encryption_type
----------------------+-----------------
 pg_monitor           |
 pg_read_all_settings |
 pg_read_all_stats    |
 pg_stat_scan_tables  |
 pg_signal_backend    |
 lab_tester           | md5
 user_465             | md5
 postgres             | md5
(8 rows)
```

Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe

> **Note**
>
> Wenn Ihr Aurora-PostgreSQL-DB-Cluster bereits eine benutzerdefinierte Parametergruppe verwendet, müssen Sie keine neue erstellen.

Eine Übersicht über Parametergruppen für Aurora finden Sie unter Erstellen einer DB-Cluster-Parametergruppe.

Der für Passwörter verwendete Passwortverschlüsselungstyp wird in einem Parameter, `password_encryption`, festgelegt. Die Verschlüsselung, die der Aurora-PostgreSQL-DB-Cluster zulässt, wird in einem anderen Parameter, `rds.accepted_password_auth_method`, festgelegt. Wenn Sie den Standardwert eines dieser Parameter ändern, müssen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe erstellen und auf Ihren Cluster anwenden.

Sie können auch die AWS Management Console oder die RDS-API verwenden, um eine benutzerdefinierte DB-Cluster-Parametergruppe erstellen. Weitere Informationen finden Sie unter Erstellen einer DB-Cluster-Parametergruppe.

Sie können jetzt die benutzerdefinierte Parametergruppe Ihrer DB-Instance zuordnen.

So erstellen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe

1. Verwenden Sie den CLI-Befehl `create-db-cluster-parameter-group` zum Erstellen der benutzerdefinierten Parametergruppe für den Cluster. Folgendes Beispiel verwendet `aurora-postgresql13` als Quelle für diese benutzerdefinierte Parametergruppe.

   Für Linux, macOSoder Unix:

   ```
   aws rds create-db-cluster-parameter-group --db-cluster-parameter-group-name 'docs-lab-scram-passwords' \
     --db-parameter-group-family aurora-postgresql13  --description 'Custom DB cluster parameter group for SCRAM'
   ```

   Windows:

   ```
   aws rds create-db-cluster-parameter-group --db-cluster-parameter-group-name "docs-lab-scram-passwords" ^
     --db-parameter-group-family aurora-postgresql13  --description "Custom DB cluster parameter group for SCRAM"
   ```

   Sie können jetzt die benutzerdefinierte Parametergruppe Ihrem Cluster zuordnen.

2. Verwenden Sie den CLI-Befehl `modify-db-cluster` zum Anwenden dieser benutzerdefinierten Parametergruppe auf Ihren Aurora-PostgreSQL-DB-Cluster.

   Für Linux, macOSoder Unix:

   ```
   aws rds modify-db-cluster --db-cluster-identifier 'your-instance-name' \
   ```

```
        --db-cluster-parameter-group-name "docs-lab-scram-passwords
```

Windows:

```
aws rds modify-db-cluster --db-cluster-identifier "your-instance-name" ^
        --db-cluster-parameter-group-name "docs-lab-scram-passwords
```

Zum erneuten Synchronisieren Ihres Aurora-PostgreSQL-DB-Clusters mit Ihrer benutzerdefinierten DB-Cluster-Parametergruppe starten Sie die primäre und alle anderen Instances des Clusters neu.

Konfigurieren der Passwortverschlüsselung für die Verwendung von SCRAM

Der Passwortverschlüsselungsmechanismus, der von einem Aurora-PostgreSQL-DB-Cluster verwendet wird, ist in der DB-Cluster-Parametergruppe auf den Parameter `password_encryption` festgelegt. Zulässige Werte sind keine Angabe, `md5` oder `scram-sha-256`. Der Standardwert hängt von der Version von Aurora PostgreSQL wie folgt ab:

- Aurora PostgreSQL 14 – Der Standardwert ist `scram-sha-256`.
- Aurora PostgreSQL 13 – Der Standardwert ist `md5`.

Mit einer benutzerdefinierten DB-Cluster-Parametergruppe , die Ihrem Aurora-PostgreSQL-DB-Cluster angefügt ist, können Sie die Werte für den Passwortverschlüsselungsparameter ändern.

Name	Values	Allowed values	Modifiable	Source	Apply type
password_encryption	scram-sha-256	md5, scram-sha-256	true	system	dynamic
rds.accepted_password_auth_method	md5+scram	md5+scram, scram	true	system	dynamic

So ändern Sie die Passwortverschlüsselungseinstellung in scram-sha-256

- Ändern Sie den Wert der Passwortverschlüsselung in scram-sha-256, wie nachfolgend gezeigt. Die Änderung kann sofort angewendet werden, da der Parameter dynamisch ist. Daher ist kein Neustart erforderlich, damit die Änderung wirksam wird.

  Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-name \
  'docs-lab-scram-passwords' --parameters
 'ParameterName=password_encryption,ParameterValue=scram-
sha-256,ApplyMethod=immediate'
```

Windows:

```
aws rds modify-db-parameter-group --db-parameter-group-name ^
  "docs-lab-scram-passwords" --parameters
 "ParameterName=password_encryption,ParameterValue=scram-
sha-256,ApplyMethod=immediate"
```

Migrieren von Passwörtern für Benutzerrollen zu SCRAM

Sie können Passwörter für Benutzerrollen wie folgt zu SCRAM migrieren.

So migrieren Sie Passwörter für Datenbankbenutzer (Rolle) von MD5 zu SCRAM

1. Melden Sie sich als Administratorbenutzer an (Standardbenutzer `postgres`), wie nachfolgend gezeigt.

   ```
   psql --host=cluster-name-instance-1.111122223333.aws-region.rds.amazonaws.com --
   port=5432 --username=postgres --password
   ```

2. Überprüfen Sie die Einstellung des `password_encryption`-Parameters auf der DB-Instance von RDS for PostgreSQL mithilfe des folgenden Befehls.

   ```
   postgres=> SHOW password_encryption;
    password_encryption
   ---------------------
    md5
    (1 row)
   ```

3. Ändern Sie den Wert dieses Parameters in scram-sha-256. Dies ist ein dynamischer Parameter, sodass Sie die Instance nach dieser Änderung nicht neu starten müssen. Überprüfen Sie den Wert erneut, um sicherzustellen, dass er jetzt auf `scram-sha-256` festgelegt ist. Gehen Sie dazu wie folgt vor.

   ```
   postgres=> SHOW password_encryption;
   ```

```
 password_encryption
---------------------
 scram-sha-256
 (1 row)
```

4. Bitten Sie alle Datenbankbenutzer, ihre Passwörter zu ändern. Stellen Sie sicher, dass Sie auch Ihr eigenes Passwort für das `postgres`-Konto ändern (der Datenbankbenutzer mit `rds_superuser`-Berechtigungen).

```
labdb=> ALTER ROLE postgres WITH LOGIN PASSWORD 'change_me';
ALTER ROLE
```

5. Wiederholen Sie den Vorgang für alle Datenbanken auf dem Aurora-PostgreSQL-DB-Cluster.

Ändern des Parameters, um SCRAM zu erfordern

Dies ist der letzte Schritt in diesem Prozess. Nachdem Sie die Änderung im folgenden Verfahren vorgenommen haben, können sich Benutzerkonten (Rollen), die nach wie vor die `md5`-Verschlüsselung für Passwörter verwenden, nicht beim Aurora-PostgreSQL-DB-Cluster anmelden.

Die `rds.accepted_password_auth_method` gibt die Verschlüsselungsmethode an, die der Aurora-PostgreSQL-DB-Cluster als Benutzerpasswort beim Anmeldevorgang akzeptiert. Der Standardwert ist `md5+scram`, was bedeutet, dass eine der beiden Methoden akzeptiert wird. Im folgenden Bild finden Sie die Standardeinstellung für diesen Parameter.

Name	Values	Allowed values	Modifiable	Source	Apply type
password_encryption	scram-sha-256	md5, scram-sha-256	true	system	dynamic
rds.accepted_password_auth_method	md5+scram	md5+scram, scram	true	system	dynamic

Die zulässigen Werte für diesen Parameter sind `md5+scram` oder nur `scram`. Durch Ändern dieses Parameterwerts in `scram` wird er erforderlich.

So ändern Sie den Parameterwert, sodass eine SCRAM-Authentifizierung für Passwörter erforderlich ist

1. Stellen Sie sicher, dass alle Datenbank-Benutzerpasswörter für alle Datenbanken auf Ihrem Aurora-PostgreSQL-DB-Cluster `scram-sha-256` für die Passwortverschlüsselung verwenden.

Fragen Sie hierzu `rds_tools` für die Rolle (Benutzer) und den Verschlüsselungstyp wie folgt ab.

```
postgres=> SELECT * FROM rds_tools.role_password_encryption_type();
  rolname        | encryption_type
  ---------------------+----------------
  pg_monitor           |
  pg_read_all_settings |
  pg_read_all_stats    |
  pg_stat_scan_tables  |
  pg_signal_backend    |
  lab_tester           | scram-sha-256
  user_465             | scram-sha-256
  postgres             | scram-sha-256
  ( rows)
```

2. Wiederholen Sie die Abfrage auf allen DB-Instances Ihres Aurora-PostgreSQL-DB-Clusters.

   Wenn alle Passwörter scram-sha-256 verwenden, können Sie fortfahren.

3. Ändern Sie den Wert der akzeptierten Passwortauthentifizierung in scram-sha-256 wie folgt.

   Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-name 'docs-
lab-scram-passwords' \
  --parameters
 'ParameterName=rds.accepted_password_auth_method,ParameterValue=scram,ApplyMethod=immediat
```

   Windows:

```
aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-name "docs-
lab-scram-passwords" ^
  --parameters
 "ParameterName=rds.accepted_password_auth_method,ParameterValue=scram,ApplyMethod=immediat
```

Sicherung von Aurora-PostgreSQL-Daten mit SSL/TLS

Amazon RDS unterstützt Secure Socket Layer (SSL) und Transport Layer Security (TLS) Verschlüsselung für Aurora PostgreSQL DB-Cluster. Mit SSL/TLS können Sie eine Verbindung zwischen Ihren Anwendungen und Ihren Aurora PostgreSQL DB-Clustern verschlüsseln. Sie

können auch erzwingen, dass alle Verbindungen zu Ihrem Aurora PostgreSQL DB-Cluster SSL/TLS verwenden. Amazon Aurora PostgreSQL unterstützt jetzt Transport Layer Security (TLS) in den Versionen 1.1 und 1.2. Wir empfehlen die Verwendung von TLS 1.2 für verschlüsselte Verbindungen. Wir haben Unterstützung für TLSv1.3 für die folgenden Versionen von Aurora PostgreSQL hinzugefügt:

- 15.3 und alle höheren Versionen
- 14.8 und höhere 14-Versionen
- 13.11 und höhere 13-Versionen
- 12.15 und höhere 12-Versionen
- 11.20 und höhere 11-Versionen

Allgemeine Informationen über SSL/TLS-Unterstützung und PostgreSQL-Datenbanken finden Sie unter SSL-Unterstützung in der PostgreSQL-Dokumentation. Informationen zur Verwendung einer SSL/TLS-Verbindung über JDBC finden Sie unter Konfiguration des Clients in der PostgreSQL-Dokumentation.

Themen

- Erfordernis einer SSL/TLS-Verbindung zu einem Aurora PostgreSQL DB-Cluster
- Ermitteln des SSL/TLS-Verbindungsstatus
- Konfigurieren von Chiffrier-Suiten für Verbindungen mit Aurora-PostgreSQL-DB-Clustern

SSL/TLS-Unterstützung ist in allen AWS Regionen für Aurora PostgreSQL verfügbar. Amazon RDS erstellt ein SSL/TLS-Zertifikat für Ihren Aurora PostgreSQL DB-Cluster, wenn der DB-Cluster erstellt wird. Wenn Sie die SSL/TLS-Zertifikatsprüfung aktivieren, enthält das SSL/TLS-Zertifikat den DB-Cluster-Endpunkt als Common Name (CN) für das SSL/TLS-Zertifikat, um Spoofing-Angriffe zu verhindern.

Um sich mit einem Aurora PostgreSQL DB-Cluster über SSL/TLS zu verbinden

1. Laden Sie das Zertifikat herunter.

   Informationen zum Herunterladen von Zertifikaten finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .
2. Importieren Sie das Zertifikat in Ihr Betriebssystem.
3. Verbinden Sie sich mit Ihrem Aurora PostgreSQL DB-Cluster über SSL/TLS.

Wenn Sie eine Verbindung über SSL/TLS herstellen, kann Ihr Client wählen, ob er die Zertifikatskette überprüfen möchte oder nicht. Wenn Ihre Verbindungsparameter `sslmode=verify-ca` oder `sslmode=verify-full` angeben, verlangt Ihr Client, dass sich die RDS CA-Zertifikate im Trust Store befinden oder von der Verbindungs-URL referenziert werden. Diese Anforderung dient zur Prüfung der Zertifikatskette, die Ihr Datenbankzertifikat signiert.

Wenn ein Client, z. B. psql oder JDBC, mit SSL/TLS-Unterstützung konfiguriert ist, versucht der Client zunächst, eine Verbindung zur Datenbank mit SSL/TLS herzustellen. Wenn der Client keine Verbindung mit SSL/TLS herstellen kann, greift er auf eine Verbindung ohne SSL/TLS zurück. Standardmäßig ist die `sslmode`-Option für JDBC- und libpq-basierte Clients auf `prefer` festgelegt.

Verwenden Sie den Parameter `sslrootcert`, um auf das Zertifikat zu verweisen, beispielsweise `sslrootcert=rds-ssl-ca-cert.pem`.

Das folgende Beispiel zeigt psql zur Herstellung einer Verbindung mit einem Aurora-PostgreSQL-DB-Cluster:

```
$ psql -h testpg.cdhmuqifdpib.us-east-1.rds.amazonaws.com -p 5432 \
    "dbname=testpg user=testuser sslrootcert=rds-ca-2015-root.pem sslmode=verify-full"
```

Erfordernis einer SSL/TLS-Verbindung zu einem Aurora PostgreSQL DB-Cluster

Sie können verlangen, dass Verbindungen zu Ihrem Aurora PostgreSQL DB-Cluster SSL/TLS verwenden, indem Sie den Parameter `rds.force_ssl` verwenden. Standardmäßig ist der Parameter `rds.force_ssl` auf 0 (aus) festgelegt. Sie können den Parameter `rds.force_ssl` auf 1 (on) setzen, um SSL/TLS für Verbindungen zu Ihrem DB-Cluster zu verlangen. Die Aktualisierung des Parameters `rds.force_ssl` setzt auch den PostgreSQL-Parameter `ssl` auf 1 (on) und modifiziert die Datei Ihres DB-Clusters `pg_hba.conf`, um die neue SSL/TLS-Konfiguration zu unterstützen.

Sie können den Parameterwert `rds.force_ssl` festlegen, indem Sie die Parametergruppe für Ihren DB-Cluster aktualisieren. Wenn es sich bei der Parametergruppe für Ihren DB-Cluster nicht um die Standardparametergruppe handelt und der Parameter `ssl` bereits auf 1 gesetzt ist, müssen Sie Ihren DB-Cluster nicht neu starten, wenn Sie den Parameter `rds.force_ssl` auf 1 setzen. Andernfalls

müssen Sie Ihren DB-Cluster neu starten, damit die Änderungen übernommen werden. Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Wenn der Parameter `rds.force_ssl` für einen DB-Cluster auf 1 gesetzt ist, wird beim Verbindungsaufbau eine Ausgabe ähnlich der folgenden angezeigt, die darauf hinweist, dass SSL/TLS jetzt erforderlich ist:

```
$ psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser
psql (9.3.12, server 9.4.4)
WARNING: psql major version 9.3, server major version 9.4.
Some psql features might not work.
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.

postgres=>
```

Ermitteln des SSL/TLS-Verbindungsstatus

Der Verschlüsselungsstatus Ihrer Verbindung wird auf dem Anmelde-Banner angezeigt, wenn Sie sich mit dem DB-Cluster verbinden:

```
Password for user master:
psql (9.3.12)
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.

postgres=>
```

Sie können auch die Erweiterung `sslinfo` laden und dann die Funktion `ssl_is_used()` aufrufen, um festzustellen, ob SSL/TLS verwendet wird. Die Funktion gibt `t` zurück, wenn die Verbindung SSL/TLS verwendet, andernfalls gibt sie `f` zurück.

```
postgres=> create extension sslinfo;
CREATE EXTENSION

postgres=> select ssl_is_used();
 ssl_is_used
---------
t
```

```
(1 row)
```

Sie können den Befehl `select ssl_cipher()` verwenden, um die SSL/TLS-Verschlüsselung zu bestimmen:

```
postgres=> select ssl_cipher();
ssl_cipher
--------------------
DHE-RSA-AES256-SHA
(1 row)
```

Wenn Sie `set rds.force_ssl` aktivieren und Ihren DB-Cluster neu starten, werden Nicht-SSL-Verbindungen abgelehnt, und die folgende Mitteilung wird angezeigt:

```
$ export PGSSLMODE=disable
$ psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser
psql: FATAL: no pg_hba.conf entry for host "host.ip", user "someuser", database
 "postgres", SSL off
$
```

Informationen zur Option `sslmode` finden Sie unter Datenbankverbindung-Steuerungsfunktionen in der PostgreSQL-Dokumentation.

Konfigurieren von Chiffrier-Suiten für Verbindungen mit Aurora-PostgreSQL-DB-Clustern

Durch die Verwendung von konfigurierbaren Chiffrier-Suiten können Sie mehr Kontrolle über die Sicherheit Ihrer Datenbankverbindungen haben. Sie können eine Liste von Chiffrier-Suiten angeben, die Sie zum Sichern von SSL/TLS-Verbindungen zu Ihrer Datenbank des Clients zulassen möchten. Mit konfigurierbaren Chiffrier-Suiten können Sie die Verbindungsverschlüsselung steuern, die Ihr Datenbankserver akzeptiert. Dies hilft, die Verwendung von unsicheren oder veralteten Chiffren zu verhindern.

Konfigurierbare Chiffrier-Suiten werden in Aurora PostgreSQL Version 11.8 und höher unterstützt.

Um die Liste der zulässigen Chiffren für die Verschlüsselung von Verbindungen anzugeben, ändern Sie die `ssl_ciphers`-Cluster-Parameter. Legen Sie den Parameter `ssl_ciphers` mithilfe der AWS Management Console, der AWS CLI oder der RDS-API auf eine Zeichenfolge von kommagetrennten

Verschlüsselungswerten in einer Cluster-Parametergruppe fest. Um Cluster-Parameter festzulegen, siehe Ändern von Parametern in einer DB-Cluster-Parametergruppe.

Die folgende Tabelle zeigt die unterstützten Verschlüsselungen für die gültigen Versionen der Aurora-PostgreSQL-Engine.

Engine-Versionen für Aurora PostgreSQL	Unterstützte Verschlüsselungen
9.6, 10.20 und niedriger, 11.15 und niedriger, 12.10 und niedriger, 13.6 und niedriger	• DHE-RSA-AES128-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-SHA • DHE-RSA-AES256-SHA256 • DHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES256-GCM-SHA384
10.21, 11.16, 12.11, 13.7, 14.3 und 14.4	• DHE-RSA-AES128-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-SHA • DHE-RSA-AES256-SHA256 • DHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA

Engine-Versionen für Aurora PostgreSQL	Unterstützte Verschlüsselungen
	• ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES256-GCM-SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Engine-Versionen für Aurora PostgreSQL	Unterstützte Verschlüsselungen
10.22 und höher, 11.17 und höher, 12.12 und höher, 13.8 und höher, 14.5 und höher und 15.2 und höher	• DHE-RSA-AES128-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-SHA • DHE-RSA-AES256-SHA256 • DHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES256-GCM-SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Engine-Versionen für Aurora PostgreSQL	Unterstützte Verschlüsselungen
	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Engine-Versionen für Aurora PostgreSQL	Unterstützte Verschlüsselungen
15.3, 14.8, 13.11, 12.15 und 11.20	• DHE-RSA-AES128-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-SHA • DHE-RSA-AES256-SHA256 • DHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES256-GCM-SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Engine-Versionen für Aurora PostgreSQL	Unterstützte Verschlüsselungen
	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384

Sie können auch den describe-motor-default-cluster-parameters-CLI-Befehl verwenden, um festzustellen, welche Chiffrier-Suiten derzeit für eine bestimmte Parametergruppenfamilie unterstützt werden. Im folgenden Beispiel wird veranschaulicht, wie Sie die zulässigen Werte für `ssl_cipher`-Cluster-Parameter für Aurora PostgreSQL 11 abrufen.

```
aws rds describe-engine-default-cluster-parameters --db-parameter-group-family aurora-
postgresql11

    ...some output truncated...
 {
  "ParameterName": "ssl_ciphers",
  "Description": "Sets the list of allowed TLS ciphers to be used on secure
 connections.",
  "Source": "engine-default",
  "ApplyType": "dynamic",
  "DataType": "list",
  "AllowedValues": "DHE-RSA-AES128-SHA,DHE-RSA-AES128-SHA256,DHE-RSA-AES128-GCM-
SHA256,DHE-RSA-AES256-SHA,DHE-RSA-AES256-SHA256,DHE-RSA-AES256-GCM-SHA384,
```

```
  ECDHE-RSA-AES128-SHA,ECDHE-RSA-AES128-SHA256,ECDHE-RSA-AES128-GCM-
SHA256,ECDHE-RSA-AES256-SHA,ECDHE-RSA-AES256-SHA384,ECDHE-RSA-AES256-GCM-
SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,

 TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,T

 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AE
  "IsModifiable": true,
  "MinimumEngineVersion": "11.8",
  "SupportedEngineModes": [
   "provisioned"
  ]
 },
    ...some output truncated...
```

Der Parameter `ssl_ciphers` ist standardmäßig auf alle zulässigen Verschlüsselungssuites eingestellt. Weitere Informationen zu Chiffren finden Sie in der ssl_ciphers-Variablen in der PostgreSQL-Dokumentation.

Aktualisieren von Anwendungen für die Verbindung zu Aurora-PostgreSQL-DB-Clustern mit neuen SSL/TLS-Zertifikaten

Am 13. Januar 2023 veröffentlichte Amazon RDS neue Zertifizierungsstellen-Zertifikate (Certificate Authority, CA) zum Herstellen von Verbindungen mit Ihren Aurora-DB-Clustern mithilfe von Secure Socket Layer oder Transport Layer Security (SSL/TLS). Im Folgenden finden Sie Informationen dazu, wie Sie Ihre Anwendungen aktualisieren, um die neuen Zertifikate verwenden zu können.

In diesem Thema finden Sie Informationen dazu, wie Sie ermitteln, ob Client-Anwendungen für die Herstellung von Verbindungen mit Ihren DB-Clustern SSL/TLS verwenden. Wenn dies der Fall ist, können Sie weiter überprüfen, ob diese Anwendungen zur Herstellung von Verbindungen Zertifikatverifizierungen erfordern.

> **Note**
>
> Einige Anwendungen sind so konfiguriert, dass sie nur dann Verbindungen mit Aurora PostgreSQL-DB-Clustern herstellen, wenn sie das Zertifikat auf dem Server erfolgreich identifizieren können.
> Für solche Anwendungen müssen Sie die Trust Stores Ihrer Client-Anwendung aktualisieren, damit diese die neuen CA-Zertifikate enthalten.

Nach der Aktualisierung der CA-Zertifikate in den Trust Stores Ihrer Client-Anwendungen können Sie die Zertifikate auf Ihren DB-Clustern rotieren. Es wird nachdrücklich empfohlen, diese Verfahren vor der Implementierung in Produktionsumgebungen in einer Entwicklungs- oder Testumgebung zu testen.

Weitere Informationen zur Zertifikatrotation finden Sie unter Rotieren Ihrer SSL/TLS-Zertifikate. Weitere Informationen zum Herunterladen von Zertifikaten finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer . Informationen zum Verwenden von SSL/TLS mit PostgreSQL-DB-Clustern finden Sie unter Sicherung von Aurora-PostgreSQL-Daten mit SSL/TLS.

Themen

Ermitteln, ob Anwendungen Verbindungen mit Aurora-PostgreSQL-DB-Clustern mithilfe von SSL herstellen

Prüfen Sie die DB-Cluster-Konfiguration auf den Wert des `rds.force_ssl`-Parameters. Standardmäßig ist der Parameter `rds.force_ssl` auf `0` festgelegt. Wenn der Parameter `rds.force_ssl` auf 1 (ein) festgelegt ist, müssen Clients SSL/TLS für Verbindungen verwenden. Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Wenn `rds.force_ssl` nicht auf 1 (an) festgelegt ist, fragen Sie `pg_stat_ssl` ab, um zu prüfen, welche Verbindungen SSL verwenden. Beispielsweise gibt die folgende Abfrage nur SSL-Verbindungen und Informationen zu den Clients zurück, die SSL verwenden.

```
select datname, username, ssl, client_addr from pg_stat_ssl inner join pg_stat_activity
 on pg_stat_ssl.pid = pg_stat_activity.pid where ssl is true and username<>'rdsadmin';
```

Nur Zeilen, die SSL/TLS-Verbindungen verwenden, werden mit Informationen zur Verbindung angezeigt. Dies ist eine Beispielausgabe.

```
 datname  | username | ssl | client_addr
----------+----------+-----+-------------
```

```
 benchdb   | pgadmin | t    | 53.95.6.13
 postgres | pgadmin | t    | 53.95.6.13
(2 rows)
```

Die vorherige Abfrage zeigt nur die aktuellen Verbindungen zum Zeitpunkt der Abfrage an. Das Fehlen von Ergebnissen weist nicht darauf hin, dass es keine Anwendungen gibt, die SSL-Verbindungen verwenden. Möglicherweise werden zu anderen Zeitpunkten weitere SSL-Verbindungen hergestellt.

Ermitteln, ob ein Client zum Herstellen von Verbindungen Zertifikatverifizierungen erfordert

Wenn ein Client wie psql oder JDBC mit SSL-Unterstützung konfiguriert ist, versucht dieser zunächst standardmäßig, die Verbindung zur Datenbank über SSL herzustellen. Wenn der Client keine Verbindung über SSL herstellen kann, stellt er die Verbindung ohne SSL her. Der für libpq-basierte Clients (wie psql) und JDBC verwendete `sslmode`-Standardmodus ist unterschiedlich. Die libpq-basierten Clients verwenden standardmäßig `prefer`. JDBC-Clients verwenden standardmäßig `verify-full`. Das Zertifikat auf dem Server wird nur verifiziert, wenn auf `verify-ca` oder `sslmode` festgelegt `sslrootcert` ist`verify-full`. Wenn das Zertifikat ungültig ist, wird ein Fehler ausgelöst.

Verwenden Sie , `PGSSLROOTCERT` um das Zertifikat mit der `PGSSLMODE` Umgebungsvariablen zu überprüfen, wobei auf `verify-ca` oder `PGSSLMODE` gesetzt ist`verify-full`.

```
PGSSLMODE=verify-full PGSSLROOTCERT=/fullpath/ssl-cert.pem psql -h
 pgdbidentifier.cxxxxxxxx.us-east-2.rds.amazonaws.com -U primaryuser -d postgres
```

Verwenden Sie das `sslrootcert` -Argument, um das Zertifikat mit `sslmode` im Verbindungszeichenfolgenformat zu überprüfen, wobei auf `verify-ca` oder `sslmode` gesetzt ist`verify-full`.

```
psql "host=pgdbidentifier.cxxxxxxxx.us-east-2.rds.amazonaws.com sslmode=verify-full
 sslrootcert=/full/path/ssl-cert.pem user=primaryuser dbname=postgres"
```

Wenn Sie beispielsweise in vorherigen Fall ein ungültiges Stammzertifikat verwenden, sehen Sie auf Ihrem Client einen Fehler ähnlich dem folgenden.

```
psql: SSL error: certificate verify failed
```

Aktualisieren des Trust Stores Ihrer Anwendung

Informationen zum Aktualisieren des Trust Stores für PostgreSQL-Anwendungen finden Sie unter Secure TCP/IP Connections with SSL in der PostgreSQL-Dokumentation.

> **Note**
>
> Wenn Sie den Trust Store aktualisieren, können Sie ältere Zertifikate beibehalten und die neuen Zertifikate einfach hinzufügen.

Aktualisieren des Trust Stores Ihrer Anwendung für JDBC

Sie können den Trust Store für Anwendungen aktualisieren, die JDBC für SSL/TLS-Verbindungen verwenden.

Informationen zum Herunterladen des Stammverzeichnisses finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

Beispiele für Skripte, die Zertifikate importieren, finden Sie unter Beispielskript für den Import von Zertifikaten in Ihren Trust Store.

Verwenden von SSL/TLS-Verbindungen für verschiedene Arten von Anwendungen

Im Folgenden finden Sie Informationen zum Verwenden von SSL/TLS-Verbindungen für verschiedene Arten von Anwendungen:

- psql

  Der Client wird über die Befehlszeile durch die Angabe von Optionen als Verbindungszeichenfolge oder Umgebungsvariablen aufgerufen. Im Fall von SSL/TLS-Verbindungen sind die relevanten Optionen `sslmode` (Umgebungsvariable `PGSSLMODE`), `sslrootcert` (Umgebungsvariable `PGSSLROOTCERT`).

  Die vollständige Liste der Optionen finden Sie unter Parameter Key Words in der PostgreSQL-Dokumentation. Die vollständige Liste der Umgebungsvariablen finden Sie unter Environment Variables in der PostgreSQL-Dokumentation.
- pgAdmin

Dieser browserbasierte Client bietet eine benutzerfreundlichere Oberfläche zum Herstellen von Verbindungen mit PostgreSQL-Datenbanken.

Informationen zum Konfigurieren von Verbindungen finden Sie in der pgAdmin-Dokumentation.

- JDBC

  JDBC ermöglicht Datenbankverbindungen mit Java-Anwendungen.

  Allgemeine Informationen zum Herstellen von Verbindungen mit PostgreSQL-Datenbanken über JDBC finden Sie unter Connecting to the Database in der PostgreSQL-Dokumentation. Informationen zum Herstellen von Verbindungen über SSL/TLS finden Sie unter Configuring the Client in der PostgreSQL-Dokumentation.

- Python

  Eine verbreitet für die Herstellung von Verbindungen mit PostgreSQL-Datenbanken verwendete Python-Bibliothek ist `psycopg2`.

  Informationen zum Verwenden von `psycopg2` finden Sie in der psycopg2-Dokumentation. Ein kurzes Tutorial zum Herstellen von Verbindungen mit PostgreSQL-Datenbanken finden Sie unter Psycopg2-Tutorial. Informationen zu den vom Verbindungsbefehl akzeptierten Optionen finden Sie unter psycopg2-Modulinhalte.

> **Important**
>
> Nachdem Sie festgestellt haben, dass Ihre Datenbankverbindungen SSL/TLS verwenden, und Ihren Anwendungsvertrauensspeicher aktualisiert haben, können Sie Ihre Datenbank so aktualisieren, dass sie die rds-ca-rsa2048-g1-Zertifikate verwendet. Anweisungen hierzu finden Sie in Schritt 3 unter Aktualisierung Ihres CA-Zertifikats durch Änderung Ihrer DB-Instance .

Verwenden der Kerberos-Authentifizierung mit Aurora PostgreSQL

Sie können Kerberos verwenden, um Benutzer zu authentifizieren, wenn sie sich mit Ihrem DB-Cluster mit PostgreSQL verbinden. Dazu konfigurieren Sie Ihren DB-Cluster so, dass AWS Directory Service for Microsoft Active Directory für die Kerberos-Authentifizierung verwendet wird. AWS Directory Service for Microsoft Active Directory wird auch als AWS Managed Microsoft AD

bezeichnet. Es ist eine Funktion, die mit AWS Directory Service verfügbar ist. Weitere Informationen finden Sie unter Was ist AWS Directory Service? im Administratorhandbuch für AWS Directory Service.

Zunächst erstellen Sie ein AWS Managed Microsoft AD-Verzeichnis, um Benutzeranmeldeinformationen zu speichern. Anschließend stellen Sie Ihrem PostgreSQL-DB-Cluster die Active Directory Domain und weitere Informationen zur Verfügung. Wenn Benutzer sich mit PostgreSQL-DB-Clustern authentifizieren, werden Authentifizierungsanforderungen an das AWS Managed Microsoft AD-Verzeichnis weitergeleitet.

Wenn Sie alle Ihre Anmeldeinformationen im selben Verzeichnis aufbewahren, können Sie Zeit und Mühe sparen. Sie haben einen zentralen Ort für die Speicherung und Verwaltung von Anmeldeinformationen für mehrere DB-Cluster. Die Verwendung eines Verzeichnisses kann auch Ihr allgemeines Sicherheitsprofil verbessern.

Außerdem können Sie von Ihrem eigenen On-Premises Microsoft Active Directory auf Anmeldeinformationen zugreifen. Dazu erstellen Sie eine vertrauensvolle Domain-Beziehung, damit das AWS Managed Microsoft AD-Verzeichnis Ihrem On-Premises Microsoft Active Directory vertraut. Auf diese Weise können Ihre Benutzer auf Ihre PostgreSQL-Clusters- mit derselben Windows Single Sign-On-Oberfläche (SSO) zugreifen, die sie auch für den Zugriff auf Workloads in Ihrem lokalen Netzwerk verwenden.

Eine Datenbank kann Kerberos, AWS Identity and Access Management (IAM) oder sowohl Kerberos- als auch IAM-Authentifizierung nutzen. Da die Kerberos- und IAM-Authentifizierung jedoch unterschiedliche Authentifizierungsmethoden bereitstellen, kann sich ein bestimmter Datenbankbenutzer nur mit der einen oder anderen Authentifizierungsmethode bei einer Datenbank anmelden, jedoch nicht mit beiden. Weitere Informationen zur IAM-Authentifizierung finden Sie unter IAM-Datenbankauthentifizierung.

Themen

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen über die Verfügbarkeit von Versionen und Regionen von Aurora PostgreSQL mit Kerberos-Authentifizierung finden Sie unter Kerberos-Authentifizierung mit Aurora PostgreSQL.

Übersicht über die Kerberos-Authentifizierung für PostgreSQL-DB-Cluster

Um die Kerberos-Authentifizierung für PostgreSQL-DB-Cluster einzurichten, führen Sie die folgenden Schritte aus, die später näher erläutert werden:

1. Verwenden Sie AWS Managed Microsoft AD zum Erstellen eines AWS Managed Microsoft AD-Verzeichnisses. Zur Erstellung des Verzeichnisses können Sie die AWS Management Console, die AWS CLI oder die AWS Directory Service-API verwenden. Stellen Sie sicher, dass Sie die relevanten ausgehenden Ports in der Verzeichnissicherheitsgruppe öffnen, damit das Verzeichnis mit der kommunizieren kann.
2. Erstellen Sie eine Rolle, die Amazon Aurora Zugriff für Aufrufe in Ihr AWS Managed Microsoft AD-Verzeichnis bereitstellt. Erstellen Sie dazu eine AWS Identity and Access Management-(IAM)-Rolle, die die verwaltete IAM-Richtlinie `AmazonRDSDirectoryServiceAccess` verwendet.

   Damit die IAM-Rolle den Zugriff zulässt, muss der Endpunkt AWS Security Token Service (AWS STS) in der richtigen AWS-Region für Ihr AWS-Konto aktiviert werden. AWS STS-Endpunkte sind standardmäßig in allen AWS-Regionen aktiviert und Sie können sie ohne weitere Aktionen verwenden. Weitere Informationen finden Sie unter AWS STS in einer AWS-Region aktivieren und deaktivieren im IAM-Benutzerhandbuch.
3. Erstellen und konfigurieren Sie Benutzer im Verzeichnis AWS Managed Microsoft AD mithilfe der Tools aus dem Microsoft Active Directory. Weitere Informationen zum Erstellen von Benutzern in Ihrem Active Directory finden Sie unter Verwalten von Benutzern und Gruppen in AWS Managed Microsoft AD im AWS Directory Service Administration Guide.
4. Wenn Sie planen, das Verzeichnis und die DB-Instance in verschiedenen AWS-Konten oder Virtual Private Clouds (VPCs) zu platzieren, konfigurieren Sie VPC-Peering. Weitere Informationen finden Sie unter Was ist VPC Peering? im Amazon VPC Peering Guide.
5. Erstellen oder ändern Sie PostgreSQL-DB-Cluster entweder über die Konsole, CLI oder RDS-API mit einer der folgenden Methoden:
   - Erstellen eines DB-Clusters von Aurora PostgreSQL und Herstellen einer Verbindung
   - Ändern eines Amazon Aurora-DB-Clusters

- Wiederherstellen aus einem DB-Cluster-Snapshot
- Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit

Sie können die Cluster- in derselben Amazon Virtual Private Cloud (VPC) wie das Verzeichnis oder in einem anderen AWS-Konto oder einer anderen VPC finden. Wenn Sie die PostgreSQL-DB- erstellen oder ändern, gehen Sie wie folgt vor:

- Geben Sie den Domänenbezeichner (d-*-Bezeichner) an, der beim Erstellen Ihres Verzeichnisses generiert wurde.
- Geben Sie außerdem den Namen der IAM-Rolle an, die Sie erstellt haben.
- Stellen Sie sicher, dass die Sicherheitsgruppe der DB-Instance eingehenden Datenverkehr von der Sicherheitsgruppe des Verzeichnisses empfangen kann.

6. Verwenden Sie die RDS-Master-Benutzer-Anmeldeinformationen, um sich mit PostgreSQL-DB-Clustern zu verbinden. Erstellen Sie den Benutzer in PostgreSQL, der extern identifiziert werden soll. Extern identifizierte Benutzer können sich über die Kerberos-Authentifizierung bei der PostgreSQL-DB- anmelden.

Einrichten der Kerberos-Authentifizierung für PostgreSQL-DB-Cluster

Um die Kerberos-Authentifizierung einzurichten, führen Sie die folgenden Schritte aus.

Themen

- Schritt 1: Erstellen Sie ein Verzeichnis mit AWS Managed Microsoft AD
- Schritt 2: (Optional) Erstellen Sie eine Vertrauensbeziehung zwischen Ihrem lokalen Active Directory und AWS Directory Service
- Schritt 3: Erstellen Sie eine IAM-Rolle für Amazon Aurora Amazon für den Zugriff auf AWS Directory Service
- Schritt 4: Anlegen und Konfigurieren von Benutzern
- Schritt 5: Aktivieren des VPC-übergreifenden Datenverkehrs zwischen dem Verzeichnis und der DB-Instance
- Schritt 6: Erstellen oder Ändern von PostgreSQL-DB-
- Schritt 7: Erstellen von PostgreSQL-Benutzern für Ihre Kerberos-Prinzipale
- Schritt 8: Konfigurieren eines PostgreSQL-Clients

Schritt 1: Erstellen Sie ein Verzeichnis mit AWS Managed Microsoft AD

AWS Directory Service erstellt ein vollständig verwaltetes Active Directory in der AWS Cloud. Wenn Sie ein AWS Managed Microsoft AD Verzeichnis erstellen, AWS Directory Service erstellt zwei Domänencontroller und DNS-Server für Sie. Die Verzeichnisserver werden in verschiedenen Subnetzen in einer VPC erstellt. Diese Redundanz trägt dazu bei, dass Ihr Verzeichnis auch im Fehlerfall erreichbar bleibt.

Wenn Sie ein AWS Managed Microsoft AD Verzeichnis erstellen, führt der AWS Directory Service die folgenden Aufgaben in Ihrem Namen aus:

- Richtet ein Active Directory in Ihrer VPC ein.
- Erstellt ein Konto für den Verzeichnisadministrator mit dem Benutzernamen `Admin` und dem angegebenen Passwort. Mit diesem Konto verwalten Sie das Verzeichnis.

  > **Important**
  >
  > Stellen Sie sicher, dass Sie dieses Passwort speichern. AWS Directory Service speichert dieses Passwort nicht und es kann nicht abgerufen oder zurückgesetzt werden.

- Erstellt eine Sicherheitsgruppe für die Verzeichniscontroller. Die Sicherheitsgruppe muss die Kommunikation mit der PostgreSQL-DB- zulassen.

AWS Erstellt beim Start AWS Directory Service for Microsoft Active Directory eine Organisationseinheit (OU), die alle Objekte Ihres Verzeichnisses enthält. Diese OU erhält den NetBIOS-Namen, den Sie beim Erstellen des Verzeichnisses eingegeben haben, und befindet sich im Domänenstamm. Der Domänenstamm gehört und wird von diesem verwaltet AWS.

Das `Admin` Konto, das mit Ihrem AWS Managed Microsoft AD Verzeichnis erstellt wurde, verfügt über Berechtigungen für die gängigsten Verwaltungsaktivitäten Ihrer Organisationseinheit:

- Erstellen, Aktualisieren oder Löschen von Benutzern
- Hinzufügen von Ressourcen zu Ihrer Domäne, etwa Datei- oder Druckserver, und anschließendes Gewähren der zugehörigen Ressourcenberechtigungen für Benutzer in der OU
- Erstellen weiterer OUs und Container
- Delegieren von Befugnissen
- Wiederherstellen von gelöschten Objekten aus dem Active Directory-Papierkorb

- Führen Sie Active Directory- und DNS-Module (Domain Name Service) für Windows PowerShell im Active Directory-Webdienst aus

Das `Admin`-Konto hat auch die Berechtigung, die folgenden domänenweiten Aktivitäten durchzuführen:

- Verwalten von DNS-Konfigurationen (Hinzufügen, Entfernen oder Aktualisieren von Datensätzen, Zonen und Weiterleitungen)
- Aufrufen von DNS-Ereignisprotokollen
- Anzeigen von Sicherheitsereignisprotokollen

Um ein Verzeichnis zu erstellen mit AWS Managed Microsoft AD

1. Wählen Sie im Navigationsbereich AWS Directory Service -Konsole den Eintrag Directories (Verzeichnisse) und wählen Sie Set up directory (Verzeichnis einrichten) aus.
2. Wählen Sie AWS Managed Microsoft AD. AWS Managed Microsoft AD ist zurzeit die einzige für Amazon Aurora unterstützte Option.
3. Wählen Sie Weiter aus.
4. Geben Sie auf der Seite Enter directory information (Verzeichnisinformationen eingeben) die folgenden Informationen ein:

   Edition

   Wählen Sie die Edition aus, die Ihre Anforderungen erfüllt.

   DNS-Name des Verzeichnisses

   Den vollständig qualifizierten Namen für das Verzeichnis, z. B. **`corp.example.com`**.

   NetBIOS-Name des Verzeichnisses

   Ein optionaler Kurzname für das Verzeichnis, z. B. `CORP`.

   Verzeichnisbeschreibung

   Eine optionale Beschreibung des Verzeichnisses.

   Administratorpasswort

   Das Passwort für den Verzeichnisadministrator. Mit der Verzeichniserstellung wird ein Administratorkonto mit dem Benutzernamen `Admin` und diesem Passwort angelegt.

Das Passwort für den Verzeichnisadministrator darf nicht das Wort "admin" enthalten. Beachten Sie beim Passwort die Groß- und Kleinschreibung und es muss 8 bis 64 Zeichen lang sein. Zudem muss es mindestens ein Zeichen aus dreien der vier folgenden Kategorien enthalten:

- Kleinbuchstaben (a–z)
- Großbuchstaben (A–Z)
- Zahlen (0–9)
- Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Passwort bestätigen

Geben Sie das Administratorpasswort erneut ein.

> **Important**
>
> Stellen Sie sicher, dass Sie dieses Passwort speichern. AWS Directory Service speichert dieses Passwort nicht und es kann nicht abgerufen oder zurückgesetzt werden.

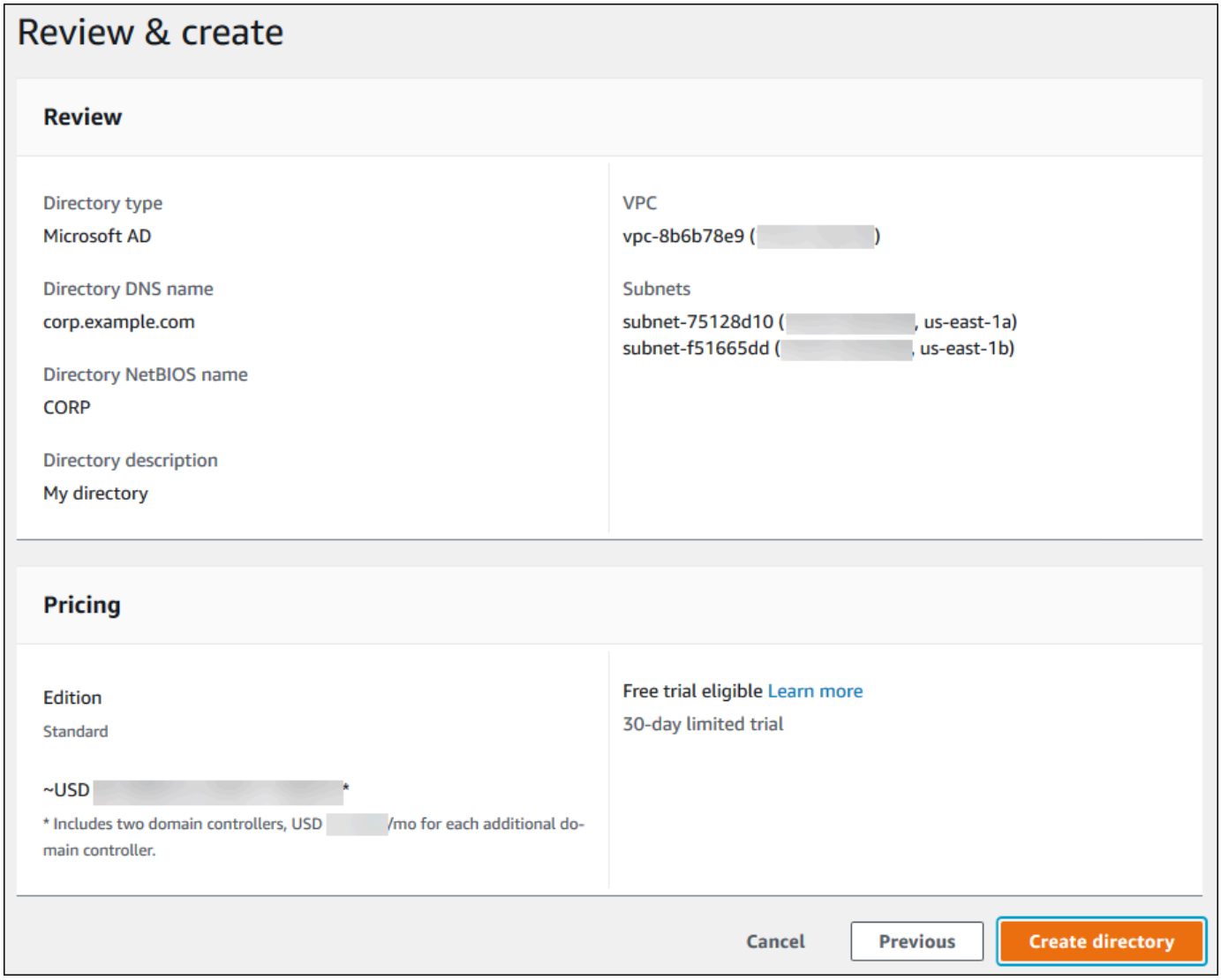
5. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Choose VPC and subnets (VPC und Subnetze wählen) die folgenden Informationen an.

   VPC

   Wählen Sie die VPC für das Verzeichnis aus. Sie können PostgreSQL-DB-Cluster in derselben VPC oder in einer anderen VPC erstellen.

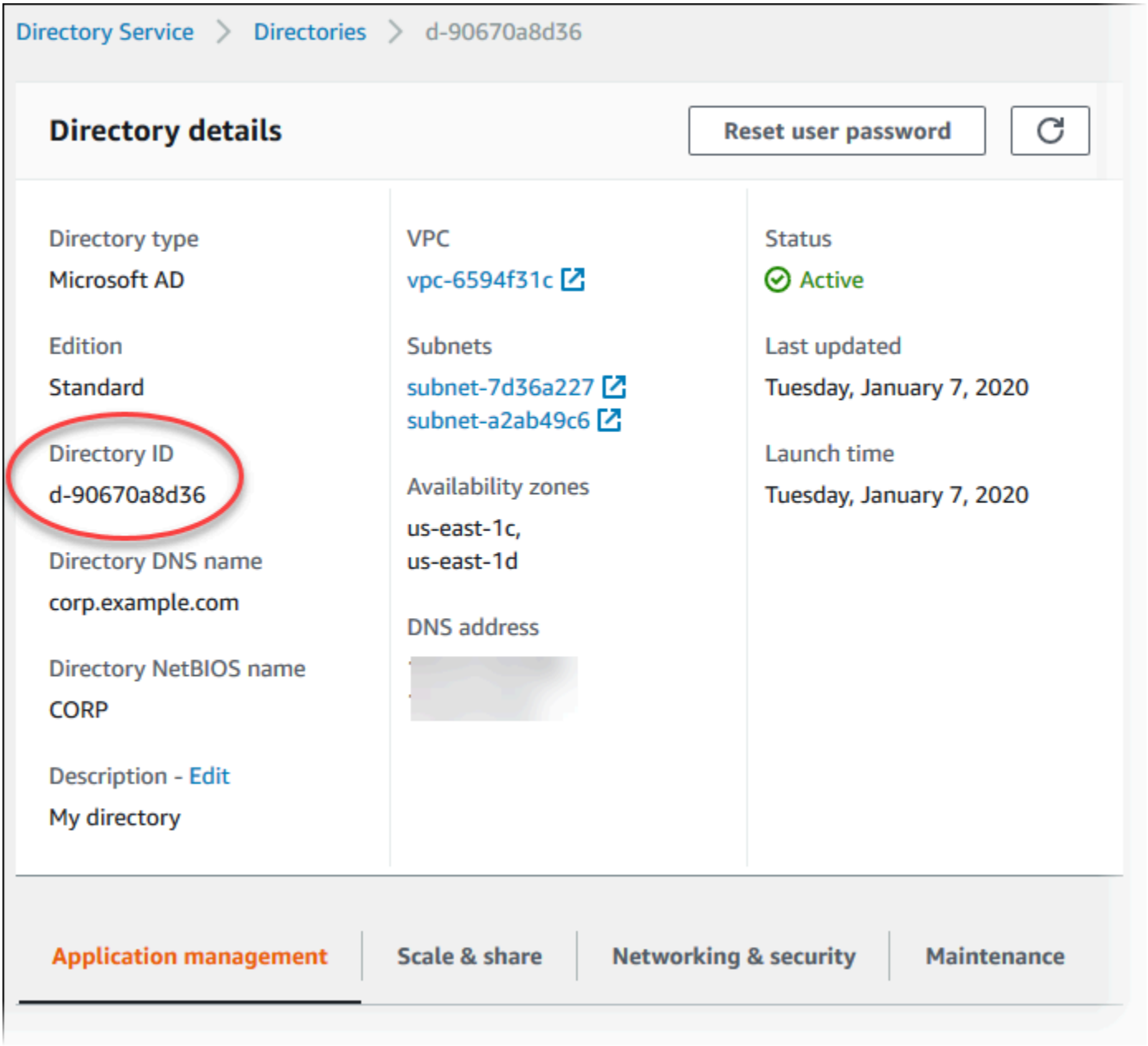
   Subnetze

   Wählen Sie Subnetze für die Verzeichnis-Server aus. Die beiden Subnetze müssen zu verschiedenen Availability-Zonen gehören.
7. Wählen Sie Weiter aus.
8. Überprüfen Sie die Verzeichnisinformationen. Wenn Änderungen erforderlich sind, klicken Sie auf Previous (Zurück) und nehmen Sie die Änderungen vor. Wenn die Informationen richtig sind, wählen Sie Create directory (Verzeichnis erstellen).



Es dauert einige Minuten, bis das Verzeichnis erstellt wurde. Wenn es erfolgreich erstellt wurde, ändert sich der Wert Status in Active (Aktiv).

Um Informationen über das Verzeichnis anzuzeigen, wählen Sie die Verzeichnis-ID in der Verzeichnisauflistung aus. Notieren Sie sich den Wert Directory ID. Sie benötigen diesen Wert, wenn Sie Ihre PostgreSQL DB-Instance erstellen oder ändern.



Schritt 2: (Optional) Erstellen Sie eine Vertrauensbeziehung zwischen Ihrem lokalen Active Directory und AWS Directory Service

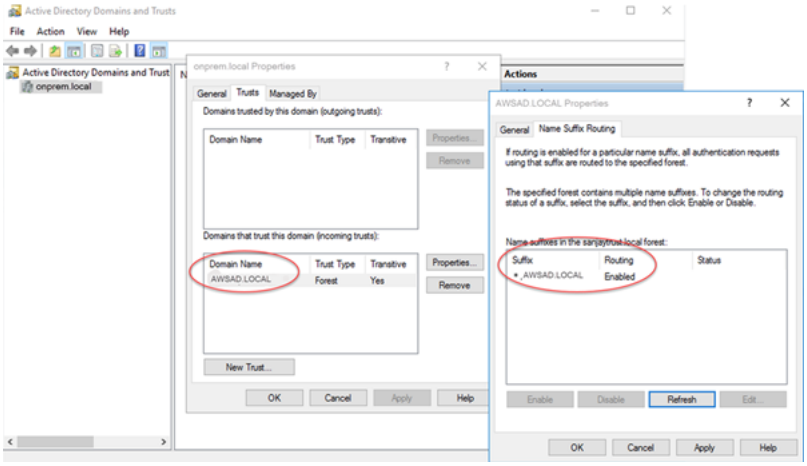
Wenn Sie Ihr eigenes lokales Microsoft Active Directory nicht verwenden möchten, fahren Sie mit for Schritt 3: Erstellen Sie eine IAM-Rolle für Amazon Aurora Amazon für den Zugriff auf AWS Directory Service.

Um die Kerberos-Authentifizierung mit Ihrem lokalen Active Directory zu erhalten, müssen Sie eine vertrauensvolle Domänenbeziehung mithilfe einer Gesamtvertrauensstellung zwischen Ihrem lokalen Microsoft Active Directory und dem AWS Managed Microsoft AD Verzeichnis (erstellt in) einrichten.

Schritt 1: Erstellen Sie ein Verzeichnis mit AWS Managed Microsoft AD Die Vertrauensstellung kann unidirektional sein, wobei das AWS Managed Microsoft AD Verzeichnis dem lokalen Microsoft Active Directory vertraut. Die Vertrauensstellung kann auch bidirektional erfolgen, wobei beide Active Directories einander vertrauen. Weitere Informationen zum Einrichten von Vertrauensstellungen mithilfe von finden Sie unter Wann AWS Directory Service sollte eine Vertrauensstellung eingerichtet werden? im Administratorhandbuch.AWS Directory Service

> **Note**
>
> Verwendung eines lokalen Microsoft Active Directory:
>
> - Windows-Clients müssen die Verbindung über den Domänennamen auf dem Endpunkt herstellen und nicht über AWS Directory Service rds.amazonaws.com. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu PostgreSQL mit Kerberos-Authentifizierung.
> - Windows-Clients können keine Verbindung über benutzerdefinierten Aurora-Endpunkte herstellen. Weitere Informationen hierzu finden Sie unter Amazon Aurora-Verbindungsverwaltung.
> - Globale Datenbanken:
>   - Windows-Clients können eine Verbindung nur über Instanzendpunkte oder Cluster-Endpunkte in der primären AWS-Region Datenbank herstellen.
>   - Windows-Clients können keine Verbindung über Clusterendpunkte auf der Sekundärseite herstellen. AWS-Regionen

Stellen Sie sicher, dass der lokale Microsoft Active Directory-Domänenname ein DNS-Suffix-Routing enthält, das der neu erstellten Vertrauensstellung entspricht. Im folgenden Screenshot wird ein Beispiel gezeigt.



Schritt 3: Erstellen Sie eine IAM-Rolle für Amazon Aurora Amazon für den Zugriff auf AWS Directory Service

Damit Amazon Aurora Sie anrufen AWS Directory Service kann, benötigt Ihr AWS Konto eine IAM-Rolle, die die verwaltete IAM-Richtlinie verwendet. `AmazonRDSDirectoryServiceAccess` Diese Rolle ermöglicht es Amazon Aurora, Aufrufe von AWS Directory Service durchzuführen. (Beachten Sie, dass sich diese IAM-Rolle für den Zugriff von der IAM-Rolle AWS Directory Service unterscheidet, für die Sie verwendet werden.) IAM-Datenbankauthentifizierung

Wenn Sie mit dem eine DB-Instance erstellen AWS Management Console und Ihr Konsolen-Benutzerkonto über die `iam:CreateRole` entsprechende Berechtigung verfügt, erstellt die Konsole automatisch die benötigte IAM-Rolle. In diesem Fall lautet der Rollenname `rds-directoryservice-kerberos-access-role`. Andernfalls müssen Sie die IAM-Rolle manuell erstellen. Wenn Sie diese IAM-Rolle erstellen`Directory Service`, wählen Sie die AWS verwaltete Richtlinie aus und hängen Sie `AmazonRDSDirectoryServiceAccess` sie an.

Weitere Informationen zum Erstellen von IAM-Rollen für einen Dienst finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS Dienst im IAM-Benutzerhandbuch.

> **Note**
>
> Die für die Windows-Authentifizierung für RDS for Microsoft SQL Server verwendete IAM-Rolle kann nicht für Amazon Aurora verwendet werden.

Alternativ können Sie Richtlinien mit den erforderlichen Berechtigungen erstellen, anstatt die verwaltete Richtlinie `AmazonRDSDirectoryServiceAccess` zu verwenden. In diesem Fall muss die IAM-Rolle die folgende IAM-Vertrauensrichtlinie haben.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die Rolle muss auch über die folgende IAM-Rollenrichtlinie verfügen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
  ]
}
```

Schritt 4: Anlegen und Konfigurieren von Benutzern

Sie können Benutzer mit dem Tool „Active Directory Users and Computers“ erstellen. Dieses Tool ist ein Active Directory Domain Service und ein Active Directory Lightweight Directory Service. Weitere Informationen finden Sie unter Hinzufügen von Benutzern und Computern zur Active-Directory-Domain. In diesem Fall handelt es sich bei Benutzern um Einzelpersonen oder andere Entitäten, z. B. um ihre Computer, die Teil der Domain sind und deren Identitäten im Verzeichnis verwaltet werden.

Um Benutzer in einem AWS Directory Service Verzeichnis zu erstellen, müssen Sie mit einer Windows-basierten Amazon EC2 EC2-Instance verbunden sein, die Mitglied des Verzeichnisses ist. AWS Directory Service Gleichzeitig müssen Sie als Benutzer angemeldet sein, der über Rechte zum Erstellen von Benutzern verfügt. Weitere Informationen finden Sie unter Erstellen eines Benutzers im AWS Directory Service Administration Guide.

Schritt 5: Aktivieren des VPC-übergreifenden Datenverkehrs zwischen dem Verzeichnis und der DB-Instance

Wenn Sie beabsichtigen, das Verzeichnis und den DB-Cluster in derselben VPC zu platzieren, überspringen Sie diesen Schritt und fahren Sie mit Schritt 6: Erstellen oder Ändern von PostgreSQL-DB- fort.

Wenn Sie das Verzeichnis und die DB-Instance in verschiedenen VPCs platzieren möchten, konfigurieren Sie den VPC-übergreifenden Datenverkehr mithilfe von VPC Peering oder AWS Transit Gateway.

Das folgende Verfahren ermöglicht den Datenverkehr zwischen VPCs mit VPC Peering. Folgen Sie den Anweisungen unter Was ist VPC Peering? im Handbuch zu Amazon Virtual Private Cloud-Peering.

Aktivieren des VPC-übergreifenden Datenverkehrs mit VPC Peering

1. Richten Sie geeignete VPC-Routing-Regeln ein, um sicherzustellen, dass Netzwerk-Datenverkehr in beide Richtungen fließen kann.
2. Stellen Sie sicher, dass die Sicherheitsgruppe der DB-Instance eingehenden Datenverkehr von der Sicherheitsgruppe des Verzeichnisses empfangen kann.
3. Stellen Sie sicher, dass keine ACL-Regel (Network Access Control List) zum Blockieren des Datenverkehrs vorhanden ist.

Wenn das Verzeichnis einem anderen AWS Konto gehört, müssen Sie das Verzeichnis gemeinsam nutzen.

Um das Verzeichnis von mehreren AWS Konten gemeinsam zu nutzen

1. Beginnen Sie mit der gemeinsamen Nutzung des Verzeichnisses mit dem AWS Konto, unter dem die DB-Instance erstellt werden soll. Folgen Sie dazu den Anweisungen unter Tutorial: Sharing your AWS Managed Microsoft AD-Directory for Seamless EC2 Domain-Join im AWS Directory Service Administrationshandbuch.

2. Melden Sie sich mit dem Konto für die DB-Instance bei der AWS Directory Service Konsole an und stellen Sie sicher, dass die Domain den SHARED Status hat, bevor Sie fortfahren.
3. Notieren Sie sich den Wert der Verzeichnis-ID, während Sie mit dem Konto für die DB-Instance bei der AWS Directory Service Konsole angemeldet sind. Sie verwenden diese Verzeichnis-ID, um die DB-Instance mit der Domäne zu verbinden.

Schritt 6: Erstellen oder Ändern von PostgreSQL-DB-

Erstellen oder ändern Sie PostgreSQL-DB-Cluster für die Verwendung mit Ihrem Verzeichnis. Sie können die Konsole, CLI oder RDS-API verwenden, um DB-Cluster einem Verzeichnis zuzuordnen. Sie können dafür eine der folgenden Möglichkeiten auswählen:

- Erstellen Sie einen neuen PostgreSQL-DB-Cluster mithilfe der Konsole, des create-db-clusterCLI-Befehls oder des RDS-API-Vorgangs CreateDBCluster. Anweisungen finden Sie unter Erstellen eines DB-Clusters von Aurora PostgreSQL und Herstellen einer Verbindung.
- Ändern Sie einen vorhandenen PostgreSQL-DB-Cluster mithilfe der Konsole, des modify-db-clusterCLI-Befehls oder des RDS-API-Vorgangs ModifyDBCluster. Anweisungen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.
- Stellen Sie mithilfe der Konsole, des CLI-Befehls -db-snapshot oder der RDS-API-Operation RestoreDB restore-db-cluster-fromDBSnapshot einen PostgreSQL-DB-Cluster aus einem DB-Snapshot wieder ClusterFrom her. Anweisungen finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.
- Stellen Sie einen PostgreSQL-DB-Cluster point-in-time mithilfe der Konsole, des restore-db-instance-topoint-in-timeCLI-Befehls oder des RDS-API-Vorgangs RestoreDB auf einem wieder her. ClusterToPointInTime Detaillierte Anweisungen finden Sie unter Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit.

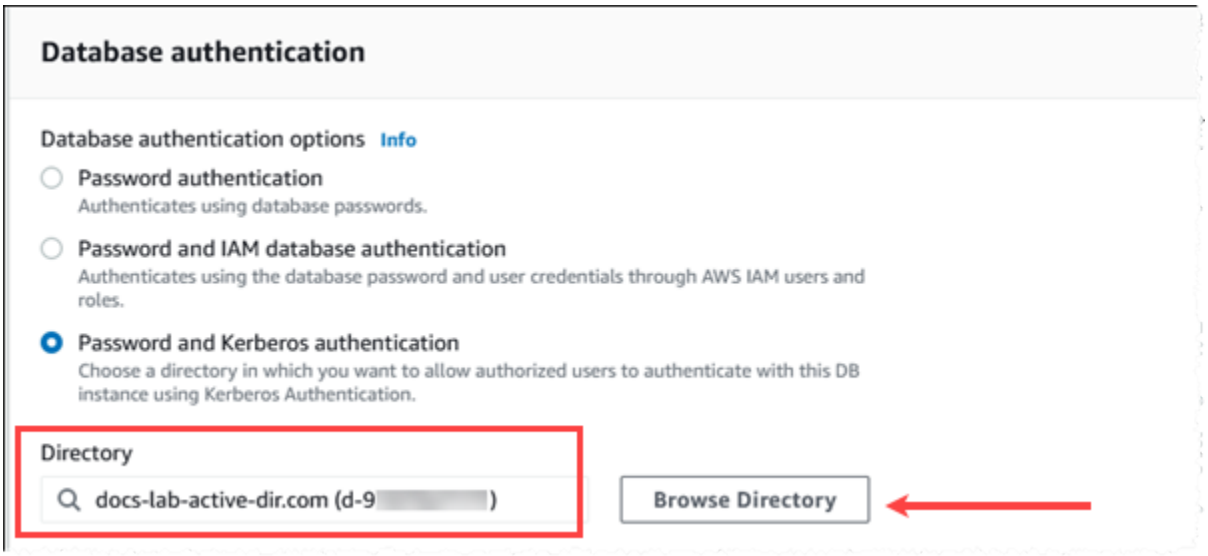
Die Kerberos-Authentifizierung wird nur für PostgreSQL-DB-Cluster- in einer VPC unterstützt. Die DB-Instance kann sich in derselben VPC wie das Verzeichnis oder in einer anderen VPC befinden. Der DB-Cluster muss eine Sicherheitsgruppe verwenden, die ausgehenden Datenverkehr innerhalb der VPC des Verzeichnisses zulässt, damit der DB-Cluster mit dem Verzeichnis kommunizieren kann.

> **Note**
>
> Die Aktivierung der Kerberos-Authentifizierung wird derzeit auf dem Aurora PostgreSQL-DB-Cluster während der Migration von RDS für PostgreSQL nicht unterstützt. Sie können die

Kerberos-Authentifizierung nur auf einem eigenständigen Aurora PostgreSQL-DB-Cluster aktivieren.

Konsole

Wenn Sie die Konsole zum Erstellen, Ändern oder Wiederherstellen eines DB-Clusters verwenden, wählen Sie Kerberos-Authentifizierung im Datenbank-Authentifizierung-Abschnitt. Dann wählen Sie Verzeichnis durchsuchen. Wählen Sie das Verzeichnis aus oder wählen Sie Erstellen eines neuen Verzeichnisses, um den Directory Service zu verwenden.



AWS CLI

Wenn Sie den verwenden AWS CLI, sind die folgenden Parameter erforderlich, damit die das von Ihnen erstellte Verzeichnis verwenden kann:

- Für den `--domain`-Parameter verwenden Sie den Domänenbezeichner („d-*“-Bezeichner), der beim Erstellen des Verzeichnisses generiert wurde.
- Verwenden Sie für den `--domain-iam-role-name`-Parameter die von Ihnen erstellte Rolle, die die verwaltete IAM-Richtlinie `AmazonRDSDirectoryServiceAccess` verwendet.

Beispielsweise ändert der folgende CLI-Befehl einen DB-Cluster zur Verwendung eines Verzeichnisses.

```
aws rds  modify-db-cluster --db-cluster-identifier mydbinstance --domain d-Directory-ID
 --domain-iam-role-name role-name
```

> **Important**
>
> Wenn Sie einen DB-Cluster ändern, um die Kerberos-Authentifizierung zu aktivieren, starten Sie den DB-Cluster neu, nachdem Sie die Änderung vorgenommen haben.

Schritt 7: Erstellen von PostgreSQL-Benutzern für Ihre Kerberos-Prinzipale

Zu diesem Zeitpunkt ist Ihr DB-Cluster von Aurora PostgreSQL mit der AWS Managed Microsoft AD -Domain verbunden. Die Benutzer, die Sie in dem Verzeichnis in Schritt 4: Anlegen und Konfigurieren von Benutzern erstellt haben, müssen als PostgreSQL-Datenbankbenutzer eingerichtet sein und über Berechtigungen verfügen, um sich bei der Datenbank anzumelden. Dazu melden Sie sich als Datenbankbenutzer mit `rds_superuser`-Rechten an. Wenn Sie beispielsweise beim Erstellen Ihres DB-Clusters von Aurora PostgreSQL die Standardeinstellungen akzeptiert haben, verwenden Sie `postgres`, wie in den folgenden Schritten gezeigt.

So erstellen Sie PostgreSQL-Datenbankbenutzer für Ihre Kerberos-Prinzipale

1. Verwenden Sie `psql`, um eine Verbindung mit dem DB-Instance-Endpunkt Ihres DB-Clusters von Aurora PostgreSQL mit `psql` herzustellen. Im folgenden Beispiel wird das `postgres`-Standardkonto für die `rds_superuser`-Rolle verwendet.

   ```
   psql --host=cluster-instance-1.111122223333.aws-region.rds.amazonaws.com --
   port=5432 --username=postgres --password
   ```

2. Erstellen Sie einen Datenbankbenutzernamen für jeden Kerberos-Prinzipal (Active-Directory-Benutzername), der Zugriff auf die Datenbank haben soll. Verwenden Sie den kanonischen Benutzernamen (Identität), wie er in der Active-Directory-Instance definiert ist, d. h. einen `alias` in Kleinbuchstaben (Benutzername in Active Directory) und den Namen der Active-Directory-Domain für diesen Benutzernamen in Großbuchstaben. Der Active-Directory-Benutzername ist ein extern authentifizierter Benutzer. Setzen Sie den Namen daher in Anführungszeichen, wie im Folgenden gezeigt.

   ```
   postgres=> CREATE USER "username@CORP.EXAMPLE.COM" WITH LOGIN;
   CREATE ROLE
   ```

3. Weisen Sie dem Datenbankbenutzer die `rds_ad`-Rolle zu.

   ```
   postgres=> GRANT rds_ad TO "username@CORP.EXAMPLE.COM";
   ```

```
GRANT ROLE
```

Nachdem Sie alle PostgreSQL-Benutzer für Ihre Active-Directory-Benutzeridentitäten erstellt haben, können Benutzer mit ihren Kerberos-Anmeldeinformationen auf den DB-Cluster von Aurora PostgreSQL zugreifen.

Es ist erforderlich, dass die Datenbankbenutzer, die sich mit Kerberos authentifizieren, dies von Client-Computern aus tun, die Mitglieder der Active Directory-Domäne sind.

Datenbankbenutzer, denen die `rds_ad`-Rolle zugewiesen wurde, können nicht auch über die `rds_iam`-Rolle verfügen. Dies gilt auch für verschachtelte Mitgliedschaften. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung.

Konfigurieren Ihres DB-Clusters von Aurora PostgreSQL für Benutzernamen, bei denen die Groß-/Kleinschreibung unterschieden wird

Die Aurora-PostgreSQL-Versionen 14.5, 13.8, 12.12 und 11.17 unterstützen den PostgreSQL-Parameter `krb_caseins_users`. Dieser Parameter unterstützt Active-Directory-Benutzernamen ohne Berücksichtigung der Groß- und Kleinschreibung. Standardmäßig ist dieser Parameter auf „false“ eingestellt, sodass bei Benutzernamen von Aurora PostgreSQL zwischen Groß- und Kleinschreibung interpretiert wird. Das ist das Standardverhalten in allen älteren Versionen von Aurora PostgreSQL. Sie können diesen Parameter in Ihrer benutzerdefinierten DB-Cluster-Parametergruppe jedoch auf `true` festlegen und Ihrem DB-Cluster von Aurora PostgreSQL erlauben, Benutzernamen ohne Berücksichtigung von Groß- und Kleinschreibung zu interpretieren. Erwägen Sie, diese Einstellung als Annehmlichkeit für Ihre Datenbankbenutzer vorzunehmen, die bei der Authentifizierung mit Active Directory manchmal die Groß- und Kleinschreibung ihres Benutzernamens falsch eingeben.

Um den `krb_caseins_users`-Parameter zu ändern, muss Ihr DB-Cluster von Aurora PostgreSQL eine benutzerdefinierte DB-Cluster-Parametergruppe verwenden. Informationen über das Arbeiten mit einer benutzerdefinierten DB-Cluster-Parametergruppe finden Sie unter Arbeiten mit Parametergruppen.

Sie können das AWS CLI oder das verwenden, AWS Management Console um die Einstellung zu ändern. Weitere Informationen finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe.

Schritt 8: Konfigurieren eines PostgreSQL-Clients

Gehen Sie folgendermaßen vor, um einen PostgreSQL-Client zu konfigurieren:

- Erstellen Sie eine krb5.conf-Datei (oder eine vergleichbare Datei), um auf die Domäne zu verweisen.
- Stellen Sie sicher, dass der Datenverkehr zwischen dem Client-Host und fließen kann AWS Directory Service. Verwenden Sie ein Netzwerk-Dienstprogramm wie Netcat für die folgenden Aufgaben:
  - Überprüfen Sie den Datenverkehr über DNS für Port 53.
  - Überprüfen Sie den Datenverkehr über TCP/UDP an Port 53 und für Kerberos (Ports 88 und 464 für AWS Directory Service.
- Stellen Sie sicher, dass der Datenverkehr zwischen dem Client-Host und der DB-Instance über den Datenbank-Port fließen kann. Verwenden Sie beispielsweise psql, um eine Verbindung herzustellen und auf die Datenbank zuzugreifen.

Im Folgenden finden Sie einen krb5.conf-Beispielinhalt für. AWS Managed Microsoft AD

```
[libdefaults]
 default_realm = EXAMPLE.COM
[realms]
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

Nachfolgend ein Beispiel für den Inhalt von krb5.conf für ein lokales Microsoft Active Directory.

```
[libdefaults]
 default_realm = EXAMPLE.COM
[realms]
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
 ONPREM.COM = {
```

```
  kdc = onprem.com
  admin_server = onprem.com
 }
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
 .onprem.com = ONPREM.COM
 onprem.com = ONPREM.COM
 .rds.amazonaws.com = EXAMPLE.COM
 .amazonaws.com.cn = EXAMPLE.COM
 .amazon.com = EXAMPLE.COM
```

Verwalten von DB-Clustern in einer Domäne

Sie können die Konsole, die CLI oder die RDS-API verwenden, um Ihre DB-Cluster und ihre Beziehung zu Ihrem Microsoft Active Directory zu verwalten. Sie können z. B. ein Active Directory zuordnen, um die Kerberos-Authentifizierung zu aktivieren. Sie können auch die Zuordnung für ein Active Directory entfernen, um die Kerberos-Authentifizierung zu deaktivieren. Sie können auch DB-Cluster verschieben, die von einem Microsoft Active Directory zu einem anderen extern authentifiziert werden.

Sie können z. B. mithilfe der CLI Folgendes tun:

- Um die Aktivierung der Kerberos-Authentifizierung für eine fehlgeschlagene Mitgliedschaft erneut zu versuchen, verwenden Sie den CLI-Befehl modify-db-cluster. Geben Sie die Verzeichnis-ID der aktuellen Mitgliedschaft für die Option `--domain` an.
- Um die Kerberos-Authentifizierung für eine DB-Instance zu deaktivieren, verwenden Sie den CLI-Befehl modify-db-cluster. Geben Sie `none` für die Option `--domain` an.
- Um eine DB-Instance von einer Domäne in eine andere zu verschieben, verwenden Sie den CLI-Befehl modify-db-cluster. Geben Sie die Domänen-ID der neuen Domäne für die Option `--domain` an.

Grundlegendes zur Domänenmitgliedschaft

Nachdem Sie Ihren DB-Cluster erstellt oder geändert haben, werden die DB-Instances zu Mitgliedern der Domäne. Sie können den Status der Domänenmitgliedschaft in der Konsole anzeigen oder den CLI-Befehl describe-db-instances ausführen. Der Status der DB-Instance kann einer der folgenden sein:

- `kerberos-enabled` – Für die DB-Instance ist die Kerberos-Authentifizierung aktiviert.
- `enabling-kerberos` – AWS ist dabei, die Kerberos-Authentifizierung auf dieser DB-Instance zu aktivieren.
- `pending-enable-kerberos` – Das Aktivieren der Kerberos-Authentifizierung ist für diese DB-Instance ausstehend.
- `pending-maintenance-enable-kerberos` – AWS versucht, die Kerberos-Authentifizierung auf der DB-Instance während des nächsten geplanten Wartungsfensters zu aktivieren.
- `pending-disable-kerberos` – Das Deaktivieren der Kerberos-Authentifizierung ist für diese DB-Instance ausstehend.
- `pending-maintenance-disable-kerberos` – AWS versucht, die Kerberos-Authentifizierung auf der DB-Instance während des nächsten geplanten Wartungsfensters zu deaktivieren.
- `enable-kerberos-failed` – Ein Konfigurationsproblem verhinderte, dass AWS die Kerberos-Authentifizierung auf der DB-Instance aktivierte. Beheben Sie das Konfigurationsproblem, bevor Sie den Befehl zum Ändern der DB-Instance erneut ausgeben.
- `disabling-kerberos` – AWS ist dabei, die Kerberos-Authentifizierung auf dieser DB-Instance zu deaktivieren.

Eine Anfrage zur Aktivierung der Kerberos-Authentifizierung kann wegen eines Netzwerkverbindungsproblems oder einer falschen IAM-Rolle fehlschlagen. In einigen Fällen kann der Versuch, die Kerberos-Authentifizierung zu aktivieren, fehlschlagen, wenn Sie einen DB-Cluster erstellen oder ändern. Wenn dies passiert, stellen Sie sicher, dass Sie die richtige IAM-Rolle verwenden, und ändern Sie dann den DB-Cluster, um der Domäne beizutreten.

Herstellen einer Verbindung zu PostgreSQL mit Kerberos-Authentifizierung

Sie können sich über die pgAdmin-Schnittstelle oder über eine Befehlszeilenschnittstelle wie psql per Kerberos-Authentifizierung mit PostgreSQL verbinden. Weitere Informationen zum Herstellen von Verbindungen finden Sie unter Herstellen einer Verbindung mit einem Amazon-Aurora-PostgreSQL-DB-Cluster. Informationen zum Abrufen des Endpunkts, der Portnummer und anderer Details, die für die Verbindung benötigt werden, finden Sie unter Anzeigen der Endpunkte für einen Aurora-Cluster.

pgAdmin

Um pgAdmin für die Verbindung zu PostgreSQL mit Kerberos-Authentifizierung zu verwenden, führen Sie die folgenden Schritte aus:

1. Starten Sie die Anwendung pgAdmin auf Ihrem Client-Computer.
2. Klicken Sie auf der Registerkarte Dashboard auf Add New Server (Neuen Server hinzufügen).
3. Geben Sie im Dialogfeld (Erstellen – Server) auf der Registerkarte Allgemein einen Namen für den Server in pgAdmin ein.
4. Geben Sie auf der Registerkarte Connection (Verbindung) die folgenden Informationen aus der Datenbank von Aurora PostgreSQL ein:
   - Geben Sie für Host den Endpunkt für die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL an. Ein Endpunkt sieht in etwa wie folgt aus:

     ```
     AUR-cluster-instance.111122223333.aws-region.rds.amazonaws.com
     ```

     Wenn Sie eine Verbindung mit einem lokalen Microsoft Active Directory von einem Windows-Client aus herstellen möchten, verwenden Sie den Domänennamen des von AWS verwalteten Active Directorys statt `rds.amazonaws.com` im Host-Endpunkt. Angenommen, der Domänenname für das AWS Managed Active Directory lautet `corp.example.com`. Für Host würde der Endpunkt wie folgt angegeben werden:

     ```
     AUR-cluster-instance.111122223333.aws-region.corp.example.com
     ```
   - Geben Sie unter Port den zugewiesenen Port ein.
   - Geben Sie unter Wartungsdatenbank den Namen der initialen Datenbank ein, mit der sich der Client verbinden soll.
   - Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Kerberos-Authentifizierung in Schritt 7: Erstellen von PostgreSQL-Benutzern für Ihre Kerberos-Prinzipale eingegeben haben.
5. Wählen Sie Save (Speichern).

Psql

Um psql für die Verbindung mit PostgreSQL mit Kerberos-Authentifizierung zu verwenden, führen Sie die folgenden Schritte aus:

1. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus.

   ```
   kinit username
   ```

Ersetzen Sie *username* durch den Benutzernamen. Geben Sie in der Eingabeaufforderung das im Microsoft Active Directory für den Benutzer gespeicherte Passwort ein.

2. Wenn der PostgreSQL-DB-Cluster eine öffentlich zugängliche VPC verwendet, geben Sie eine IP-Adresse für Ihren DB-Cluster-Endpunkt in Ihrer `/etc/hosts`-Datei auf dem EC2-Client ein. Die folgenden Befehle rufen beispielsweise die IP-Adresse ab und fügen sie dann in die `/etc/hosts`-Datei ein.

```
% dig +short PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com
;; Truncated, retrying in TCP mode.
ec2-34-210-197-118.AWS-Region.compute.amazonaws.com.
34.210.197.118

% echo " 34.210.197.118  PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com" >> /etc/
hosts
```

   Wenn Sie eine lokale Microsoft Active Directory von einem Windows-Client verwenden, müssen Sie eine Verbindung über einen speziellen Endpunkt herstellen. Anstatt die Amazon-Domäne `rds.amazonaws.com` im Host-Endpunkt zu verwenden, verwenden Sie den Domänennamen des AWS-Managed Active Directory.

   Angenommen, der Domänenname für IhrAWS Managed Active Directory lautet `corp.example.com`. Verwenden Sie dann das Format *PostgreSQL-endpoint.AWS-Region.corp.example.com* für den Endpunkt und legen Sie es in der `/etc/hosts`-Datei ab.

```
% echo " 34.210.197.118  PostgreSQL-endpoint.AWS-Region.corp.example.com" >> /etc/
hosts
```

3. Verwenden Sie den folgenden psql-Befehl, um sich bei einem PostgreSQL-DB-Cluster anzumelden, der/die in Active Directory integriert ist. Verwenden Sie einen Cluster oder Instance-Endpunkt.

```
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-
Region.rds.amazonaws.com postgres
```

   Um sich beim PostgreSQL DB-Cluster von einem Windows-Client aus unter Verwendung eines lokalen Active Directory anzumelden, verwenden Sie den folgenden psql-Befehl mit dem Domänennamen aus dem vorhergehenden Schritt (`corp.example.com`):

```
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-
Region.corp.example.com postgres
```

Verwenden von AD-Sicherheitsgruppen für die Aurora PostgreSQL-Zugriffskontrolle

Ab den Versionen Aurora PostgreSQL 14.10 und 15.5 kann die Aurora PostgreSQL-Zugriffskontrolle mithilfe des AWS Directory Service für Microsoft Active Directory (AD) -Sicherheitsgruppen verwaltet werden. Frühere Versionen von Aurora PostgreSQL unterstützen die Kerberos-basierte Authentifizierung mit AD nur für einzelne Benutzer. Jeder AD-Benutzer musste explizit für den DB-Cluster bereitgestellt werden, um Zugriff zu erhalten.

Anstatt jeden AD-Benutzer je nach Geschäftsanforderungen explizit für den DB-Cluster bereitzustellen, können Sie AD-Sicherheitsgruppen wie unten beschrieben nutzen:

- AD-Benutzer sind Mitglieder verschiedener AD-Sicherheitsgruppen in einem Active Directory. Diese werden nicht vom DB-Clusteradministrator vorgegeben, sondern basieren auf Geschäftsanforderungen und werden von einem AD-Administrator verwaltet.
- DB-Cluster-Administratoren erstellen DB-Rollen in DB-Instances auf der Grundlage von Geschäftsanforderungen. Diese DB-Rollen können unterschiedliche Berechtigungen oder Privilegien haben.
- DB-Cluster-Administratoren konfigurieren eine Zuordnung von AD-Sicherheitsgruppen zu DB-Rollen auf DB-Cluster-Basis.
- DB-Benutzer können mit ihren AD-Anmeldeinformationen auf DB-Cluster zugreifen. Der Zugriff basiert auf der Mitgliedschaft in einer AD-Sicherheitsgruppe. AD-Benutzer erhalten oder verlieren automatisch Zugriff auf der Grundlage ihrer AD-Gruppenmitgliedschaft.

Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen, bevor Sie die Erweiterung für AD-Sicherheitsgruppen einrichten:

- Richten Sie die Kerberos-Authentifizierung für PostgreSQL-DB-Cluster ein. Weitere Informationen finden Sie unter Kerberos-Authentifizierung für PostgreSQL-DB-Cluster einrichten.

> **Note**
>
> Überspringen Sie für AD-Sicherheitsgruppen Schritt 7: PostgreSQL-Benutzer für Ihre Kerberos-Prinzipale in diesem Einrichtungsverfahren erstellen.

- Verwaltung eines DB-Clusters in einer Domäne. Weitere Informationen finden Sie unter Verwalten eines DB-Clusters in einer Domäne.

Einrichtung der Erweiterung pg_ad_mapping

Aurora PostgreSQL bietet jetzt eine `pg_ad_mapping` Erweiterung zur Verwaltung der Zuordnung zwischen AD-Sicherheitsgruppen und DB-Rollen im Aurora PostgreSQL-Cluster. Weitere Hinweise zu den Funktionen von finden Sie unter. `pg_ad_mapping` Verwenden von Funktionen aus der Erweiterung `pg_ad_mapping`

Um die `pg_ad_mapping` Erweiterung auf Ihrem Aurora PostgreSQL-DB-Cluster einzurichten, fügen Sie sie zunächst `pg_ad_mapping` zu den gemeinsam genutzten Bibliotheken in der benutzerdefinierten DB-Cluster-Parametergruppe für Ihren Aurora PostgreSQL-DB-Cluster hinzu. Hinweise zum Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe finden Sie unter. Arbeiten mit Parametergruppen Als Nächstes installieren Sie die `pg_ad_mapping` Erweiterung. Die Schritte in diesem Abschnitt veranschaulichen die Vorgehensweise. Sie können das AWS Management Console oder das verwenden AWS CLI.

Sie müssen über Berechtigungen als `rds_superuser`-Rolle verfügen, um alle diese Aufgaben ausführen zu können.

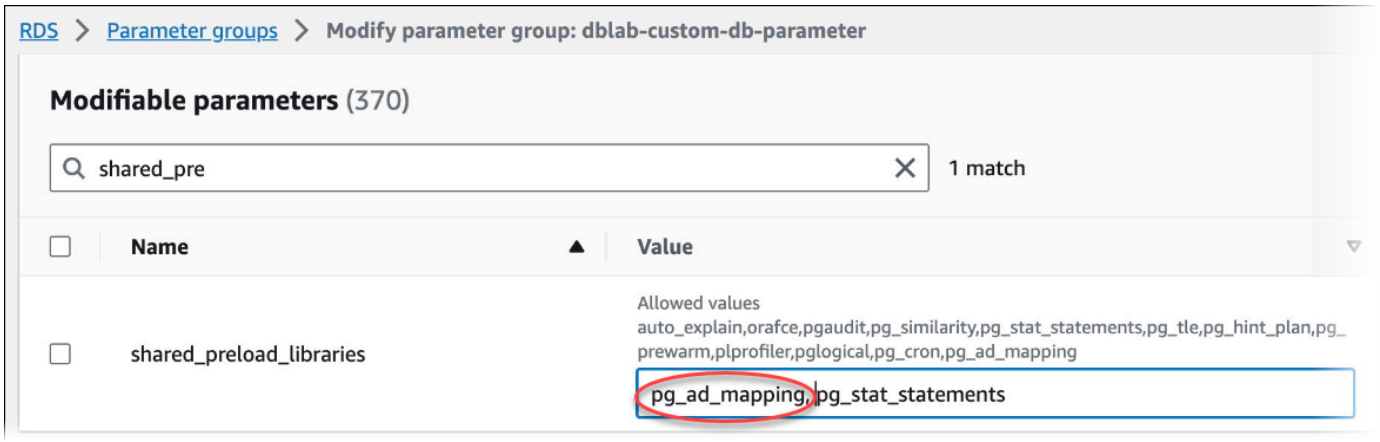
Bei den folgenden Schritten wird davon ausgegangen, dass Ihr Aurora PostgreSQL-DB-Cluster einer benutzerdefinierten DB-Cluster-Parametergruppe zugeordnet ist.

Konsole

Um die Erweiterung einzurichten **`pg_ad_mapping`**

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Writer-Instance Ihres Aurora PostgreSQL-DB-Clusters aus.
3. Öffnen Sie die Registerkarte Konfiguration für Ihre Aurora PostgreSQL DB-Cluster-Writer-Instance. Suchen Sie in den Instance-Details den Link Parameter group (Parametergruppe).
4. Wählen Sie den Link aus, um die benutzerdefinierten Parameter zu öffnen, die Ihrem DB-Cluster von Aurora PostgreSQL zugeordnet sind.
5. Geben Sie in das Suchfeld Parameters (Parameter) `shared_pre` ein, um den `shared_preload_libraries`-Parameter zu finden.

6. Wählen Sie Edit parameters (Parameter bearbeiten) aus, um auf die Eigenschaftswerte zuzugreifen.
7. Fügen Sie `pg_ad_mapping` der Liste im Feld Values (Werte) hinzu. Verwenden Sie ein Komma, um Elemente in der Werteliste zu trennen.



8. Starten Sie die Writer-Instance Ihres Aurora PostgreSQL-DB-Clusters neu, damit Ihre Änderung des `shared_preload_libraries` Parameters wirksam wird.
9. Wenn die Instance verfügbar ist, überprüfen Sie, ob `pg_ad_mapping` initialisiert wurde. Verwenden Sie`psql`, um eine Verbindung zur Writer-Instance Ihres Aurora PostgreSQL-DB-Clusters herzustellen, und führen Sie dann den folgenden Befehl aus.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pg_ad_mapping
(1 row)
```

10. Sobald `pg_ad_mapping` initialisiert ist, können Sie die Erweiterung erstellen. Sie müssen die Erweiterung nach der Initialisierung der Bibliothek erstellen, um die von dieser Erweiterung bereitgestellten Funktionen nutzen zu können.

```
CREATE EXTENSION pg_ad_mapping;
```

11. Schließen Sie die `psql`-Sitzung.

```
labdb=> \q
```

AWS CLI

Um pg_ad_mapping einzurichten

Um pg_ad_mapping mit dem einzurichten, rufen Sie die modify-db-parameter-groupOperation auf AWS CLI, um diesen Parameter zu Ihrer benutzerdefinierten Parametergruppe hinzuzufügen, wie im folgenden Verfahren gezeigt.

1. Verwenden Sie den folgenden AWS CLI Befehl, um den Parameter zu erweiternpg_ad_mapping. `shared_preload_libraries`

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=pg_ad_mapping,ApplyMethod=pending-
reboot" \
   --region aws-region
```

2. Verwenden Sie den folgenden AWS CLI Befehl, um die Writer-Instance Ihres Aurora PostgreSQL-DB-Clusters neu zu starten, sodass das pg_ad_mapping initialisiert wird.

```
aws rds reboot-db-instance \
    --db-instance-identifier writer-instance \
    --region aws-region
```

3. Wenn die Instance verfügbar ist, können Sie überprüfen, ob `pg_ad_mapping` initialisiert wurde. Verwenden Sie`psql`, um eine Verbindung zur Writer-Instance Ihres Aurora PostgreSQL-DB-Clusters herzustellen, und führen Sie dann den folgenden Befehl aus.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pg_ad_mapping
(1 row)
```

   Wenn pg_ad_mapping initialisiert ist, können Sie jetzt die Erweiterung erstellen.

```
CREATE EXTENSION pg_ad_mapping;
```

4. Schließen Sie die `psql`-Sitzung, damit Sie die AWS CLI verwenden können.

```
labdb=> \q
```

Die Active Directory-Gruppen-SID wird abgerufen in PowerShell

Eine Sicherheits-ID (SID) wird verwendet, um einen Sicherheitsprinzipal oder eine Sicherheitsgruppe eindeutig zu identifizieren. Immer wenn eine Sicherheitsgruppe oder ein Konto in Active Directory erstellt wird, wird ihr eine SID zugewiesen. Um die SID der AD-Sicherheitsgruppe aus dem Active Directory abzurufen, können Sie das Cmdlet Get-ADGroup vom Windows-Client-Computer verwenden, der mit dieser Active Directory-Domäne verbunden ist. Der Identity-Parameter gibt den Active Directory-Gruppennamen an, um die entsprechende SID abzurufen.

Im folgenden Beispiel wird die SID der AD-Gruppe *adgroup1* zurückgegeben.

```
C:\Users\Admin> Get-ADGroup -Identity adgroup1 | select SID

             SID
-----------------------------------------------
S-1-5-21-3168537779-1985441202-1799118680-1612
```

Zuordnung der DB-Rolle zur AD-Sicherheitsgruppe

Sie müssen die AD-Sicherheitsgruppen in der Datenbank explizit als PostgreSQL-DB-Rolle bereitstellen. Ein AD-Benutzer, der Teil mindestens einer bereitgestellten AD-Sicherheitsgruppe ist, erhält Zugriff auf die Datenbank. Sie sollten einer AD-Gruppe keine sicherheitsbasierte DB-Rolle gewährenrds_ad role. *Die Kerberos-Authentifizierung für die Sicherheitsgruppe wird ausgelöst, indem das Domainnamensuffix wie user1@example.com verwendet wird.* Diese DB-Rolle kann keine Passwort- oder IAM-Authentifizierung verwenden, um Zugriff auf die Datenbank zu erhalten.

> **Note**
>
> AD-Benutzer, denen eine entsprechende DB-Rolle in der Datenbank rds_ad zugewiesen wurde, können sich nicht als Teil der AD-Sicherheitsgruppe anmelden. Sie erhalten Zugriff über die DB-Rolle als Einzelbenutzer.

Accounts-Group ist beispielsweise eine Sicherheitsgruppe in AD, für die Sie diese Sicherheitsgruppe in Aurora PostgreSQL als Accounts-Rolle bereitstellen möchten.

AD-Sicherheitsgruppe	PostgreSQL-DB-Rolle
Kontengruppe	Kontenrolle

Wenn Sie die DB-Rolle der AD-Sicherheitsgruppe zuordnen, müssen Sie sicherstellen, dass für die DB-Rolle das LOGIN-Attribut gesetzt ist und dass sie über die CONNECT-Privilegien für die erforderliche Anmeldedatenbank verfügt.

```
postgres => alter role accounts-role login;

ALTER ROLE
postgres => grant connect on database accounts-db to accounts-role;
```

Der Administrator kann nun mit der Erstellung der Zuordnung zwischen der AD-Sicherheitsgruppe und der PostgreSQL-DB-Rolle fortfahren.

```
admin=>select pgadmap_set_mapping('accounts-group', 'accounts-role', <SID>, <Weight>);
```

Informationen zum Abrufen der SID der AD-Sicherheitsgruppe finden Sie unter. Die Active Directory-Gruppen-SID wird abgerufen in PowerShell

Es kann vorkommen, dass ein AD-Benutzer mehreren Gruppen angehört. In diesem Fall erbt der AD-Benutzer die Rechte der DB-Rolle, der die höchste Gewichtung zugewiesen wurde. Wenn die beiden Rollen dasselbe Gewicht haben, erbt der AD-Benutzer die Rechte der DB-Rolle, die der kürzlich hinzugefügten Zuordnung entspricht. Es wird empfohlen, Gewichtungen anzugeben, die den relativen Berechtigungen/Privilegien der einzelnen DB-Rollen entsprechen. Je höher die Berechtigungen oder Privilegien einer DB-Rolle, desto höher die Gewichtung, die dem Zuordnungseintrag zugewiesen werden sollte. Dadurch wird die Mehrdeutigkeit vermieden, wenn zwei Zuordnungen dasselbe Gewicht haben.

Die folgende Tabelle zeigt ein Beispiel für die Zuordnung von AD-Sicherheitsgruppen zu Aurora PostgreSQL-DB-Rollen.

AD-Sicherheitsgruppe	PostgreSQL-DB-Rolle	Gewicht
Kontengruppe	Kontenrolle	7
Vertriebsgruppe	Rolle im Vertrieb	10
Entwicklungsgruppe	Entwicklungsrolle	7

Im folgenden Beispiel erbt sie die Rechte von sales-role, `user1` da sie die höhere Gewichtung hat, und erbt gleichzeitig `user2` die Rechte von, `dev-role` wie das Mapping für diese Rolle danach erstellt wurde`accounts-role`, die dieselbe Gewichtung haben wie. `accounts-role`

Username	Mitgliedschaft in einer Sicherheitsgruppe
Benutzer 1	Kundengruppe Vertriebsgruppe
Benutzer 2	Kontengruppe Dev-Gruppe

Die psql-Befehle zum Erstellen, Auflisten und Löschen der Zuordnungen sind unten aufgeführt. Derzeit ist es nicht möglich, einen einzelnen Zuordnungseintrag zu ändern. Der bestehende Eintrag muss gelöscht und die Zuordnung neu erstellt werden.

```
admin=>select pgadmap_set_mapping('accounts-group', 'accounts-role', 'S-1-5-67-890',
 7);
admin=>select pgadmap_set_mapping('sales-group', 'sales-role', 'S-1-2-34-560', 10);
admin=>select pgadmap_set_mapping('dev-group', 'dev-role', 'S-1-8-43-612', 7);

admin=>select * from pgadmap_read_mapping();

ad_sid       | pg_role        | weight | ad_grp
-------------+----------------+--------+---------------
S-1-5-67-890 | accounts-role | 7      | accounts-group
S-1-2-34-560 | sales-role    | 10     | sales-group
S-1-8-43-612 | dev-role      | 7      | dev-group
(3 rows)
```

Protokollierung/Prüfung der AD-Benutzeridentität

Verwenden Sie den folgenden Befehl, um die Datenbankrolle zu ermitteln, die vom aktuellen Benutzer oder vom Sitzungsbenutzer geerbt wurde:

```
postgres=>select session_user, current_user;

session_user | current_user
-------------+--------------
dev-role     | dev-role

(1 row)
```

Verwenden Sie den folgenden Befehl, um die Identität des AD-Sicherheitsprinzipals zu ermitteln:

```
postgres=>select principal from pg_stat_gssapi where pid = pg_backend_pid();

 principal
-------------------------
 user1@example.com

(1 row)
```

Derzeit ist die AD-Benutzeridentität in den Auditprotokollen nicht sichtbar. Der `log_connections` Parameter kann aktiviert werden, um den Aufbau einer DB-Sitzung zu protokollieren. Weitere Informationen finden Sie unter log_connections. Die Ausgabe hierfür beinhaltet die AD-Benutzeridentität, wie unten dargestellt. Die dieser Ausgabe zugeordnete Backend-PID kann dann dabei helfen, Aktionen dem tatsächlichen AD-Benutzer zuzuordnen.

```
pgrole1@postgres:[615]:LOG: connection authorized: user=pgrole1
 database=postgres application_name=psql GSS (authenticated=yes, encrypted=yes,
 principal=Admin@EXAMPLE.COM)
```

Einschränkungen

- Microsoft Entra ID, bekannt als Azure Active Directory, wird nicht unterstützt.

Verwenden von Funktionen aus der Erweiterung **pg_ad_mapping**

`pg_ad_mapping`Die Erweiterung bot Unterstützung für die folgenden Funktionen:

pgadmap_set_mapping

Diese Funktion stellt die Zuordnung zwischen der AD-Sicherheitsgruppe und der Datenbankrolle mit einer zugehörigen Gewichtung her.

Syntax

```
pgadmap_set_mapping(
ad_group,
db_role,
ad_group_sid,
weight)
```

Argumente

Parameter	Beschreibung
ad_group	Name der AD-Gruppe. Der Wert darf nicht Null oder eine leere Zeichenfolge sein.
db_role	Datenbankrolle, die der angegebenen AD-Gruppe zugeordnet werden soll. Der Wert darf nicht Null oder eine leere Zeichenfo lge sein.
ad_group_sid	Sicherheits-ID, die zur eindeutigen Identifizierung der AD-Gruppe verwendet wird. Der Wert beginnt mit 'S-1-' und darf weder Null noch eine leere Zeichenfolge sein. Weitere Informati onen finden Sie unter Die Active Directory-Gruppen-SID wird abgerufen in PowerShell.

Parameter	Beschreibung
Gewicht	Gewicht, das der Datenbankrolle zugeordnet ist. Die Rolle mit der höchsten Gewichtung hat Vorrang, wenn der Benutzer Mitglied mehrerer Gruppen ist. Der Standardwert für das Gewicht ist 1.

Rückgabetyp

None

Nutzungshinweise

Diese Funktion fügt eine neue Zuordnung von der AD-Sicherheitsgruppe zur Datenbankrolle hinzu. Sie kann nur auf der primären DB-Instance des DB-Clusters von einem Benutzer mit der Berechtigung rds_superuser ausgeführt werden.

Beispiele

```
postgres=> select pgadmap_set_mapping('accounts-group','accounts-
role','S-1-2-33-12345-67890-12345-678',10);

pgadmap_set_mapping

(1 row)
```

pgadmap_read_mapping

Diese Funktion listet die Zuordnungen zwischen der AD-Sicherheitsgruppe und der DB-Rolle auf, die mithilfe der Funktion festgelegt wurden. `pgadmap_set_mapping`

Syntax

```
pgadmap_read_mapping()
```

Argumente

None

Rückgabetyp

Parameter	Beschreibung
ad_group_sid	Sicherheits-ID, die zur eindeutigen Identifizierung der AD-Gruppe verwendet wird. Der Wert beginnt mit 'S-1-' und darf weder Null noch eine leere Zeichenfolge sein. Weitere Informationen erhalten Sie unter .accounts-role@example.com Die Active Directory-Gruppen-SID wird abgerufen in PowerShell
db_role	Datenbankrolle, die der angegebenen AD-Gruppe zugeordnet werden soll. Der Wert darf nicht Null oder eine leere Zeichenfolge sein.
Gewicht	Gewicht, das der Datenbankrolle zugeordnet ist. Die Rolle mit der höchsten Gewichtung hat Vorrang, wenn der Benutzer Mitglied mehrerer Gruppen ist. Der Standardwert für das Gewicht ist 1.
ad_group	Name der AD-Gruppe. Der Wert darf nicht Null oder eine leere Zeichenfolge sein.

Nutzungshinweise

Rufen Sie diese Funktion auf, um alle verfügbaren Zuordnungen zwischen der AD-Sicherheitsgruppe und der DB-Rolle aufzulisten.

Beispiele

```
postgres=> select * from pgadmap_read_mapping();

ad_sid                              | pg_role       | weight | ad_grp
------------------------------------+---------------+--------+-----------------
S-1-2-33-12345-67890-12345-678      | accounts-role | 10     | accounts-group
(1 row)

(1 row)
```

pgadmap_reset_mapping

Diese Funktion setzt eine oder alle Zuordnungen zurück, die mit der Funktion festgelegt wurden. `pgadmap_set_mapping`

Syntax

```
pgadmap_reset_mapping(
ad_group_sid,
db_role,
weight)
```

Argumente

Parameter	Beschreibung
ad_group_sid	Sicherheits-ID, die zur eindeutigen Identifizierung der AD-Gruppe verwendet wird.
db_role	Datenbankrolle, die der angegebenen AD-Gruppe zugeordnet werden soll.
Gewicht	Gewicht, das der Datenbankrolle zugeordnet ist.

Wenn keine Argumente angegeben werden, werden alle Zuordnungen von AD-Gruppen zu DB-Rollen zurückgesetzt. Entweder müssen alle Argumente angegeben werden oder keine.

Rückgabetyp

`None`

Nutzungshinweise

Rufen Sie diese Funktion auf, um eine bestimmte AD-Gruppe zur DB-Rollenzuordnung zu löschen oder um alle Zuordnungen zurückzusetzen. Diese Funktion kann nur von einem Benutzer mit entsprechenden Rechten auf der primären DB-Instance des DB-Clusters ausgeführt werden. `rds_superuser`

Beispiele

```
postgres=> select * from pgadmap_read_mapping();

   ad_sid                        | pg_role      | weight      | ad_grp
---------------------------------+--------------+-------------+-------------------
 S-1-2-33-12345-67890-12345-678 | accounts-role| 10          | accounts-group
 S-1-2-33-12345-67890-12345-666 | sales-role   | 10          | sales-group

(2 rows)
postgres=> select pgadmap_reset_mapping('S-1-2-33-12345-67890-12345-678', 'accounts-
role', 10);

pgadmap_reset_mapping
(1 row)

postgres=> select * from pgadmap_read_mapping();

   ad_sid                        | pg_role      | weight      | ad_grp
---------------------------------+--------------+-------------+---------------
 S-1-2-33-12345-67890-12345-666 | sales-role   | 10          | sales-group

(1 row)
postgres=> select pgadmap_reset_mapping();

pgadmap_reset_mapping
(1 row)

postgres=> select * from pgadmap_read_mapping();

   ad_sid                        | pg_role      | weight      | ad_grp
---------------------------------+--------------+-------------+--------------
 (0 rows)
```

Migrieren von Daten nach Amazon Aurora mit PostgreSQL-Kompatibilität

Sie haben mehrere Möglichkeiten, Daten aus einer vorhandenen Datenbank in einen Amazon Aurora PostgreSQL-kompatible Edition-DB-Cluster zu migrieren. Die verfügbaren Migrationsoptionen

sind auch von der Quelldatenbank und der Menge der zu migrierenden Daten abhängig. Folgende Optionen sind verfügbar:

Migrieren einer RDS-for-PostgreSQL-DB-Instance unter Verwendung eines Snapshots

Sie können Daten direkt von einem RDS-for-PostgreSQL-DB-Snapshot in einen Aurora-PostgreSQL-DB-Cluster migrieren.

Migrieren einer RDS-for-PostgreSQL-DB-Instance unter Verwendung eines Aurora-Lesereplikats

Sie können auch Daten aus einer RDS-for-PostgreSQL-DB-Instance migrieren, indem Sie ein Aurora-PostgreSQL-Lesereplikat einer RDS-for-PostgreSQL-DB-Instance erstellen. Wenn die Replikat-Verzögerung zwischen der RDS-for-PostgreSQL-DB-Instance und dem Aurora-PostgreSQL-Lesereplikat Null ist, können Sie die Replikation stoppen. An diesem Punkt können Sie die Aurora-Read Replica zu einem eigenständigen Aurora PostgreSQL-DB-Cluster für das Lesen und Schreiben machen.

Importieren von Daten aus Amazon S3 in Aurora PostgreSQL

Sie können Daten migrieren, indem Sie sie Amazon S3 in eine Tabelle importieren, die zu einem Aurora PostgreSQL-DB-Cluster gehört.

Migrieren aus einer Datenbank, die nicht PostgreSQL-kompatibel ist

Sie können AWS Database Migration Service (AWS DMS) verwenden, um Daten aus einer Datenbank zu migrieren, die nicht PostgreSQL-kompatibel ist. Weitere Informationen finden Sie AWS DMS unter Was ist der AWS Database Migration Service? im AWS Database Migration Service Benutzerhandbuch.

> **Note**
>
> Die Aktivierung der Kerberos-Authentifizierung wird derzeit auf dem Aurora PostgreSQL-DB-Cluster während der Migration von RDS für PostgreSQL nicht unterstützt. Sie können die Kerberos-Authentifizierung nur auf einem eigenständigen Aurora PostgreSQL-DB-Cluster aktivieren.

Eine Liste, AWS-Regionen wo Aurora verfügbar ist, finden Sie unter Amazon Aurora im Allgemeine AWS-Referenz.

> **Important**
>
> Wenn Sie planen, eine RDS for PostgreSQL-DB-Instance in naher Zukunft auf einen Aurora PostgreSQL-DB-Cluster zu migrieren, empfehlen wir Ihnen dringend, Upgrades von automatischen Unterversionen für die DB-Instance zu Beginn der Migrationsplanungsphase zu deaktivieren. Die Migration nach Aurora PostgreSQL kann sich verzögern, wenn die RDS for PostgreSQL-Version von Aurora PostgreSQL noch nicht unterstützt wird. Informationen zu Aurora PostgreSQL-Versionen finden Sie unter Engine-Versionen für Amazon Aurora-PostgreSQL.

Migrieren eines Snapshots einer RDS-for-PostgreSQL-DB-Instance in einen Aurora-PostgreSQL-DB-Cluster

Sie können einen DB-Snapshot einer RDS-PostgreSQL-DB-Instance migrieren und so einen Aurora-for-PostgreSQL-DB-Cluster erstellen. Der neue Aurora-PostgreSQL-DB-Cluster wird mit den Daten der ursprünglichen RDS-for-PostgreSQL-DB-Instance gefüllt. Informationen zum Erstellen von DB-Snapshots finden Sie unter Erstellen eines DB-Snapshots.

In einigen Fällen befindet sich der DB-Snapshot möglicherweise nicht AWS-Region dort, wo Sie Ihre Daten speichern möchten. Wenn ja, verwenden Sie die Amazon-RDS-Konsole zum Kopieren des DB-Snapshots in diese AWS-Region. Informationen zum Kopieren von DB-Snapshots finden Sie unter Kopieren eines DB-Snapshots.

Sie können RDS-for-PostgreSQL-Snapshots migrieren, die mit den in der angegebenen AWS-Region verfügbaren Aurora-PostgreSQL-Versionen kompatibel sind. Beispielsweise können Sie ein Snapshot von einer DB-Instance mit RDS for PostgreSQL 11.1 auf Aurora PostgreSQL Version 11.4, 11.7, 11.8 oder 11.9 in Region USA West (Nordkalifornien) migrieren. Sie können RDS for PostgreSQL 10.11 Snapshot zu Aurora PostgreSQL 10.11, 10.12, 10.13 und 10.14 migrieren. Mit anderen Worten, der RDS-for-PostgreSQL-Snapshot muss im Vergleich zu Aurora PostgreSQL die gleiche oder eine niedrigere Unterversion verwenden.

Sie können auch wählen, dass Ihr neuer Aurora PostgreSQL DB-Cluster im Ruhezustand verschlüsselt wird, indem Sie eine AWS KMS key. Diese Option steht nur für unverschlüsselte DB-Snapshots zu Verfügung.

Um einen RDS for PostgreSQL-DB-Snapshot zu einem Aurora PostgreSQL-DB-Cluster zu migrieren, können Sie die AWS Management Console AWS CLI, oder die RDS-API verwenden. Wenn Sie die

verwenden AWS Management Console, ergreift die Konsole die erforderlichen Aktionen, um sowohl den DB-Cluster als auch die primäre Instance zu erstellen.

Konsole

So migrieren Sie einen PostgreSQL-DB-Snapshot mithilfe der RDS-Konsole

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Klicken Sie auf Snapshots (Snapshots).
3. Wählen Sie auf der Seite Snapshots den RDS-for-PostgreSQL-Snapshot aus, den Sie zu einem Aurora-PostgreSQL-DB-Cluster migrieren möchten.
4. Wählen Sie Actions (Aktionen) und wählen Sie Migrate snapshot (Snapshot migrieren).
5. Legen Sie auf der Seite Migrate Database (Datenbank migrieren) Folgendes fest:

   - DB-Engine-Version: Wählen Sie eine DB-Engine-Version, die Sie für die neue migrierte Instance verwenden möchten.
   - DB-Instance-ID: Geben Sie einen Namen für den DB-Cluster ein, der für Ihr Konto in dem AWS-Region von Ihnen ausgewählten Konto eindeutig ist. Dieser Bezeichner wird in den Endpunktadressen für die Instances im DB-Cluster verwendet. Sie können dem Namen einige Informationen hinzufügen, z. B. die von Ihnen gewählte DB-Engine AWS-Region und die von Ihnen gewählte DB-Engine angeben**`aurora-cluster1`**.

     Für den DB-Instance-Bezeichner gelten folgende Einschränkungen:

     - Er muss zwischen 1 und 63 alphanumerische Zeichen oder Bindestriche enthalten.
     - Das erste Zeichen muss ein Buchstabe sein.
     - Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
     - Es muss für alle DB-Instances pro AWS -Konto und AWS-Region eindeutig sein.
   - DB-Instance-Klasse: Wählen Sie eine DB-Instance-Klasse, die über ausreichend Speicher und Kapazität für Ihre Datenbank verfügt, z. B. `db.r6g.large`. Aurora-Cluster-Volumes nehmen automatisch an Größe zu, wenn die Datenmenge in Ihrer Datenbank zunimmt. Sie müssen daher nur eine DB-Instance-Klasse auswählen, die den aktuellen Speicheranforderungen entspricht. Weitere Informationen finden Sie unter Übersicht über Amazon-Aurora-Speicher.
   - Virtual Private Cloud (VPC): Wenn bereits eine VPC vorhanden ist, können Sie diese mit dem Aurora PostgreSQL-DB-Cluster verwenden, indem Sie ihre VPC-ID auswählen, z. B. `vpc-`

`a464d1c1`. Weitere Informationen zum Erstellen einer VPC finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4).

Anderenfalls können Sie von Amazon RDS eine neue VPC erstellen lassen, indem Sie auf Create new VPC (Neue VPC erstellen) klicken.

- DB-Subnetzgruppe: Wenn bereits eine Subnetzgruppe vorhanden ist, können Sie diese mit dem Aurora-PostgreSQL-DB-Cluster verwenden, indem Sie Ihre Subnetzgruppen-ID auswählen, z. B. `gs-subnet-group1`.
- Public Access (Öffentlicher Zugang): Wählen Sie Nein aus, um festzulegen, dass nur Ressourcen innerhalb der VPC auf Instances im DB-Cluster zugreifen dürfen. Wählen Sie Ja aus, um anzugeben, dass Ressourcen im öffentlichen Netzwerk auf Instances im DB-Cluster zugreifen dürfen.

> **Note**
>
> Der Produktions-DB-Cluster muss sich nicht unbedingt in einem öffentlichen Subnetz befinden, da nur die Anwendungsserver Zugriff auf ihren DB-Cluster benötigen. Wenn sich das DB-Cluster nicht in einem öffentlichen Subnetz befinden soll, stellen Sie Public Access (Öffentlicher Zugang) auf No (Nein).

- VPC-Sicherheitsgruppe: Wählen Sie eine VPC-Sicherheitsgruppe aus, um den Zugriff auf Ihre Datenbank zu ermöglichen.
- Availability Zone: Wählen Sie die Availability Zone zum Hosten der primären Instance des Aurora PostgreSQL-DB-Clusters aus. Damit Amazon RDS eine Availability Zone für Sie auswählt, klicken Sie auf Keine Präferenz.
- Database Port (Datenbankport): Geben Sie den Standardport ein, der beim Verbinden der Instances im Aurora PostgreSQL-DB-Cluster verwendet werden soll. Der Standardwert ist `5432`.

> **Note**
>
> Möglicherweise lässt die Firewall eines Unternehmens den Zugriff auf Standard-Ports, wie z. B. den PostgreSQL-Standard-Port 5432, nicht zu. Geben Sie in diesem Fall einen Port ein, der von der Firewall Ihres Unternehmens zugelassen wird.
> Sie benötigen diesen Portwert später, wenn Sie eine Verbindung mit dem Aurora PostgreSQL-DB-Cluster herstellen.

- Enable Encryption (Verschlüsselung aktivieren): Wählen Sie Enable Encryption (Verschlüsselung aktivieren) aus, um Ihr neues Aurora PostgreSQL-DB-Cluster im Ruhezustand zu verschlüsseln. Wählen Sie außerdem einen KMS-Schlüssel als Wert AWS KMS key.
- Auto minor version upgrade (Upgrade einer Unterversion automatisch durchführen): Wählen Sie Enable auto minor version upgrade (Upgrade einer Unterversion automatisch durchführen) aus, wenn Aktualisierungen der PostgreSQL-DB-Engine-Version automatisch im Aurora PostgreSQL-DB-Cluster installiert werden sollen, sobald sie verfügbar sind.

  Die Option Auto Minor Version Upgrade (Upgrade einer Unterversion automatisch durchführen) gilt nur bei Upgrades für Engine-Unterversionen von PostgreSQL für Ihren Aurora PostgreSQL-DB-Cluster. Regelmäßige Patches zur Aufrechterhaltung der Systemstabilität sind davon nicht betroffen.

6. Wählen Sie Migrate (Migrieren) aus, um den DB-Snapshot zu migrieren.
7. Wählen Sie Datenbanken, um den neuen DB-Cluster zu sehen. Wählen Sie den neuen DB-Cluster an, um den Fortschritt der Migration zu überwachen. Wenn die Migration abgeschlossen ist, lautet der Status für den Cluster Available (Verfügbar). Auf der Registerkarte Konnektivität und Sicherheit finden Sie den Cluster-Endpunkt, der für die Verbindung mit der primären Writer-Instanz des DB-Clusters verwendet werden soll. Weitere Informationen zum Herstellen einer Verbindung mit einem Aurora PostgreSQL-DB-Cluster finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

AWS CLI

Die Verwendung von AWS CLI , um einen RDS for PostgreSQL-DB-Snapshot zu einem Aurora PostgreSQL zu migrieren, umfasst zwei separate Befehle. AWS CLI Zunächst verwenden Sie den `restore-db-cluster-from-snapshot` AWS CLI Befehl create a new Aurora PostgreSQL DB-Cluster. Dann erstellen Sie mit dem Befehl `create-db-instance` die primäre DB-Instance im neuen Cluster, um die Migration abzuschließen. Das folgende Verfahren erstellt einen Aurora-PostgreSQL-DB-Cluster mit einer primären DB-Instance, die dieselbe Konfiguration wie die DB-Instance hat, die zum Erstellen des Snapshots verwendet wurde.

Einen RDS-for-PostgreSQL-DB-Snapshot auf einen Aurora-PostgreSQL-DB-Cluster migrieren

1. Verwenden Sie den describe-db-snapshotsBefehl, um Informationen über den DB-Snapshot zu erhalten, den Sie migrieren möchten. Sie können den Parameter `--db-instance-`

`identifier` oder `--db-snapshot-identifier` im Befehl angeben. Wenn Sie keinen dieser Parameter angeben, erhalten Sie alle Snapshots.

```
aws rds describe-db-snapshots --db-instance-identifier <your-db-instance-name>
```

2. Der Befehl gibt alle Konfigurationsdetails für alle Snapshots zurück, die aus der angegebenen DB-Instance erstellt wurden. Suchen Sie in der Ausgabe nach dem Snapshot, den Sie migrieren möchten, und suchen Sie nach seinem Amazon-Ressourcennamen (ARN). Weitere Informationen zu Amazon-RDS-ARNs finden Sie unter Amazon Relational Database Service (Amazon RDS). Der ARN sieht folgendermaßen oder ähnlich aus.

```
“DBSnapshotArn": "arn:aws:rds:aws-region:111122223333:snapshot:<snapshot_name>"
```

   In der Ausgabe finden Sie auch Konfigurationsdetails zur RDS-for-PostgreSQL-DB-Instance, z. B. die Engine-Version, den zugewiesenen Speicher, ob die DB-Instance verschlüsselt ist oder nicht und so weiter.

3. Verwenden Sie den Befehl restore-db-cluster-from-snapshot, um die Migration zu starten. Geben Sie die folgenden Parameter an:

   - `--db-cluster-identifier` – Der Name, den Sie dem Aurora-PostgreSQL-DB-Cluster geben möchten. Dieser Aurora-DB-Cluster ist das Ziel für Ihre DB-Snapshot-Migration.
   - `--snapshot-identifier` – Der Amazon-Ressourcenname (ARN) des zu migrierenden DB-Snapshot.
   - `--engine` – Geben Sie `aurora-postgresql` für die Aurora-DB-Cluster-Engine an.
   - `--kms-key-id` – Mit diesem optionalen Parameter können Sie einen verschlüsselten Aurora-PostgreSQL-DB-Cluster aus einem unverschlüsselten DB-Snapshot erstellen. Sie können auch einen anderen Verschlüsselungsschlüssel für den DB-Cluster auswählen als den Schlüssel, der für den DB-Snapshot verwendet wird.

     > **Note**
     >
     > Aus einem verschlüsselten DB-Snapshot kann kein unverschlüsselter Aurora-PostgreSQL-DB-Cluster erstellt werden.

   Ohne den wie folgt angegebenen `--kms-key-id` Parameter erstellt der AWS CLI Befehl restore-db-cluster-from-snapshot einen leeren Aurora PostgreSQL-DB-Cluster, der entweder mit

demselben Schlüssel wie der DB-Snapshot verschlüsselt ist oder unverschlüsselt ist, wenn der Quell-DB-Snapshot nicht verschlüsselt ist.

FürLinux, oder: macOS Unix

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier cluster-name \
    --snapshot-identifier arn:aws:rds:aws-region:111122223333:snapshot:your-
snapshot-name \
    --engine aurora-postgresql
```

Windows:

```
aws rds restore-db-cluster-from-snapshot ^
    --db-cluster-identifier new_cluster ^
    --snapshot-identifier arn:aws:rds:aws-region:111122223333:snapshot:your-
snapshot-name ^
    --engine aurora-postgresql
```

4. Der Befehl gibt Details zum Aurora-PostgreSQL-DB-Cluster zurück, der für die Migration erstellt wird. Sie können den Status des Aurora PostgreSQL-DB-Clusters mit dem describe-db-clusters AWS CLI Befehl überprüfen.

```
aws rds describe-db-clusters --db-cluster-identifier cluster-name
```

5. Wenn der DB-Cluster „verfügbar“ wird, verwenden Sie den create-db-instanceBefehl, um den Aurora PostgreSQL-DB-Cluster mit der DB-Instance zu füllen, die auf Ihrem Amazon RDS-DB-Snapshot basiert. Geben Sie die folgenden Parameter an:

   - `--db-cluster-identifier` – Der Name des neuen Aurora-PostgreSQL-DB-Clusters, den Sie im vorherigen Schritt erstellt haben.
   - `--db-instance-identifier` – Der Name, den Sie der DB-Instance zuweisen möchten. Diese Instance wird zum Primärknoten in Ihrem Aurora-PostgreSQL-DB-Cluster.
   - `----db-instance-class` – Geben Sie die zu verwendende DB-Instance-Klasse an. Wählen Sie aus den DB-Instance-Klassen, die von der Aurora-PostgreSQL-Version unterstützt werden, zu der Sie migrieren. Weitere Informationen finden Sie unter DB-Instance-Klassenarten und Unterstützte DB-Engines für DB-Instance-Klassen.
   - `--engine` – Geben Sie `aurora-postgresql` für die DB-Instance an.

Sie können die DB-Instance auch mit einer anderen Konfiguration als den Quell-DB-Snapshot erstellen, indem Sie die entsprechenden Optionen im Befehl übergeben. `create-db-instance` AWS CLI Weitere Informationen finden Sie im create-db-instanceBefehl.

Für LinuxmacOS, oderUnix:

```
aws rds create-db-instance \
    --db-cluster-identifier cluster-name \
    --db-instance-identifier --db-instance-class db.instance.class \
    --engine aurora-postgresql
```

Windows:

```
aws rds create-db-instance ^
    --db-cluster-identifier cluster-name ^
    --db-instance-identifier --db-instance-class db.instance.class ^
    --engine aurora-postgresql
```

Wenn der Migrationsprozess abgeschlossen ist, verfügt der Aurora-PostgreSQL-Cluster über eine ausgefüllte primäre DB-Instance.

Datenmigration von einer RDS-for-PostgreSQL-DB-Instance zu einem Aurora-PostgreSQL-DB-Cluster unter Verwendung eines Aurora–Lesereplikats

Sie können eine RDS-for-PostgreSQL-DB-Instance als Grundlage für einen neuen Aurora-PostgreSQL-DB-Cluster verwenden, indem Sie eine Aurora-Lesereplikat für den Migrationsprozess verwenden. Die Aurora-Read-Replica-Option ist nur für die Migration innerhalb desselben AND-Kontos verfügbar AWS-Region und nur verfügbar, wenn die Region eine kompatible Version von Aurora PostgreSQL für Ihre RDS for PostgreSQL-DB-Instance anbietet. Kompatibel bedeutet, dass die Aurora-PostgreSQL-Version mit der RDS-for-PostgreSQL-Version identisch ist oder dass es sich um eine höhere Nebenversion in derselben Hauptversionsfamilie handelt.

Um diese Technik beispielsweise zum Migrieren einer RDS-for-PostgreSQL-11.14-DB-Instance verwenden zu können, muss die Region Aurora PostgreSQL Version 11.14 oder eine höhere Nebenversion in der PostgreSQL-Version-11-Familie anbieten.

Themen

Übersicht über das Migrieren von Daten mittels einer Aurora-Read Replica

Migrieren von einer RDS-for-PostgreSQL-DB-Instance zu einem Aurora-PostgreSQL-DB-Cluster ist ein mehrstufiges Verfahren. Zuerst erstellen Sie ein Aurora-Lesereplikat Ihrer Quell-RDS-Instance-for-PostgreSQL-DB-Instance. Dies startet einen Replikationsprozess von Ihrer RDS-for-PostgreSQL-DB-Instance zu einem speziellen DB-Cluster, der als Replikat-Cluster bekannt ist. Der Replikat-Cluster besteht ausschließlich aus einem Aurora-Lesereplikat (einer Reader-Instance).

Sobald der Replikat-Cluster vorhanden ist, überwachen Sie die Verzögerung zwischen ihm und dem Quell-RDS-for-PostgreSQL-DB-Instance. Wenn die Replikatverzögerung Null (0) ist, können Sie den Replikat-Cluster hochstufen. Die Replikation wird beendet, der Replikat-Cluster wird zu einem eigenständigen Aurora-DB-Cluster hochgestuft, und der Reader wird zur Writer-Instance für den Cluster befördert. Sie können dann Instances zum Aurora-PostgreSQL-DB-Cluster hinzufügen, um

Ihren Aurora-PostgreSQL-DB-Cluster für Ihren Anwendungsfall zu skalieren. Sie können die RDS-for-PostgreSQL-DB-Instance auch löschen, falls Sie keine weitere Notwendigkeit mehr dafür haben.

> **Note**
>
> Es kann mehrere Stunden pro Terabyte Daten dauern, bis die Migration abgeschlossen ist.

Sie können kein Aurora-Lesereplikat erstellen, falls die RDS-for-PostgreSQL-DB-Instance bereits über ein Aurora-Lesereplikat verfügt oder ein regionsübergreifendes Lesereplikat enthält.

Vorbereiten der Migration von Daten mithilfe einer Aurora Read Replica

Während des Migrationsprozesses mit Aurora-Lesereplikat werden Aktualisierungen, die mit den Daten der Quell-RDS-for-PostgreSQL-DB-Instance vorgenommen werden, asynchron in diesem Aurora-Lesereplikat des Replica-Clusters repliziert. Der Prozess verwendet die native Streaming-Replikationsfunktion von PostgreSQL, die Write-Ahead-Log-Segmente (WAL) auf der Quell-Instance speichert. Bevor Sie mit diesem Migrationsprozess beginnen, stellen Sie sicher, dass die Instance über genügend Speicherkapazität verfügt, indem Sie die Werte für die in der Tabelle aufgeführten Metriken überprüfen.

Metrik	Beschreibung
`FreeStorageSpace`	Den verfügbaren Speicherplatz. Einheiten: Byte
`OldestReplicationSlotLag`	Der Verzögerungsgröße für WAL-Daten in der Replika, die die höchste Verzögerung aufweist. Einheiten: Megabyte
`RDSToAuroraPostgreSQLReplicaLag`	Die Zeit in Sekunden, wie lange ein Aurora PostgreSQL-DB-Cluster hinter der RDS-DB-Quell-Instance liegt.
`TransactionLogsDiskUsage`	Der von den Transaktionsprotokollen verwendete Festplattenspeicher. Einheiten: Megabyte

Weitere Informationen zur Überwachung Ihrer RDS-Instance finden Sie unter Überwachung im Amazon RDS-Benutzerhandbuch.

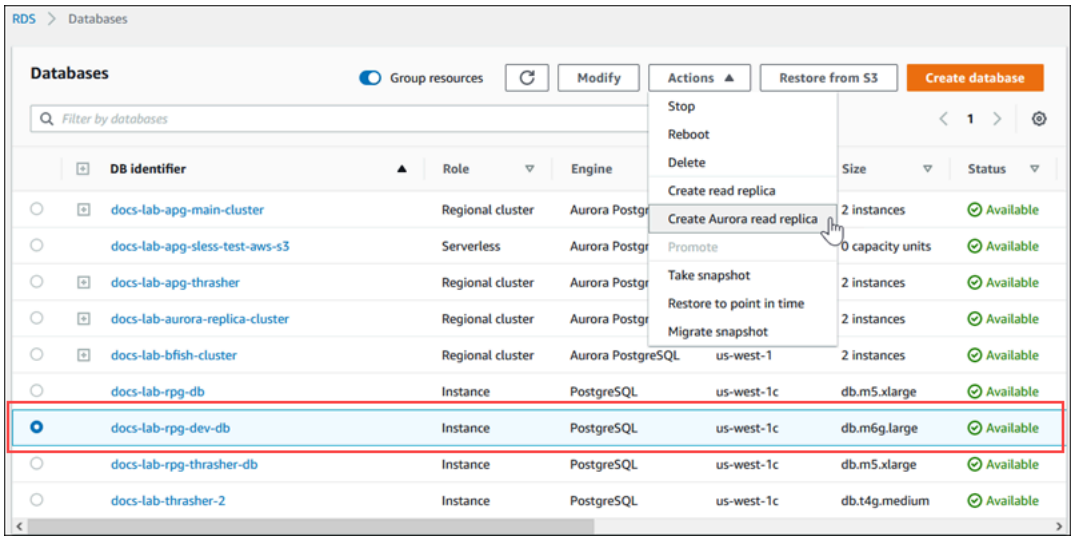
Erstellen einer Aurora Read Replica

Sie können eine Aurora-Read Replica für eine RDS for PostgreSQL-DB-Instance erstellen, indem Sie den oder den AWS Management Console verwenden. AWS CLI Die Option zum Erstellen einer Aurora-Read Replica mit dem AWS Management Console ist nur verfügbar, wenn das eine kompatible Aurora PostgreSQL-Version AWS-Region anbietet. Das heißt, es ist nur verfügbar, wenn es eine Aurora-PostgreSQL-Version gibt, die mit der RDS-for-PostgreSQL-Version oder einer höheren Nebenversion in derselben Hauptversionsfamilie identisch ist.

Konsole

Sie erstellen Sie eine Aurora Read Replica aus einer PostgreSQL-DB-Instance

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie die RDS-for-PostgreSQL-DB-Instance aus, die Sie als Quelle für Ihr Aurora-Lesereplikat verwenden möchten. Wählen Sie für Actions (Aktionen) Create Aurora read replica (Aurora Read Replica erstellen) aus. Wenn diese Auswahl nicht angezeigt wird, bedeutet dies, dass eine kompatible Aurora-PostgreSQL-Version in der Region nicht verfügbar ist.



4. Auf der Seite Einstellungen für Aurora-Lesereplikat erstellen konfigurieren Sie die Eigenschaften für den Aurora-PostgreSQL-DB-Cluster wie in der folgenden Tabelle dargestellt. Das Replica-DB-Cluster wird aus einem Snapshot der Quell-DB-Instance unter Verwendung des gleichen

Master-Benutzernamens und Kennworts wie die Quelle erstellt, sodass Sie diese derzeit nicht ändern können.

Option	Beschreibung
DB-Instance-Klasse	Wählen Sie eine DB-Instance-Klasse aus, die die Verarbeitungs- und Speicheranforderungen der primären Instance im DB-Cluster erfüllt. Weitere Informationen finden Sie unter Aurora DB-Instance-Klassen.
Multi-AZ-Bereitstellung	Während der Migration nicht verfügbar
DB-Instance-Kennung	Geben Sie den Namen ein, den Sie der DB-Instan ce zuweisen möchten. Dieser Bezeichner wird in der Endpunktadresse für die primäre Instance des neuen DB-Clusters verwendet. Für den DB-Instance-Bezeichner gelten folgende Einschränkungen: • Er muss zwischen 1 und 63 alphanumerische Zeichen oder Bindestriche enthalten. • Das erste Zeichen muss ein Buchstabe sein. • Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten. • Sie muss für alle DB-Instances, für jedes AWS Konto und für jedes Konto eindeutig sein AWS-Region.
Virtual Private Cloud (VPC)	Wählen Sie die VPC zum Hosten des DB-Clusters aus. Wählen Sie Create new VPC (Neue VPC erstellen) aus, damit Amazon RDS eine VPC für Sie erstellt. Weitere Informationen finden Sie unter Vorausset zungen für DB-Cluster.

Option	Beschreibung
DB-Subnetzgruppe	Wählen Sie die DB-Subnetzgruppe aus, die für den DB-Cluster verwendet werden soll. Wählen Sie Create new DB subnet group (Neue DB-Subnetzgruppe erstellen) aus, wenn Amazon RDS eine DB-Subnet zgruppe für Sie erstellen soll. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.
Öffentliche Zugänglichkeit	Klicken Sie auf Ja, um dem DB-Cluster eine öffentlic he IP-Adresse zuzuweisen. Wählen Sie andernfalls Nein. Die Instances in Ihrem DB-Cluster können eine Mischung aus öffentlichen und privaten DB-Instan ces sein. Weitere Informationen darüber, wie Sie den öffentlichen Zugriff für Instances deaktivieren, finden Sie unter Ausblenden einer DB-Clusters in einer VPC vor dem Internet.
Availability Zone	Legen Sie fest, ob Sie eine bestimmte Availability Zone angeben möchten. Weitere Informationen über Availability Zones finden Sie unter Regionen und Availability Zones.
VPC-Sicherheitsgruppen	Wählen Sie eine oder mehrere VPC-Sicherheitsgru ppen aus, um den Netzwerkzugriff auf den DB-Cluste r zu sichern. Wählen Sie Create new VPC security group (Neue VPC-Sicherheitsgruppe erstellen) aus, damit Amazon RDS eine VPC-Sicherheitsgruppe für Sie erstellt. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.

Option	Beschreibung
Datenbankport	Geben Sie den Port an, über den Anwendungen und Dienstprogramme auf die Datenbank zugreifen können. Aurora PostgreSQL-DB-Cluster haben standardmäßig den Standard-PostgreSQL-Port 5432 eingestellt. Die Firewalls einiger Unternehm en blockieren Verbindungen mit diesem Port. Wenn die Firewall Ihres Unternehmens den Standardport blockiert, wählen Sie einen anderen Port für den neuen DB-Cluster aus.
DB-Parametergruppe	Wählen Sie eine DB-Parametergruppe für den Aurora-PostgreSQL-DB-Cluster aus. Aurora verfügt über eine DB-Standardparametergruppe, die Sie verwenden können, oder Sie können Ihre eigene DB-Parame tergruppe erstellen. Weitere Informationen zu DB-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.
DB-Cluster-Parametergruppe	Wählen Sie eine DB-Cluster-Parametergruppe für den Aurora-PostgreSQL-DB-Cluster aus. Aurora verfügt über eine DB-Cluster-Standardparametergruppe, die Sie verwenden können, oder Sie können Ihre eigene DB-Cluster-Parametergruppe erstellen. Weitere Informationen zu DB-Cluster-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.
Verschlüsselung	Wählen Sie Enable encryption (Verschlüsselung aktivieren) aus, wenn das neue Aurora-DB-Cluster im Ruhezustand verschlüsselt werden soll. Wenn Sie Verschlüsselung aktivieren wählen, wählen Sie auch einen KMS-Schlüssel als Wert AWS KMS key .

Option	Beschreibung
Priorität	Wählen Sie eine Failover-Priorität für den DB-Cluste r aus. Wenn Sie keinen Wert auswählen, wird als Standard tier-1 (Tier-1) eingestellt. Diese Priorität bestimmt die Reihenfolge, in der Aurora-Replikate bei der Wiederherstellung nach einem Ausfall der primären Instance hochgestuft werden. Weitere Informationen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.
Aufbewahrungszeitraum für Backups	Wählen Sie den Zeitraum (zwischen 1 und 35 Tage) für die Aufbewahrung von Sicherungskopien der Datenbank in Aurora aus. Sicherungskopien können sekundengenau für point-in-time Wiederherstellungen (PITR) Ihrer Datenbank verwendet werden.
Verbesserte Überwachung	Wählen Sie Erweiterte Überwachung aktivieren aus, um die Erfassung von Metriken in Echtzeit für das Betriebssystem zu aktivieren, in dem Ihr DB-Cluster ausgeführt wird. Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).
Überwachungsrolle	Nur verfügbar, wenn Enable Enhanced Monitoring (Erweiterte Überwachung aktivieren) festgelegt ist. Legen Sie die zu „Enhanced Monitoring“ (Erweiterten Überwachung) verwendete AWS Identity and Access Management -(IAM)-Rolle fest. Weitere Informati onen finden Sie unter Einrichten und Aktivieren von „Enhanced Monitoring“ (Erweiterte Überwachung).
Granularität	Nur verfügbar, wenn Enable Enhanced Monitoring (Erweiterte Überwachung aktivieren) festgelegt ist. Mit ihr können Sie die Zeitspanne zwischen den Erfassung en der Kennzahlen des DB-Clusters in Sekunden festlegen.

Option	Beschreibung
Kleinere Versions-Updates automatisch aktivieren	Klicken Sie auf Ja, wenn Sie möchten, dass Ihr Aurora PostgreSQL-DB-Cluster automatisch Upgrades für PostgreSQL-DB-Engine-Unterversionen erhält, sobald sie verfügbar werden. Die Option Auto Minor Version Upgrade (Upgrade einer Unterversion automatisch durchführen) gilt nur bei Upgrades für Engine-Unterversionen von PostgreSQL für Ihren Aurora PostgreSQL-DB-Cluster. Regelmäßige Patches zur Aufrechterhaltung der Systemstabilität sind davon nicht betroffen.
Wartungsfenster	Wählen Sie den wöchentlichen Zeitraum aus, in dem Systemwartungen durchgeführt werden können.

5. Wählen Sie Read Replica erstellen aus.

AWS CLI

Um mithilfe von eine Aurora-Read Replica aus einer RDS-Quell-DB-Instance für PostgreSQL zu erstellen, verwenden Sie zunächst den create-db-clusterCLI-Befehl AWS CLI, um einen leeren Aurora-DB-Cluster zu erstellen. Sobald der DB-Cluster existiert, verwenden Sie den Befehl create-db-instance, um die primäre Instance für Ihren DB-Cluster zu erstellen. Die primäre Instance ist die erste in einem Aurora-DB-Cluster erstellte Instance. In diesem Fall wird sie zunächst als Aurora-Lesereplikat Ihrer RDS-for-PostgreSQL-DB-Instance erstellt. Wenn der Prozess abgeschlossen wird, wurde Ihre RDS-for-PostgreSQL-DB-Instance effektiv zu einem Aurora-PostgreSQL-DB-Cluster migriert.

Sie müssen das Hauptbenutzerkonto (normalerweise `postgres`), sein Passwort oder den Datenbanknamen nicht angeben. Die Aurora-Read Replica bezieht diese automatisch von der Quell-RDS für PostgreSQL-DB-Instance, die Sie beim Aufrufen der Befehle identifizieren. AWS CLI

Sie müssen allerdings die Engine-Version angeben, die für den Aurora-PostgreSQL-DB-Cluster und die DB-Instance verwendet werden soll. Die von Ihnen angegebene Version sollte mit der Quell-DB-Instance von RDS for PostgreSQL übereinstimmen. Wenn die Quell-DB-Instance von RDS for PostgreSQL verschlüsselt ist, müssen Sie auch die Verschlüsselung für die primäre Instance des

Aurora-PostgreSQL-DB-Clusters angeben. Die Migration einer verschlüsselten Instance zu einem unverschlüsselten Aurora-DB-Cluster wird nicht unterstützt.

In den folgenden Beispielen wird ein Aurora-PostgreSQL-DB-Cluster mit dem Namen `my-new-aurora-cluster` erstellt, der eine unverschlüsselte RDS-DB-Quell-Instance verwenden soll. Sie erstellen zuerst den Aurora-PostgreSQL-DB-Cluster, indem Sie den CLI-Befehl `create-db-cluster` aufrufen. Das Beispiel zeigt, wie Sie den optionalen Parameter `--storage-encrypted` verwenden, um anzugeben, dass der DB-Cluster verschlüsselt werden soll. Da die Quell-DB nicht verschlüsselt ist, wird `--kms-key-id` verwendet, um den zu verwendenden Schlüssel anzugeben. Weitere Informationen zu den erforderlichen und optionalen Parametern finden Sie in der Liste, die auf das Beispiel folgt.

Für, oder: Linux macOS Unix

```
aws rds create-db-cluster  \
    --db-cluster-identifier my-new-aurora-cluster \
    --db-subnet-group-name my-db-subnet
    --vpc-security-group-ids sg-11111111
    --engine aurora-postgresql \
    --engine-version same-as-your-rds-instance-version \
    --replication-source-identifier arn:aws:rds:aws-region:111122223333:db/rpg-source-
db \
    --storage-encrypted \
    --kms-key-id arn:aws:kms:aws-
region:111122223333:key/11111111-2222-3333-444444444444
```

Windows:

```
aws rds create-db-cluster  ^
    --db-cluster-identifier my-new-aurora-cluster ^
    --db-subnet-group-name my-db-subnet ^
    --vpc-security-group-ids sg-11111111 ^
    --engine aurora-postgresql ^
    --engine-version same-as-your-rds-instance-version ^
    --replication-source-identifier arn:aws:rds:aws-region:111122223333:db/rpg-source-
db ^
    --storage-encrypted ^
    --kms-key-id arn:aws:kms:aws-
region:111122223333:key/11111111-2222-3333-444444444444
```

In der folgenden Liste finden Sie weitere Informationen zu einigen der im Beispiel gezeigten Optionen. Sofern nicht anders angegeben, sind diese Parameter erforderlich.

- `--db-cluster-identifier` – Sie müssen Ihrem neuen Aurora-PostgreSQL-DB-Cluster einen Namen geben.
- `--db-subnet-group-name` – Erstellen Sie Ihren Aurora-PostgreSQL-DB-Cluster im selben DB-Subnetz wie die DB-Quell-Instance.
- `--vpc-security-group-ids` – Legen Sie die Sicherheitsgruppe für Ihren Aurora-PostgreSQL-DB-Cluster fest.
- `--engine-version` – Legen Sie die Version fest, die Sie für den Aurora-PostgreSQL-DB-Cluster verwenden möchten. Dies sollte die gleiche sein wie die Version, die von Ihrer Quell-DB-Instance von RDS for PostgreSQL verwendet wird.
- `--replication-source-identifier` – Identifizieren Sie Ihre RDS-for-PostgreSQL-DB-Instance über den Amazon-Ressourcennamen (ARN). Weitere Informationen zu Amazon-RDS-ARNs finden Sie unter Amazon Relational Database Service (Amazon RDS) in der Allgemeine AWS-Referenz Ihres DB-Clusters.
- `--storage-encrypted` Optional. Verwenden Sie diese Option, wenn die Verschlüsselung wie folgt angegeben werden muss:
  - Verwenden Sie diesen Parameter, wenn die Quell-DB-Instance über verschlüsselten Speicher verfügt. Der Aufruf von `create-db-cluster` schlägt fehl, wenn Sie diesen Parameter nicht mit einer Quell-DB-Instance verwenden, die über verschlüsselten Speicher verfügt. Wenn Sie einen anderen Schlüssel für den Aurora-PostgreSQL-DB-Cluster verwenden möchten als den von der Quell-DB-Instance verwendeten Schlüssel, müssen Sie auch die `--kms-key-id` angeben.
  - Verwenden Sie diese Option, wenn der Speicher der Quell-DB-Instance unverschlüsselt ist, der Aurora-PostgreSQL-DB-Cluster jedoch die Verschlüsselung verwenden soll. In diesem Fall müssen Sie auch den Verschlüsselungsschlüssel identifizieren, der mit dem `--kms-key-id`-Parameter verwendet werden soll.
- `--kms-key-id` Optional. Wenn Sie diese Option verwenden, können Sie den Schlüssel angeben, der für die Speicherverschlüsselung (`--storage-encrypted`) verwendet werden soll, indem Sie den ARN, die ID, den Alias-ARN oder den Aliasnamen des Schlüssels angeben. Dieser Parameter wird nur für die folgenden Situationen benötigt:
  - Wenn Sie einen anderen Schlüssel für den Aurora-PostgreSQL-DB-Cluster auswählen möchten als den, der von der Quell-DB-Instance verwendet wird.

- Wenn Sie einen verschlüsselten Cluster aus einer unverschlüsselten Quelle erstellen möchten. In diesem Fall müssen Sie den Schlüssel angeben, den Aurora PostgreSQL für die Verschlüsselung verwenden soll.

Nachdem Sie den Aurora-PostgreSQL-DB-Cluster erstellt haben, erstellen Sie die primäre Instance mithilfe des CLI-Befehls `create-db-instance`, wie im Folgenden gezeigt:

Für LinuxmacOS, oderUnix:

```
aws rds create-db-instance \
    --db-cluster-identifier my-new-aurora-cluster \
    --db-instance-class db.x2g.16xlarge \
    --db-instance-identifier rpg-for-migration \
    --engine aurora-postgresql
```

Windows:

```
aws rds create-db-instance ^
    --db-cluster-identifier my-new-aurora-cluster ^
    --db-instance-class db.x2g.16xlarge ^
    --db-instance-identifier rpg-for-migration ^
    --engine aurora-postgresql
```

In der folgenden Liste finden Sie weitere Informationen zu einigen der im Beispiel gezeigten Optionen.

- `--db-cluster-identifier` – Der Name des neuen Aurora-PostgreSQL-DB-Clusters, den Sie im vorherigen Schritt mit dem Befehl `create-db-instance` erstellt haben.
- `--db-instance-class` – Der Name der DB-Instance-Klasse, die für Ihre primäre Instance verwendet werden soll, z. B. `db.r4.xlarge`, `db.t4g.medium`, `db.x2g.16xlarge` usw. Eine Liste der verfügbaren DB-Instance-Klassen finden Sie unter DB-Instance-Klassenarten.
- `--db-instance-identifier` – Geben Sie den Namen an, den Ihre primäre Instance erhalten soll.
- `--engine aurora-postgresql` – Geben Sie `aurora-postgresql` für die Engine an.

RDS-API

Wenn Sie ein Aurora-Lesereplikat aus einer Quell-DB-Instance von RDS for PostgreSQL erstellen möchten, verwenden Sie zuerst die RDS-API-Operation `CreateDBCluster`, um einen neuen Aurora-DB-Cluster für das Aurora-Lesereplikat zu erstellen, das aus Ihrer RDS-for-PostgreSQL-Quell-DB-Instance erstellt wird. Wenn der Aurora-PostgreSQL-DB-Cluster verfügbar ist, verwenden Sie `CreateDBInstance`, um die primäre Instance für den Aurora-DB-Cluster zu erstellen.

Sie müssen das Hauptbenutzerkonto (normalerweise `postgres`), sein Passwort oder den Datenbanknamen nicht angeben. Das Aurora-Lesereplikat bezieht diese Angaben automatisch aus der RDS-for-PostgreSQL-Quell-DB-Instance, die in `ReplicationSourceIdentifier` angegeben ist.

Sie müssen allerdings die Engine-Version angeben, die für den Aurora-PostgreSQL-DB-Cluster und die DB-Instance verwendet werden soll. Die von Ihnen angegebene Version sollte mit der Quell-DB-Instance von RDS for PostgreSQL übereinstimmen. Wenn die Quell-DB-Instance von RDS for PostgreSQL verschlüsselt ist, müssen Sie auch die Verschlüsselung für die primäre Instance des Aurora-PostgreSQL-DB-Clusters angeben. Die Migration einer verschlüsselten Instance zu einem unverschlüsselten Aurora-DB-Cluster wird nicht unterstützt.

Wenn Sie den Aurora-DB-Cluster für das Aurora-Lesereplikat erstellen möchten, verwenden Sie die RDS-API-Operation `CreateDBCluster` mit folgenden Parametern:

- `DBClusterIdentifier` – Der Name des zu erstellenden DB-Clusters.
- `DBSubnetGroupName` – Der Name der DB-Subnetzgruppe, die mit diesem DB-Cluster verknüpft werden soll.
- `Engine=aurora-postgresql` – Der Name der zu verwendenden Engine.
- `ReplicationSourceIdentifier` – Der Amazon Resource Name (ARN) für die PostgreSQL-Quell-DB-Instance. Weitere Informationen zu Amazon-RDS-ARNs finden Sie unter Amazon Relational Database Service (Amazon RDS) in der Allgemeine Amazon Web Services-Referenz. Wenn `ReplicationSourceIdentifier` eine verschlüsselte Quelle identifiziert, verwendet Amazon RDS Ihren Standard-KMS-Schlüssel, es sei denn, Sie geben mit der Option `KmsKeyId` einen anderen Schlüssel an.
- `VpcSecurityGroupIds` – Eine Liste der Amazon-EC2-VPC-Sicherheitsgruppen, die mit diesem DB-Cluster verknüpft werden sollen.
- `StorageEncrypted` – Gibt an, ob der DB-Cluster verschlüsselt ist. Wenn Sie diesen Parameter verwenden, ohne auch die `ReplicationSourceIdentifier` anzugeben, verwendet Amazon RDS Ihren KMS-Standardschlüssel.

- `KmsKeyId` – Der Schlüssel für einen verschlüsselten Cluster. Wenn Sie diese Option verwenden, können Sie den Schlüssel angeben, der für die Speicherverschlüsselung verwendet werden soll, indem Sie den ARN, die ID, den Alias-ARN oder den Aliasnamen des Schlüssels angeben.

Weitere Informationen finden Sie unter `CreateDBCluster` in der Amazon-RDS-API-Referenz.

Sobald der Aurora-DB-Cluster verfügbar ist, können Sie eine primäre Instance dafür erstellen, indem Sie die RDS-API-Operation `CreateDBInstance` mit folgenden Parametern verwenden:

- `DBClusterIdentifier` – Der Name Ihres DB-Clusters.
- `DBInstanceClass` – Der Name der DB-Instance-Klasse, die für Ihre primäre Instance verwendet werden soll.
- `DBInstanceIdentifier` – Der Name Ihrer primären Instance.
- `Engine=aurora-postgresql` – Der Name der zu verwendenden Engine.

Weitere Informationen finden Sie unter `CreateDBInstance` in der Amazon-RDS-API-Referenz.

Hochstufen einer Aurora Read Replica

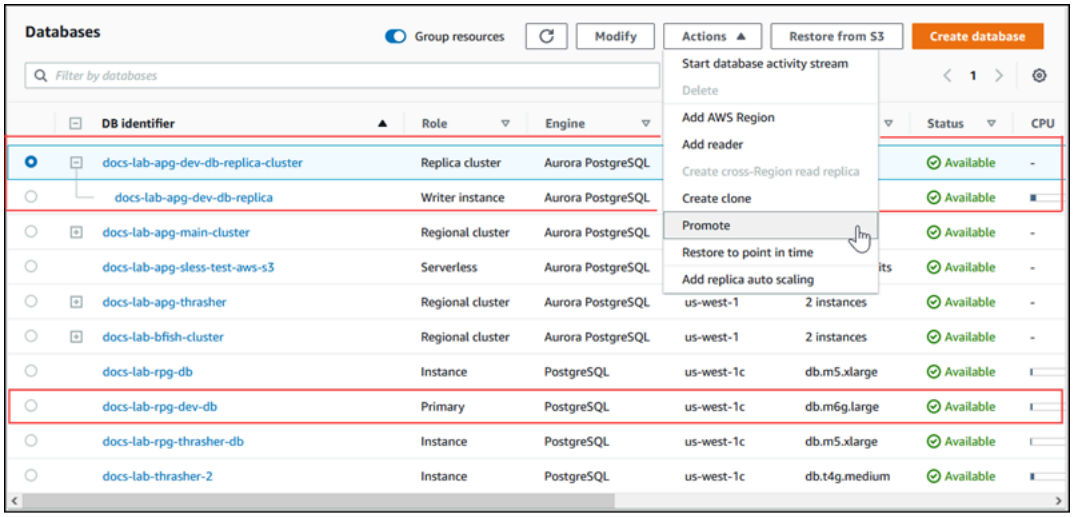
Die Migration zu Aurora PostgreSQL ist erst abgeschlossen, wenn Sie den Replikat-Cluster hochgestuft haben. Löschen Sie also die RDS-for-PostgreSQL-Quell-DB-Instance noch nicht.

Stellen Sie vor dem Hochladen des Replikat-Clusters sicher, dass die RDS-for-PostgreSQL-DB-Instance keine prozessinternen Transaktionen oder andere Aktivitäten enthält, die in die Datenbank schreiben. Wenn die Replikatverzögerung auf dem Aurora-Lesereplikat Null (0) erreicht, können Sie den Replikatcluster heraufstufen. Weitere Informationen zum Überwachen der Replikatverzögerung finden Sie unter Überwachung einer Aurora PostgreSQL-Replikation und Metriken auf Instance-Ebene für Amazon Aurora.

Konsole

So stufen Sie eine Aurora-Read Replica zu einem Aurora-DB-Cluster hoch:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den Replikatcluster aus.



4. Wählen Sie für Actions (Aktionen)Promote (Hochstufen) aus. Dies kann einige Minuten dauern und zu Ausfallzeiten führen.

Wenn der Prozess abgeschlossen ist, ist der Aurora-Replikatcluster ein regionaler Aurora-PostgreSQL-DB-Cluster mit einer Writer-Instance, die die Daten aus der RDS-for-PostgreSQL-DB-Instance enthält.

AWS CLI

Verwenden Sie den Befehl, um eine Aurora-Read Replica zu einem eigenständigen DB-Cluster hochzustufen. promote-read-replica-db-cluster AWS CLI

Example

FürLinux, odermacOS: Unix

```
aws rds promote-read-replica-db-cluster \
    --db-cluster-identifier myreadreplicacluster
```

Windows:

```
aws rds promote-read-replica-db-cluster ^
    --db-cluster-identifier myreadreplicacluster
```

RDS-API

Verwenden Sie den RDS-API-Vorgang PromoteReadReplica dbCluster, um eine Aurora-Read Replica zu einem eigenständigen DB-Cluster hochzustufen.

Nachdem Sie den Replikatcluster hochgestuft haben, können Sie bestätigen, dass das Hochstufen abgeschlossen wurde, indem Sie das Ereignisprotokoll wie folgt überprüfen.

Um zu bestätigen, dass das Aurora-Replikatcluster hochgestuft wurde

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Auf der Seite Events (Ereignisse) finden Sie den Namen Ihres Clusters in der Liste Source (Quelle). Jedes Ereignis hat eine Quelle, einen Typ, eine Uhrzeit und eine Nachricht. Sie können alle Ereignisse sehen, die in Ihrem AWS-Region für Ihr Konto aufgetreten sind. Ein erfolgreiches Hochstufen generiert die folgende Nachricht.

   ```
   Promoted Read Replica cluster to a stand-alone database cluster.
   ```

Nach Abschluss der Hochstufung wird die Verknüpfung zwischen der Quell-RDS-for-PostgreSQL-DB-Instance und dem Aurora-PostgreSQL-DB-Cluster aufgehoben. Sie können Ihre Clientanwendungen für den Zugriff auf den Endpunkt des Aurora-Lesereplikats konfigurieren. Weitere Informationen zu den Aurora-Endpunkten finden Sie unter Amazon Aurora-Verbindungsverwaltung. Nun können Sie die DB-Instance bei Bedarf sicher löschen.

Verbesserung der Abfrageleistung für Aurora PostgreSQL mit Aurora-optimierten Lesevorgängen

Mit Aurora-optimierten Lesevorgängen können Sie eine schnellere Abfrageverarbeitung mit Aurora PostgreSQL erreichen. Eine Aurora-PostgreSQL-DB-Instance, die Aurora-optimierte Lesevorgänge verwendet, bietet eine bis zu achtmal verbesserte Abfragelatenz und bis zu 30 % Kosteneinsparungen für Anwendungen mit großen Datensätzen, die die Speicherkapazität einer DB-Instance überschreiten.

Themen

- Übersicht über Aurora-optimierte Lesevorgänge in PostgreSQL
- Verwenden von Aurora-optimierten Lesevorgängen
- Anwendungsfälle für Aurora-optimierte Lesevorgänge
- Überwachen von DB-Instances, die Aurora-optimierte Lesevorgänge verwenden

- Bewährte Methoden für Aurora-optimierte Lesevorgänge

Übersicht über Aurora-optimierte Lesevorgänge in PostgreSQL

Aurora-optimierte Lesevorgänge sind standardmäßig verfügbar, wenn Sie einen DB-Cluster erstellen, der Graviton-basierte R6GD- und Intel-basierte R6ID-Instances mit NVMe-Speicher (Non-Volatile Memory Express) verwendet. Dies ist in den folgenden Versionen von PostgreSQL verfügbar:

- 16.1 und alle höheren Versionen
- 15.4 und höhere Versionen
- 14.9 und höhere Versionen

Aurora-optimierte Lesevorgänge unterstützen zwei Funktionen: mehrstufigen Cache und temporäre Objekte.

Mehrstufiger Cache mit optimierten Lesevorgängen – Mithilfe eines mehrstufigen Caches können Sie die Caching-Kapazität Ihrer DB-Instance um das bis zu Fünffache des Instance-Speichers erweitern. Dadurch wird der Cache automatisch so verwaltet, dass er die aktuellsten, transaktionskonsistenten Daten enthält. Dadurch entfällt für Anwendungen der Aufwand, die Datenaktualität externer, auf Ergebnismengen basierender Caching-Lösungen zu verwalten. Dies bietet eine bis zu achtmal bessere Latenz für Abfragen, bei denen zuvor Daten aus dem Aurora-Speicher abgerufen wurden.

In Aurora ist der Wert für `shared_buffers` in der Standardparametergruppe normalerweise auf etwa 75% des verfügbaren Speichers festgelegt. Für die Instance-Typen r6gd und r6id reduziert Aurora den `shared_buffers` Speicherplatz jedoch um 4,5%, um die Metadaten für den Optimized Reads-Cache zu hosten.

Temporäre Objekte mit optimierten Lesevorgängen – Mit temporären Objekten können Sie eine schnellere Abfrageverarbeitung erreichen, indem Sie die von PostgreSQL generierten temporären Dateien im lokalen NVMe-Speicher ablegen. Dadurch wird der Datenverkehr zu Elastic Block Storage (EBS) über das Netzwerk reduziert. Es bietet eine bis zu zweimal bessere Latenz und einen besseren Durchsatz für erweiterte Abfragen, bei denen große Datenmengen sortiert, zusammengeführt oder zusammengeführt werden, die nicht in die auf einer DB-Instance verfügbare Speicherkapazität passen.

In einem E/A-optimierten Aurora-Cluster verwenden optimierte Lesevorgänge sowohl Tiered Cache als auch temporäre Objekte auf NVMe-Speicher. Mit der für optimierte Lesevorgänge

aktivierten mehrstufigen Cache-Funktion weist Aurora den doppelten Instance-Speicher für temporäre Objekte zu, etwa 10 % des Speichers für interne Operationen und den verbleibenden Speicher als mehrstufigen Cache. In einem Aurora-Standard-Cluster verwenden optimierte Lesevorgänge nur temporäre Objekte.

Engine	Cluster-Speicherkonfiguration	Temporäre Objekte mit optimierten Lesevorgängen	Optimierter mehrstufiger Cache mit optimierten Lesevorgängen	Unterstützte Versionen
Aurora PostgreSQL-Compatible Edition	Standard	Ja	Nein	Aurora PostgreSQL Version 16.1 und alle höheren Versionen, 15.4 und höher, Version 14.9 und höher
	I/O-optimiert	Ja	Ja	

> **Note**
>
> Ein Wechsel zwischen E/A-optimierten Clustern und Standard-Clustern auf einer NVMe-basierten DB-Instance-Klasse führt zu einem sofortigen Neustart der Datenbank-Engine.

Verwenden Sie in Aurora PostgreSQL den `temp_tablespaces` Parameter, um den Tablespace zu konfigurieren, in dem die temporären Objekte gespeichert werden.

Verwenden Sie den folgenden Befehl, um zu überprüfen, ob die temporären Objekte konfiguriert sind:

```
postgres=> show temp_tablespaces;
temp_tablespaces
---------------------
aurora_temp_tablespace
(1 row)
```

Der `aurora_temp_tablespace` ist ein von Aurora konfigurierter Tabellenbereich, der auf den lokalen NVMe-Speicher verweist. Sie können diesen Parameter nicht ändern oder zum Amazon-EBS-Speicher zurückkehren.

Verwenden Sie den folgenden Befehl, um zu überprüfen, ob der Cache der optimierten Lesevorgänge aktiviert ist:

```
postgres=> show shared_preload_libraries;
                shared_preload_libraries
-----------------------------------------------------------
rdsutils,pg_stat_statements,aurora_optimized_reads_cache
```

Verwenden von Aurora-optimierten Lesevorgängen

Wenn Sie eine Aurora PostgreSQL-DB-Instance mit einer der NVMe-basierten DB-Instances bereitstellen, verwendet die DB-Instance automatisch Aurora Optimized Reads.

Führen Sie einen der folgenden Schritte aus, um Aurora-optimierte Lesevorgänge zu aktivieren:

- Erstellen Sie einen Aurora-PostgreSQL-DB-Cluster mit einer der NVMe-basierten DB-Instance-Klassen. Weitere Informationen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.
- Ändern Sie eine vorhandene Aurora-PostgreSQL-DB-Instance so, dass eine der NVMe-basierten DB-Instance-Klassen verwendet wird. Weitere Informationen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Aurora Optimized Reads ist überall verfügbar AWS-Regionen , wo eine oder mehrere DB-Instance-Klassen mit lokalem NVMe-SSD-Speicher unterstützt werden. Weitere Informationen finden Sie unter Aurora DB-Instance-Klassen.

Um zurück zu einer Aurora-Instance mit nicht optimierten Lesevorgängen zu wechseln, ändern Sie die DB-Instance-Klasse Ihrer Aurora-Instance auf die ähnliche Instance-Klasse ohne kurzlebigen NVMe-Speicher für Ihre Datenbank-Workloads. Wenn die aktuelle DB-Instance-Klasse beispielsweise db.r6gd.4xlarge ist, wählen Sie db.r6g.4xlarge aus, um zurückzuwechseln. Weitere Informationen finden Sie unter Ändern einer Amazon-DB-Instance.

Anwendungsfälle für Aurora-optimierte Lesevorgänge

Optimierter mehrstufiger Cache mit optimierten Lesevorgängen

Im Folgenden sind einige Anwendungsfälle aufgeführt, für die optimierte Lesevorgänge mit gestuftem Cache von Vorteil sein können:

- Internetanwendungen wie Zahlungsabwicklung, Rechnungsstellung und E-Commerce mit strengen Leistungs-SLAs.
- Echtzeit-Dashboards für Berichte, die Hunderte von Punktabfragen zur Erfassung von Metriken und Daten ausführen.
- Generative KI-Anwendungen mit der Erweiterung pgvector zur Suche nach exakten oder nächstgelegenen Nachbarn in Millionen von Vektoreinbettungen.

Temporäre Objekte mit optimierten Lesevorgängen

Im Folgenden sind einige Anwendungsfälle aufgeführt, für die optimierte Lesevorgänge von Vorteil sein können:

- Analytische Abfragen mit Common Table Expressions (CTEs), abgeleiteten Tabellen und Gruppierungsoperationen.
- Lesereplikate, die die nicht optimierten Abfragen für eine Anwendung verarbeiten.
- Bedarfsgesteuerte oder dynamische Berichtsabfragen mit komplexen Operationen wie GROUP BY und ORDER BY, für die nicht immer die entsprechenden Indizes verwendet werden können.
- `CREATE INDEX`oder Operationen zum Sortieren. `REINDEX`
- Andere Workloads, die interne temporäre Tabellen verwenden.

Überwachen von DB-Instances, die Aurora-optimierte Lesevorgänge verwenden

Sie können Ihre Abfragen, die den mehrstufigen Cache mit optimierten Lesevorgängen zum Aktivieren von Lesevorgängen verwenden, wie im folgenden Beispiel dargestellt mit dem Befehl EXPLAIN überwachen:

```
Postgres=> EXPLAIN (ANALYZE, BUFFERS) SELECT c FROM sbtest15 WHERE id=100000000


QUERY PLAN
------------------------------------------------------------------------------------------
 Index Scan using sbtest15_pkey on sbtest15  (cost=0.57..8.59 rows=1 width=121) (actual
 time=0.287..0.288 rows=1 loops=1)
```

```
   Index Cond: (id = 100000000)
   Buffers: shared hit=3 read=2 aurora_orcache_hit=2
   I/O Timings: shared/local read=0.264
 Planning:
   Buffers: shared hit=33 read=6 aurora_orcache_hit=6
   I/O Timings: shared/local read=0.607
 Planning Time: 0.929 ms
 Execution Time: 0.303 ms
(9 rows)
Time: 2.028 ms
```

> **Note**
>
> `aurora_orcache_hit`und `aurora_storage_read` Felder im `Buffers` Abschnitt des Erläuterungsplans werden nur angezeigt, wenn Optimierte Lesevorgänge aktiviert sind und ihre Werte größer als Null sind. Das gelesene Feld ist die Summe der `aurora_storage_read` Felder `aurora_orcache_hit` und.

Sie können DB-Instances, die Aurora Optimized Reads verwenden, anhand der folgenden CloudWatch Metriken überwachen:

- `AuroraOptimizedReadsCacheHitRatio`
- `FreeEphemeralStorage`
- `ReadIOPSEphemeralStorage`
- `ReadLatencyEphemeralStorage`
- `ReadThroughputEphemeralStorage`
- `WriteIOPSEphemeralStorage`
- `WriteLatencyEphemeralStorage`
- `WriteThroughputEphemeralStorage`

Diese Metriken liefern Daten über den verfügbaren Instance-Speicher, die IOPS und den Durchsatz. Weitere Informationen zu diesen Metriken finden Sie unter Metriken auf Instance-Ebene für Amazon Aurora.

Sie können die pg_proctab-Erweiterung auch zum Überwachen des NVMe-Speichers verwenden.

```
postgres=>select * from pg_diskusage();

major | minor |       devname       | reads_completed | reads_merged | sectors_read |
 readtime | writes_completed | writes_merged | sectors_written | writetime | current_io
 | iotime  | totaliotime
------+-------+---------------------+-----------------+--------------+--------------
+----------+------------------+---------------+-----------------+-----------
+------------+---------+-------------
      |       | rdstemp             |           23264 |            0 |       191450 |
  11670 |         1750892 |             0 |        24540576 |    819350 |          0 |
 3847580 |      831020
      |       | rdsephemeralstorage |           23271 |            0 |       193098 |
   2620 |           114961 |             0 |        13845120 |    130770 |          0 |
  215010 |      133410
(2 rows)
```

Bewährte Methoden für Aurora-optimierte Lesevorgänge

Nutzen Sie die folgenden bewährten Methoden für Aurora-optimierte Lesevorgänge:

- Überwachen Sie den im Instance-Speicher verfügbaren Speicherplatz anhand der CloudWatch Metrik`FreeEphemeralStorage`. Wenn der Instance-Speicher aufgrund der Arbeitslast auf der DB-Instance sein Limit erreicht, optimieren Sie die Parallelität und die Abfragen, die stark temporäre Objekte verwenden, oder ändern Sie ihn so, dass er eine größere DB-Instance-Klasse verwendet.
- Überwachen Sie die CloudWatch Metrik für die Trefferquote im Cache für optimierte Lesevorgänge. Operationen wie VACUUM ändern sehr schnell eine große Anzahl von Blöcken. Dies kann zu einem vorübergehenden Rückgang der Trefferrate führen. Die `pg_prewarm`-Erweiterung kann verwendet werden, um Daten in den Puffer-Cache zu laden, so dass Aurora einige dieser Blöcke proaktiv in den Cache der optimierten Lesevorgänge schreiben kann.
- Sie können das Cluster-Cache-Management (CCM) aktivieren, um den Puffer-Cache und den mehrstufigen Cache auf einem Tier-0-Reader aufzuwärmen, der als Failover-Ziel verwendet wird. Wenn CCM aktiviert ist, wird der Puffer-Cache regelmäßig gescannt, um Seiten, die bereinigt werden können, in den mehrstufigen Cache zu schreiben. Weitere Informationen zu CCM finden Sie unter Schnelle Wiederherstellung nach Failover mit der Cluster-Cacheverwaltung für Aurora PostgreSQL.

Verwenden von Babelfish for Aurora PostgreSQL

Babelfish for Aurora PostgreSQL erweitert Ihren DB-Cluster von Aurora PostgreSQL um die Möglichkeit, Datenbankverbindungen von SQL-Server-Clients zu akzeptieren. Mit Babelfish können Anwendungen, die ursprünglich für SQL Server entwickelt wurden, direkt mit Aurora PostgreSQL mit wenigen Codeänderungen im Vergleich zu einer herkömmlichen Migration und ohne Änderung der Datenbanktreiber arbeiten. Weitere Informationen zur Migration von in eine VPC finden Sie unter Migrieren einer SQL-Server-Datenbank zu Babelfish for Aurora PostgreSQL.

Babelfish bietet einen zusätzlichen Endpunkt für einen Aurora-PostgreSQL-Datenbankcluster, der es erlaubt, das SQL-Server-Wire-Level-Protokoll und häufig verwendete SQL-Server-Anweisungen zu verstehen. Clientanwendungen, die das Wire-Protokoll Tabular Data Stream (TDS) verwenden, können sich nativ mit dem TDS-Listener-Port von Aurora PostgreSQL verbinden. Weitere Informationen zu TDS finden Sie unter [MS-TDS]: Tabellarisches Datenstromprotokoll auf der Microsoft-Website.

> **Note**
>
> Babelfish for Aurora PostgreSQL unterstützt TDS-Versionen 7.1 bis 7.4.

Babelfish bietet auch Zugriff auf Daten über die PostgreSQL-Verbindung. Standardmäßig sind beide von Babelfish unterstützten SQL-Dialekte über ihre nativen Wire-Protokolle an den folgenden Ports verfügbar:

- Der SQL-Server-Dialekt (T-SQL), Clients stellen eine Verbindung mit Port 1433 her.
- PostgreSQL-Dialekt (PL/pgSQL), Clients stellen eine Verbindung mit Port 5432 her.

Babelfish führt die Transact-SQL-Sprache (T-SQL) mit einigen Unterschieden aus. Weitere Informationen finden Sie unter Unterschiede zwischen Babelfish für Aurora PostgreSQL und SQL Server.

In den folgenden Abschnitten finden Sie Informationen zum Einrichten und Verwenden eines DB-Clusters von Babelfish for Aurora PostgreSQL.

Themen

- Babelfish-Einschränkungen
- Grundlagen der Babelfish-Architektur und -Konfiguration

- Erstellen eines DB-Clusters von Babelfish for Aurora PostgreSQL
- Migrieren einer SQL-Server-Datenbank zu Babelfish for Aurora PostgreSQL
- Datenbankauthentifizierung mit Babelfish für Aurora PostgreSQL
- Verbinden mit einem Babelfish-DB-Cluster
- Arbeiten mit Babelfish
- Fehlerbehebung bei Babelfish
- Deaktivieren von Babelfish
- Babelfish-Versions-Updates
- Referenz für Babelfish for Aurora PostgreSQL

Babelfish-Einschränkungen

Bei Babelfish für Aurora PostgreSQL gelten aktuell die folgenden Einschränkungen:

- Derzeit werden folgende Aurora-Funktionen von Babelfish nicht unterstützt:
  - Blau/Grün-Bereitstellungen von Amazon RDS
  - AWS Identity and Access Management
  - Datenbank-Aktivitätsstreams (DAS)
  - Logische Replikation in PostgreSQL
  - RDS-Daten-API mit Aurora PostgreSQL Serverless v2 und bereitgestellt
  - RDS-Proxy mit RDS für SQL Server
  - SCRAM (Salted Challenge Response Authentication Mechanism)
  - Abfrage-Editor
- Babelfish unterstützt derzeit keine Kerberos-basierte Authentifizierung für Active-Directory-Gruppen.
- Babelfish bietet keine Unterstützung für die folgenden Anforderungen der Client-Treiber-API:
  - API-Anforderungen mit den Verbindungsattributen im Zusammenhang mit Microsoft Distributed Transaction Coordinator (MSDTC) werden nicht unterstützt. Dazu gehören XA-Aufrufe der SQLServerXAResource-Klasse im JDBC-Treiber des SQL-Servers.
  - Babelfish unterstützt Verbindungspooling mit Treibern, die die neuesten Versionen des TDS-Protokolls verwenden. Bei älteren Treibern werden API-Anforderungen mit den Verbindungsattributen und Methoden im Zusammenhang mit dem Verbindungspooling nicht unterstützt.
- Babelfish unterstützt derzeit die folgenden Aurora-PostgreSQL-Erweiterungen nicht:
  - `bloom`
  - `btree_gin`
  - `btree_gist`
  - `citext`
  - `cube`
  - `hstore`
  - `hypopg`
  - Logische Replikation mithilfe von `pglogical`

  - `ltree`
  - `pgcrypto`
  - Abfrageplanverwaltung mit `apg_plan_mgmt`

  Weitere Informationen zu PostgreSQL-Erweiterungen finden Sie unter Arbeiten mit Erweiterungen und Fremddaten-Wrappern.
- Der Open-Source-JTDS-Treiber, der als Alternative zum JDBC-Treiber von Microsoft konzipiert wurde, wird nicht unterstützt.

Grundlagen der Babelfish-Architektur und -Konfiguration

Sie verwalten den DB-Cluster der mit Aurora PostgreSQL kompatiblen Edition, auf dem Babelfish ausgeführt wird, genau wie jeden anderen Aurora-DB-Cluster. Sie profitieren also von der Skalierbarkeit, der hohen Verfügbarkeit mit Failover-Unterstützung und der integrierten Replikation, die von einem Aurora-DB-Cluster bereitgestellt wird. Weitere Informationen zu diesen Funktionen finden Sie unter Verwalten von Performance und Skalierung für einen Aurora-DB-Cluster, Hohe Verfügbarkeit für Amazon Aurora und Replikation mit Amazon Aurora. Sie haben auch Zugriff auf viele andere AWS Tools und Dienstprogramme, darunter die folgenden:

- Amazon CloudWatch ist ein Überwachungs- und Beobachtbarkeitsservice, der Ihnen Daten und umsetzbare Erkenntnisse liefert. Weitere Informationen finden Sie unter Überwachen von Amazon Aurora-Metriken mit Amazon CloudWatch.
- Performance Insights ist eine Funktion zur Optimierung und Überwachung der Datenbank-Performance, mit der Sie die Belastung Ihrer Datenbank schnell beurteilen können. Weitere Informationen hierzu finden Sie unter Überwachung mit Performance Insights auf .
- Die globalen Aurora-Datenbanken umfassen mehrere AWS-Regionen, ermöglichen globale Lesevorgänge mit geringer Latenz und ermöglichen eine schnelle Wiederherstellung nach dem seltenen Ausfall, der sich auf ein gesamtes AWS-Region System auswirken kann. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Global Databases.
- Automatisches Software-Patching sorgt dafür, dass Ihre Datenbank stets up-to-date über die neuesten Sicherheits- und Funktionspatches verfügt, sobald diese verfügbar sind.
- Amazon-RDS-Ereignisse informieren Sie per E-Mail oder SMS-Nachricht über wichtige Datenbankereignisse wie ein automatisiertes Failover. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora-Ereignissen.

Im Folgenden erfahren Sie mehr über die Babelfish-Architektur und wie die von Ihnen migrierten SQL-Server-Datenbanken von Babelfish behandelt werden. Wenn Sie Ihren Babelfish-DB-Cluster erstellen, müssen Sie vorab einige Entscheidungen im Hinblick auf eine oder mehrere Datenbanken, Sortierungen und andere Details treffen.

Themen

Babelfish-Architektur

Wenn Sie einen Aurora-PostgreSQL-Cluster erstellen, bei dem Babelfish aktiviert ist, stellt Aurora den Cluster mit einer PostgreSQL-Datenbank namens `babelfish_db` bereit. In dieser Datenbank befinden sich alle migrierten SQL Server-Objekte und Strukturen.

> **Note**
>
> In einem Aurora-PostgreSQL-Cluster ist der Datenbankname `babelfish_db` für Babelfish reserviert. Wenn Sie eine eigene „babelfish_db“-Datenbank auf einem Babelfish-DB-Cluster erstellen, wird verhindert, dass Aurora Babelfish erfolgreich bereitstellt.

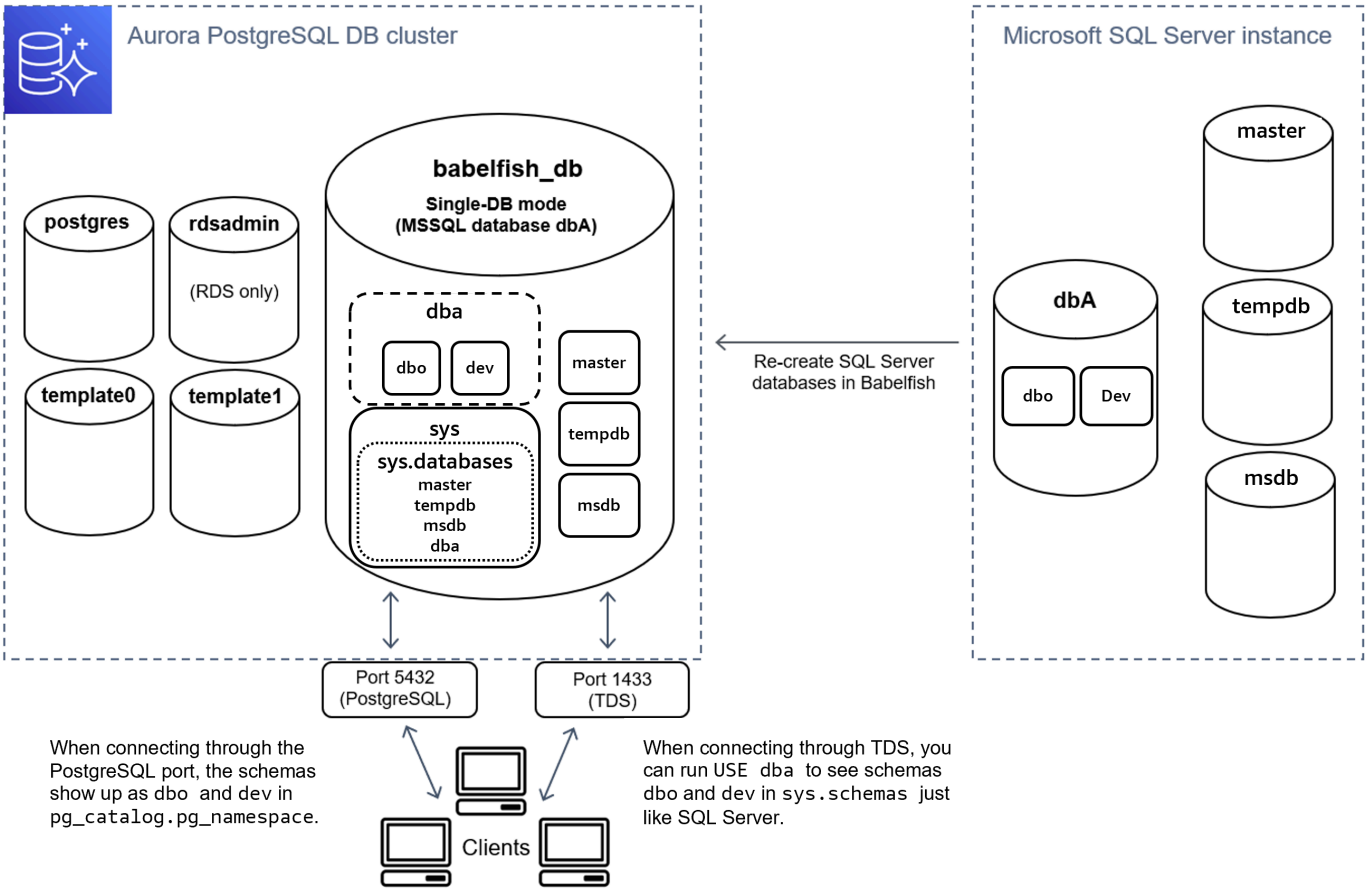
Wenn Sie eine Verbindung zum TDS-Port herstellen, wird die Sitzung in der `babelfish_db`-Datenbank. Von T-SQL sieht die Struktur ähnlich aus wie eine Verbindung mit einer SQL Server-Instanz. Die `master`-, `msdb`- und `tempdb`-Datenbanken und der `sys.databases`-Katalog sind zu sehen. Sie können zusätzliche Benutzerdatenbanken erstellen und mit der USE-Anweisung zwischen Datenbanken wechseln. Wenn Sie eine SQL Server-Benutzerdatenbank erstellen, wird sie in die `babelfish_db` PostgreSQL-Datenbank eingebracht. Ihre Datenbank behält datenbankübergreifende Syntax und Semantik bei, die denen von SQL Server entsprechen oder ähnlich sind.

Verwenden von Babelfish mit einer einzigen Datenbank oder mehreren Datenbanken

Wenn Sie einen Aurora-PostgreSQL-Cluster erstellen, der mit Babelfish verwendet werden soll, wählen Sie zwischen der Verwendung einer einzelnen SQL Server-Datenbank für sich selbst oder

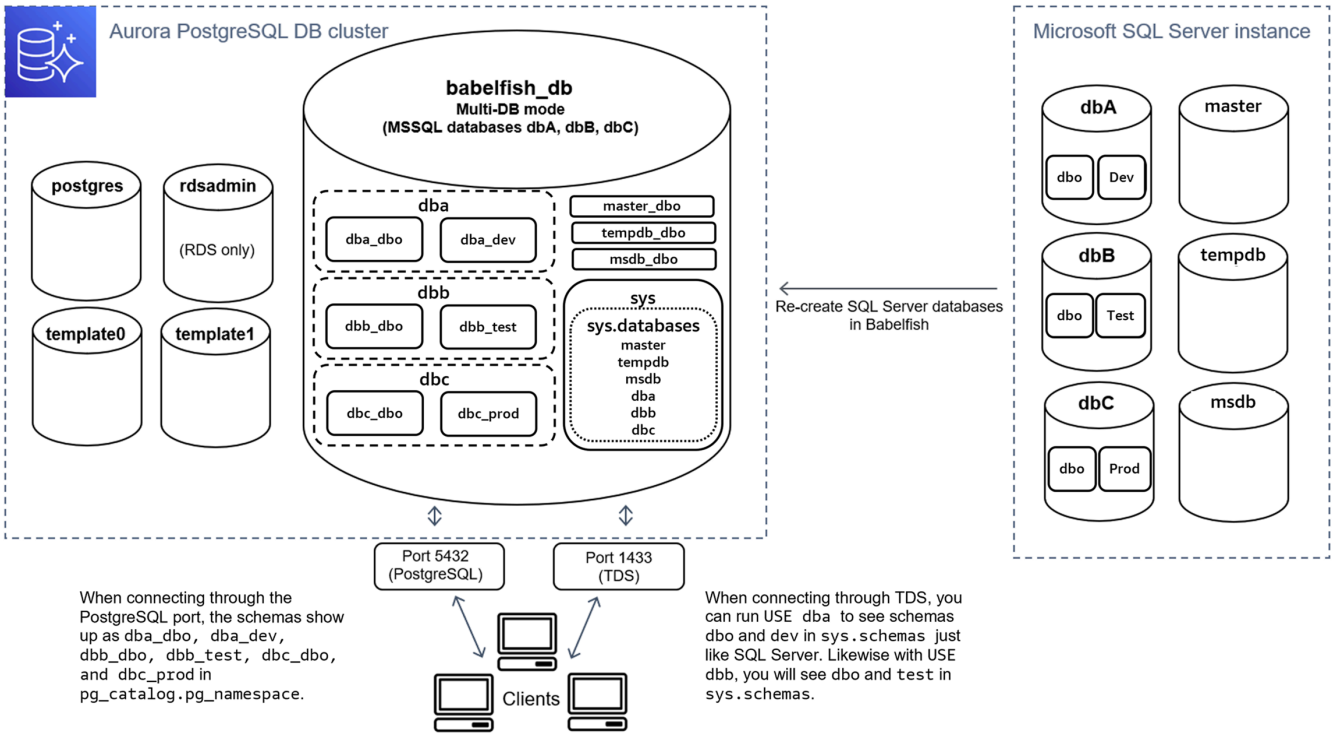
mehrere SQL Server-Datenbanken zusammen. Ihre Wahl wirkt sich darauf aus, wie die Namen von SQL Server-Schemas innerhalb der `babelfish_db`-Datenbank aus Aurora PostgreSQL erscheinen. Der Migrationsmodus wird im `migration_mode`-Parameter gespeichert. Sie dürfen diesen Parameter nicht ändern, nachdem Sie Ihren Cluster erstellt haben, da Sie ggf. den Zugriff auf alle zuvor erstellten SQL-Objekte verlieren.

Im Einzeldatenbank-Modus bleiben die Schemanamen der SQL-Server-Datenbank in der `babelfish_db`-Datenbank von PostgreSQL unverändert. Wenn Sie nur eine einzelne Datenbank migrieren möchten, können die Schemanamen der migrierten Benutzerdatenbank in PostgreSQL mit denselben Namen referenziert werden, die in SQL Server verwendet werden. Zum Beispiel: Das dbo- und `smith`-Schema befinden sich in der dbA-Datenbank.



Wenn Sie sich über TDS verbinden, können Sie `USE dba` starten, um Schemas dbo und `dev` von T-SQL zu sehen, wie Sie es in SQL Server tun würden. Die unveränderten Schemanamen sind auch von PostgreSQL aus sichtbar.

Im Mehrfachdatenbankmodus werden die Schemanamen von Benutzerdatenbanken zu `dbname_schemaname`, wenn von PostgreSQL aus darauf zugegriffen wird. Die Schemanamen bleiben gleich, wenn von T-SQL aus darauf zugegriffen wird.



Wie im Bild gezeigt, sind der Mehrfachdatenbankmodus und der Einzeldatenbankmodus identisch mit SQL Server, wenn Sie eine Verbindung über den TDS-Port herstellen und T-SQL verwenden. Beispielsweise listet `USE dbA` Schemata `dbo` und `dev` genau wie in SQL Server auf. Die zugeordneten Schemanamen wie `dba_dbo` und `dba_dev` sind von PostgreSQL aus sichtbar.

Jede Datenbank enthält immer noch Ihre Schemas. Der Name jeder Datenbank wird dem Namen des SQL Server-Schemas vorangestellt, wobei ein Unterstrich als Trennzeichen verwendet wird, z. B.:

- `dba` enthält `dba_dbo` und `dba_dev`.
- `dbb` enthält `dbb_dbo` und `dbb_test`.
- `dbc` enthält `dbc_dbo` und `dbc_prod`.

Innerhalb der `babelfish_db`-Datenbank muss der T-SQL-Benutzer immer noch `USE dbname` ausführen, um den Datenbankkontext zu ändern, so dass das Erscheinungsbild ähnlich wie bei SQL Server bleibt.

Auswahl eines Migrationsmodus

Jeder Migrationsmodus hat Vor- und Nachteile. Wählen Sie Ihren Migrationsmodus basierend auf der Anzahl der Benutzerdatenbanken, die Sie haben, und Ihren Migrationsplänen aus. Nachdem Sie einen Cluster für die Verwendung mit Babelfish erstellt haben, dürfen Sie den Migrationsmodus nicht mehr ändern, da Sie ggf. den Zugriff auf alle zuvor erstellten SQL-Objekte verlieren. Berücksichtigen Sie bei der Auswahl eines Migrationsmodus die Anforderungen Ihrer Benutzerdatenbanken und Clients.

Wenn Sie einen Cluster zur Verwendung mit Babelfish erstellen, erstellt Aurora PostgreSQL die Systemdatenbanken `master` und `tempdb`. Wenn Sie Objekte in den Systemdatenbanken erstellt oder geändert haben (`master` oder `tempdb`), stellen Sie sicher, dass Sie diese Objekte in Ihrem neuen Cluster neu erstellen. Im Gegensatz zu SQL Server initialisiert Babelfish `tempdb` nach einem Neustart des Clusters nicht neu.

Verwenden Sie in den folgenden Fällen den Migrationsmodus einer einzelnen Datenbank:

- Wenn Sie eine einzelne SQL Server-Datenbank migrieren. Im Einzeldatenbankmodus sind migrierte Schemanamen identisch mit den ursprünglichen SQL-Server-Schemanamen. Dadurch werden Codeänderungen an vorhandenen SQL-Abfragen reduziert, wenn Sie sie für die Ausführung mit einer PostgreSQL-Verbindung optimieren möchten.
- Wenn Ihr Endziel eine vollständige Migration zur nativen Aurora PostgreSQL ist. Konsolidieren Sie Ihre Schemas vor der Migration in einem einzigen Schema (`dbo`) und migrieren Sie dann in einen einzelnen Cluster, um die erforderlichen Änderungen zu verringern.

Verwenden Sie in den folgenden Fällen den Migrationsmodus für mehrere Datenbanken:

- Wenn Sie die standardmäßige SQL-Server-Umgebung mit mehreren Benutzerdatenbanken in derselben Instance wünschen.
- Wenn mehrere Benutzerdatenbanken zusammen migriert werden müssen.

Einstellungen der DB-Cluster-Parametergruppe für Babelfish

Wenn Sie einen Aurora-PostgreSQL-DB-Cluster erstellen und Turn on Babelfish (Babelfish aktivieren) auswählen, wird beim Klicken auf Create new (Neu erstellen) automatisch eine DB-Cluster-Parametergruppe für Sie erstellt. Diese DB-Cluster-Parametergruppe basiert auf der DB-Cluster-Parametergruppe von Aurora PostgreSQL für die Aurora-PostgreSQL-Version, die für die Installation ausgewählt wurde, z. B. Aurora PostgreSQL Version 14. Sie wird unter Verwendung der folgenden allgemeinen Konvention benannt:

```
custom-aurora-postgresql14-babelfish-compat-3
```

Sie können die folgenden Einstellungen während des Cluster-Erstellungsprozesses ändern, aber einige davon können nicht geändert werden, sobald sie in der benutzerdefinierten Parametergruppe gespeichert sind. Wählen Sie daher Folgendes sorgfältig aus:

- Einzelne Datenbank oder mehrere Datenbanken
- Standardgebietsschema für Sortierungen
- Name der Sortierung
- DB-Parametergruppe

Wenn Sie eine vorhandene DB-Cluster-Parametergruppe von Aurora PostgreSQL Version 13 oder höher verwenden möchten, bearbeiten Sie die Gruppe und legen Sie den `babelfish_status`-Parameter auf on fest. Geben Sie alle Babelfish-Optionen an, bevor Sie Ihren Aurora-PostgreSQL-Cluster erstellen. Weitere Informationen hierzu finden Sie unter Arbeiten mit Parametergruppen.

Die folgenden Parameter steuern die Präferenzen von Babelfish. Sofern in der Beschreibung nicht anders angegeben, können Parameter geändert werden. Der Standardwert ist in der Beschreibung enthalten. Gehen Sie wie folgt vor, um die zulässigen Werte für jeden Parameter anzuzeigen:

> **Note**
>
> Wenn Sie eine neue DB-Parametergruppe mit einer DB-Instance verknüpfen, werden die geänderten statischen und dynamischen Parameter erst nach Neustart der DB-Instance angewendet. Wenn Sie jedoch dynamische Parameter in der DB-Parametergruppe ändern, nachdem Sie sie der DB-Instance zugeordnet haben, werden diese Änderungen sofort ohne Neustart angewendet.

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie die Parametergruppe für Ihren `default.aurora-postgresql14`-DB-Cluster in der Liste aus.
4. Geben Sie den Namen eines Parameters in das Suchfeld ein. Geben Sie beispielsweise `babelfishpg_tsql.default_locale` in das Suchfeld ein, um diesen Parameter, seinen Standardwert und die zulässigen Einstellungen anzuzeigen.

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
babelfishpg_tds.tds_default_numeric_scale	Legt den Standardmaßstab des numerischen Typs fest, der in den Metadaten der TDS-Spalte gesendet werden soll, wenn die Engine keine angibt. (Standardwert: 8) (Zulässig: 0–38)	dynamisch	true
babelfishpg_tds.tds_default_numeric_precision	Eine Ganzzahl, die die Standardgenauigkeit des numerischen Typs festlegt, der in den Metadaten der TDS-Spalte gesendet werden soll, wenn die Engine keine angibt. (Standardwert: 38) (Zulässig: 1–38)	dynamisch	true
babelfishpg_tds.tds_default_packet_size	Eine Ganzzahl, die die Standardpaketgröße für die	dynamisch	true

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
	Verbindung von SQL-Server-Clients festlegt. (Standard wert: 4096) (Zulässig: 512–32767)		
babelfishpg_tds.tds_default_protocol_version	Eine Ganzzahl, die eine Standardversion des TDS-Protokolls zum Verbinden von Clients festlegt. (Standardwert: DEFAULT) (Zulässig : TDSv7.0, TDSv7.1, TDSv7.1.1, TDSv7.2, TDSv7.3A, TDSv7.3B, TDSv7.4, DEFAULT)	dynamisch	true
babelfishpg_tds.default_server_name	Ein String, der den Standardnamen des Babelfish-Servers bezeichnet. (Standard wert: Microsoft SQL Server) (Zulässig: null)	dynamisch	true
babelfishpg_tds.tds_debug_log_level	Eine Ganzzahl, die die Protokollierungsst ufe in TDS festlegt; 0 schaltet die Protokoll ierung aus. (Standard wert: 1) (Zulässig: 0, 1, 2, 3)	dynamisch	true

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
babelfishpg_tds.listen_adressen	Ein String, der den Host-Namen oder die IP-Adresse oder -Adressen festlegt, an denen TDS überwacht werden soll. Dieser Parameter kann nicht geändert werden, nachdem der Babelfish-DB-Cluster erstellt wurde. (Standardwert: *) (Zulässig: null)	–	false
babelfishpg_tds.port	Eine Ganzzahl, die den TCP-Port festlegt, der für Anfragen in der SQL-Server-Syntax verwendet wird. (Standardwert: 1433) (Zulässig: 1–65535)	statisch	true

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
babelfishpg_tds.tds_ssl_encrypt	Ein Boolescher Wert, der die Verschlüsselung für Daten, die den TDS-Listener-Port durchqueren, ein- (0) oder ausschaltet (1). Ausführliche Informationen zur Verwendung von SSL für Clientverbindungen finden Sie unter SSL-Einstellungen und Clientverbindungen für Babelfish. (Standardwert: 0) (Zulässig: 0, 1)	dynamisch	true
babelfishpg_tds.tds_ssl_max_protocol_version	Ein String, der die höchste SSL/TLS-Protokollversion angibt, die für die TDS-Sitzung verwendet werden soll. (Standardwert: 'TLSv1.2') (Zulässig: 'TLSv1', 'TLSv1.1', 'TLSv1.2')	dynamisch	true

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
babelfishpg_tds.tds_ssl_min_protocol_version	Ein String, der die niedrigste SSL/TLS-Protokollversion angibt, die für die TDS-Sitzung verwendet werden soll. (Standard: 'TLSv1.2' von Aurora PostgreSQL Version 16, 'TLSv1' für Versionen älter als Aurora PostgreSQL Version 16) (Zulässig: 'TLSv1', 'TLSv1.1', 'TLSv1.2')	dynamisch	true
babelfishpg_tds.unix_socket_directories	Ein String, der das Unix-Socket-Verzeichnis des TDS-Servers bezeichnet. Dieser Parameter kann nicht geändert werden, nachdem der Babelfish-DB-Cluster erstellt wurde. (Standardwert: /tmp) (Zulässig: null)	–	false

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
babelfishpg_tds.unix_socket_group	Ein String, der die Unix-Socket-Gruppe des TDS-Servers bezeichnet. Dieser Parameter kann nicht geändert werden, nachdem der Babelfish-DB-Cluster erstellt wurde. (Standardwert: rdsdb) (Zulässig: null)	–	false
babelfishpg_tsql.default_locale	Ein String, der das Standardgebietsschema für Babelfish-Sortierungen angibt. Das Standardgebietsschema ist nur das Gebietsschema und enthält keine Qualifikatoren. Stellen Sie diesen Parameter ein, wenn Sie einen Babelfish DB-Cluster bereitstellen. Nachdem der DB-Cluster bereitgestellt wurde, werden Änderungen an diesem Parameter ignoriert. (Standardwert: en_US) (Zulässig: Siehe - Tabellen)	statisch	true

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
babelfishpg_tsql.migration_mode	Eine nicht änderbare Liste, die die Unterstützung für Einzel- oder Mehrbenutzerdatenbanken angibt. Stellen Sie diesen Parameter ein, wenn Sie einen Babelfish DB-Cluster bereitstellen. Nach der Bereitstellung des DB-Clusters können Sie den Wert dieses Parameters nicht mehr ändern. (Standard: Multi-DB aus Aurora PostgreSQL Version 16, Single-DB für Versionen älter als Aurora PostgreSQL Version 16) (Zulässig: Single-DB, Multi-DB, Null)	statisch	true

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
babelfishpg_tsql.server_colation_name	Ein String, der den Namen der Sortierung angibt, die für Aktionen auf Serverebene verwendet wird. Stellen Sie diesen Parameter ein, wenn Sie einen Babelfish DB-Cluster bereitstellen. Ändern Sie nach der Bereitstellung des DB-Clusters den Wert dieses Parameters nicht. (Standardwert: bbf_unicode_general_ci_as) (Zulässig: Siehe -Tabellen)	statisch	true
babelfishpg_tsql.version	Ein String, der die Ausgabe der Variablen @@VERSION festlegt. Ändern Sie diesen Wert nicht für Aurora-PostgreSQL-DB-Cluster. (Standardwert: null) (Zulässig: default)	dynamisch	true

Parameter	Beschreibung	Typ anwenden	Ist modifizierbar
rds.babelfish_status	Ein String, der den Status der Babelfish-Funktionalität festlegt. Wenn dieser Parameter auf `datatypes only` gesetzt ist, ist Babelfish ausgeschaltet, aber SQL Server-Datentypen sind weiterhin verfügbar. (Standardwert: off) (Zulässig: on, off, datatypesonly)	statisch	true
unix_socket_permissions	Eine Ganzzahl, die die Unix-Socket-Berechtigungen des TDS-Servers festlegt. Dieser Parameter kann nicht geändert werden, nachdem der Babelfish-DB-Cluster erstellt wurde. (Standardwert: 0700) (Zulässig: 0–511)	–	false

SSL-Einstellungen und Clientverbindungen für Babelfish

Wenn ein Client eine Verbindung mit dem TDS-Port (Standardwert `1433`) herstellt, vergleicht Babelfish die Secure Sockets Layer (SSL)-Einstellung, die während des Client-Handshake gesendet wurde, mit der Babelfish-SSL-Parametereinstellung (`tds_ssl_encrypt`). Babelfish bestimmt dann, ob eine Verbindung zulässig ist. Wenn eine Verbindung zulässig ist, wird das Verschlüsselungsverhalten je nach Ihren Parametereinstellungen und der Unterstützung für die Verschlüsselung des Clients entweder erzwungen oder nicht.

Die folgende Tabelle zeigt, wie sich Babelfish für jede Kombination verhält.

Client SSL-Einstellungen	SSL-Einstellung für Babelfish	Verbindung zulässig?	Wert wird an den Client zurückgegeben
ENCRYPT_OFF	tds_ssl_encrypt=0	Zulässig, das Anmeldepaket ist verschlüsselt	ENCRYPT_OFF
ENCRYPT_OFF	tds_ssl_encrypt=1	Zulässig, die gesamte Verbindung ist verschlüsselt	ENCRYPT_REQ
ENCRYPT_ON	tds_ssl_encrypt=0	Zulässig, die gesamte Verbindung ist verschlüsselt	ENCRYPT_ON

Client SSL-Einstellungen	SSL-Einstellung für Babelfish	Verbindung zulässig?	Wert wird an den Client zurückgegeben
ENCRYPT_ON	tds_ssl_encrypt=1	Zulässig, die gesamte Verbindung ist verschlüsselt	ENCRYPT_ON
ENCRYPT_NOT_SUP	tds_ssl_encrypt=0	Ja	ENCRYPT_NOT_SUP
ENCRYPT_NOT_SUP	tds_ssl_encrypt=1	Nein, Verbindung geschlossen	ENCRYPT_REQ
ENCRYPT_REQ	tds_ssl_encrypt=0	Zulässig, die gesamte Verbindung ist verschlüsselt	ENCRYPT_ON
ENCRYPT_REQ	tds_ssl_encrypt=1	Zulässig, die gesamte Verbindung ist verschlüsselt	ENCRYPT_ON
ENCRYPT_CLIENT_CERT	tds_ssl_encrypt=0	Nein, Verbindung geschlossen	Nicht unterstützt

Client SSL-Einstellungen	SSL-Einstellung für Babelfish	Verbindung zulässig?	Wert wird an den Client zurückgegeben
ENCRYPT_CLIENT_CERT	tds_ssl_encrypt=1	Nein, Verbindung geschlossen	Nicht unterstützt

Von Babelfish unterstützte Sortierungen

Wenn Sie einen Aurora-PostgreSQL-DB-Cluster mit Babelfish erstellen, wählen Sie eine Sortierung für Ihre Daten aus. Eine Sortierung gibt die Sortierreihenfolge und Bitmuster an, die den Text oder die Zeichen in einer bestimmten menschlichen Schriftsprache erzeugen. Eine Sortierung enthält Regeln zum Vergleich von Daten für einen bestimmten Satz von Bitmustern. Die Sortierung bezieht sich auf die Lokalisierung. Verschiedene Gebietsschemas wirken sich auf die Zeichenzuordnung, die Sortierreihenfolge und dergleichen aus. Sortierattribute spiegeln sich in den Namen verschiedener Sortierungen wider. Weitere Informationen zu den Attributen finden Sie unter Babelfish collation attributes table.

Babelfish ordnet SQL Server-Sortierungen vergleichbaren Sortierungen von Babelfish zu. Babelfish definiert Unicode-Sortierungen mit kulturell sensiblen Zeichenfolgenvergleiche und Sortierreihenfolge vorab. Babelfish bietet auch eine Möglichkeit, die Sortierungen in Ihrer SQL Server-DB in die am engsten übereinstimmende Babelfish-Sollation zu übersetzen. Lokalspezifische Sortierungen werden für verschiedene Sprachen und Regionen bereitgestellt.

Einige Sortierungen geben eine Codepage an, die einer clientseitigen Kodierung entspricht. Babelfish wird abhängig von der Sortierung jeder Ausgabespalte automatisch von der Servercodierung in die Clientcodierung übersetzt.

Babelfish unterstützt die Sortierungen, die in der Babelfish supported collations table aufgeführt sind. Babelfish ordnet SQL Server-Sortierungen vergleichbaren Sortierungen von Babelfish zu.

Babelfish verwendet Version 153.80 der ICU-Sortierbibliothek (International Components for Unicode). Weitere Informationen zu ICU-Sortierungen finden Sie unter Sortierung in der ICU-Dokumentation. Weitere Informationen zu PostgreSQL und Sortierungen finden Sie unter Unterstützung von Sortierungen in der PostgreSQL-Dokumentation.

Themen

DB-Cluster-Parameter, die die Sortierung und das Gebietsschema steuern

Die folgenden Parameter wirken sich auf das Sortierverhalten aus.

babelfishpg_tsql.default_locale

Dieser Parameter gibt das Standardgebietsschema an, das von der Sortierung verwendet wird. Dieser Parameter wird in Kombination mit den Attributen in der Babelfish collation attributes table verwendet, um Sortierungen für eine bestimmte Sprache und Region anzupassen. Der Standardwert für diesen Parameter ist `en-US`.

Das Standardgebietsschema gilt für alle Babelfish-Sortierungen, die mit den Buchstaben „BBF“ beginnen, und für alle SQL-Server-Sortierungen, die Babelfish-Sortierungen zugeordnet sind. Wenn die Einstellung für diesen Parameter auf einem vorhandenen Babelfish-DB-Cluster geändert wird, hat dies keinen Einfluss auf das Gebietsschema vorhandener Sortierungen. Eine Liste der Sortierungen finden Sie in der Babelfish supported collations table.

babelfishpg_tsql.server_colation_name

Dieser Parameter gibt die Standardsortierung für den Server (DB-Cluster-Instance von Aurora PostgreSQL) und die Datenbank an. Der Standardwert ist `sql_latin1_general_cp1_ci_as`. Die `server_collation_name`muss ein sein `CI_AS`-Sortierung, da in T-SQL die Serversortierung bestimmt, wie Bezeichner verglichen werden.

Wenn Sie Ihren Babelfish-DB-Cluster erstellen, wählen Sie den Collation name (Name der Sortierung) aus der auswählbaren Liste aus. Dazu gehören die Sortierungen in der Babelfish supported collations table. Ändern Sie nicht das `server_collation_name` nachdem die Babelfish-Datenbank erstellt wurde.

Die Einstellungen, die Sie beim Erstellen Ihres DB-Clusters von Babelfish for Aurora PostgreSQL auswählen, werden in der DB-Cluster-Parametergruppe gespeichert, die dem Cluster für diese Parameter zugeordnet ist, und legen dessen Sortierverhalten fest.

Deterministische und nicht deterministische Sortierungen und Babelfish

Babelfish unterstützt deterministische und nicht deterministische Kollationen:

- Eine deterministische Sortierung wertet Zeichen mit identischen Bytesequenzen als gleich aus. Dies bedeutet, dass `x` und `X` bei einer deterministischen Sortierung nicht gleich sind. Deterministische Sortierungen können Groß- und Kleinschreibung (CS) und Akzente (AS) berücksichtigen.

- Eine nicht deterministische Sortierung erfordert keine identische Übereinstimmung. Eine nicht deterministische Kollation bewertet `x` und `X` gleich. Bei nicht deterministischen Kollatierungen wird zwischen Groß- und Kleinschreibung (CI) und akzentunempfindlich (KI) berücksichtigt.

In der folgenden Tabelle finden Sie einige Verhaltensunterschiede zwischen Babelfish und PostgreSQL im Hinblick auf die Verwendung deterministischer Sortierungen.

Babelfish	PostgreSQL
Unterstützt die LIKE-Klausel bei CI_AS-Sortierungen.	Unterstützt die LIKE-Klausel bei nicht deterministischen Sortierungen nicht.
Unterstützt die `LIKE`-Klausel bei KI-Sortierungen nicht.	
Unterstützt keine Pattern-Matching-Operationen bei nicht deterministischen Sortierungen.	

Eine Liste anderer Einschränkungen und Verhaltensunterschiede für Babelfish im Vergleich zu SQL Server und PostgreSQL finden Sie unter Einschränkungen und Verhaltensunterschiede von Sortierungen.

Babelfish und SQL Server folgen einer Benennungskonvention für Sortierungen, die die Sortierattribute beschreiben, wie in der folgenden Tabelle dargestellt.

Attribut	Beschreibung
AI	Akzentunempfindlich.
AS	Akzentsensibel.
BIN2	BIN2 fordert die Sortierung von Daten in Codepunkt-Reihenfolge an. Die Reihenfolge der Unicode-Codepunkte entspricht der gleichen Zeichenreihenfolge für UTF-8-, UTF-16- und UCS-2-Kodierungen. Die Codepunkt-Reihenfolge ist eine schnelle deterministische Sortierung.
CI	Berücksichtigt Groß- und Kleinschreibung nicht.
CS	Groß-/Kleinschreibung ist zu beachten.

Attribut	Beschreibung
PREF	Verwenden Sie eine PREF-Sortierung, um Großbuchstaben vor Kleinbuch staben zu sortieren. Wenn beim Vergleich die Groß- und Kleinschreibung nicht berücksichtigt wird, wird die Großbuchstabenversion vor der Kleinbuch stabenversion sortiert, wenn keine andere Unterscheidung vorliegt. Die ICU-Bibliothek unterstützt Großbuchstaben mit `colCaseFirst=upper` , aber nicht für CI_AS-Sortierungen. PREF kann nur auf `CS_AS` deterministische Kollationen angewendet werden.

Von Babelfish unterstützte Sortierungen

Verwenden Sie die folgenden Sortierungen als Serversortierung oder Objektsortierung.

Sortier-ID	Hinweise
bbf_unicode_general_ci_as	Unterstützt den Vergleich zwischen Groß- und Kleinschreibung und den LIKE Operator.
bbf_unicode_cp1_ci_as	Nichtdeterministische Kollation auch bekannt als CP1252.
bbf_unicode_CP1250_ci_as	Nichtdeterministische Kollation wird verwendet, um Texte in mitteleuropäischen und osteuropäischen Sprachen darzustellen, die lateinische Schrift verwenden.
bbf_unicode_CP1251_ci_as	Nichtdeterministische Kollation für Sprachen, die das kyrillische Skript verwenden.
bbf_unicode_cp1253_ci_as	Nichtdeterministische Kollation repräsentierte früher das moderne Griechisch.
bbf_unicode_cp1254_ci_as	Nichtdeterministische Kollation, die Türkisch unterstützt.

Sortier-ID	Hinweise
bbf_unicode_cp1255_ci_as	Nichtdeterministische Kollation, die Hebräisch unterstützt.
bbf_unicode_cp1256_ci_as	Nichtdeterministische Kollation wird verwendet, um Sprachen zu schreiben, die arabische Schrift verwenden.
bbf_unicode_cp1257_ci_as	Nichtdeterministische Kollationwird verwendet, um estnische, lettische und litauische Sprachen zu unterstützen.
bbf_unicode_cp1258_ci_as	Nichtdeterministische Kollation wird verwendet, um vietnames ische Schriftzeichen zu schreiben.
bbf_unicode_cp874_ci_as	Nichtdeterministische Kollation wrid verwendet, um thailändische Charaktere zu schreiben.
sql_latin1_general_cp1250_c i_as	Nicht deterministische Einzelbyte-Zeichencodierung wird verwendet, um lateinische Zeichen darzustellen.
sql_latin1_general_cp1251_c i_as	Nichtdeterministische Kollation, die lateinische Zeichen unterstüt zt.
sql_latin1_general_cp1_ci_as	Nichtdeterministische Kollation, die lateinische Zeichen unterstüt zt.
sql_latin1_general_cp1253_c i_as	Nichtdeterministische Kollation, die lateinische Zeichen unterstüt zt.
sql_latin1_general_cp1254_c i_as	Nichtdeterministische Kollation, die lateinische Zeichen unterstüt zt.
sql_latin1_general_cp1255_c i_as	Nichtdeterministische Kollation, die lateinische Zeichen unterstüt zt.

Sortier-ID	Hinweise
sql_latin1_general_cp1256_ci_as	Nichtdeterministische Kollation, die lateinische Zeichen unterstützt.
sql_latin1_general_cp1257_ci_as	Nichtdeterministische Kollation, die lateinische Zeichen unterstützt.
sql_latin1_general_cp1258_ci_as	Nichtdeterministische Kollation, die lateinische Zeichen unterstützt.
chinese_prc_ci_as	Nicht deterministische Sortierung, die Chinesisch (VR China) unterstützt.
cyrillic_general_ci_as	Nicht deterministische Kollation, die Kyrillisch unterstützt.
finnish_swedish_ci_as	Nicht deterministische Kollatierung, die Finnisch unterstützt.
french_ci_as	Nicht deterministische Kollatierung, die Französisch unterstützt.
japanese_ci_as	Nicht deterministische Sortierung, die Japanisch unterstützt. Wird in Babelfish 2.1.0 und höheren Versionen unterstützt.
korean_wansung_ci_as	Nicht deterministische Sortierung, die Koreanisch unterstützt (mit Wörterbuchsortierung).
latin1_general_ci_as	Nicht deterministische Sortierung, die lateinische Zeichen unterstützt.
modern_spanish_ci_as	Nicht deterministische Kollatierung, die das moderne Spanisch unterstützt.

Sortier-ID	Hinweise
polish_ci_as	Nicht deterministische Kollatierung, die Polnisch unterstützt.
thai_ci_as	Nicht deterministische Kollatierung, die Thai unterstützt.
traditional_spanish_ci_as	Nicht deterministische Sortierung, die Spanisch unterstützt (traditionelle Sortierung).
turkish_ci_as	Nicht deterministische Kollatierung, die Türkisch unterstützt.
ukrainisch_ci_as	Nicht deterministische Kollatierung, die Ukrainisch unterstützt.
vietnamesisch_ci_as	Nicht deterministische Kollatierung, die Vietnamesen unterstützt.

Sie können die folgenden Sortierungen als Objektsortierungen verwenden.

Dialekt	Deterministische Optionen	Nicht deterministische Optionen
Arabisch	Arabic_CS_AS	Arabic_CI_AS, Arabic_CI_AI
Chinesisch	Chinese_CS_AS	Chinese_CI_AS, Chinese_CI_AI
Kyrillic_ Allgemein	Cyrillic_General_CS_AS	Cyrillic_General_CI_AS, Cyrillic_ General_CI_AI
Estnisch	Estonian_CS_AS	Estonian_CI_AS, Estonisch_CI_AI
Finnish_S chwedisch	Finnish_Swedish_CS_AS	Finnish_Swedish_CI_AS, Finnish_S wedish_CI_AI

Dialekt	Deterministische Optionen	Nicht deterministische Optionen
Französisch	französisch_cs_as	French_CI_AS, French_CI_AI
Griechisch	Greek_CS_AS	Greek_ci_as, griech_ci_AI
Hebräisch	Hebrew_CS_AS	Hebräisch_CI_AS, Hebräisch_CI_AI
Japanisch (Babelfish 2.1.0 und höher)	Japanese_CS_AS	Japanese_CI_AI, Japanese_CI_AS
Korean_Wamsung	Korean_wamsung_cs_as	Korean_wamsung_ci_as, korean_wamsung_ci_AI
Modern_Spanisch	Modern_Spanish_CS_AS	Modern_Spanish_CI_AS, Modern_Spanish_CI_AI
Mongolisch	Mongolisch_CS_AS	Mongolian_CI_AS, Mongolian_CI_AI
Polnisch	Polish_CS_AS	Polish_ci_as, polish_ci_AI
Thailändisch	Thai_cs_as	Thai_CI_AS, Thai_CI_AI
Traditional_Spanisch	Traditional_Spanish_CS_AS	Traditional_Spanish_CI_AS, Traditional_Spanish_CI_AI
Türkisch	Türkisch_CS_AS	Turkish_ci_as, Türkisch_CI_AI
Ukrainisch	Ukranian_CS_AS	Ukranian_ci_as, Ukranian_ci_AI

Dialekt	Deterministische Optionen	Nicht deterministische Optionen
Vietnamesisch	Vietnamese_CS_AS	Vietnamese_CI_AS, Vietnames e_CI_AI

Standardsortierung in Babelfish

Bisher lautete die Standardsortierung der sortierbaren Datentypen `pg_catalog.default`. Die Datentypen und Objekte, die von diesen Datentypen abhängen, werden unter Berücksichtigung der Groß- und Kleinschreibung sortiert. Diese Bedingung wirkt sich möglicherweise auf die T-SQL-Objekte des Datensatzes aus, der ohne Berücksichtigung der Groß- und Kleinschreibung sortiert wird. Ab Babelfish 2.3.0 entspricht die Standardsortierung für die sortierbaren Datentypen (außer TEXT und NTEXT) der Sortierung im Parameter `babelfishpg_tsql.server_collation_name`. Wenn Sie ein Upgrade auf Babelfish 2.3.0 durchführen, wird die Standardsortierung bei der Erstellung des DB-Clusters automatisch ausgewählt, was keine sichtbaren Auswirkungen hat.

Verwalten von Sortierungen

Die ICU-Bibliothek bietet Sortierversionsverfolgung, um sicherzustellen, dass Indizes, die von Sortierungen abhängen, neu dexiert werden können, wenn eine neue Version der ICU verfügbar wird. Um festzustellen, ob Ihre aktuelle Datenbank Sortierungen enthält, die aktualisiert werden müssen, können Sie die folgende Abfrage verwenden, nachdem Sie eine Verbindung mit `psql` oder `pgAdmin` hergestellt haben:

```
SELECT pg_describe_object(refclassid, refobjid,
    refobjsubid) AS "Collation",
    pg_describe_object(classid, objid, objsubid) AS "Object"
    FROM pg_depend d JOIN pg_collation c ON refclassid = 'pg_collation'::regclass
    AND refobjid = c.oid WHERE c.collversion <> pg_collation_actual_version(c.oid)
    ORDER BY 1, 2;
```

Diese Abfrage gibt beispielsweise die folgende Ausgabe zurück:

```
 Collation | Object
-----------+--------
(0 rows)
```

In diesem Beispiel müssen keine Sortierungen aktualisiert werden.

Zum Abrufen einer Auflistung der vordefinierten Sortierungen in Ihrer Babelfish-Datenbank können Siepsql oder pgAdmin mit der folgenden Abfrage verwenden:

```
SELECT * FROM pg_collation;
```

Vordefinierte Sortierungen werden in der sys.fn_helpcollations-Tabelle gespeichert. Mit dem folgenden Befehl können Sie Informationen über eine Sortierung anzeigen (z. B. die Flags „lcid“, „style“ und „collatate“). Wenn Sie eine Auflistung aller Sortierungen mit sqlcmd abrufen möchten, verbinden Sie sich mit dem T-SQL-Port (standardmäßig 1433) und führen Sie die folgende Abfrage aus:

```
1> :setvar SQLCMDMAXVARTYPEWIDTH 40
2> :setvar SQLCMDMAXFIXEDTYPEWIDTH 40
3> SELECT * FROM fn_helpcollations()
4> GO
name                                    description
--------------------------------------- ---------------------------------------
arabic_cs_as                            Arabic, case-sensitive, accent-sensitive
arabic_ci_ai                            Arabic, case-insensitive, accent-insensi
arabic_ci_as                            Arabic, case-insensitive, accent-sensiti
bbf_unicode_bin2                        Unicode-General, case-sensitive, accent-
bbf_unicode_cp1250_ci_ai                Default locale, code page 1250, case-ins
bbf_unicode_cp1250_ci_as                Default locale, code page 1250, case-ins
bbf_unicode_cp1250_cs_ai                Default locale, code page 1250, case-sen
bbf_unicode_cp1250_cs_as                Default locale, code page 1250, case-sen
bbf_unicode_pref_cp1250_cs_as           Default locale, code page 1250, case-sen
bbf_unicode_cp1251_ci_ai                Default locale, code page 1251, case-ins
bbf_unicode_cp1251_ci_as                Default locale, code page 1251, case-ins
bbf_unicode_cp1254_ci_ai                Default locale, code page 1254, case-ins
...
(124 rows affected)
```

Die im Beispiel gezeigten Zeilen 1 und 2 schränken die Ausgabe nur zu Lesbarkeitszwecken der Dokumentation ein.

```
1> SELECT SERVERPROPERTY('COLLATION')
2> GO
serverproperty
------------------------------------------------------------------------------
sql_latin1_general_cp1_ci_as
```

```
(1 rows affected)
1>
```

Einschränkungen und Verhaltensunterschiede von Sortierungen

Babelfish verwendet die ICU-Bibliothek zur Sortierunterstützung. PostgreSQL ist mit einer bestimmten Version der ICU erstellt und kann höchstens mit einer Version einer Sortierung übereinstimmen. Variationen zwischen Versionen sind unvermeidbar, ebenso geringfügige Schwankungen im Laufe der Zeit, während sich die Sprachen entwickeln. Im folgenden Abschnitt werden einige der bekannten Einschränkungen und Verhaltensvarianten von Babelfish-Sortierungen aufgeführt:

- Indizes und Sortierungstypabhängigkeit – Ein Index für einen benutzerdefinierten Typ, der von der International Components for Unicode (ICU)-Sortierungsbibliothek (die von Babelfish verwendete Bibliothek) abhängt, wird nicht ungültig, wenn sich die Version der Bibliothek ändert.
- COLLATIONPROPERTY-Funktion – Sortiereigenschaften werden nur für die unterstützten Babelfish-BBF-Sortierungen implementiert. Weitere Informationen hierzu finden Sie unter Babelfish supported collations table.
- Unterschiede bei Unicode-Sortierregeln – SQL-Sortierungen für SQL Server sortieren mit Unicode codierte Daten (`nchar` und `nvarchar`) anders als Daten, die nicht mit Unicode codiert sind (`char` und `varchar`). Babelfish-Datenbanken sind immer UTF-8-codiert und wenden Unicode-Sortierregeln unabhängig vom Datentyp immer einheitlich an, sodass die Sortierreihenfolge für `char` oder `varchar` die gleiche ist wie für `nchar` oder `nvarchar`.
- Sekundär gleiche Sortierungen und Sortierverhalten – Die Standard-ICU-Unicode-Sortierung sekundär gleich (`CI_AS`) sortiert Satzzeichen und andere nicht alphanumerische Zeichen vor numerischen Zeichen und numerische Zeichen vor alphabetischen Zeichen. Die Reihenfolge der Satzzeichen und anderer Sonderzeichen ist jedoch unterschiedlich.
- Teritiäre Sortierung, Umgehung für ORDER BY – SQL-Sortierungen wie `SQL_Latin1_General_Pref_CP1_CI_AS` unterstützen die `TERTIARY_WEIGHTS`-Funktion und die Möglichkeit, Strings zu sortieren, die gleichermaßen in einer `CI_AS`-Sortierung verglichen werden, die zuerst in Großbuchstaben sortiert werden soll: `ABC`, `ABc`, `AbC`, `Abc`, `aBC`, `aBc`, `abC` und schließlich `abc`. Daher bewertet die analytische Funktion `DENSE_RANK OVER (ORDER BY column)` diese Strings als denselben Rang, ordnet sie jedoch zuerst in einer Partition in Großbuchstaben an.

  Sie können ein ähnliches Ergebnis mit Babelfish erzielen, indem Sie eine `COLLATE`-Klausel zu einer `ORDER BY`-Klausel hinzufügen, die eine Tertiäre `CS_AS` angibt,, welche

`@colCaseFirst=upper` spezifiziert. Der `colCaseFirst`-Modifizierer gilt jedoch nur für Strings, die tertiär gleich sind (anstatt sekundär gleich wie bei einer `CI_AS`-Sortierung). Daher können Sie tertiäre SQL-Sollationen nicht mit einer einzigen ICU-Sortierung emulieren.

Als Problemumgehung empfehlen wir, Anwendungen zu ändern, die eine `SQL_Latin1_General_Pref_CP1_CI_AS`-Kollation zur Verwendung der `BBF_SQL_Latin1_General_CP1_CI_AS`-Kollation nutzt. Dann fügen Sie `COLLATE BBF_SQL_Latin1_General_Pref_CP1_CS_AS` zu einer beliebigen `ORDER BY`-Klausel für diese Spalte hinzu.

- Zeichenerweiterung – Eine Zeichenerweiterung behandelt ein einzelnes Zeichen als eine Zeichenfolge auf der Primärebene. Die `CI_AS`-Standardsortierung von SQL Server unterstützt die Zeichenerweiterung. ICU-Sortierungen unterstützen die Zeichenerweiterung nur für akzentunempfindliche Sortierungen.

  Wenn eine Zeichenerweiterung erforderlich ist, verwenden Sie eine `AI`-Sortierung für Vergleiche. Solche Sortierungen werden derzeit jedoch vom LIKE Operator nicht unterstützt.

- Codierung von char und varchar – Wenn SQL-Sortierungen für `char`- oder `varchar`-Datentypen verwendet werden, wird die Sortierreihenfolge für Zeichen vor ASCII 127 durch die spezifische Code Page für diese SQL-Sortierung bestimmt. Bei SQL-Sortierungen können Strings, die als `char` oder `varchar` deklariert sind, anders sortiert werden als Strings, die als `nchar` oder `nvarchar` deklariert sind.

  PostgreSQL kodiert alle Strings mit der Datenbankkodierung, damit alle Zeichen in UTF-8 konvertiert und nach Unicode-Regeln sortiert werden.

  Da SQL-Sollationen nchar- und nvarchar-Datentypen mithilfe von Unicode-Regeln sortieren, codiert Babelfish alle Strings auf dem Server mit UTF-8. Babelfish sortiert nchar- und nvarchar-Strings genauso wie Char- und Varchar-Strings unter Verwendung von Unicode-Regeln.

- Ergänzende Zeichen – Die SQL-Server-Funktionen `NCHAR`, `UNICODE` und `LEN` unterstützen Zeichen für Codepunkte außerhalb der Unicode Basic Multilingual Plane (BMP). Im Gegensatz dazu verwenden Nicht-SC-Sollationen Ersatzpaarzeichen, um zusätzliche Zeichen zu behandeln. Für Unicode-Datentypen kann SQL Server bis zu 65.535 Zeichen mit UCS-2 oder dem gesamten Unicode-Bereich (1.114.114 Zeichen) darstellen, wenn zusätzliche Zeichen verwendet werden.

- Kana-sensible (KS) Sortierungen – Eine kana-sensible (KS) Sortierung behandelt japanische `Hiragana`- und `Katakana`-Kana-Zeichen anders. Die Intensivstation unterstützt den japanischen Sortierstandard `JIS X 4061`. Der jetzt veraltete `colhiraganaQ [on | off]` lokale Modifikator

bietet möglicherweise die gleiche Funktionalität wie KS-Sortierungen. KS-Sortierungen mit demselben Namen wie SQL Server werden derzeit jedoch nicht von Babelfish unterstützt.

- Breitenempfindliche (WS) Sortierungen – Wenn ein Einzelbyte-Zeichen (halbe Breite) und das gleiche Zeichen, das als Doppelbyte-Zeichen (volle Breite) dargestellt wird, unterschiedlich behandelt werden, wird die Sortierung als breitenempfindlich (width-sensitive, WS) bezeichnet. WS-Sortierungen mit dem gleichen Namen wie SQL Server werden derzeit von Babelfish nicht unterstützt.
- Variationsauswahl-sensible (VSS) Sortierungen – Variationsauswahl-sensible (VSS) Sortierungen unterscheiden zwischen ideographischen Variationsauswahlen in japanischen Sortierungen `Japanese_Bushu_Kakusu_140` und `Japanese_XJIS_140`. Eine Variationssequenz besteht aus einem Basiszeichen plus einem zusätzlichen Variationsselektor. Wenn Sie nicht die `_VSS`-Option wählen, wird der Variationsselektor im Vergleich nicht berücksichtigt.

  VSS-Sortierungen werden derzeit nicht von Babelfish unterstützt.
- BIN- und BIN2-Sortierungen – Eine BIN2-Sortierung sortiert Zeichen nach Codepunkt-Reihenfolge. Die binäre Byte-für-Byte-Reihenfolge von UTF-8 behält die Reihenfolge der Unicode-Codepunkte bei, daher ist dies wahrscheinlich auch die Sortierung mit der besten Leistung. Wenn die Unicode-Codepunkt-Reihenfolge für eine Anwendung funktioniert, sollten Sie eine BIN2-Sortierung verwenden. Die Verwendung einer BIN2-Sollation kann jedoch dazu führen, dass Daten auf dem Client in einer kulturell unerwarteten Reihenfolge angezeigt werden. Im Laufe der Zeit werden Unicode neue Zuordnungen zu Kleinbuchstaben hinzugefügt, sodass die `LOWER`-Funktion auf verschiedenen Versionen der Intensivstation unterschiedlich funktionieren kann. Dies ist ein Sonderfall des allgemeineren Sortierungsproblems und nicht als etwas, das für die BIN2-Sollation spezifisch ist.

  Babelfish bietet eine `BBF_Latin1_General_BIN2`-Kollation mit der Babelfish-Distribution, um in Unicode-Codepunkt-Reihenfolge zusammenzufassen. In einer BIN-Sollation wird nur das erste Zeichen als wchar sortiert. Die verbleibenden Zeichen werden byte für Byte sortiert, effektiv in Codepunkt-Reihenfolge entsprechend ihrer Kodierung. Dieser Ansatz folgt nicht den Unicode-Sollationsregeln und wird von Babelfish nicht unterstützt.
- Nicht deterministische Sortierungen und CHARINDEX-Einschränkung – Für Babelfish-Versionen, die älter als Version 2.1.0 sind, können Sie CHARINDEX nicht mit nicht deterministischen Sortierungen verwenden. Standardmäßig verwendet Babelfish eine Sortierung ohne Berücksichtigung der Groß- und Kleinschreibung (nicht deterministisch). Die Verwendung von CHARINDEX für ältere Versionen von Babelfish löst den folgenden Laufzeitfehler aus:

```
nondeterministic collations are not supported for substring searches
```

> **Note**
>
> Diese Einschränkung und Problemumgehung gelten nur für Babelfish Version 1.x (13.x-Versionen von Aurora PostgreSQL). Babelfish 2.1.0 und höhere Releases haben dieses Problem nicht.

Dieses Problem können Sie mit einer der folgenden Methoden umgehen:

- Konvertieren Sie den Ausdruck explizit in eine Kollatierung mit Berücksichtigung der Groß- und Kleinschreibung und wandeln Sie die Groß- oder Kleinschreibung beider Argumente um, indem Sie LOWER oder UPPER anwenden. Der Aufruf `SELECT charindex('x', a) FROM t1` führt beispielsweise zu folgender Ausgabe:

  ```
  SELECT charindex(LOWER('x'), LOWER(a COLLATE sql_latin1_general_cp1_cs_as)) FROM t1
  ```

- Erstellen Sie eine SQL-Funktion f_charindex und ersetzen Sie CHARINDEX-Aufrufe durch Aufrufe der folgenden Funktion:

  ```
  CREATE function f_charindex(@s1 varchar(max), @s2 varchar(max)) RETURNS int
  AS
  BEGIN
  declare @i int = 1
  WHILE len(@s2) >= len(@s1)
  BEGIN
    if LOWER(@s1) = LOWER(substring(@s2,1,len(@s1))) return @i
    set @i += 1
    set @s2 = substring(@s2,2,999999999)
  END
  return 0
  END
  go
  ```

Verwalten der Babelfish-Fehlerbehandlung mit Escape-Schraffuren

Babelfish ahmt das SQL-Verhalten in Bezug auf den Kontrollfluss und den Transaktionsstatus nach Möglichkeit nach. Wenn Babelfish auf einen Fehler stößt, gibt es nach Möglichkeit einen Fehlercode zurück, der dem SQL Server-Fehlercode ähnelt. Wenn Babelfish den Fehler keinem SQL-Server-Code zuordnen kann, gibt es einen festen Fehlercode (`33557097`) zurück und führt spezifische Aktionen basierend auf der Art des Fehlers wie folgt aus:

- Bei Kompilierzeitfehlern führt Babelfish ein Rollback für die Transaktion aus.
- Wenn es sich um einen Laufzeitfehler handelt, beendet Babelfish den Stapel und führt ein Rollback für die Transaktion aus.
- Bei einem Protokollfehler zwischen Client und Server wird kein Rollback der Transaktion ausgeführt.

Wenn ein Fehlercode nicht einem äquivalenten Code zugeordnet werden kann und der Code für einen ähnlichen Fehler verfügbar ist, wird der Fehlercode dem alternativen Code zugeordnet. Zum Beispiel die Verhaltensweisen, die SQL Server-Codes `8143` und `8144` verursachen, sind beide als `8143` mappiert.

Fehler, die nicht mappiert werden können, respektieren ein `TRY... CATCH`-Konstrukt nicht.

Sie können `@@ERROR` nutzen, um einen SQL Server-Fehlercode zurückzugeben, oder die `@@PGERROR`-Funktion, um einen PostgreSQL-Fehlercode zurückzugeben. Sie können auch die `fn_mapped_system_error_list`-Funktion nutzen, um eine Liste der zugeordneten Fehlercodes zurückzugeben. Weitere Informationen zu PostgreSQL-Fehlercodes finden Sie unter Die PostgreSQL-Website.

Ändern der Escape-Schraffureinstellungen in Babelfish

Um besser mit Anweisungen umzugehen, die scheitern könnten, definiert Babelfish bestimmte Optionen, die als Escape-Schraffuren bezeichnet werden. Eine Escape-Luke ist eine Option, die das Verhalten von Babelfish angibt, wenn es auf eine nicht unterstütztes Funktion oder eine nicht unterstützte Syntax stößt.

Sie können die `sp_babelfish_configure` gespeicherte Prozedur zur Steuerung der Einstellungen einer Escape-Schraffur nutzen. Verwenden Sie das Skript, um die Escape-Schraffur auf `ignore` oder `strict` zu setzen. Wenn es auf `strict` eingestellt ist, gibt Babelfish einen Fehler zurück, den Sie korrigieren müssen, bevor Sie fortfahren.

Schließen Sie das `server`-Schlüsselwort ein, um die Änderungen auf die aktuelle Sitzung und auf Clusterebene anzuwenden.

Die Verwendung ist wie folgt:

- Um alle Escape-Schraffuren und ihren Status sowie Nutzungsinformationen aufzulisten, führen Sie `sp_babelfish_configure` aus.
- Führen Sie den Befehl `sp_babelfish_configure '`*`hatch_name`*`'` aus, um die benannten Escape-Schraffuren und ihre Werte für die aktuelle oder clusterweite Sitzung aufzulisten, wo *`hatch_name`* die Kennung einer oder mehrerer Escape-Schraffuren *`hatch_name`* SQL-Platzhalter wie '%' verwenden kann.
- Um eine oder mehrere Escape-Schraffuren auf den angegebenen Wert festzulegen, führen Sie `sp_babelfish_configure ['`*`hatch_name`*`' [, 'strict'|'ignore' [, 'server']]]` aus. Um die Einstellungen auf einer clusterweiten Ebene dauerhaft zu machen, schließen Sie das `server`-Schlüsselwort ein, wie im Folgenden dargestellt:

  ```
  EXECUTE sp_babelfish_configure 'escape_hatch_unique_constraint', 'ignore', 'server'
  ```

  Um sie nur für die aktuelle Sitzung festzulegen, verwenden Sie `server` nicht.
- Führen Sie `sp_babelfish_configure 'default'` (Babelfish 1.2.0 und höher) aus, um alle Escape-Schraffuren auf ihre Standardwerte zurückzusetzen.

Die Zeichenfolge, die die Schraffur (oder Schraffuren) identifiziert, kann SQL-Platzhalter enthalten. Im Folgenden werden beispielsweise alle Syntax-Escape-Schraffuren festgelegt auf `ignore` für den Aurora-PostgreSQL-Cluster.

```
EXECUTE sp_babelfish_configure '%', 'ignore', 'server'
```

In der folgenden Tabelle finden Sie Beschreibungen und Standardwerte für die vordefinierten Escape-Schraffuren von Babelfish.

Escape-Luke	Beschreibung	Standard
`escape_hatch_checkpoint`	Erlaubt die Verwendung der CHECKPOINT-Anweisung im prozeduralen Code, die	ignore

Escape-Luke	Beschreibung	Standard
	CHECKPOINT-Anweisung ist derzeit jedoch nicht implementiert.	
`escape_hatch_constraint_name_for_default`	Steuert das Verhalten von Babelfish im Zusammenhang mit Standardbeschränkungsnamen.	ignore
`escape_hatch_database_misc_options`	Steuert das Verhalten von Babelfish im Zusammenhang mit den folgenden Optionen in CREATE oder ALTER DATABASE: CONTAINMENT, DB_CHAINING, TRUSTWORTHY, PERSISTENT_LOG_BUFFER.	ignore
`escape_hatch_for_replication`	Steuert das Verhalten von Babelfish im Zusammenhang mit der [NOT] FOR REPLICATION-Klausel beim Erstellen oder Ändern einer Tabelle.	strict
`escape_hatch_fulltext`	Steuert das Verhalten von Babelfish im Zusammenhang mit FULLTEXT-Features wie DEFAULT_FULLTEXT_LANGUAGE in CREATE/ALTER DATABASE, CREATE FULLTEXT INDEX oder sp_fulltext_database.	ignore

Escape-Luke	Beschreibung	Standard
`escape_hatch_ignore_dup_key`	Steuert das Verhalten von Babelfish im Zusammenhang mit CREATE/ALTER TABLE und CREATE INDEX. Wenn IGNORE_DUP_KEY=ON gilt, wird ein Fehler ausgelöst, wenn die Einstellung `strict` (Standard wert) festgelegt ist, oder der Fehler ignoriert, wenn die Einstellung `ignore` lautet (Babelfish Version 1.2.0 und höher).	strict
`escape_hatch_index_clustering`	Steuert das Verhalten von Babelfish im Zusammenh ang mit den Schlüsselwörtern CLUSTERED oder NONCLUSTE RED für Indizes und PRIMARY KEY- oder UNIQUE-Einschränku ngen. Wenn CLUSTERED ignoriert wird, wird der Index oder die Einschränkung immer noch so erstellt, als wäre NONCLUSTE RED angegeben worden.	ignore
`escape_hatch_index_columnstore`	Steuert das Verhalten von Babelfish im Zusammenhang mit der COLUMNSTORE-Klause l. Wenn Sie `ignore` angeben, erstellt Babelfish einen regulären B-Baum-Index.	strict

Escape-Luke	Beschreibung	Standard
`escape_hatch_join_hints`	Steuert das Verhalten von Schlüsselwörtern in einem JOIN-Operator: LOOP, HASH, MERGE, REMOTE, REDUCATE, REDISTRIBUTE, REPLICATE.	ignore
`escape_hatch_language_non_english`	Steuert das Verhalten von Babelfish im Zusammenhang mit anderen Sprachen als Englisch für Nachrichten auf dem Bildschirm. Babelfish unterstützt derzeit nur `us_english` für Nachrichten auf dem Bildschirm. SET LANGUAGE verwendet möglicherweise eine Variable, die den Sprachnamen enthält, sodass die tatsächlich festgelegte Sprache nur zur Laufzeit erkannt werden kann.	strict
`escape_hatch_login_hashed_password`	Wenn es ignoriert wird, unterdrückt der Fehler für das Schlüsselwort `HASHED` für `CREATE LOGIN` und `ALTER LOGIN`.	strict
`escape_hatch_login_misc_options`	Wenn es ignoriert wird, unterdrückt der Fehler bei anderen Schlüsselwörtern außer `HASHED`, `´MUST_CHANGE` , `OLD_PASSWORD` und `UNLOCK` für `CREATE LOGIN` und `ALTER LOGIN`.	strict

Escape-Luke	Beschreibung	Standard
`escape_hatch_login_old_password`	Wenn es ignoriert wird, unterdrückt der Fehler für das Schlüsselwort `OLD_PASSWORD` für `CREATE LOGIN` und `ALTER LOGIN`.	strict
`escape_hatch_login_password_must_change`	Wenn es ignoriert wird, unterdrückt der Fehler für das Schlüsselwort `MUST_CHANGE` für `CREATE LOGIN` und `ALTER LOGIN`.	strict
`escape_hatch_login_password_unlock`	Wenn es ignoriert wird, unterdrückt der Fehler für das Schlüsselwort `UNLOCK` für `CREATE LOGIN` und `ALTER LOGIN`.	strict
`escape_hatch_nocheck_add_constraint`	Steuert das Verhalten von Babelfish im Zusammenhang mit der WITH CHECK- oder NOCHECK-Klausel für Einschränkungen.	strict
`escape_hatch_nocheck_existing_constraint`	Steuert das Verhalten von Babelfish im Zusammenhang mit FOREIGN KEY- oder CHECK-Einschränkungen.	strict

Escape-Luke	Beschreibung	Standard
`escape_hatch_query_hints`	Steuert das Verhalten von Babelfish im Zusammenhang mit Abfragehinweisen. Wenn diese Option auf ignorieren eingestellt ist, ignoriert der Server Hinweise, die die OPTION (...) -Klausel verwenden, um Aspekte der Abfrageverarbeitung anzugeben. Beispiele sind SELECT FROM... OPTION (JOIN-HASH ZUSAMMENFÜHREN, MAXRECURSION 10)).	ignore
`escape_hatch_rowversion`	Steuert das Verhalten der Datentypen ROWVERSION und TIMESTAMP. Weitere Informationen zur Nutzung finden Sie unter Verwenden von Babelfish-Funktionen mit eingeschränkter Implementierung.	strict
`escape_hatch_schemabinding_function`	Steuert das Verhalten von Babelfish im Zusammenhang mit der WITH SCHEMABINDING-Klausel. Standardmäßig wird die WITH SCHEMABINDING-Klausel ignoriert, wenn sie mit dem Befehl CREATE oder ALTER FUNCTION angegeben wird.	ignore

Escape-Luke	Beschreibung	Standard
`escape_hatch_schemabinding_procedure`	Steuert das Verhalten von Babelfish im Zusammenhang mit der WITH SCHEMABINDING-Klausel. Standardmäßig wird die WITH SCHEMABINDING-Klausel ignoriert, wenn sie mit dem Befehl CREATE oder ALTER PROCEDURE angegeben wird.	ignore
`escape_hatch_rowguidcol_column`	Steuert das Verhalten von Babelfish im Zusammenhang mit der ROWGUIDCOL-Klausel beim Erstellen oder Ändern einer Tabelle.	strict
`escape_hatch_schemabinding_trigger`	Steuert das Verhalten von Babelfish im Zusammenhang mit der WITH SCHEMABINDING-Klausel. Standardmäßig wird die WITH SCHEMABINDING-Klausel ignoriert, wenn sie mit dem Befehl CREATE oder ALTER TRIGGER angegeben wird.	ignore
`escape_hatch_schemabinding_view`	Steuert das Verhalten von Babelfish im Zusammenhang mit der WITH SCHEMABINDING-Klausel. Standardmäßig wird die WITH SCHEMABINDING-Klausel ignoriert, wenn sie mit dem Befehl CREATE oder ALTER VIEW angegeben wird.	ignore

Escape-Luke	Beschreibung	Standard
`escape_hatch_session_settings`	Steuert das Verhalten von Babelfish in Richtung nicht unterstützter SET-Anweisungen auf Sitzungsebene.	ignore
`escape_hatch_showplan_all`	Steuert das Verhalten von Babelfish in Bezug auf SET SHOWPLAN_ALL und SET STATISTICS PROFILE. Wenn sie auf „ignore“ eingestellt sind, verhalten sie sich wie SET BABELFISH_SHOWPLAN_ALL und SET BABELFISH_STATISTICS PROFILE; wenn sie auf „strict“ festgelegt sind, werden sie stillschweigend ignoriert.	strict
`escape_hatch_storage_on_partition`	Steuert das Verhalten von Babelfish im Zusammenhang mit der `ON partition_scheme column` -Klausel beim Definieren der Partitionierung. Babelfish implementiert derzeit keine Partitionierung.	strict

Escape-Luke	Beschreibung	Standard
`escape_hatch_storage_options`	Escape-Schraffur für jede Speicheroption, die in CREATE, ALTER DATABASE, TABLE, INDEX verwendet. Dazu gehören Klauseln (LOG) ON, TEXTIMAGE _ON, FILESTREAM_ON, die Speicherorte (Partitionen, Dateigruppen) für Tabellen, Indizes und Einschränkungen sowie für eine Datenbank definiere n. Diese Escape-Schraffurei nstellung gilt für alle diese Klauseln (einschließlich ON [PRIMARY] und ON „DEFAULT“). Die Ausnahme ist, wenn eine Partition für eine Tabelle oder einen Index mit ON partition _scheme (Spalte) angegeben wird.	ignore
`escape_hatch_table_hints`	Steuert das Verhalten von Tabellenhinweisen, die mit der WITH (...) -Klausel angegeben wurden.	ignore

Escape-Luke	Beschreibung	Standard
`escape_hatch_unique_constraint`	Bei Einstellung auf „strict“ (streng) kann ein obskurer semantisc her Unterschied zwischen SQL Server und PostgreSQL bei der Handhabung von NULL-Wert en in indizierten Spalten Fehler auslösen. Der semantische Unterschied tritt nur in unrealist ischen Anwendungsfällen auf, sodass Sie diese Escape-Schraffur auf „ignore“ (Ignorieren) festlegen können, um den Fehler nicht anzuzeigen.	strict

Erstellen eines DB-Clusters von Babelfish for Aurora PostgreSQL

Diese Version von Babelfish for Aurora PostgreSQL wird von Aurora PostgreSQL Version 13.4 und höher unterstützt.

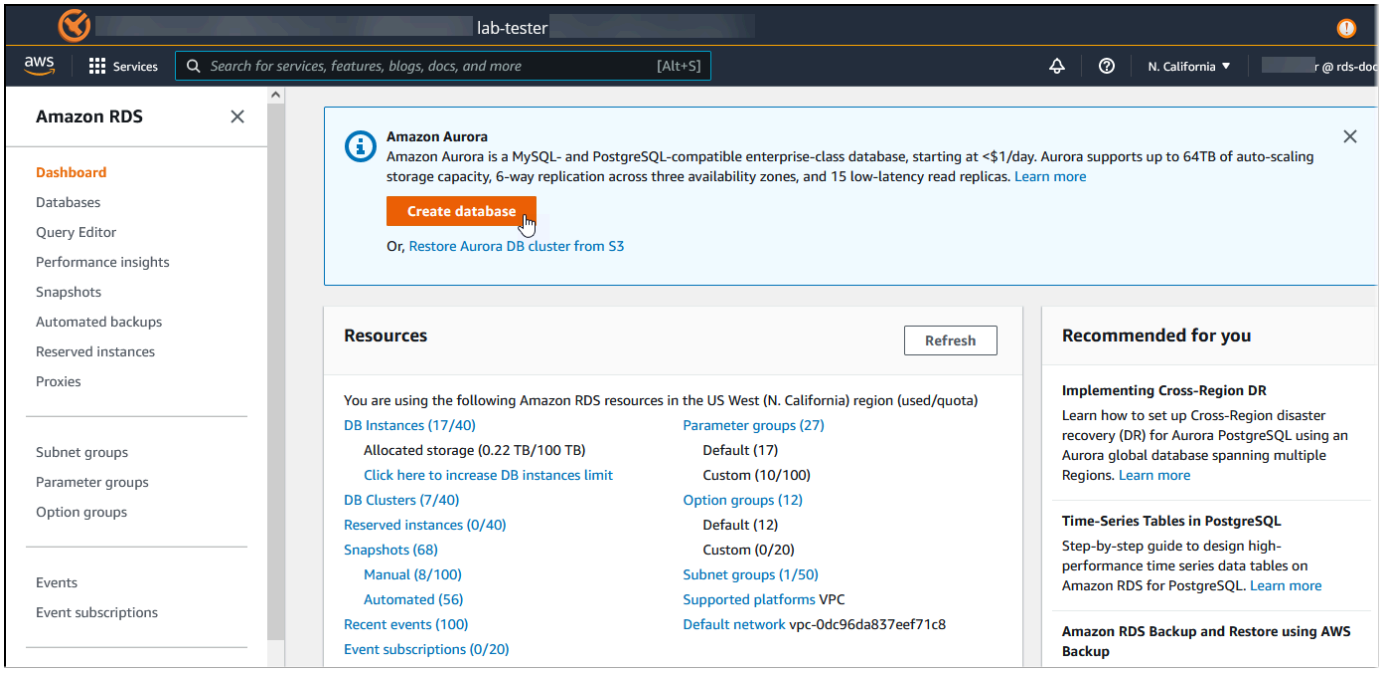
Sie können AWS Management Console oder AWS CLI verwenden, um einen Aurora-PostgreSQL-Cluster mit Babelfish zu erstellen.

> **Note**
>
> In einem Aurora-PostgreSQL-Cluster ist der Datenbankname `babelfish_db` für Babelfish reserviert. Das Erstellen einer eigenen „babelfish_db“-Datenbank auf einem Babelfish für Aurora PostgreSQL verhindert, dass Aurora Babelfish erfolgreich bereitstellt.

Konsole

So erstellen Sie einen Cluster mit Babelfish, der mit AWS Management Console läuft

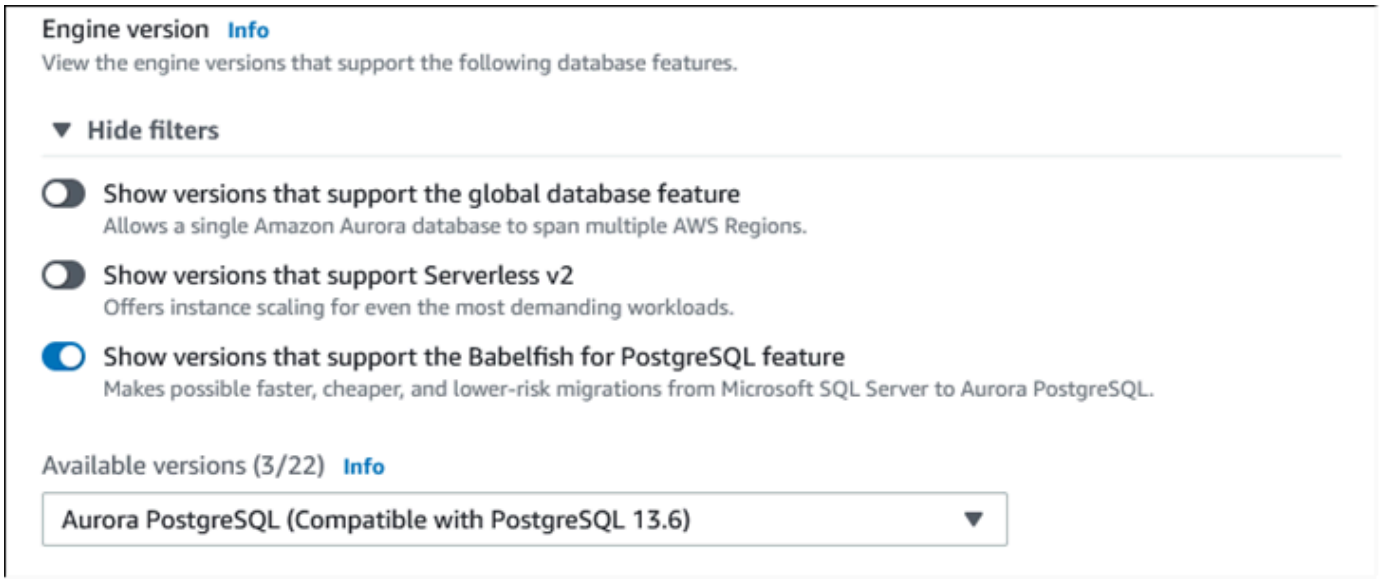
1. Öffnen Sie die Amazon RDS-Konsole unter https://console.aws.amazon.com/rds/ und wählen Sie Erstellen einer Datenbank aus.



2. Für Wählen Sie eine Datenbankerstellungsmethode aus führen Sie einen der folgenden Schritte aus:

- Um detaillierte Engine-Optionen festzulegen, wählen Sie Standard erstellen aus.
- Um vorkonfigurierte Optionen zu verwenden, die Best Practices für einen Aurora-Cluster unterstützen, wählen Sie Einfache Erstellung aus.

3. Wählen Sie als Engine-Typ Aurora (PostgreSQL-kompatibel).
4. Wählen Sie Filter anzeigen und danach Versionen anzeigen, welche die Funktion Babelfish für PostgreSQL-Funktion unterstützen, um die Engine-Typen aufzulisten, die Babelfish unterstützen. Babelfish wird derzeit von Aurora PostgreSQL Version 13.4 und höher unterstützt.
5. Für Verfügbare Versionen, wählen Sie eine Aurora-PostgreSQL-Version. Die neuesten Babelfish-Funktionen erhalten Sie, wenn Sie die höchste Aurora-PostgreSQL-Hauptversion auswählen.



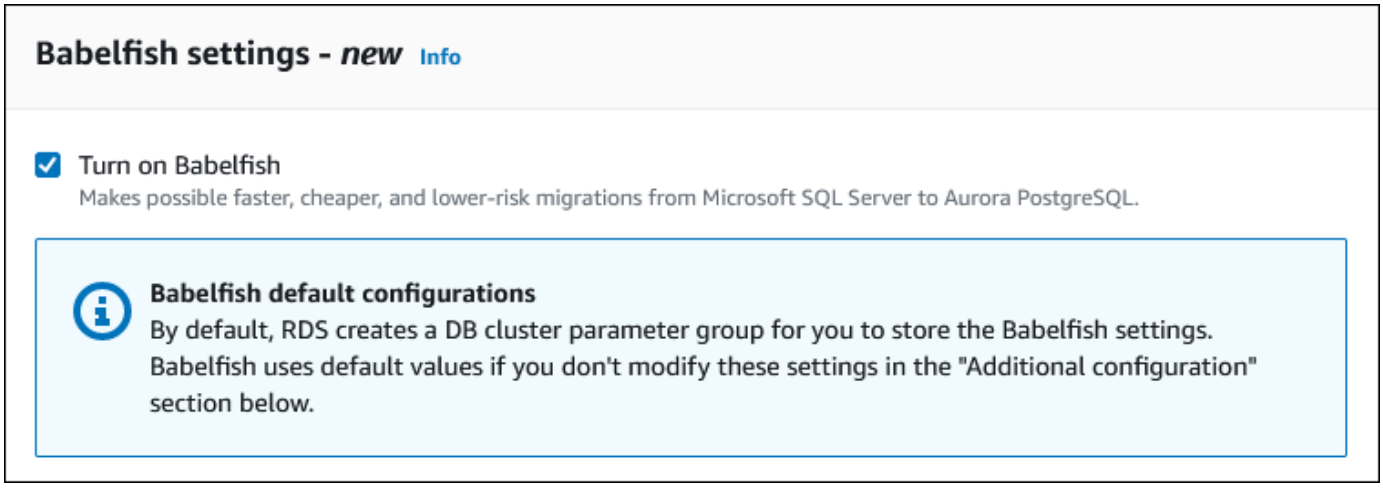
6. Wählen Sie unter Templates (Vorlagen) die Vorlage für Ihr Anwendungsszenario aus.
7. Für DB-Cluster-ID, geben Sie einen Namen ein, den Sie später in der DB-Clusterliste leicht finden können.
8. Für Master username (Masterbenutzername), geben Sie einen Administratorbenutzernamen ein. Der Standardwert für Aurora PostgreSQL ist `postgres`. Sie können den Standardwert akzeptieren oder einen anderen Namen auswählen. Um beispielsweise der Benennungskonvention zu folgen, die in Ihren SQL-Server-Datenbanken verwendet wird, können Sie `sa` (Systemadministrator) als Hauptbenutzername eingeben.

   Wenn Sie keinen Benutzer mit dem Namen `sa` zu diesem Zeitpunkt erstellen, können Sie später einen mit Ihrer Wahl des Kunden erstellen. Verwenden Sie nach dem Erstellen des Benutzers

den Befehl `ALTER SERVER ROLE`, um ihn der `sysadmin`-Gruppe (Rolle) für den Cluster hinzuzufügen.

> **Warning**
>
> Der Master-Benutzername muss immer Kleinbuchstaben verwenden, andernfalls kann der DB-Cluster keine Verbindung zu Babelfish über den TDS-Port herstellen.

9. Erstellen Sie für Master password (Hauptpasswort) ein sicheres Passwort und bestätigen Sie es.
10. Für die folgenden Optionen bis zum Abschnitt Babelfish Einstellungen, geben Sie Ihre DB-Cluster-Einstellungen an. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.
11. Um die Babelfish-Funktionalität verfügbar zu machen, wählen Sie Aktivieren Sie Babelfish aus.



12. Für DB-Cluster-Parametergruppe führen Sie einen der folgenden Schritte aus:

    - Klicken Sie auf Neue erstellen, um eine neue Parametergruppe zu erstellen, bei der Babelfish aktiviert ist.
    - Klicken Sie auf Wählen Sie existierende, um eine vorhandene Parametergruppe zu verwenden. Wenn Sie eine vorhandene Gruppe verwenden, müssen Sie die Gruppe ändern, bevor Sie den Cluster erstellen, und fügen Sie Werte für Babelfish-Parameter hinzu. Informationen zum Festlegen von Parametern finden Sie unter Einstellungen der DB-Cluster-Parametergruppe für Babelfish.

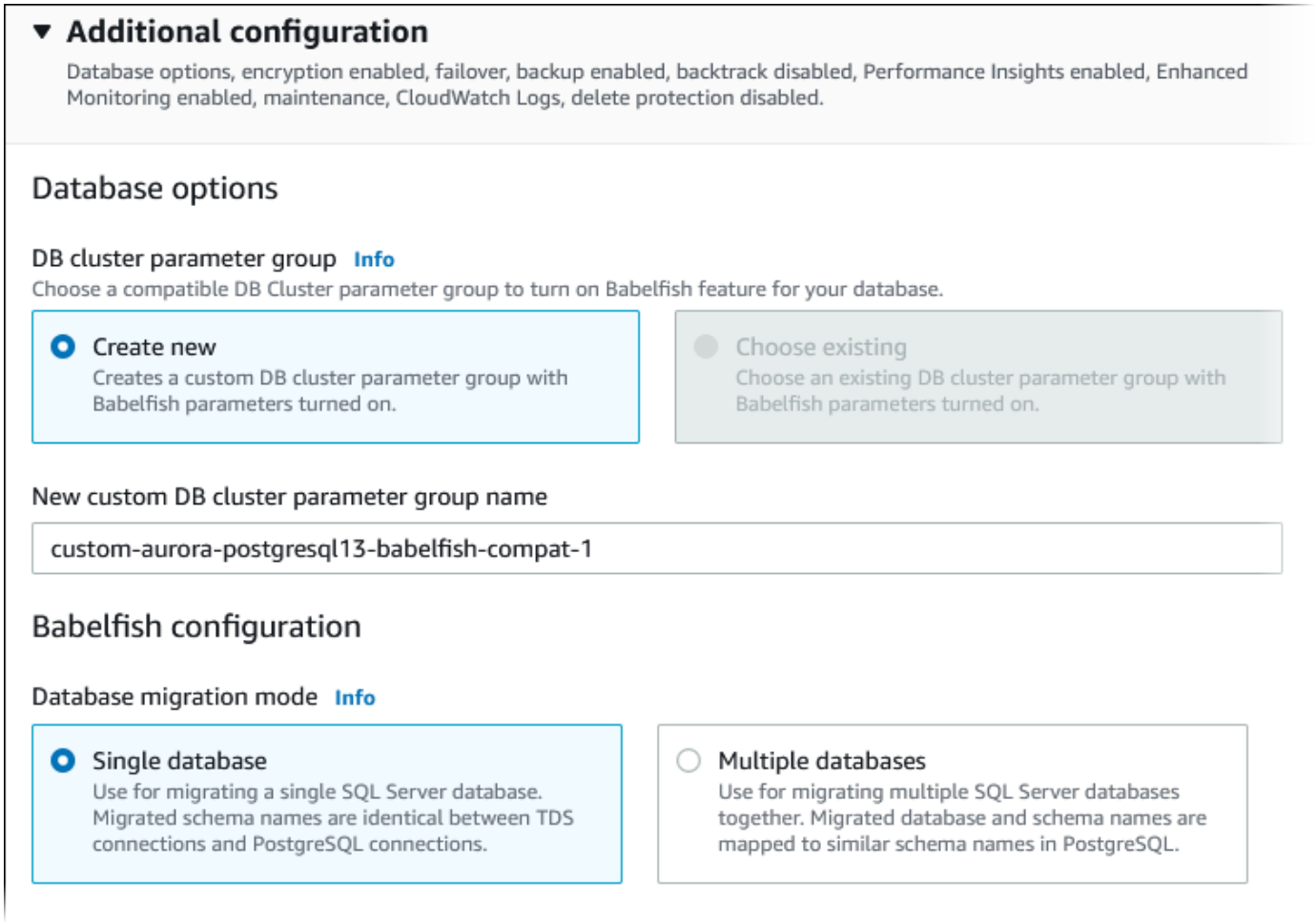
      Wenn Sie eine vorhandene Gruppe verwenden, geben Sie den Gruppennamen in das folgende Feld ein.

13. Wählen Sie für Migration Mode eine der nachstehenden Optionen aus:

- Einzelne Datenbank, um eine einzelne SQL Server-Datenbank zu migrieren.

  In einigen Fällen können Sie mehrere Benutzerdatenbanken zusammen migrieren, wobei Ihr Endziel eine vollständige Migration zur nativen Aurora PostgreSQL ohne Babelfish ist. Wenn die endgültigen Anträge konsolidierte Schemas erfordern (ein einziges dbo-Schema), stellen Sie sicher, dass Sie Ihre SQL Server-Datenbanken zuerst in einer einzigen SQL-Server-Datenbank konsolidieren. Migrieren Sie dann zu Babelfish mit dem Einzelne Datenbank-Modus.
- Mehrere Datenbanken, um mehrere SQL Server-Datenbanken zu migrieren (die aus einer einzigen SQL Server-Installation stammen). Der Mehrfachdatenbankmodus konsolidiert nicht mehrere Datenbanken, die nicht von einer einzigen SQL Server-Installation stammen. Weitere Informationen zum Migrieren mehrerer Datenbanken finden Sie unter Verwenden von Babelfish mit einer einzigen Datenbank oder mehreren Datenbanken.

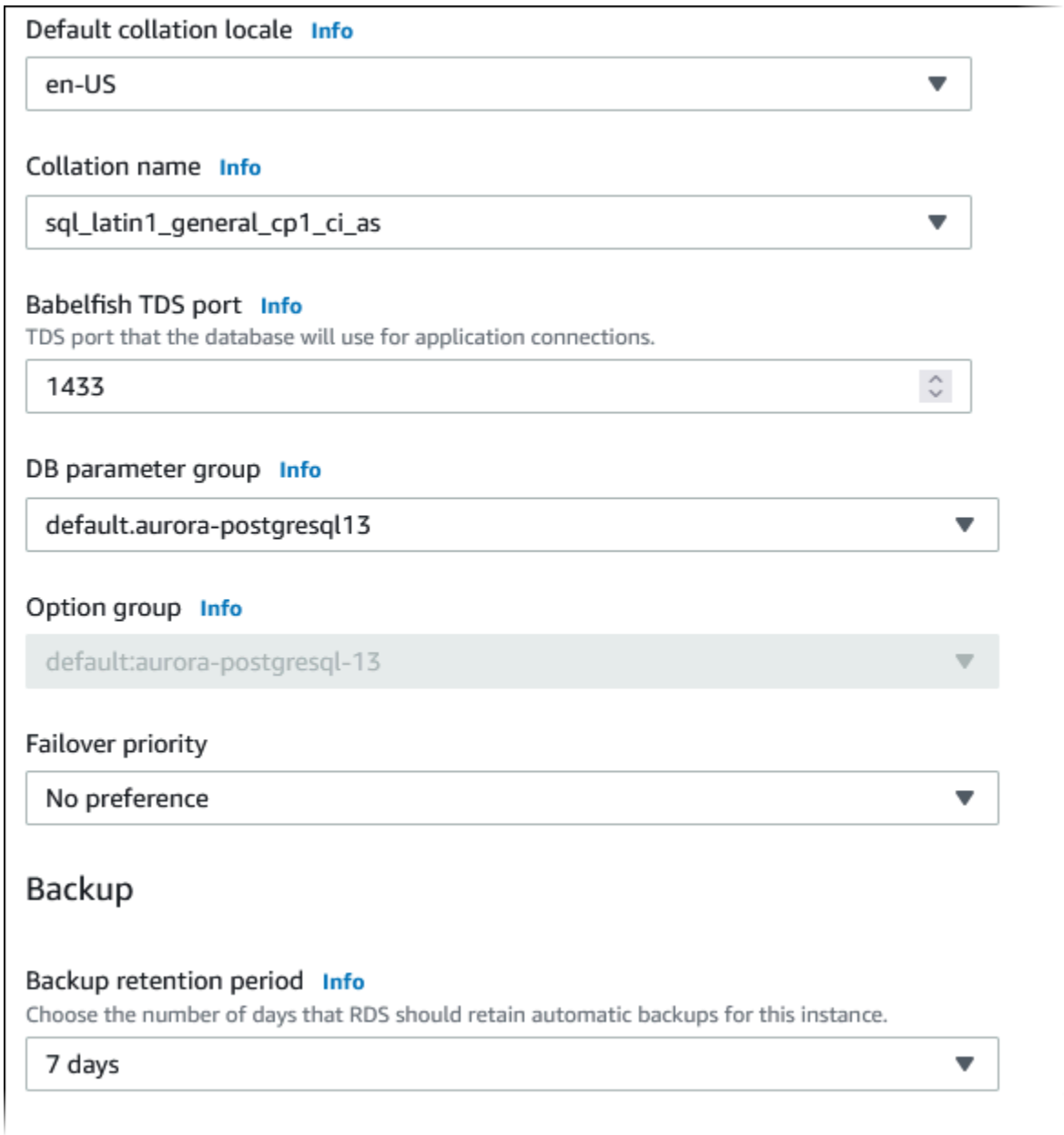
> **Note**
>
> Ab Aurora PostgreSQL 16 Version werden standardmäßig mehrere Datenbanken als Datenbankmigrationsmodus ausgewählt.



14. Für Standardmäßige Sortierreihenfolgen geben Sie das Gebietsschema des Servers ein. Der Standardwert ist `en-US`. Ausführliche Informationen zu Aliassen finden Sie unter Von Babelfish unterstützte Sortierungen.
15. Für Name der Sortierung, geben Sie Ihre Standardsortierung ein. Der Standardwert ist `sql_latin1_general_cp1_ci_as`. Weitere Informationen hierzu finden Sie unter Von Babelfish unterstützte Sortierungen.
16. Geben Sie für den Babelfish TDS-Port den Standardport `1433` ein. Derzeit unterstützt Babelfish nur den Port `1433` für Ihren DB-Cluster.
17. Für DB-Parametergruppe wählen Sie eine Parametergruppe aus oder lassen Sie Aurora eine neue Gruppe mit Standardeinstellungen erstellen.
18. Für Failover priority (Failover-Priorität) wählen Sie eine Failover-Priorität für die Instance aus. Wenn Sie keinen Wert auswählen, wird als Standard `tier-1` gesetzt. Diese Priorität bestimmt die Reihenfolge, in der -Replicas bei der Wiederherstellung nach einem Ausfall der primären

Instance hochgestuft werden. Weitere Informationen finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.

19. Wählen Sie für Aufbewahrungszeitraum für Backups die Dauer (1–35 Tage) aus, die Aurora Backup-Kopien der Datenbank aufbewahrt. Sie können Sicherungskopien für point-in-time Wiederherstellungen (PITR) Ihrer Datenbank bis zur zweiten verwenden. Der Standardaufbewahrungszeitraum beträgt sieben Tage.

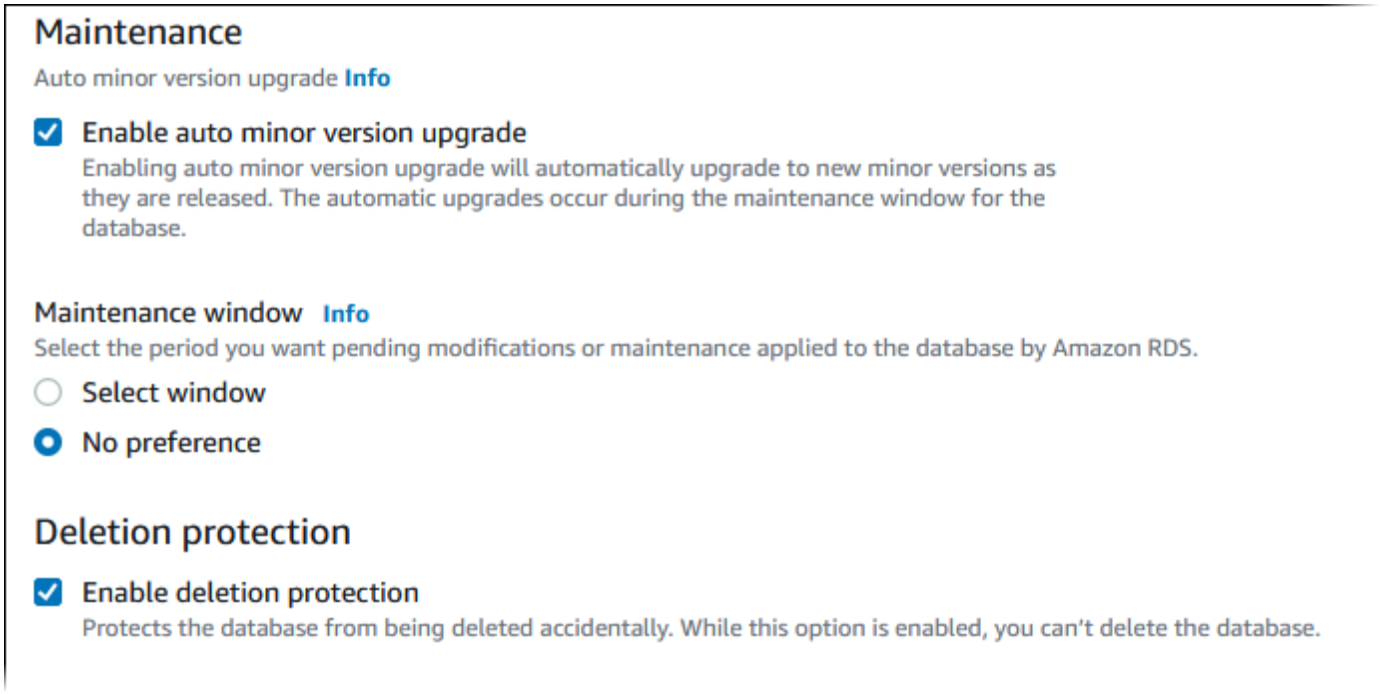


20. Wählen Sie Tags zu Snapshots kopieren, wenn beim Erstellen eines Snapshots DB-Instance-Tags in den DB-Snapshot kopiert werden sollen.

21. Klicken Sie auf Enable encryption (Verschlüsselung aktivieren), um die Verschlüsselung im Ruhezustand (Aurora-Speicherverschlüsselung) für diesen DB-Cluster einzuschalten.
22. Klicken Sie auf Enable Performance Insights (Performance Insights aktivieren), um Amazon RDS Performance Insights zu aktivieren.
23. Wählen Sie Enable enhanced monitoring (Erweiterte Überwachung aktivieren) aus, um die Erfassung von Metriken in Echtzeit für das Betriebssystem zu aktivieren, in dem Ihr DB-Cluster ausgeführt wird.
24. Wählen Sie PostgreSQL-Protokoll aus, um die Protokolldateien in Amazon CloudWatch Logs zu veröffentlichen.
25. Klicken Sie auf Automatischer Unterversion-Upgrade aktivieren, um Ihren Aurora-DB-Cluster automatisch zu aktualisieren, wenn ein Minor-Versions-Upgrade verfügbar ist.
26. Für Maintenance window (Wartungsfenster) gehen Sie wie folgt vor:

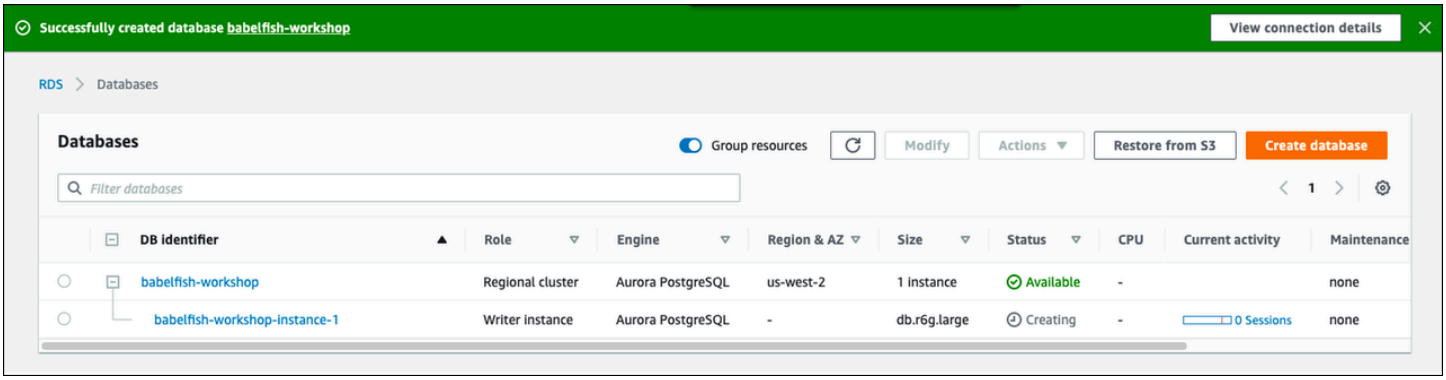
    - Um einen Zeitpunkt auszuwählen, an dem Amazon RDS Änderungen vornehmen oder Wartungsarbeiten durchführen kann, wählen Sie Fenster wählen aus.
    - Um die Amazon RDS-Wartung zu einem ungeplanten Zeitpunkt durchzuführen, wählen Sie Keine Präferenz aus.
27. Wählen Sie Enable deletion protection (Löschschutz aktivieren), um Ihre Datenbank vor versehentlichem Löschen zu schützen.

    Wenn Sie diese Funktion aktivieren, können Sie die Datenbank nicht direkt löschen. Stattdessen müssen Sie den Datenbankcluster ändern und diese Funktion deaktivieren, bevor Sie die Datenbank löschen.



28. Wählen Sie Datenbank erstellen aus.

Ihre neue Datenbank für Babelfish finden Sie in der Auflistung Datenbanken. Die Spalte Status zeigt Verfügbar an, wenn die Bereitstellung abgeschlossen ist.



AWS CLI

Wenn Sie einen Babelfish for Aurora PostgreSQL erstellen: Mit der AWS CLI müssen Sie dem Befehl den Namen der DB-Cluster-Parametergruppe übergeben, die für den Cluster verwendet werden soll. Weitere Informationen finden Sie unter Voraussetzungen für DB-Cluster.

Bevor Sie die AWS CLI verwenden können um einen Aurora-PostgreSQL-Cluster mit Babelfish zu erstellen, gehen Sie wie folgt vor:

- Wählen Sie Ihre Endpunkt-URL aus der Liste der Services unter Amazon Aurora Aurora-Endpunkte und -Kontingente aus.
- Erstellen einer Parametergruppe für das Cluster. Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.
- Ändern Sie die Parametergruppe und fügen Sie den Parameter hinzu, der Babelfish aktiviert.

So erstellen Sie ein Aurora-PostgreSQL-DB-Cluster über die AWS CLI

Die folgenden Beispiele verwenden den standardmäßigen Hauptbenutzernamen, `postgres`. Ersetzen Sie den Namen nach Bedarf durch den Benutzernamen, den Sie für Ihren DB-Cluster erstellt haben, z. B. `sa` bzw. den Benutzernamen, den Sie anstelle des Standardwerts ausgewählt haben.

1. Erstellen Sie eine Parametergruppe.

   Für Linux, macOSoder Unix:

   ```
   aws rds create-db-cluster-parameter-group \
   --endpoint-url endpoint-url \
   --db-cluster-parameter-group-name parameter-group \
   --db-parameter-group-family aurora-postgresql14 \
   --description "description"
   ```

   Windows:

   ```
   aws rds create-db-cluster-parameter-group ^
   --endpoint-url endpoint-URL ^
   --db-cluster-parameter-group-name parameter-group ^
   --db-parameter-group-family aurora-postgresql14 ^
   --description "description"
   ```

2. Ändern Sie Ihre Parametergruppe, um Babelfish zu aktivieren.

   Für Linux, macOSoder Unix:

   ```
   aws rds modify-db-cluster-parameter-group \
   --endpoint-url endpoint-url \
   --db-cluster-parameter-group-name parameter-group \
   ```

```
--parameters
 "ParameterName=rds.babelfish_status,ParameterValue=on,ApplyMethod=pending-reboot"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
--endpoint-url endpoint-url ^
--db-cluster-parameter-group-name paramater-group ^
--parameters
 "ParameterName=rds.babelfish_status,ParameterValue=on,ApplyMethod=pending-reboot"
```

3. Identifizieren Sie Ihre DB-Subnetzgruppe und die Sicherheitsgruppen-ID der Virtual Private Cloud (VPC) für Ihren neuen DB-Cluster und rufen Sie dann den create-db-cluster Befehl auf.

   Für Linux, macOSoder Unix:

   ```
   aws rds create-db-cluster \
   --db-cluster-identifier  cluster-name\
   --master-username postgres \
   --manage-master-user-password \
   --engine aurora-postgresql \
   --engine-version 14.3            \
   --vpc-security-group-ids security-group \
   --db-subnet-group-name subnet-group-name \
   --db-cluster-parameter-group-name parameter-group
   ```

   Windows:

   ```
   aws rds create-db-cluster ^
   --db-cluster-identifier cluster-name ^
   --master-username postgres ^
   --manage-master-user-password ^
   --engine aurora-postgresql ^
   --engine-version 14.3 ^
   --vpc-security-group-ids security-group ^
   --db-subnet-group-name subnet-group ^
   --db-cluster-parameter-group-name parameter-group
   ```

   In diesem Beispiel wird die Option `--manage-master-user-password` zum Generieren des Hauptbenutzerpassworts und zum Verwalten dieses Passworts in Secrets Manager angegeben. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS

Secrets Manager. Alternativ können Sie die Option `--master-password` verwenden, um das Passwort selbst festzulegen und zu verwalten.

4. Erstellen Sie die primäre Instance für Ihren DB-Cluster explizit. Verwenden Sie den Namen des Clusters, den Sie in Schritt 3 erstellt haben, als `--db-cluster-identifier` Argument, wenn Sie den create-db-instance Befehl aufrufen, wie im Folgenden gezeigt.

   Für Linux, macOSoder Unix:

```
aws rds create-db-instance \
--db-instance-identifier instance-name \
--db-instance-class db.r6g \
--db-subnet-group-name subnet-group \
--db-cluster-identifier cluster-name \
--engine aurora-postgresql
```

   Windows:

```
aws rds create-db-instance ^
--db-instance-identifier instance-name ^
--db-instance-class db.r6g ^
--db-subnet-group-name subnet-group ^
--db-cluster-identifier cluster-name ^
--engine aurora-postgresql
```

Migrieren einer SQL-Server-Datenbank zu Babelfish for Aurora PostgreSQL

Sie können Babelfish for Aurora PostgreSQL verwenden, um die Migration einer SQL-Server-Datenbank zu einem DB-Cluster von Amazon Aurora PostgreSQL zu erleichtern. Vor der Migration überprüfen Sie Verwenden von Babelfish mit einer einzigen Datenbank oder mehreren Datenbanken.

Themen

Übersicht über den Migrationsprozess

In der folgenden Zusammenfassung sind die Schritte aufgeführt, die erforderlich sind, damit Ihre SQL-Server-Anwendung mit Babelfish arbeiten kann. Informationen zu den Tools, die Sie für die Export- und Importprozesse verwenden können, sowie weitere Informationen finden Sie unter Importieren/Exportieren von Tools für die Migration von SQL Server zu Babelfish. Zum Laden der Daten empfehlen wir die Verwendung AWS DMS mit einem Aurora PostgreSQL-DB-Cluster als Zielendpunkt.

1. Erstellen Sie einen neuen DB-Cluster von Aurora PostgreSQL und lassen Sie Babelfish aktiviert. Um zu erfahren wie dies geht, vgl. Erstellen eines DB-Clusters von Babelfish for Aurora PostgreSQL.

   Um die verschiedenen SQL-Artefakte zu importieren, die aus Ihrer SQL-Server-Datenbank exportiert werden, verbinden Sie sich mithilfe eines nativen SQL-Server-Tools wie sqlcmd mit dem Babelfish-Cluster. Weitere Informationen finden Sie unter Verbinden mit Ihrem DB-Cluster mithilfe eines SQL Server-Clients.
2. Exportieren Sie die Datendefinitionssprache (DDL) in Ihrer SQL-Server-Datenbank, die Sie migrieren möchten. Die DDL ist SQL-Code, der Datenbankobjekte beschreibt, die Benutzerdaten (wie Tabellen, Indizes und Ansichten) und vom Benutzer geschriebenen Datenbankcode (wie gespeicherte Prozeduren, benutzerdefinierte Funktionen und Trigger) enthalten.

   Weitere Informationen finden Sie unter Migrieren zu Babelfish mit SQL Server Management Studio (SSMS).
3. Führen Sie ein Bewertungstool aus, um den Umfang aller Änderungen zu bewerten, die Sie möglicherweise vornehmen müssen, damit Babelfish die auf SQL Server ausgeführte Anwendung

effektiv unterstützen kann. Weitere Informationen finden Sie unter Auswertung und Handhabung von Unterschieden zwischen SQL Server und Babelfish.

4. Überprüfen Sie die Einschränkungen des AWS DMS Zielendpunkts und aktualisieren Sie das DDL-Skript nach Bedarf. Weitere Informationen finden Sie unter Einschränkungen bei der Verwendung eines PostgreSQL-Zielendpunkts mit Babelfish-Tabellen in Verwenden von Aurora PostgreSQL als Ziel.
5. Führen Sie die DDL auf Ihrem neuen Babelfish-DB-Cluster innerhalb Ihrer angegebenen T-SQL-Datenbank aus, um nur die Schemas, benutzerdefinierten Datentypen und Tabellen mit ihren Primärschlüsseleinschränkungen zu erstellen.
6. Wird verwendet AWS DMS , um Ihre Daten von SQL Server zu Babelfish-Tabellen zu migrieren. Verwenden Sie für die kontinuierliche Replikation mit Change Data Capture bei SQL Server oder SQL Replication Aurora PostgreSQL anstelle von Babelfish als Endpunkt. Informationen dazu finden Sie im Artikel Verwendung von Babelfish für Aurora PostgreSQL als Ziel für AWS Database Migration Service.
7. Wenn das Laden der Daten abgeschlossen ist, erstellen Sie alle verbleibenden T-SQL-Objekte, die die Anwendung auf Ihrem Babelfish-Cluster unterstützen.
8. Konfigurieren Sie Ihre Client-Anwendung neu, um eine Verbindung mit dem Babelfish-Endpunkt statt mit der SQL-Server-Datenbank herzustellen. Weitere Informationen finden Sie unter Verbinden mit einem Babelfish-DB-Cluster.
9. Ändern Sie Ihre Anwendung nach Bedarf und testen Sie sie erneut. Weitere Informationen finden Sie unter Unterschiede zwischen Babelfish für Aurora PostgreSQL und SQL Server.

Sie müssen nach wie vor Ihre clientseitigen SQL-Abfragen bewerten. Die aus Ihrer SQL-Server-Instance generierten Schemas konvertieren nur den serverseitigen SQL-Code. Wir empfehlen, die folgenden Schritte auszuführen:

- Erfassen Sie clientseitige Abfragen mit dem SQL Server Profiler anhand der vordefinierten Vorlage TSQL_Replay. Diese Vorlage erfasst Informationen zu T-SQL-Anweisungen, die Sie dann für iterative Optimierung und Tests wiedergeben können. Sie können den Profiler über das Menü Tools in SQL Server Management Studio starten. Klicken Sie auf SQL Server Profiler, um den Profiler zu öffnen und die Vorlage TSQL_Replay auszuwählen.

  Zur Verwendung für Ihre Babelfish-Migration starten Sie eine Nachverfolgung und führen Sie Ihre Anwendung dann mit Ihren Funktionstests aus. Der Profiler erfasst die T-SQL-Anweisungen. Stoppen Sie nach dem Abschluss des Tests die Nachverfolgung. Speichern Sie das Ergebnis mit

Ihren clientseitigen Abfragen in einer XML-Datei (File (Datei) > Save as (Speichern unter) > Trace XML File for Replay (XML-Datei für Wiederholung nachverfolgen)).

Weitere Informationen finden Sie unter SQL Server Profiler in der Microsoft-Dokumentation. Weitere Informationen zur TSQL_Replay-Vorlage finden Sie unter Vorlagen für SQL Server Profiler.

- Für Anwendungen mit komplexen clientseitigen SQL-Abfragen empfehlen wir Ihnen, diese mit Babelfish Compass auf Babelfish-Kompatibilität zu analysieren. Wenn die Analyse ergibt, dass die clientseitigen SQL-Anweisungen nicht unterstützte SQL-Funktionen enthalten, überprüfen Sie die SQL-Aspekte in der Clientanwendung und nehmen Sie ggf. Änderungen vor.
- Sie können die SQL-Abfragen auch als erweiterte Ereignisse (XEL-Format) erfassen. Verwenden Sie dazu den SSMS XEvent Profiler. Nachdem Sie die XEL-Datei generiert haben, extrahieren Sie die SQL-Anweisungen in XML-Dateien, die Compass dann verarbeiten kann. Weitere Informationen finden Sie unter Verwenden des SSMS XEvent Profilers in der Microsoft-Dokumentation.

Wenn Sie mit allen Tests, Analysen und Änderungen an Ihrer migrierten Anwendung zufrieden sind, können Sie Ihre Babelfish-Datenbank für die Produktion verwenden. Beenden Sie dazu die ursprüngliche Datenbank und leiten Sie Live-Clientanwendungen auf den Babelfish-TDS-Port um.

> **Note**
>
> AWS DMS unterstützt jetzt das Replizieren von Daten aus Babelfish. Weitere Informationen finden Sie unter Unterstützt AWS DMS jetzt Babelfish for Aurora PostgreSQL als Quelle.

Auswertung und Handhabung von Unterschieden zwischen SQL Server und Babelfish

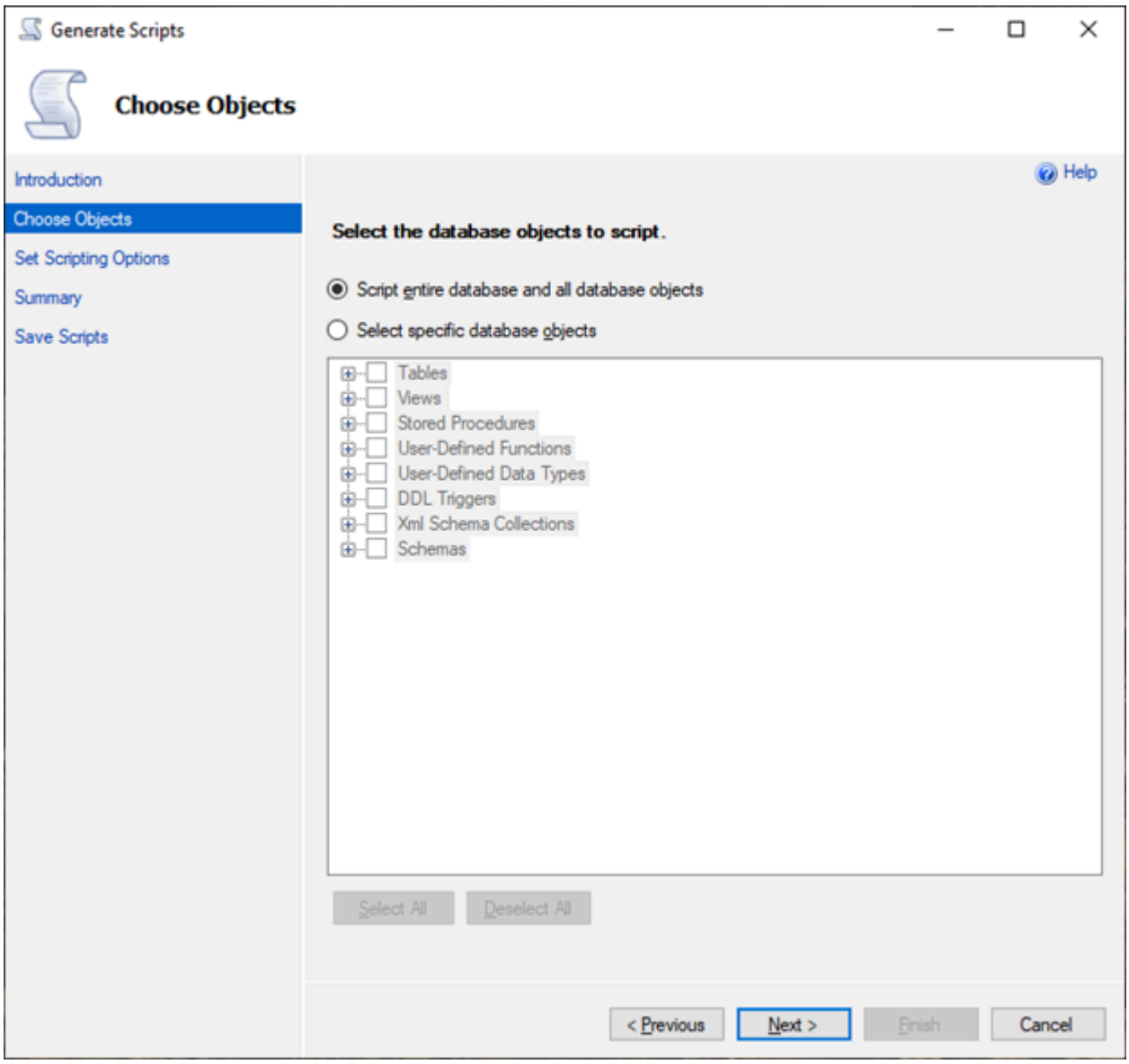
Für beste Ergebnisse empfehlen wir Ihnen, den generierten DDL/DML und den Client-Abfragecode auszuwerten, bevor Sie Ihre SQL-Server-Datenbankanwendung tatsächlich zu Babelfish migrieren. Abhängig von der Babelfish-Version und den spezifischen Funktionen von SQL Server, die Ihre Anwendung implementiert, müssen Sie möglicherweise Ihre Anwendung umgestalten oder Alternativen für Funktionen verwenden, die in Babelfish nicht vollständig unterstützt werden.

- Verwenden Sie zur Bewertung Ihres SQL-Server-Anwendungscodes Babelfish Compass für die generierte DDL, um festzustellen, wie viel T-SQL-Code von Babelfish unterstützt wird. Identifizieren Sie T-SQL-Code, für den vor der Ausführung in Babelfish möglicherweise Änderungen erforderlich sind. Weitere Informationen zu diesem Tool finden Sie unter Babelfish Compass Tool auf. GitHub

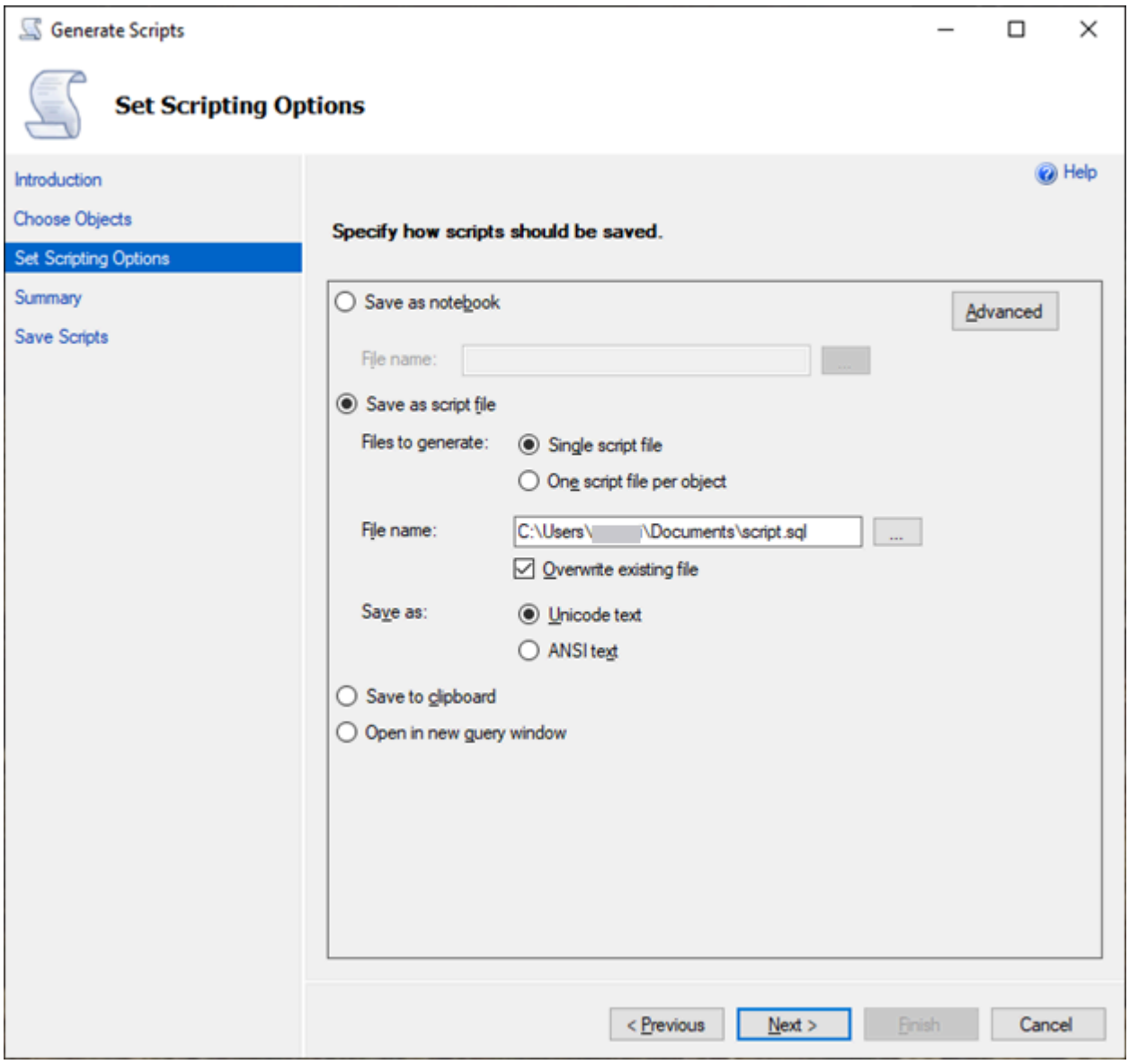
> **Note**
>
> Babelfish Compass ist ein Open-Source-Tool. Melde alle Probleme mit Babelfish Compass über den Support GitHub statt über den AWS Support.

Sie können den Generate Script Wizard mit SQL Server Management Studio (SSMS) verwenden, um die SQL-Datei zu generieren, die von Babelfish Compass oder CLI bewertet wird. AWS Schema Conversion Tool Wir empfehlen die folgenden Schritte, um die Bewertung zu optimieren.

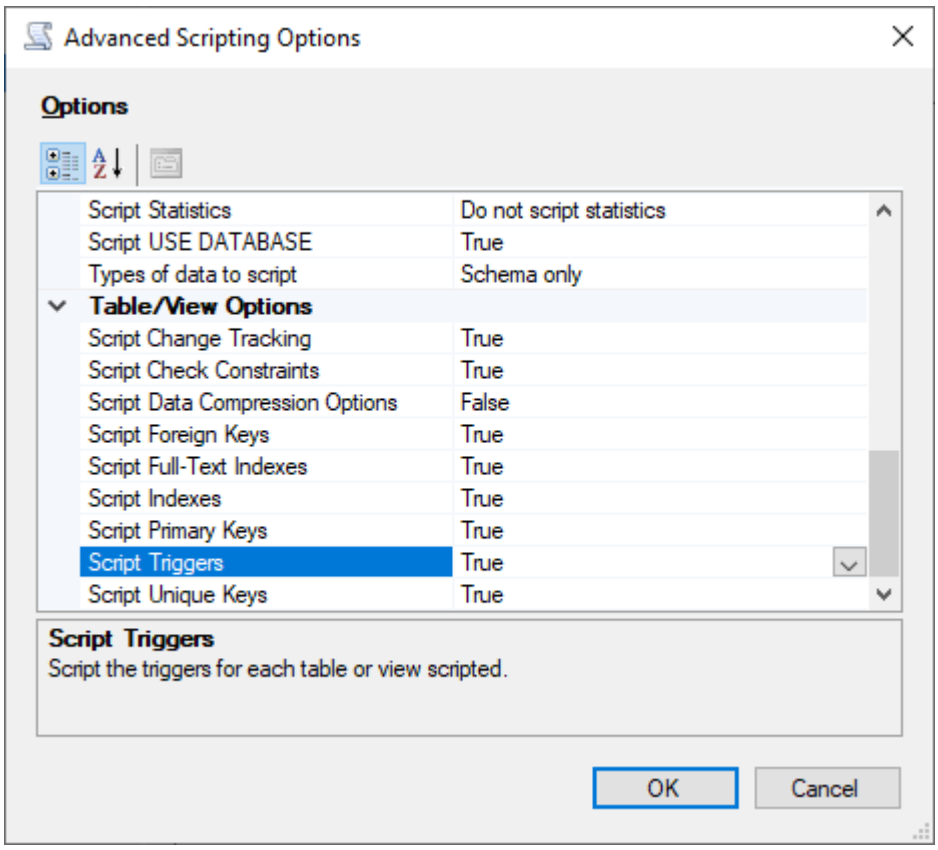
1. Wählen Sie auf der Seite Choose Objects (Objekte auswählen) die Option Script entire database and all database objects (Gesamte Datenbank und alle Datenbankobjekte in das Skript aufnehmen) aus.



2. Wählen Sie für Set Scripting Options (Scripting-Optionen festlegen) die Option Save as script file (Als Skriptdatei speichern) und Single script file (Einzelne Skriptdatei) aus.



3. Wählen Sie Advanced (Erweitert) aus, um die standardmäßigen Scripting-Optionen zu ändern und Funktionen zu identifizieren, die für eine vollständige Bewertung normalerweise auf „False“ (Falsch) festgelegt sind:
   - Skriptänderungsverfolgung auf „True“ (Wahr)
   - Skriptvolltextindizes auf „True“ (Wahr)
   - Skriptauslöser auf „True“ (Wahr)
   - Skriptanmeldungen auf „True“ (Wahr)
   - Skripteigentümer auf „True“ (Wahr)
   - Skriptberechtigungen auf Objektebene auf „True“ (Wahr)
   - Skriptsortierungen auf „True“ (Wahr)



4. Führen Sie die restlichen Schritte im Assistenten aus, um die Datei zu generieren.

Importieren/Exportieren von Tools für die Migration von SQL Server zu Babelfish

Wir empfehlen die Verwendung AWS DMS als primäres Tool für die Migration von SQL Server zu Babelfish. Babelfish unterstützt jedoch verschiedene andere Möglichkeiten, Daten mithilfe von SQL-Server-Tools zu migrieren, darunter die folgenden.

- SQL Server Integration Services (SSIS) für alle Versionen von Babelfish. Weitere Informationen finden Sie unter Migration von SQL Server zu Aurora PostgreSQL mit SSIS und Babelfish.
- Verwenden Sie den Import/Export-Assistenten von SSMS für Babelfish-Versionen 2.1.0 und höher. Dieses Tool ist nicht nur über das SSMS, sondern auch als eigenständiges Tool verfügbar. Weitere Informationen finden Sie unter Willkommen beim SQL-Server-Assistenten für Import und Export in der Microsoft-Dokumentation.
- Mit dem Microsoft-Dienstprogramm zum Kopieren von Massendaten (bcp) können Sie Daten einer Instance von Microsoft SQL Server in eine Datendatei im von Ihnen angegebenen Format kopieren. Weitere Informationen finden Sie unter bcp-Hilfsprogramm in der Microsoft-Dokumentation. Babelfish unterstützt jetzt die Datenmigration mit dem BCP-Client und das bcp-

Dienstprogramm unterstützt jetzt `-E`-Flags (für Identitätsspalten) und -b-Flags (für stapelweise Einfügungen). Bestimmte bcp-Optionen werden nicht unterstützt, einschließlich `-C`, `-T`, `-G`, `-K`, `-R`, `-V` und `-h`.

Migrieren zu Babelfish mit SQL Server Management Studio (SSMS)

Wir empfehlen, separate Dateien für jeden der spezifischen Objekttypen zu generieren. Sie können den Assistenten zum Generieren von Skripts in SSMS zunächst für jeden Satz von DDL-Anweisungen verwenden und dann die Objekte als Gruppe ändern, um alle während der Bewertung festgestellten Probleme zu beheben.

Führen Sie diese Schritte aus, um die Daten mithilfe von AWS DMS oder anderen Datenmigrationsmethoden zu migrieren. Führen Sie zuerst diese Methoden zum Erstellen von Skripts aus, um die Daten schneller und besser in die Babelfish-Tabellen in Aurora PostgreSQL zu laden.

1. Führen Sie `CREATE SCHEMA`-Anweisungen aus.
2. Führen Sie `CREATE TYPE`-Anweisungen aus, um benutzerdefinierte Datentypen zu erstellen.
3. Führen Sie grundlegende `CREATE TABLE`-Anweisungen mit den Primärschlüsseln oder eindeutigen Einschränkungen aus.

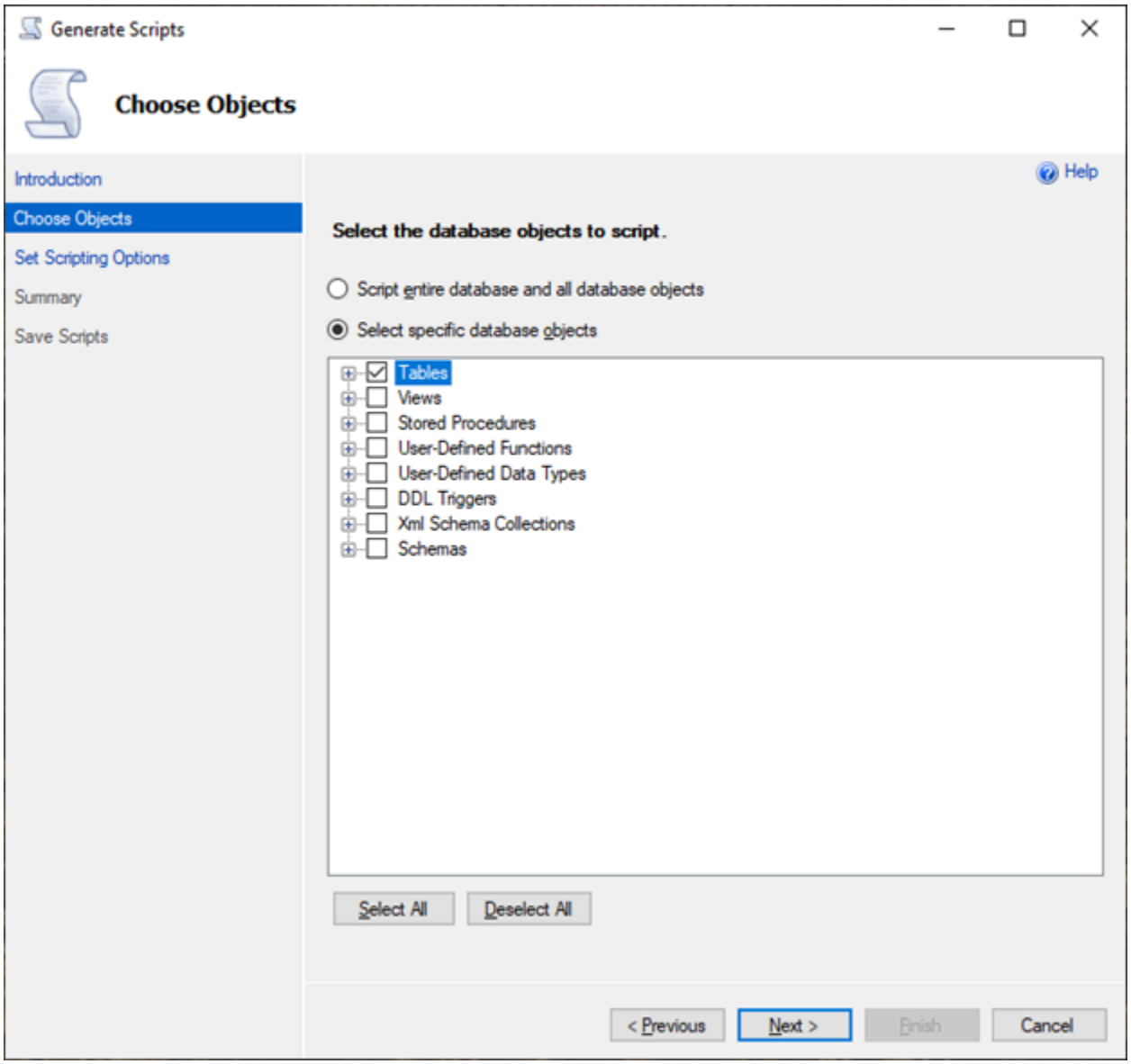
Führen Sie das Laden der Daten mit dem empfohlenen Import-/Export-Tool durch. Führen Sie die geänderten Skripts für die folgenden Schritte aus, um die verbleibenden Datenbankobjekte hinzuzufügen. Sie benötigen die Create-Table-Anweisungen, um diese Skripts für die Einschränkungen, Auslöser und Indizes auszuführen. Nachdem die Skripts generiert wurden, löschen Sie die Create-Table-Anweisungen.

1. Führen Sie `ALTER TABLE`-Anweisungen für die Prüfbeschränkungen, Fremdschlüsseleinschränkungen und Standardeinschränkungen aus.
2. Führen Sie `CREATE TRIGGER`-Anweisungen aus.
3. Führen Sie `CREATE INDEX`-Anweisungen aus.
4. Führen Sie `CREATE VIEW`-Anweisungen aus.
5. Führen Sie `CREATE STORED PROCEDURE`-Anweisungen aus.

So generieren Sie Skripts für jeden Objekttyp

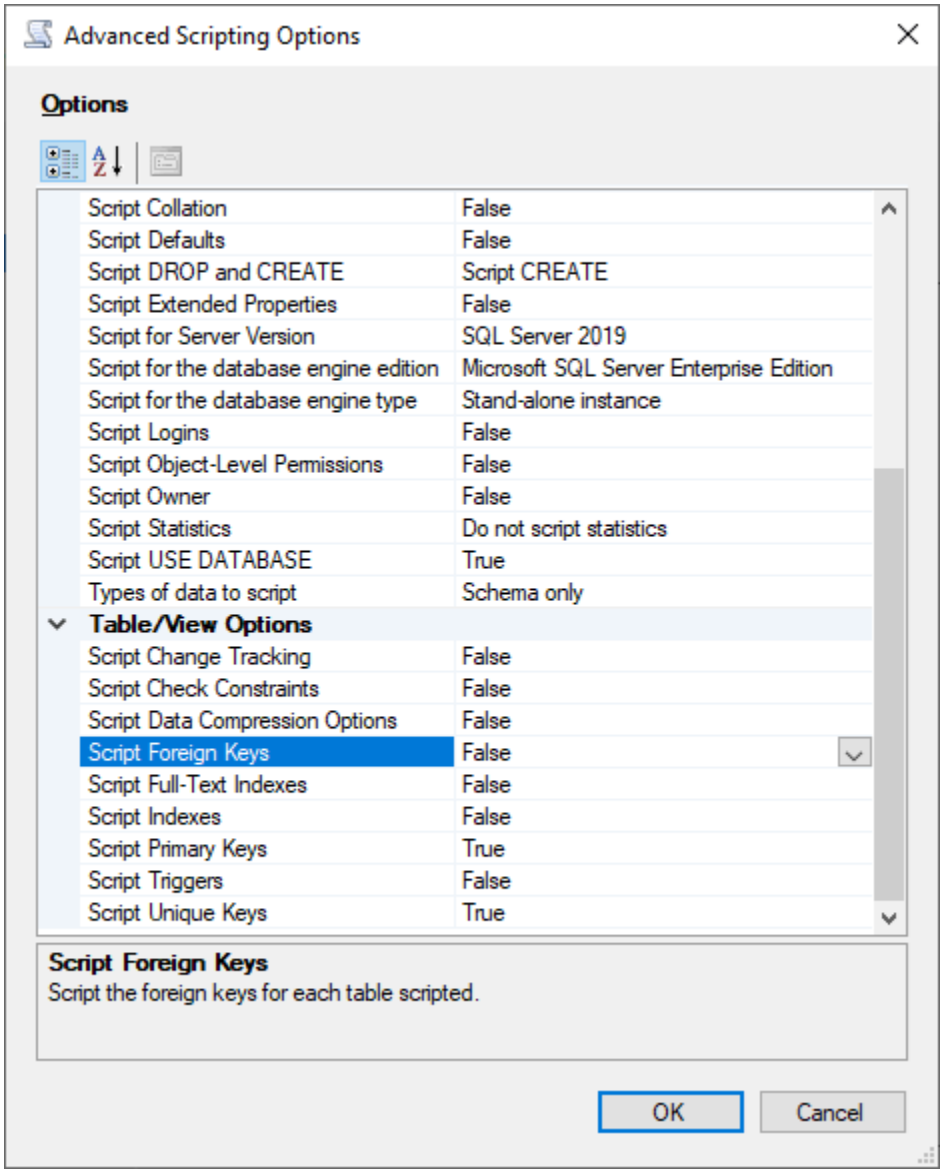
Führen Sie die folgenden Schritte aus, um die grundlegenden Create-Table-Anweisungen mithilfe des Assistenten zum Erstellen von Skripts in SSMS zu erstellen. Führen Sie die gleichen Schritte aus, um Skripts für die verschiedenen Objekttypen zu generieren.

1. Stellen Sie eine Verbindung zu Ihrer vorhandenen SQL-Server-Instance her.
2. Öffnen Sie das Kontextmenü (rechte Maustaste) für einen Datenbanknamen.
3. Wählen Sie Tasks (Aufgaben) und dann Generate Scripts... (Skripts generieren).
4. Klicken Sie im Bereich Choose Objects (Objekte auswählen) auf Select specific database objects (Bestimmte Datenbankobjekte auswählen). Klicken Sie auf Tables (Tabellen) und wählen Sie alle Tabellen aus. Wählen Sie Next (Weiter), um fortzufahren.

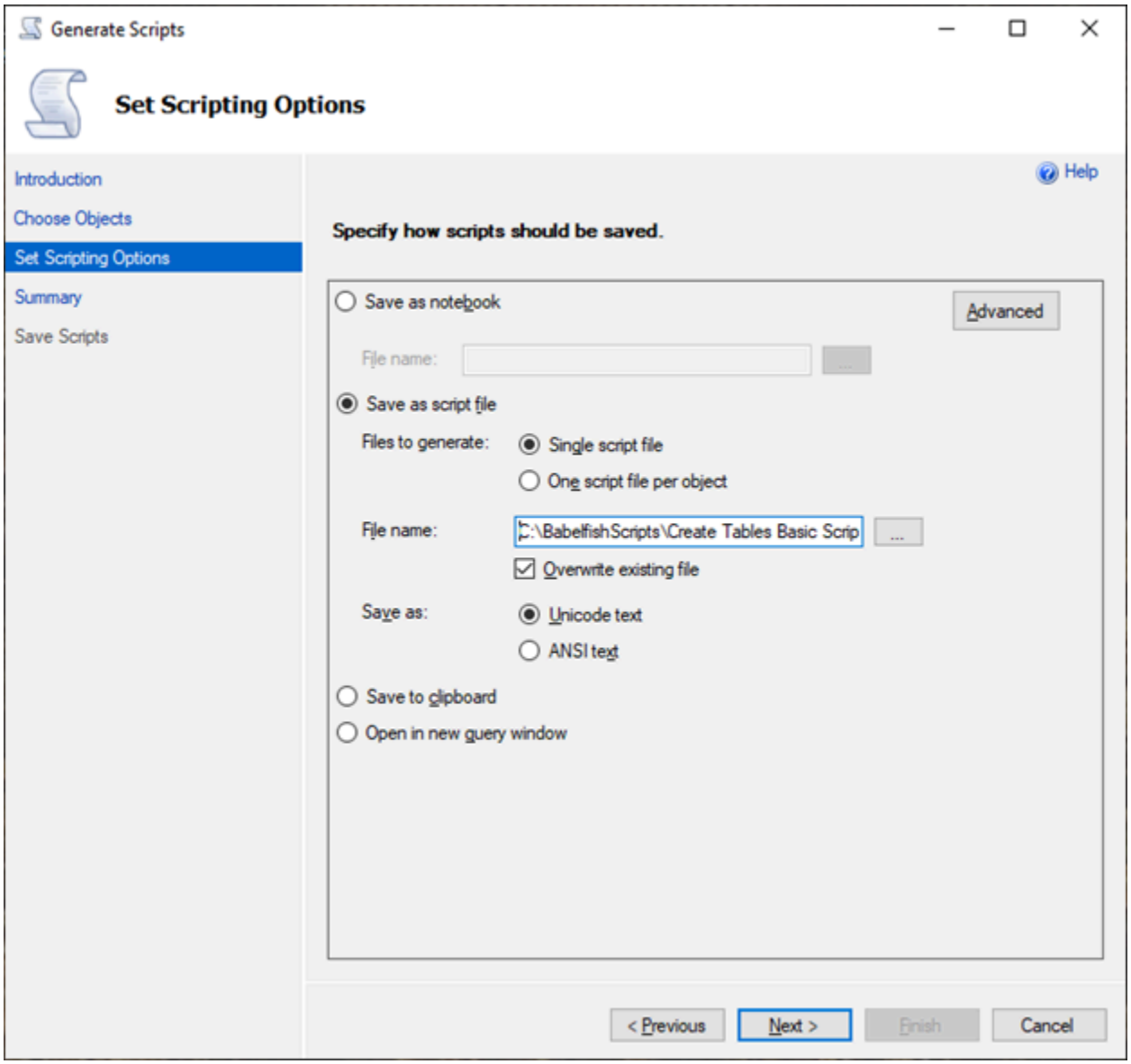


5. Wählen Sie auf der Seite Set Scripting Options (Scripting-Optionen festlegen) die Option Advanced (Erweitert) aus, um die Einstellungen Options (Optionen) zu öffnen. Um die grundlegenden Create-Table-Anweisungen zu generieren, ändern Sie die folgenden Standardwerte:

   - „Script Defaults“ (Skriptstandardwerte) auf „False“ (Falsch).
   - „Script Extended Properties“ (Erweiterte Skripteigenschaften) auf „False“ (Falsch). Babelfish unterstützt keine erweiterten Eigenschaften.
   - „Script Check Constraints“ (Skriptprüfeinschränkungen) auf „False“ (Falsch). „Script Foreign Keys“ (Skriptfremdschlüssel) auf „False“ (Falsch).



6. Wählen Sie OK aus.
7. Wählen Sie auf der Seite Set Scripting Options (Scripting-Optionen festlegen) die Option Save as script file (Als Skriptdatei speichern) und dann die Option Single script file (Einzelne Skriptdatei) aus. Geben Sie unter File name (Dateiname) einen Namen ein.



8. Wählen Sie Next (Weiter) aus, um die Seite Summary wizard (Übersichtsassistent) aufzurufen.
9. Wählen Sie Next (Weiter) aus, um die Skriptgenerierung zu starten.

   Sie können mit dem Generieren von Skripten für die anderen Objekttypen im Assistenten fortfahren. Anstatt nach dem Speichern der Datei Finish (Beenden) auszuwählen, klicken Sie dreimal auf die Schaltfläche Previous (Zurück), um zur Seite Choose Objects (Objekte

auswählen) zurückzukehren. Wiederholen Sie dann die Schritte im Assistenten, um Skripten für die anderen Objekttypen zu generieren.

Datenbankauthentifizierung mit Babelfish für Aurora PostgreSQL

Babelfish für Aurora PostgreSQL unterstützt zwei Möglichkeiten zum Authentifizieren von Datenbankbenutzern. Die Passwort-Authentifizierung ist standardmäßig für alle Babelfish-DB-Cluster verfügbar. Sie können auch Kerberos-Authentifizierung für denselben DB-Cluster hinzufügen.

Themen

Passwort-Authentifizierung mit Babelfish

Babelfish for Aurora PostgreSQL unterstützt die Passwortauthentifizierung. Passwörter werden verschlüsselt auf der Festplatte gespeichert. Weitere Informationen über die Authentifizierung in einem Aurora-PostgreSQL-Cluster finden Sie unter Sicherheit in Amazon Aurora PostgreSQL.

Sie werden möglicherweise jedes Mal aufgefordert, wenn Sie eine Verbindung zu Babelfish herstellen. Jeder Benutzer, der zu Aurora PostgreSQL migriert oder auf Aurora erstellt wurde, kann dieselben Anmeldeinformationen sowohl am SQL Server-Port als auch am PostgreSQL-Port verwenden. Babelfish erzwingt keine Passwortrichtlinien, aber wir empfehlen Ihnen, Folgendes zu tun:

- Es muss sich um ein komplexes Passwort mit mindestens acht (8) Zeichen handeln.
- Durchsetzen einer Richtlinie zum Ablauf des Kennworts.

Verwenden Sie den Befehl `SELECT * FROM pg_user;`, um eine vollständige Liste der Datenbankbenutzer zu überprüfen.

Kerberos-Authentifizierung mit Babelfish

Die Version 15.2 von Babelfish für Aurora PostgreSQL unterstützt die Authentifizierung bei Ihrem DB-Cluster mithilfe von Kerberos. Diese Methode ermöglicht es Ihnen, die Microsoft Windows-Authentifizierung zum Authentifizieren von Benutzern zu verwenden, wenn diese eine Verbindung mit Ihrer Babelfish-Datenbank herstellen. Dazu müssen Sie Ihren DB-Cluster so konfigurieren, dass AWS Directory Service for Microsoft Active Directory für die Kerberos-Authentifizierung verwendet wird. Weitere Informationen finden Sie unter Was ist AWS Directory Service im AWS Directory Service-Administratorhandbuch.

Einrichten der Kerberos-Authenifizierung

Der DB-Cluster von Babelfish für Aurora PostgreSQL kann eine Verbindung über zwei verschiedene Ports herstellen, die Einrichtung der Kerberos-Authentifizierung ist jedoch ein einmaliger Vorgang. Daher müssen Sie zuerst die Kerberos-Authentifizierung für Ihren DB-Cluster einrichten. Weitere Informationen finden Sie unter Einrichten der Kerberos-Authentifizierung. Stellen Sie nach Abschluss der Einrichtung sicher, dass Sie mithilfe von Kerberos eine Verbindung mit einem PostgreSQL-Client herstellen können. Weitere Informationen finden Sie unter Herstellen einer Verbindung mithilfe der Kerberos-Authentifizierung.

Anmeldung und Benutzerbereitstellung in Babelfish

Windows-Anmeldungen, die über den Tabular Data Stream (TDS)-Port erstellt wurden, können entweder mit dem TDS-Port oder dem PostgreSQL-Port verwendet werden. Zunächst muss die Anmeldung, die Kerberos für die Authentifizierung verwenden kann, vom TDS-Port aus bereitgestellt werden, bevor sie von den T-SQL-Benutzern und -Anwendungen genutzt werden, um eine Verbindung mit einer Babelfish-Datenbank herzustellen. Beim Erstellen von Windows-Anmeldungen können Administratoren die Anmeldung entweder mit dem DNS-Domain-Namen oder dem NetBIOS-Domain-Namen angeben. In der Regel ist die NetBIOS-Domain die Subdomain des DNS-Domain-Namens. Wenn der DNS-Domain-Name beispielsweise `CORP.EXAMPLE.COM` lautet, kann die NetBIOS-Domain `CORP` sein. Wenn das NetBIOS-Domain-Namenformat für eine Anmeldung bereitgestellt wird, muss eine Zuordnung zum DNS-Domain-Namen vorhanden sein.

Verwalten der Zuordnung von NetBIOS-Domain-Namen zum DNS-Domain-Namen

Um Zuordnungen zwischen dem NetBIOS-Domain-Namen und dem DNS-Domain-Namen zu verwalten, bietet Babelfish gespeicherte Systemprozeduren zum Hinzufügen, Entfernen und Kürzen von Zuordnungen. Nur ein Benutzer mit einer `sysadmin`-Rolle kann diese Verfahren ausführen.

Verwenden Sie die von Babelfish bereitgestellte gespeicherte Systemprozedur `babelfish_add_domain_mapping_entry`, um eine Zuordnung zwischen NetBIOS und DNS-Domain-Namen zu erstellen. Beide Argumente müssen einen gültigen Wert haben und dürfen nicht NULL sein.

Example

```
EXEC babelfish_add_domain_mapping_entry 'netbios_domain_name',
 'fully_qualified_domain_name'
```

Das folgende Beispiel zeigt, wie die Zuordnung zwischen dem NetBIOS-Namen CORP und dem DNS-Domain-Namen CORP.EXAMPLE.COM erstellt wird.

Example

```
EXEC babelfish_add_domain_mapping_entry 'corp', 'corp.example.com'
```

Verwenden Sie die gespeicherte Systemprozedur „babelfish_remove_domain_mapping_entry“, um einen vorhandenen Zuordnungseintrag zu löschen.

Example

```
EXEC babelfish_remove_domain_mapping_entry 'netbios_domain_name'
```

Das folgende Beispiel zeigt, wie Sie die Zuordnung für den NetBIOS-Namen CORP entfernen.

Example

```
EXEC babelfish_remove_domain_mapping_entry 'corp'
```

Verwenden Sie die gespeicherte Systemprozedur babelfish_truncate_domain_mapping_table, um alle vorhandenen Zuordnungseinträge zu löschen:

Example

```
EXEC babelfish_truncate_domain_mapping_table
```

Verwenden Sie die folgende Abfrage, um alle Zuordnungen zwischen NetBIOS und dem DNS-Domain-Namen anzuzeigen.

Example

```
SELECT netbios_domain_name, fq_domain_name FROM babelfish_domain_mapping;
```

Verwalten von Anmeldungen

Erstellen von Anmeldungen

Stellen Sie über den TDS-Endpunkt eine Verbindung mit der DB her, indem Sie eine Anmeldung verwenden, die über die entsprechenden Berechtigungen verfügt. Wenn kein Datenbankbenutzer für die Anmeldung angelegt wurde, wird die Anmeldung dem Gastbenutzer zugeordnet. Wenn der Gastbenutzer nicht aktiviert ist, schlägt der Anmeldeversuch fehl.

Erstellen Sie eine Windows-Anmeldung mit der folgenden Abfrage. Die Option `FROM WINDOWS` ermöglicht die Authentifizierung mit Active Directory.

```
CREATE LOGIN login_name FROM WINDOWS [WITH DEFAULT_DATABASE=database]
```

Example

Das folgende Beispiel zeigt das Erstellen einer Anmeldung für den Active Directory-Benutzer [corp \test1] mit der Standarddatenbank db1.

```
CREATE LOGIN [corp\test1] FROM WINDOWS WITH DEFAULT_DATABASE=db1
```

In diesem Beispiel wird davon ausgegangen, dass eine Zuordnung zwischen der NetBIOS-Domain CORP und dem DNS-Domain-Namen CORP.EXAMPLE.COM besteht. Wenn es keine Zuordnung gibt, müssen Sie den DNS-Domain-Namen [CORP.EXAMPLE.COM\test1] angeben.

> **Note**
>
> Anmeldungen, die auf Active-Directory-Benutzern basieren, sind auf Namen mit weniger als 21 Zeichen beschränkt.

Löschen von Anmeldung

Um eine Anmeldung zu löschen, verwenden Sie dieselbe Syntax wie für jede beliebige Anmeldung, wie im folgenden Beispiel gezeigt:

```
DROP LOGIN [DNS domain name\login]
```

Ändern von Anmeldungen

Wenn Sie eine Anmeldung ändern möchten, verwenden Sie dieselbe Syntax wie für jede beliebige Anmeldung, wie im folgenden Beispiel gezeigt:

```
ALTER LOGIN [DNS domain name\login] { ENABLE|DISABLE|WITH DEFAULT_DATABASE=[master] }
```

Der Befehl ALTER LOGIN unterstützt eingeschränkte Optionen für Windows-Anmeldungen, darunter folgende:

- DISABLE – zum Deaktivieren einer Anmeldung. Sie können eine deaktivierte Anmeldung nicht für die Authentifizierung verwenden.
- ENABLE – zum Aktivieren einer deaktivierten Anmeldung.
- DEFAULT_DATABASE – zum Ändern der Standarddatenbank einer Anmeldung.

> **Note**
>
> Die gesamte Passwortverwaltung erfolgt über AWS Directory Service, sodass der Befehl ALTER LOGIN Datenbankadministratoren nicht erlaubt, Passwörter für Windows-Logins zu ändern oder festzulegen.

Herstellen einer Verbindung mit Babelfish für Aurora PostgreSQL mit Kerberos-Authentifizierung

Normalerweise authentifizieren sich die Datenbankbenutzer, die die Kerberos-Authentifizierung nutzen, über ihren Client-Computer. Diese Computer sind Mitglieder der Active-Directory-Domain. Sie verwenden die Windows-Authentifizierung von ihren Client-Anwendungen aus, um auf den Server von Babelfish für Aurora PostgreSQL am TDS-Port zuzugreifen.

Herstellen einer Verbindung mit Babelfish für Aurora PostgreSQL am PostgreSQL-Port mit Kerberos-Authentifizierung

Sie können Anmeldungen, die über den TDS-Port erstellt wurden, entweder mit dem TDS-Port oder dem PostgreSQL-Port verwenden. PostgreSQL verwendet für Benutzernamen jedoch standardmäßig Vergleiche unter Berücksichtigung der Groß- und Kleinschreibung. Damit Aurora PostgreSQL

Kerberos-Benutzernamen ohne Berücksichtigung von Groß- und Kleinschreibung interpretiert, müssen Sie den Parameter `krb_caseins_users` in der benutzerdefinierten Babelfish-Cluster-Parametergruppe auf `true` festlegen. Dieser Parameter ist standardmäßig auf `false` festgelegt. Weitere Informationen finden Sie unter Konfigurieren von Benutzernamen, bei denen die Groß-/Kleinschreibung unterschieden wird. Darüber hinaus müssen Sie den Anmeldebenutzernamen im Format <login@DNS domain name> über die PostgreSQL-Client-Anwendungen angeben. Das Format <DNS domain name\login> kann nicht verwendet werden.

Häufig auftretende Fehler

Sie können Gesamtstruktur-Vertrauensstellungen zwischen Ihrem On-Premises Microsoft Active Directory und dem AWS Managed Microsoft AD konfigurieren. Weitere Informationen finden Sie unter Erstellen einer Vertrauensstellung. Anschließend müssen Sie eine Verbindung über einen speziellen Domain-spezifischen Endpunkt herstellen, anstatt die Amazon-Domain `rds.amazonaws.com` im Host-Endpunkt zu verwenden. Wenn Sie nicht den richtigen Domain-spezifischen Endpunkt verwenden, wird möglicherweise folgende Fehlermeldung angezeigt:

```
Error: “Authentication method "NTLMSSP" not supported (Microsoft SQL Server, Error:
 514)"
```

Dieser Fehler tritt auf, wenn der TDS-Client das Serviceticket für die angegebene Endpunkt-URL nicht zwischenspeichern kann. Weitere Informationen finden Sie unter Herstellen einer Verbindung mithilfe der Kerberos-Authentifizierung.

Verbinden mit einem Babelfish-DB-Cluster

Zum Herstellen einer Verbindung mit Babelfish verbinden Sie sich mit dem Endpunkt des Aurora-PostgreSQL-Clusters, auf dem Babelfish ausgeführt wird. Ihr Client kann einen der folgenden Clienttreiber verwenden, die mit TDS Version 7.1 bis 7.4 kompatibel sind:

- Upgrades für Open Database Connectivity (ODBC)-Treiber
- OLE DB Treiber/msoledBSQL
- Java Database Connectivity (JDBC) Version 8.2.2 (mssql-jdbc-8.2.2) und höher
- SqlClient Microsoft-Datenanbieter für SQL Server
- .NET-Datenprovider für SQL Server
- SQL Server Native Client 11.0 (veraltet)
- OLE DB Provider/SQLOLEDB (veraltet)

Mit Babelfish führen Sie Folgendes aus:

- SQL Server-Tools, Anwendungen und Syntax auf dem TDS-Port, standardmäßig Port 1433.
- PostgreSQL-Tools, Anwendungen und Syntax auf dem PostgreSQL-Port standardmäßig Port 5432.

Weitere Informationen zum Herstellen einer Verbindung mit Aurora PostgreSQL im Allgemeinen finden Sie unter Herstellen einer Verbindung mit einem Amazon-Aurora-PostgreSQL-DB-Cluster.

> **Note**
>
> Entwicklertools von Drittanbietern, die den SQL Server OLEDB-Anbieter für den Zugriff auf Metadaten verwenden, werden nicht unterstützt. Wir empfehlen Ihnen, für diese Tools SQL Server-JDBC-, ODBC- oder SQL Native-Clientverbindungen zu verwenden.

Themen

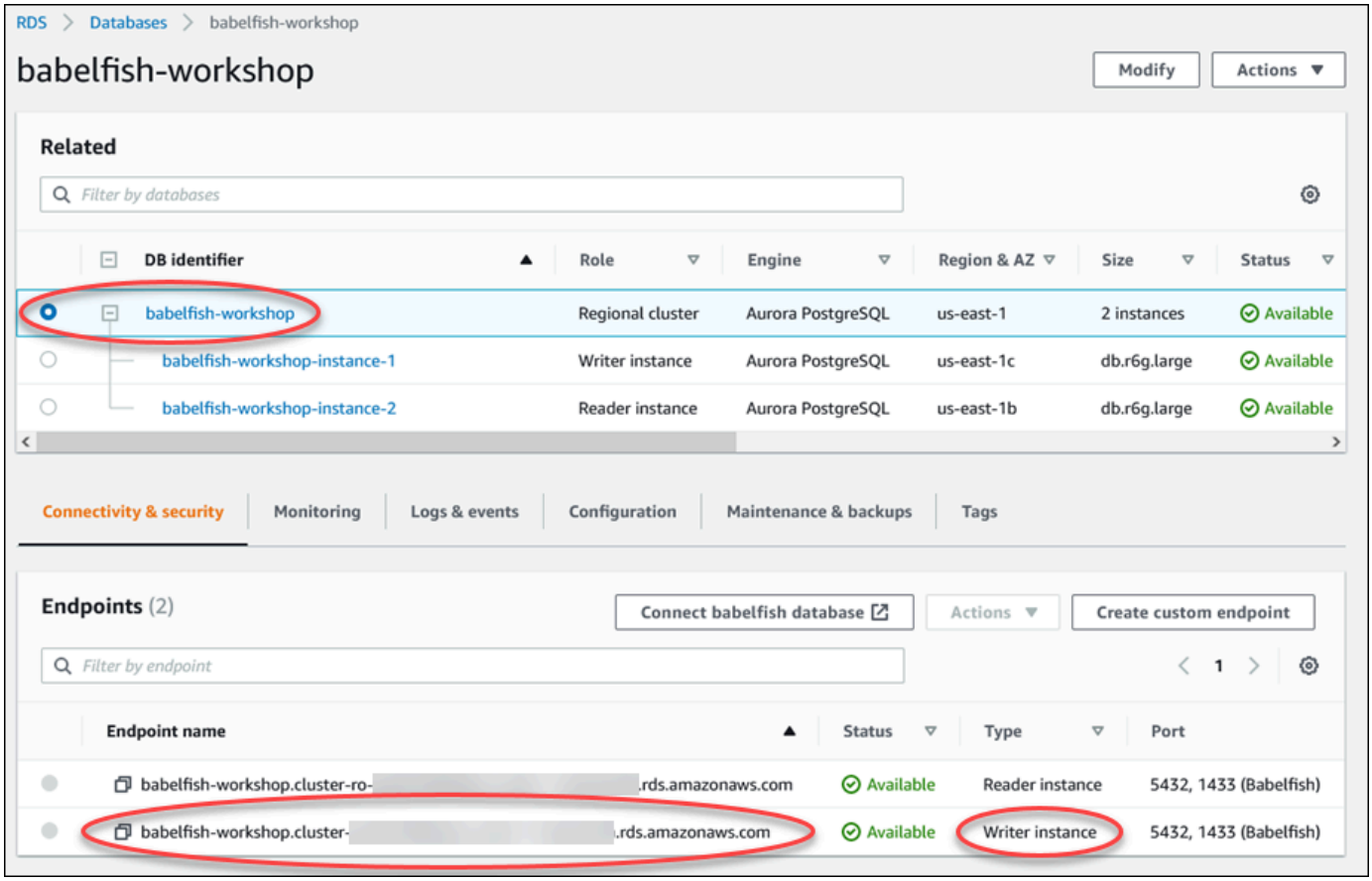
- Verbinden mit Ihrem DB-Cluster mit einem PostgreSQL-Client

Finden des Writer-Endpunkts und der Portnummer

Zum Herstellen einer Verbindung mit Ihrem Babelfish-DB-Cluster verwenden Sie den Endpunkt, der mit der (primären) Writer-Instance des DB-Clusters verknüpft ist. Die Instance muss den Status Available (Verfügbar) haben. Es kann bis zu 20 Minuten dauern, bis die Instances verfügbar sind, nachdem Sie den DB-Cluster von Babelfish for Aurora PostgreSQL erstellt haben.

So finden Sie Ihren Datenbank-Endpunkt

1. Öffnen Sie die -Konsole für Babelfish.
2. Wählen Sie aus dem Navigationsbereich Datenbanken aus.
3. Wählen Sie Ihren DB-Cluster von Babelfish for Aurora PostgreSQL in der Liste aus, um die Details anzuzeigen.
4. Auf Konnektivität & Sicherheit, notieren Sie sich den verfügbaren Cluster Endpunkte-Werte. Verwenden Sie den Cluster-Endpunkt für die Schreibinstanz in Ihrer Verbindung für Anwendungen, die Lese- oder Schreibvorgänge ausführen.



Weitere Informationen über Aurora-DB-Cluster finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Herstellen von C#- oder JDBC-Clientverbindungen mit Babelfish

Im Folgenden finden Sie einige Beispiele für die Verwendung von C#- und JDBC-Klassen zum Verbinden mit Babelfish for Aurora PostgreSQL.

Example : Verwenden von C#-Code zum Herstellen einer Verbindung mit einem DB-Cluster

```
string dataSource = 'babelfishServer_11_24';

//Create connection
connectionString = @"Data Source=" + dataSource
    +";Initial Catalog=your-DB-name"
    +";User ID=user-id;Password=password";

SqlConnection cnn = new SqlConnection(connectionString);
cnn.Open();
```

Example : Verwenden generischer JDBC-API-Klassen und -Schnittstellen zum Herstellen einer Verbindung mit einem DB-Cluster

```
String dbServer =
   "database-babelfish.cluster-123abc456def.us-east-1-rds.amazonaws.com";
String connectionUrl = "jdbc:sqlserver://" + dbServer + ":1433;" +
    "databaseName=your-DB-name;user=user-id;password=password";

// Load the SQL Server JDBC driver and establish the connection.
System.out.print("Connecting Babelfish Server ... ");
Connection cnn = DriverManager.getConnection(connectionUrl);
```

Example : Verwenden von SQL-Server-spezifischen JDBC-Klassen und -Schnittstellen zum Herstellung einer Verbindung mit einem DB-Cluster

```
// Create datasource.
SQLServerDataSource ds = new SQLServerDataSource();
ds.setUser("user-id");
ds.setPassword("password");
String babelfishServer =
   "database-babelfish.cluster-123abc456def.us-east-1-rds.amazonaws.com";

ds.setServerName(babelfishServer);
ds.setPortNumber(1433);
ds.setDatabaseName("your-DB-name");
```

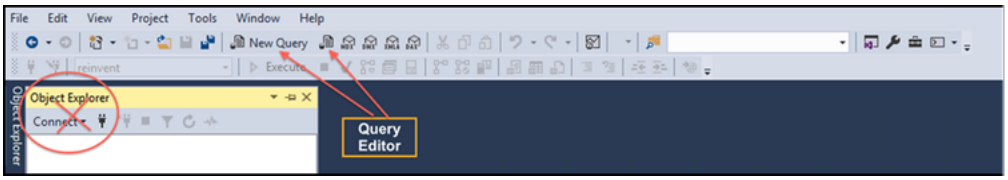
```
Connection con = ds.getConnection();
```

Verbinden mit Ihrem DB-Cluster mithilfe eines SQL Server-Clients

Sie können einen SQL Server-Client verwenden, um sich mit Babelfish am TDS-Port zu verbinden. Ab Babelfish 2.1.0 und in höheren Versionen können Sie den SSMS Object Explorer oder den SSMS-Abfrage-Editor verwenden, um eine Verbindung mit Ihrem Babelfish-Cluster herzustellen.

Einschränkungen

- In Babelfish 2.1.0 und älteren Versionen, funktioniert `PARSE` zum Prüfen der SQL-Syntax nicht so, wie es sollte. Anstatt die Syntax zu überprüfen, ohne die Abfrage auszuführen, führt der Befehl `PARSE` die Abfrage aus, zeigt aber keine Ergebnisse an. Bei der Verwendung der SMSS-Tastenkombination <Strg><F5> zur Überprüfung der Syntax tritt das gleiche anomale Verhalten auf, d. h., Babelfish führt die Abfrage unerwartet aus, ohne eine Ausgabe zu liefern.
- Babelfish unterstützt MARS (Multiple Active Result Sets) nicht. Stellen Sie sicher, dass alle Clientanwendungen, die Sie für die Verbindung mit Babelfish verwenden, nicht auf MARS eingestellt sind.
- Mit Babelfish 1.3.0 und älteren Versionen wird nur der Abfrage-Editor für SSMS unterstützt. Um SSMS mit Babelfish zu verwenden, öffnen Sie unbedingt das Verbindungsdialogfeld des Abfrage-Editors in SSMS und nicht im Objekt-Explorer. Wenn das Dialogfeld des Objekt-Explorers tatsächlich geöffnet wird, brechen Sie das Dialogfeld ab und öffnen den Abfrage-Editor erneut. In der folgenden Abbildung finden Sie die Menüoptionen, die Sie beim Herstellen einer Verbindung mit Babelfish 1.3.0 oder älteren Versionen auswählen können.



Weitere Informationen über Interoperabilität und Verhaltensunterschiede zwischen SQL Server und Babelfish finden Sie unter Unterschiede zwischen Babelfish für Aurora PostgreSQL und SQL Server.

Herstellen einer Verbindung mit dem DB-Cluster mit sqlcmd

Sie können eine Verbindung zu einem Aurora-PostgreSQL-DB-Cluster herstellen und mit diesem interagieren, der Babelfish unterstützt, indem Sie nur Version 19.1 und einen früheren SQL-Server-`sqlcmd`Befehlszeilenclient verwenden. SSMS Version 19.2 wird für die Verbindung mit einem Babelfish-Cluster nicht unterstützt. Verwenden Sie den nachfolgenden Befehl, um eine Verbindung herzustellen.

```
sqlcmd -S endpoint,port -U login-id -P password -d your-DB-name
```

Es handelt sich um folgende Optionen:

- `-S` ist der Endpunkt und (optional) TDS-Port des DB-Clusters.
- `-U` ist der Anmeldename des Benutzers.
- `-P` ist das Passwort, das dem Benutzer zugeordnet ist.
- `-d` ist der Name deiner Babelfish-Datenbank.

Nach der Verbindung können Sie viele der gleichen Befehle verwenden, die Sie mit SQL Server verwenden. Einige Beispiele finden Sie unter Abrufen von Informationen aus dem Babelfish-Systemkatalog.

Herstellen einer Verbindung mit dem DB-Cluster mit SSMS

Mit Microsoft SQL Server Management Studio (SSMS) können Sie eine Verbindung mit einem DB-Cluster von Aurora PostgreSQL herstellen, der Babelfish ausführt. SSMS enthält eine Vielzahl von Tools, darunter den SQL-Server-Assistenten für Import und Export, der in Migrieren einer SQL-Server-Datenbank zu Babelfish for Aurora PostgreSQL behandelt wird. Weitere Informationen zu SSMS finden Sie unter Download von SQL Server Management Studio (SSMS) in der Microsoft-Dokumentation.

Stellen Sie eine Verbindung mit Ihrer Babelfish-Datenbank mit SSMS wie folgt her:

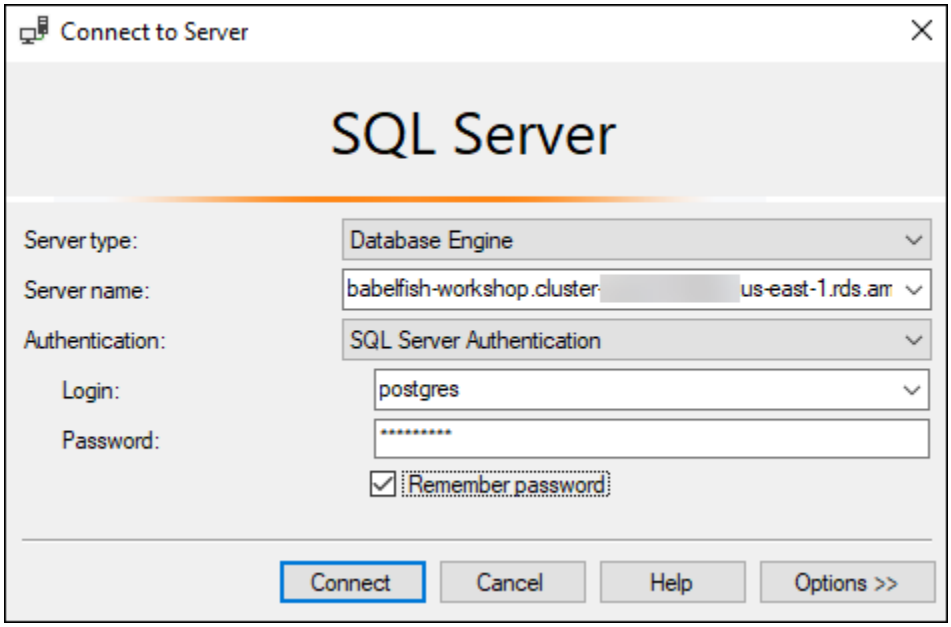
1. Starten Sie SSMS.
2. Öffnen Sie das Dialogfeld Mit Server verbinden. Führen Sie einen der folgenden Schritte aus, um mit der Verbindung fortzufahren:
   - Klicken Sie auf Neue Abfrage.
   - Wenn der Abfrage-Editor geöffnet ist, wählen Sie Abfragen, Connection (Verbindung), Verbinden aus.
3. Stellen Sie folgende Informationen für Ihre Datenbank bereit:
   a. Wählen Sie für Servertyp die Option Datenbank-Engine aus.
   b. Geben Sie für Server name (Servername) den DNS-Namen ein. Ihr Servername sollte beispielsweise wie folgt aussehen.

```
cluster-name.cluster-555555555555.aws-region.rds.amazonaws.com,1433
```

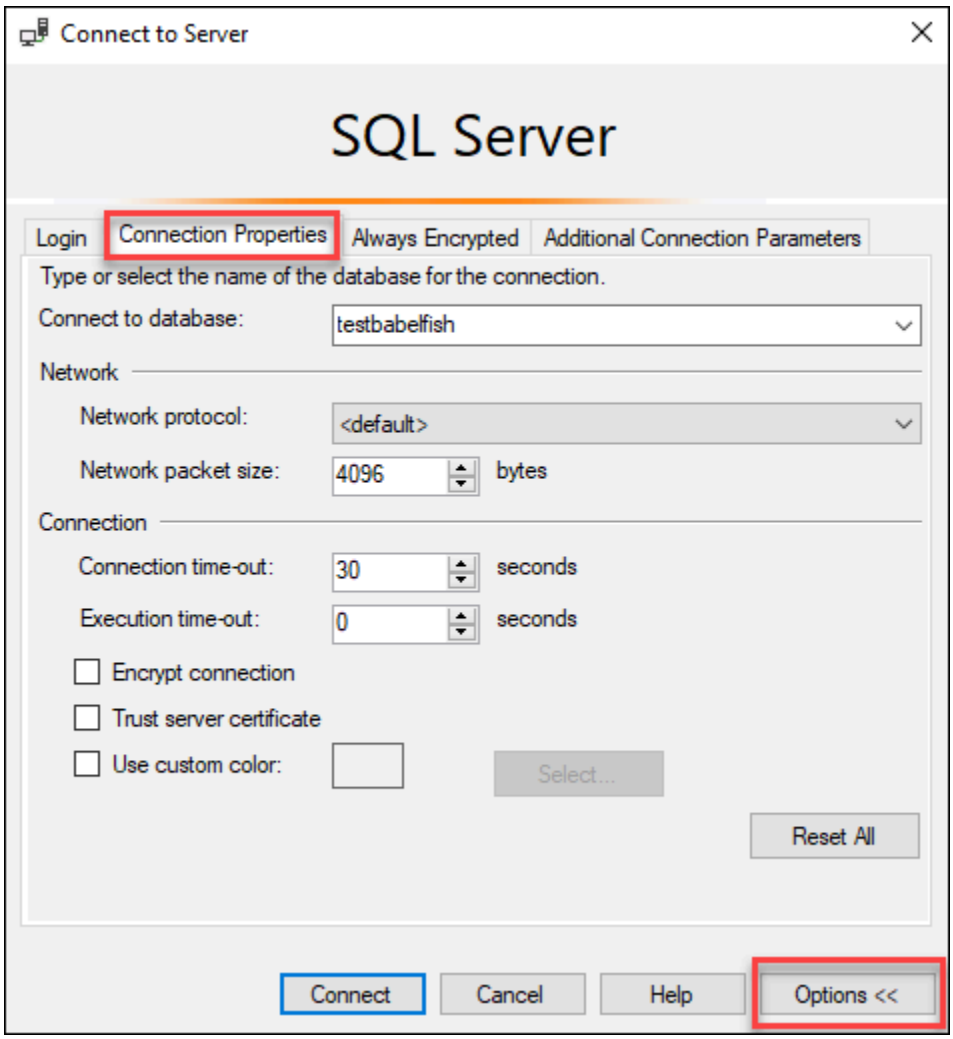
c. Wählen Sie für Authentifizierung die Option SQL Server-Authentifizierung aus.

d. Für Anmeldung geben Sie den Benutzernamen ein, den Sie beim Erstellen Ihrer Datenbank ausgewählt haben.

e. Für Passwort geben Sie das Passwort ein, das Sie beim Erstellen Ihrer Datenbank ausgewählt haben.



4. (Optional) Wählen Sie Optionen und wählen Sie dann die Registerkarte Verbindungseigenschaften.



5. (Optional) Für Verbindung zur Datenbank herstellen, geben Sie den Namen der migrierten SQL Server-Datenbank an, mit der eine Verbindung hergestellt werden soll, und wählen Sie Verbinden aus.

   Wenn eine Meldung angezeigt wird, die angibt, dass SSMS keine Verbindungszeichenfolgen anwenden kann, wählen Sie OK aus.

   Wenn Sie Probleme haben, sich mit Babelfish zu verbinden, finden Sie weitere Informationen unter Verbindungsfehler.

   Weitere Informationen zu Verbindungsproblemen mit SQL Server finden Sie unter Fehlerbehebung bei Verbindungen mit Ihrer SQL-Server-DB-Instance im Amazon-RDS-Benutzerhandbuch.

Verbinden mit Ihrem DB-Cluster mit einem PostgreSQL-Client

Sie können einen PostgreSQL-Client verwenden, um eine Verbindung mit Babelfish auf dem PostgreSQL-Port herzustellen.

Herstellen einer Verbindung mit Ihrem psql

Sie können den PostgreSQL-Client von der PostgreSQL-Website herunterladen. Folgen Sie den Anweisungen für Ihr Betriebssystem, um diese Version zu installieren.

Sie können einen Aurora-PostgreSQL-DB-Cluster abfragen, der Babelfish mit dem Befehlszeilen-Client `psql` unterstützt. Verwenden Sie beim Herstellen der Verbindung den PostgreSQL-Port (standardmäßig Port 5432). In der Regel müssen Sie die Portnummer nicht angeben, es sei denn, Sie haben die Standardeinstellung geändert. Verwenden Sie den folgenden Befehl, um eine Verbindung mit Babelfish über den `psql`-Client herzustellen:

```
psql -h bfish-db.cluster-123456789012.aws-region.rds.amazonaws.com
-p 5432 -U postgres -d babelfish_db
```

Dabei werden die folgenden Parameter verwendet:

- `-h` – Der Hostname des DB-Clusters (Cluster-Endpunkt), auf den Sie zugreifen möchten.
- `-p` – Die Nummer des PostgreSQL-Ports, der für die Verbindung mit der DB-Instance verwendet wird.
- `-d` – Die Datenbank, mit der Sie eine Verbindung herstellen möchten. Der Standardwert ist `babelfish_db`.
- `-U` – Das Datenbank-Benutzerkonto, auf das Sie zugreifen möchten. (Das Beispiel zeigt den Standard-Hauptbenutzernamen.)

Wenn Sie einen SQL-Befehl auf dem PSQL-Client ausführen, beenden Sie den Befehl mit einem Semikolon. Der folgende SQL-Befehl fragt beispielsweise die pg_tables Systemansicht ab, um Informationen über jede Tabelle in der Datenbank zurückzugeben.

```
SELECT * FROM pg_tables;
```

Der PSQL-Client verfügt auch über eine Reihe von integrierten Metakommanden. Eine metacommand ist eine Verknüpfung, die die Formatierung anpasst oder eine Verknüpfung bereitstellt,

die Metadaten in einem einfach zu bedienenden Format zurückgibt. Beispielsweise gibt der Meta-Befehl in etwa die ähnlichen Informationen wie der vorige SQL_Befehl zurück:

```
\d
```

Metacommands müssen nicht mit einem Semikolon (;) beendet werden.

Um den PSQL-Client zu beenden, geben Sie \q ein.

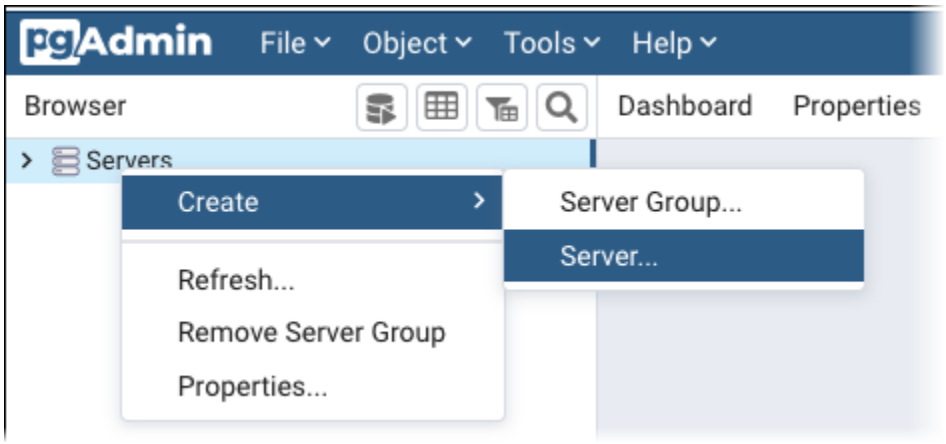
Weitere Informationen über die Verwendung des PSQL-Clients zum Abfragen eines Aurora-PostgreSQL-Clusters finden Sie unter Die PostgreSQL-Dokumentation.

Herstellen einer Verbindung mit dem DB-Cluster mit pgAdmin

Sie können den pgAdmin-Client verwenden, um im nativen PostgreSQL-Dialekt auf Ihre Daten zuzugreifen.

Stellen Sie eine Verbindung zum Cluster mit dem pgAdmin-Client wie folgt her:

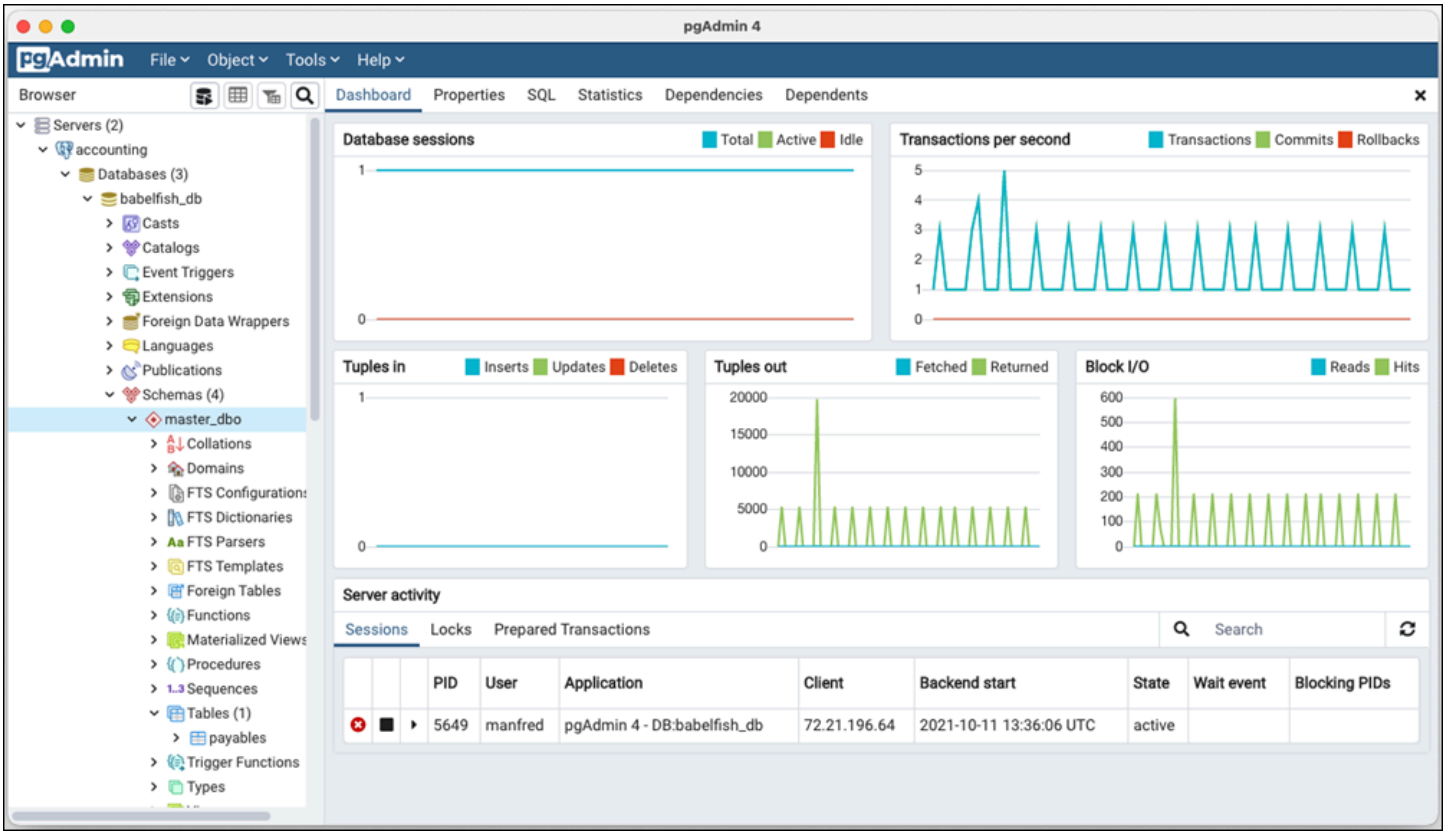
1. Laden Sie den pgAdmin-Client von pgAdmin Webseite herunter.
2. Öffnen Sie den Client und authentifizieren Sie sich bei pgAdmin.
3. Öffnen Sie das Kontextmenü (rechte Maustaste) für Server und klicken Sie auf und danach auf Erstellen, Server.



4. Geben Sie die Informationen im Dialogfeld Erstellen - Server ein.

   Auf erConnection (Verbindung) geben Sie die Aurora-PostgreSQL-Clusteradresse für Host und die PostgreSQL-Portnummer (standardmäßig 5432) für Port ein. Geben Sie Authentifizierungsdetails an und wählen Sie Save aus.

Nach der Verbindung können Sie die pgAdmin-Funktionalität verwenden, um Ihren Aurora-PostgreSQL-Cluster am PostgreSQL-Port zu überwachen und zu verwalten.



Weitere Informationen hierzu finden Sie auf der Webseite pgAdmin.

Arbeiten mit Babelfish

Im Folgenden finden Sie Nutzungsinformationen für Babelfish, darunter einige Unterschiede zwischen Babelfish und SQL Server sowie zwischen Babelfish- und PostgreSQL-Datenbanken.

Themen

Abrufen von Informationen aus dem Babelfish-Systemkatalog

Sie können Informationen über die Datenbankobjekte abrufen, die in Ihrem Babelfish-Cluster gespeichert sind, indem Sie viele der Systemansichten abfragen, die auch in SQL Server verwendet werden. Jede neue Version von Babelfish bietet Unterstützung für weitere Systemansichten. Eine Liste der derzeit verfügbaren Ansichten finden Sie in der Tabelle SQL Server system catalog views.

Diese Systemansichten enthalten Informationen aus dem Systemkatalog (`sys.schemas`). Bei Babelfish enthalten diese Ansichten sowohl SQL-Server- als auch PostgreSQL-Systemschemas. Zum Abfragen von Informationen zum Systemkatalog in Babelfish können Sie den TDS-Port oder den PostgreSQL-Port verwenden, wie in den folgenden Beispielen gezeigt.

- Fragen Sie den T-SQL-Port mit **`sqlcmd`** oder einem anderen SQL-Server-Client ab.

```
1> SELECT * FROM sys.schemas
2> GO
```

  Diese Abfrage gibt SQL-Server- und Aurora-PostgreSQL-Systemschemas zurück, wie im Folgenden dargestellt.

```
name
```

```
------------------------------------------------------------
demographic_dbo
public
sys
master_dbo
tempdb_dbo
...
```

- Fragen Sie den PostgreSQL-Port mit **`psql`** oder **`pgAdmin`** ab. In diesem Beispiel verwenden wir den Metabefehl `psql` zum Auflisten von Schemas (`\dn`):

  ```
  babelfish_db=> \dn
  ```

  Die Abfrage gibt dieselbe Ergebnismenge zurück wie die von `sqlcmd` am T-SQL-Port.

  ```
          List of schemas
               Name
  ------------------------------

   demographic_dbo

   public
   sys
   master_dbo
   tempdb_dbo
  ...
  ```

SQL-Server-Systemkataloge in Babelfish verfügbar

In der folgenden Tabelle finden Sie die derzeit in Babelfish implementierten SQL-Server-Ansichten. Weitere Informationen über die Systemkataloge in SQL Server finden Sie unter Systemkatalogansichten (Transact-SQL) in der Microsoft-Dokumentation.

Name der Ansicht	Beschreibung oder Babelfish-Beschränkung (falls vorhanden)
`sys.all_columns`	Alle Spalten in allen Tabellen und Ansichten
`sys.all_objects`	Alle Objekte in allen Schemas

Name der Ansicht	Beschreibung oder Babelfish-Beschränkung (falls vorhanden)
`sys.all_sql_modules`	Die Vereinigung von `sys.sql_modules` und `sys.system_sql_modules`
`sys.all_views`	Alle Ansichten in allen Schemas
`sys.columns`	Alle Spalten in benutzerdefinierten Tabellen und Ansichten
`sys.configurations`	Die Unterstützung von Babelfish ist auf eine einzige schreibgeschützte Konfiguration beschränkt.
`sys.data_spaces`	Enthält eine Zeile für jeden Datenbereich. Dies kann eine Dateigruppe, ein Partitionsschema oder eine FILESTREAM-Datendateigruppe sein.
`sys.database_files`	Eine Ansicht pro Datenbank, die eine Zeile für jede Datei einer Datenbank enthält, wie sie in der Datenbank selbst gespeichert ist.
`sys.database_mirroring`	Weitere Informationen finden Sie unter sys.database_mirroring in der Microsoft-Transact-SQL-Dokumentation.
`sys.database_principals`	Weitere Informationen finden Sie unter sys.database_principals in der Microsoft-Transact-SQL-Dokumentation.
`sys.database_role_members`	Weitere Informationen finden Sie unter sys.database_role_members in der Microsoft-Transact-SQL-Dokumentation.
`sys.databases`	Alle Datenbanken in allen Schemas

Name der Ansicht	Beschreibung oder Babelfish-Beschränkung (falls vorhanden)
`sys.dm_exec_connections`	Weitere Informationen finden Sie unter sys.dm_exec_connections in der Microsoft-Transact-SQL-Dokumentation.
`sys.dm_exec_sessions`	Weitere Informationen finden Sie unter sys.dm_exec_sessions in der Microsoft-Transact-SQL-Dokumentation.
`sys.dm_hadr_database_replica_states`	Weitere Informationen finden Sie unter sys.dm_hadr_database_replica_states in der Microsoft-Transact-SQL-Dokumentation.
`sys.dm_os_host_info`	Weitere Informationen finden Sie unter sys.dm_os_host_info in der Microsoft-Transact-SQL-Dokumentation.
`sys.endpoints`	Weitere Informationen finden Sie unter sys.endpoints in der Microsoft-Transact-SQL-Dokumentation.
`sys.indexes`	Weitere Informationen finden Sie unter sys.indexes in der Microsoft-Transact-SQL-Dokumentation.
`sys.languages`	Weitere Informationen finden Sie unter sys.languages in der Microsoft-Transact-SQL-Dokumentation.
`sys.schemas`	Alle Schemas
`sys.server_principals`	Alle Logins und Rollen
`sys.sql_modules`	Weitere Informationen finden Sie unter sys.sql_modules in der Microsoft-Transact-SQL-Dokumentation.

Name der Ansicht	Beschreibung oder Babelfish-Beschränkung (falls vorhanden)
`sys.sysconfigures`	Die Unterstützung von Babelfish ist auf eine einzige schreibgeschützte Konfiguration beschränkt.
`sys.syscurconfigs`	Die Unterstützung von Babelfish ist auf eine einzige schreibgeschützte Konfiguration beschränkt.
`sys.sysprocesses`	Weitere Informationen finden Sie unter sys.sysprocesses in der Microsoft-Transact-SQL-Dokumentation.
`sys.system_sql_modules`	Weitere Informationen finden Sie unter sys.system_sql_modules in der Microsoft-Transact-SQL-Dokumentation.
`sys.table_types`	Weitere Informationen finden Sie unter sys.table_types in der Microsoft-Transact-SQL-Dokumentation.
`sys.tables`	Alle Tabellen in einem Schema
`sys.xml_schema_collections`	Weitere Informationen finden Sie unter sys.xml_schema_collections in der Microsoft-Transact-SQL-Dokumentation.

PostgreSQL implementiert Systemkataloge, die den SQL Server-Objektkatalogansichten ähneln. Eine vollständige Liste der Systemkataloge finden Sie unter Systemkataloge in der PostgreSQL-Dokumentation.

Von Babelfish unterstützte DDL-Exporte

Ab den Versionen Babelfish 2.4.0 und 3.1.0 unterstützt Babelfish DDL-Exporte mit verschiedenen Tools. Sie können diese Funktion beispielsweise von SQL Server Management Studio (SSMS) aus verwenden, um die Datendefinitionsskripte für verschiedene Objekte in einer Datenbank von Babelfish für Aurora PostgreSQL zu generieren. Anschließend können Sie die generierten DDL-

Befehle in diesem Skript verwenden, um dieselben Objekte in einer anderen Datenbank von Babelfish für Aurora PostgreSQL oder SQL Server zu erstellen.

Babelfish unterstützt DDL-Exporte für die folgenden Objekte in den angegebenen Versionen.

Liste von Objekten	2.4.0	3.1.0
Tabelle USER	Ja	Ja
Primärschlüssel	Ja	Ja
Fremdschlüssel	Ja	Ja
Eindeutigkeitseinschränkungen	Ja	Ja
Indizes	Ja	Ja
Einschränkungen prüfen	Ja	Ja
Ansichten	Ja	Ja
Gespeicherte Prozeduren	Ja	Ja
Benutzerdefinierte Funktionen	Ja	Ja
Funktionen mit Tabellenwerten	Ja	Ja
Auslöser	Ja	Ja
Benutzerdefinierte Datentypen	Nein	Nein
Benutzerdefinierte Tabellentypen	Nein	Nein
Benutzer	Nein	Nein
Anmeldungen	Nein	Nein
Sequenzen	Nein	Nein
Rollen	Nein	Nein

Einschränkungen bei den exportierten DDLs

- Verwenden von Escape-Schraffuren, bevor die Objekte mit den exportierten DDLs neu erstellt werden – Babelfish unterstützt nicht alle Befehle im exportierten DDL-Skript. Verwenden Sie Escape-Schraffuren, um Fehler zu vermeiden, die beim Neuerstellen der Objekte aus den DDL-Befehlen in Babelfish entstehen. Weitere Informationen zu Escape-Schraffuren finden Sie unter Verwalten der Babelfish-Fehlerbehandlung mit Escape-Schraffuren.
- Objekte, die CHECK-Einschränkungen mit expliziten COLLATE-Klauseln enthalten – Die Skripts mit diesen Objekten, die aus einer SQL Server-Datenbank generiert wurden, haben unterschiedliche, aber gleichwertige Sortierungen wie in der Babelfish-Datenbank. Beispielsweise werden einige Sortierungen, wie sql_latin1_general_cp1_cs_as, sql_latin1_general_cp1251_cs_as und latin1_general_cs_as, als latin1_general_cs_as generiert, was der Windows-Sortierung am nächsten kommt.

Unterschiede zwischen Babelfish für Aurora PostgreSQL und SQL Server

Babelfish ist ein sich weiterentwickelnder Aurora-PostgreSQL-Service, der seit dem ersten Angebot in Aurora PostgreSQL 13.4 in jeder Version um weitere Funktionen ergänzt wurde. Babelfish wurde entwickelt, um T-SQL-Semantik zusätzlich zu PostgreSQL über den T-SQL-Dialekt unter Verwendung des TDS-Ports zur Verfügung zu stellen. Jede neue Version von Babelfish bietet weitere Funktionen, die besser auf die T-SQL-Funktionalität und das -Verhalten ausgerichtet sind, wie in der Tabelle Unterstützte Funktionalität in Babelfish nach Version gezeigt. Für optimale Ergebnisse bei der Arbeit mit Babelfish sollten Sie die Unterschiede verstehen, die derzeit zwischen dem von SQL Server unterstützten T-SQL und Babelfish für die neueste Version bestehen. Weitere Informationen hierzu finden Sie unter T-SQL-Unterschiede bei Babelfish.

Zusätzlich zu den Unterschieden zwischen T-SQL, das von Babelfish unterstützt wird, und SQL Server, müssen Sie möglicherweise auch Interoperabilitätsprobleme zwischen Babelfish und PostgreSQL im Kontext des DB-Clusters von Aurora PostgreSQL berücksichtigen. Wie bereits erwähnt, unterstützt Babelfish T-SQL-Semantik zusätzlich zu PostgreSQL über den T-SQL-Dialekt unter Verwendung des TDS-Ports. Gleichzeitig kann auf die Babelfish-Datenbank auch über den Standard-PostgreSQL-Port mit SQL-Anweisungen von PostgreSQL zugegriffen werden. Wenn Sie erwägen, sowohl PostgreSQL- als auch Babelfish-Funktionen in einer Produktionsbereitstellung zu verwenden, müssen Sie sich der potenziellen Interoperabilitätsprobleme zwischen Schemanamen, Bezeichnern, Berechtigungen, Transaktionssemantik, verschiedenen Ergebnismengen, Standardsortierungen usw. bewusst sein. Einfach ausgedrückt, wenn PostgreSQL-Anweisungen oder PostgreSQL-Zugriffe im Kontext von Babelfish auftreten, kann es zu Interferenzen zwischen

PostgreSQL und Babelfish kommen, die möglicherweise Syntax, Semantik und Kompatibilität beeinträchtigen können, wenn neue Versionen von Babelfish veröffentlicht werden. Vollständige Informationen und Anleitungen zu allen Überlegungen finden Sie in der Anleitung zur Interoperabilität von Babelfish in der Dokumentation von Babelfish für PostgreSQL.

> **Note**
>
> Bevor Sie sowohl die native PostgreSQL-Funktionalität als auch die Babelfish-Funktionalität im selben Anwendungskontext verwenden, empfehlen wir Ihnen dringend, die Probleme, die in der Anleitung zur Interoperabilität von Babelfish der Dokumentation von Babelfish für PostgreSQL erörtert werden, zu berücksichtigen. Diese Interoperabilitätsprobleme (Aurora PostgreSQL und Babelfish) sind nur relevant, wenn Sie die PostgreSQL-Datenbank-Instance im selben Anwendungskontext wie Babelfish verwenden möchten.

Themen

- Babelfish-Dump und Wiederherstellung
- T-SQL-Unterschiede bei Babelfish
- Transaktionsisolationsstufen in Babelfish

Babelfish-Dump und Wiederherstellung

Ab Version 4.0.0 und 3.4.0 können Babelfish-Benutzer jetzt die Dump- und Wiederherstellungsprogramme verwenden, um ihre Datenbanken zu sichern und wiederherzustellen. Weitere Informationen finden Sie unter Babelfish-Dump und Wiederherstellung. Diese Funktion baut auf PostgreSQL-Dump- und Wiederherstellungsdienstprogrammen auf. Weitere Informationen finden Sie unter pg_dump und unter pg_restore. Um dieses Feature effektiv in Babelfish nutzen zu können, müssen Sie PostgreSQL-basierte Tools verwenden, die speziell für Babelfish angepasst sind. Die Backup- und Wiederherstellungsfunktion für Babelfish unterscheidet sich erheblich von der von SQL Server. Weitere Informationen zu diesen Unterschieden finden Sie unter Unterschiede bei der Dump- und Wiederherstellungsfunktion: Babelfish und SQL Server. Babelfish für Aurora PostgreSQL bietet zusätzliche Funktionen zum Sichern und Wiederherstellen von Amazon-Aurora-PostgreSQL-DB-Clustern. Weitere Informationen finden Sie unter Sichern und Wiederherstellen eines Amazon-Aurora-DB-Clusters.

T-SQL-Unterschiede bei Babelfish

Im Folgenden finden Sie eine Tabelle der T-SQL-Funktionen, die in der aktuellen Version von Babelfish unterstützt werden, mit einigen Anmerkungen zu Unterschieden im Verhalten gegenüber dem von SQL Server.

Weitere Informationen über den Support für verschiedene Versionen finden Sie unter Unterstützte Funktionalität in Babelfish nach Version. Weitere Informationen zu Funktionen, die derzeit nicht unterstützt werden, finden Sie unter Nicht unterstützte Funktionalität in Babelfish.

Babelfish ist mit der PostgreSQL-kompatiblen Edition von Aurora verfügbar. Weitere Informationen zu Babelfish-Versionen finden Sie unter Versionshinweise für Aurora PostgreSQL.

Funktionalität oder Syntax	Beschreibung des Verhaltens oder Unterschieds
\ (Zeilenfortsetzungszeichen)	Das Zeilenfortsetzungszeichen (ein umgekehrter Schrägstrich vor einem Zeilenumbruch) für Zeichen- und Hexadezimalzeichen folgen wird derzeit nicht unterstützt. Für Zeichenfolgen wird der Backslash für neue Zeile als Zeichen in der Zeichenfolge interpretiert. Bei Hexadezimalzeichenfolgen führt der Backslash für neue Zeile zu einem Syntaxfehler.
@@Version	Das Format des von `@@version` zurückgegebenen Wertes unterscheidet sich geringfügig von dem von SQL Server zurückgegebenen Wert. Ihr Code funktioniert möglicherweise nicht richtig, wenn er von der Formatierung von `@@version` abhängt.
Aggregationsfunktionen	Aggregatfunktionen werden teilweise unterstützt (AVG, COUNT, COUNT_BIG, GROUPING, MAX, MIN, STRING_AGG und SUM werden unterstützt). Eine Liste der nicht unterstützten Aggregatf unktionen finden Sie unter Nicht unterstützte Funktionen.
ALTER TABLE	Unterstützt nur das Hinzufügen oder Löschen einer einzelnen Spalte oder Einschränkung.
ALTER TABLE..ALTER COLUMN	NULL und NOT NULL können derzeit nicht angegeben werden. Wenn Sie die Nullfähigkeit einer Spalte ändern möchten,

Funktionalität oder Syntax	Beschreibung des Verhaltens oder Unterschieds
	verwenden Sie die PostgreSQL-Anweisung ALTER TABLE..{SET|DROP} NOT NULL.
Leere Spaltennamen ohne Spaltenalias	Die `sqlcmd`- und `psql`-Dienstprogramme behandeln Spalten mit leeren Namen unterschiedlich: • SQL Server `sqlcmd` gibt einen leeren Spaltennamen zurück. • PostgreSQL `psql` gibt einen generierten Spaltennamen zurück.
Die Funktion CHECKSUM	Babelfish und SQL Server verwenden unterschiedliche Hashing-Algorithmen für die CHECKSUM-Funktion. Infolgedessen können sich die von der CHECKSUM-Funktion in Babelfish generierten Hashwerte von denen unterscheiden, die von der CHECKSUM-Funktion in SQL Server generiert wurden.
Standardeinstellung der Spalte	Beim Erstellen einer Spalte wird der Name der Einschränkung ignoriert. Verwenden Sie die folgende Syntax, um eine Spalte zu löschen: `ALTER TABLE...ALTER COLUMN..DROP DEFAULT...`
Beschränkungen	PostgreSQL unterstützt das Ein- und Ausschalten einzelner Einschränkungen nicht. Die Aussage wird ignoriert und eine Warnung ausgegeben.
Beschränkungen, die mit (absteigenden) DESC-Spalten erstellt wurden	Einschränkungen werden mit ASC-Spalten (aufsteigend) erstellt.
Einschränkungen mit IGNORE_DUP_KEY	Einschränkungen werden ohne diese Eigenschaft erstellt.

Funktionalität oder Syntax	Beschreibung des Verhaltens oder Unterschieds
SERVERROLLE ERSTELLEN , ÄNDERN, LÖSCHEN	SERVERROLLE ÄNDERN wird nur für `sysadmin` unterstützt. Alle anderen Syntax wird nicht unterstützt. Der T-SQL-Benutzer in Babelfish hat eine Erfahrung, die SQL Server für die Konzepte eines Logins (Serverprinzipals), einer Datenbank und eines Datenbankbenutzers (Datenbankprinzipal) ähnelt.
CREATE, ALTER LOGIN-Klauseln werden mit eingeschränkter Syntax unterstützt	Das CREATE LOGIN... PASSWORD-Klausel,... DEFAULT_DATABASE-Klausel und... DEFAULT_LANGUAGE-Klausel werden unterstützt. Der ALTER LOGIN... PASSWORD-Klausel wird unterstützt, aber ALTER LOGIN... OLD_PASSWORD-Klausel wird nicht unterstützt. Nur ein Login, der ein sysadmin-Mitglied ist, kann ein Passwort ändern.
Sortierung der Groß- und Kleinschreibung erstellen	Sortierungen unter Berücksichtigung der Groß-/Kleinschreibung werden mit der CREATE DATABASE-Anweisung nicht unterstützt.
CREATE DATABASE Schlüsselwörter und Klaus	Optionen außer COLLATE und CONTAINMENT=NONE werden nicht unterstützt. Die COLLATE-Klausel wird akzeptiert und wird immer auf den Wert von `babelfishpg_tsql.server_collation_name` gesetzt.
CREATE SCHEMA... unterstützende Klauseln	Sie können den Befehl CREATE SCHEMA verwenden, um ein leeres Schema zu erstellen. Verwenden Sie zusätzliche Befehle, um Schemaobjekte zu erstellen.
Die Werte der Datenbank-ID sind bei Babelfish unterschiedlich	Die Master- und tempdb-Datenbanken sind keine Datenbank-IDs 1 und 2.

Funktionalität oder Syntax	Beschreibung des Verhaltens oder Unterschieds
Die Funktion FORMAT für den Datentyp wird mit den folgenden Einschränkungen unterstützt	Der einstellige Meridian wird nicht unterstützt. Das Format „yyy“ in SQL Server gibt 4 Ziffern für Jahre über 1000 zurück, für andere jedoch nur 3 Ziffern. Die Formate „g“ und „R“ werden nicht unterstützt Die Übersetzung des Gebietsschemas „vi-VN“ unterscheidet sich geringfügig.
Bezeichner größer als 63 Zeichen	PostgreSQL unterstützt maximal 63 Zeichen für Bezeichner. Babelfish konvertiert Bezeichner, die länger als 63 Zeichen sind, in einen Namen, der einen Hash des ursprünglichen Namens enthält. Beispiel: Eine Tabelle, die als „AB(ABC12345678901 23456789012345678901234567890123456789012345678 78901234567890“ erstellt wurde, kann in „ABC12345678901234 56789012345678901234567890123456789012345678901234567890“ konvertiert werden.
Unterstützung für IDTITÄT	`IDENTITY` Spalten werden für Datentypen `tinyint`, `smallint`, `int`, `bigint`, `numeric` und `decimal` unterstützt. SQL Server unterstützt Genauigkeit auf 38 Stellen für Datentype n `numeric` und `decimal` in IDENTITY-Spalten. PostgreSQL unterstützt Genauigkeit auf 19 Stellen für Datentype n `numeric` und `decimal` in IDENTITY-Spalten.
Indizes mit IGNORE_DU P_KEY	Die Syntax, die einen Index erstellt, der IGNORE_DUP_KEY enthält, erstellt einen Index, als würde diese Eigenschaft weggelassen.
Indizes mit mehr als 32 Spalten	Ein Index darf nicht mehr als 32 Spalten enthalten. Eingeschl ossene Indexspalten zählen in PostgreSQL auf das Maximum, jedoch nicht in SQL Server.

Funktionalität oder Syntax	Beschreibung des Verhaltens oder Unterschieds
Indizes (gruppiert)	Gruppierte Indizes werden erstellt, als ob NONCLUSTERED angegeben worden wäre.
Index-Klausel	Die folgenden Klauseln werden ignoriert: FILLFACTOR, ALLOW_PAGE_LOCKS, ALLOW_ROW_LOCKS, PAD_INDEX , STATISTICS_NORECOMPUTE, OPTIMIZE_FOR_SEQUE NTIAL_KEY, SORT_IN_TEMPDB, DROP_EXISTING, ONLINE, COMPRESSION_DELAY, MAXDOP und DATA_COMP RESSION
JSON-Support	Die Reihenfolge der Name-Wert-Paare ist nicht garantiert. Der Array-Typ bleibt jedoch unberührt.
LOGIN-Objekte	Alle Optionen für LOGIN-Objekte werden nicht unterstützt, mit Ausnahme von PASSWORD, DEFAULT_DATABASE, DEFAULT_LANGUAGE, ENABLE, DISABLE.
NEWSEQUENTIALID-Fu nktion	Als NEWID implementiert; sequentielles Verhalten ist nicht garantiert. Beim Anrufen von `NEWSEQUENTIALID` generiert PostgreSQL einen neuen GUID-Wert.
Die OUTPUT-Klausel wird mit den folgenden Einschrän kungen unterstützt	OUTPUT und OUTPUT INTO werden in derselben DML-Abfrage nicht unterstützt. Verweise auf Nicht-Zieltabelle von UPDATE- oder DELETE-Operationen in einer OUTPUT-Klausel werden nicht unterstützt. AUSGABE… GELÖSCHT *, EINGEFÜGT* werden in derselben Abfrage nicht unterstützt.
Begrenzung von Prozedur- oder	Babelfish unterstützt maximal 100 Parameter für eine Prozedur oder Funktion.
ROWGUIDCOL	Diese Klausel wird derzeit ignoriert. Referenzfragen `$GUIDG0L` verursachen einen Syntaxfehler.

Funktionalität oder Syntax	Beschreibung des Verhaltens oder Unterschieds
Unterstützung für SEQUENCE	SEQUENCE-Objekte werden für die Datentypen tinyint, smallint, int, bigint, numeric und decimal unterstützt. Aurora PostgreSQL unterstützt Genauigkeit auf 19 Stellen für Datentypen numerisch und dezimal in einer SEQUENCE.
Rollen auf Serverebene	Die Rolle `sysadmin` auf Serverebene wird unterstützt. Andere Rollen auf Serverebene (außer `sysadmin`) werden nicht unterstützt.
Andere Rollen auf Datenbank ebene als `db_owner`	Die Rollen `db_owner` auf Datenbankebene und die benutzerd efinierten Rollen auf Datenbankebene werden unterstützt. Andere Rollen auf Datenbankebene (als db_owner) werden nicht unterstützt.
SQL-Schlüsselwort `SPARSE`	Das Schlüsselwort SPARSE wird akzeptiert und ignoriert.
SQL Schlüsselwortklausel `ON filegroup`	Diese Klausel wird derzeit ignoriert.
SQL-Schlüsselwörter `CLUSTERED` und `NONCLUSTE RED` für Indizes und Beschränkungen	Babelfish akzeptiert und ignoriert `CLUSTERED` und `NONCLUSTE RED` -Schlüsselwörter.
`sysdatabases.cmptl evel`	`sysdatabases.cmptlevel` ist immer auf 120 eingestellt.
tempdb wird beim Neustart nicht neu initialisiert	Permanente Objekte (wie Tabellen und Prozeduren), die in tempdb erstellt wurden, werden beim Neustart der Datenbank nicht entfernt.
TEXTIMAGE_ON Dateigruppe	Babelfish ignoriert die `TEXTIMAGE_ON` *`filegroup`* -Klausel.
Zeitgenauigkeit	Babelfish unterstützt eine 6-stellige Genauigkeit für Sekundenb ruchteile. Bei diesem Verhalten sind keine negativen Auswirkun gen zu erwarten.

Funktionalität oder Syntax	Beschreibung des Verhaltens oder Unterschieds
Transaktionsisolierungsstufen	READUNCOMTED wird genauso behandelt wie READCOMTED.
Virtuell berechnete Spalten (nicht persistent)	Virtuell berechnete Spalten werden als persistent erstellt.
Ohne SCHEMABINDING-Klausel	Diese Klausel wird in Funktionen, Prozeduren, Triggern oder Ansichten nicht unterstützt. Das Objekt wird erstellt, aber als ob WITH SCHEMABINDING angegeben wurde.

Transaktionsisolationsstufen in Babelfish

Babelfish unterstützt die Transaktionsisolationsstufen READ UNCOMMITTED, READ COMMITTED und SNAPSHOT. Ab Babelfish 3.4 werden zusätzliche Isolationsstufen REPEATABLE READ und SERIALIZABLE unterstützt. Alle Isolationsstufen in Babelfish werden mit dem Verhalten der entsprechenden Isolationsstufen in PostgreSQL unterstützt. SQL Server und Babelfish verwenden unterschiedliche zugrunde liegende Mechanismen für die Implementierung von Transaktionsisolationsstufen (Blockierung für gleichzeitigen Zugriff, Sperren, die von Transaktionen gehalten werden, Fehlerbehandlung usw.). Und es gibt einige geringfügige Unterschiede in der Funktionsweise des gleichzeitigen Zugriffs für verschiedene Workloads. Weitere Informationen zu diesem PostgreSQL-Verhalten finden Sie unter Transaktionsisolierung.

Themen

Übersicht über die Transaktionsisolationsstufen

Die ursprünglichen SQL Server-Transaktionsisolierungsstufen basieren auf pessimistischen Sperren, bei denen nur eine Kopie von Daten vorhanden ist und Abfragen Ressourcen wie Zeilen sperren müssen, bevor sie darauf zugreifen können. Später wurde eine Variante der Isolationsstufe „Read Committed“ eingeführt. Dies ermöglicht die Verwendung von Zeilenversionen, um eine bessere Parallelität zwischen Lesern und Autoren zu gewährleisten, die den Zugriff ohne Blockierung verwenden. Darüber hinaus ist eine neue Isolationsstufe namens Snapshot verfügbar. Außerdem werden Zeilenversionen verwendet, um eine bessere Gleichzeitigkeit zu gewährleisten als REPEATABLE READ Isolation Level, indem gemeinsame Sperren für Lesedaten vermieden werden, die bis zum Ende der Transaktion gehalten werden.

Im Gegensatz zu SQL Server basieren alle Transaktionsisolationsstufen in Babelfish auf optimistischer Sperre (MVCC). Jede Transaktion sieht einen Snapshot der Daten entweder am Anfang der Anweisung (READ COMMITTED) oder am Anfang der Transaktion (REPEATABLE READ, SERIALIZABLE), unabhängig vom aktuellen Status der zugrunde liegenden Daten. Daher kann sich das Ausführungsverhalten gleichzeitiger Transaktionen in Babelfish von SQL Server unterscheiden.

Betrachten Sie beispielsweise eine Transaktion mit Isolationsstufe SERIALIZABLE, die zunächst in SQL Server blockiert wurde, später aber erfolgreich ist. Es kann in Babelfish aufgrund eines Serialisierungskonflikts mit einer gleichzeitigen Transaktion fehlschlagen, die dieselben Zeilen liest oder aktualisiert. Es kann auch Fälle geben, in denen die Ausführung mehrerer gleichzeitiger Transaktionen im Vergleich zu SQL Server zu einem anderen Endergebnis in Babelfish führt. Anwendungen, die Isolationsstufen verwenden, sollten gründlich auf Parallelitätsszenarien getestet werden.

Isolationsstufen in SQL Server	Babelfish-Isolationsstufe	PostgreSQL-Isolationsstufe	Kommentare
READ UNCOMMITTED	READ UNCOMMITTED	READ UNCOMMITTED	Read Uncommitted entspricht Read Committed in Babelfish/PostgreSQL
READ COMMITTED	READ COMMITTED	READ COMMITTED	SQL Server Read Committed basiert auf pessimistischen Sperren, Babelfish Read Committed basiert auf Snapshot (MVCC).
READ COMMITTED SNAPSHOT	READ COMMITTED	READ COMMITTED	Beide sind Snapshot-basiert (MVCC), aber nicht genau gleich.
SNAPSHOT	SNAPSHOT	REPEATABLE READ	Genau gleich.
REPEATABLE READ	REPEATABLE READ	REPEATABLE READ	SQL Server Repeatable Read basiert auf pessimistischen Sperren, Babelfish Repeatable Read is Snapshot (MVCC).

Isolationsstufen in SQL Server	Babelfish-Isolationsstufe	PostgreSQL-Isolationsstufe	Kommentare
SERIALIZABLE	SERIALIZABLE	SERIALIZABLE	SQL Server Serializable ist eine pessimistische Isolation, Babelfish Serializable ist Snapshot (MVCC)-basiert.

> **Note**
>
> Die Tabellenhinweise werden derzeit nicht unterstützt und ihr Verhalten wird mithilfe der vordefinierten Escape-Schraffur von Babelfish gesteuert`escape_hatch_table_hints`.

Einrichten der Transaktionsisolationsstufen

Verwenden Sie den folgenden Befehl, um Transaction Isolation Level festzulegen:

Example

```
SET TRANSACTION ISOLATION LEVEL { READ UNCOMMITTED | READ COMMITTED | REPEATABLE READ |
 SNAPSHOT | SERIALIZABLE }
```

Aktivieren oder Deaktivieren von Transaktionsisolationsstufen

Die Transaktionsisolationsstufen REPEATABLE READ und SERIALIZABLE sind in Babelfish standardmäßig deaktiviert und Sie müssen sie explizit aktivieren, indem Sie die `babelfishpg_tsql.isolation_level_repeatable_read` Escape-Schraffur `babelfishpg_tsql.isolation_level_serializable` oder auf `pg_isolation` mit setzen`sp_babelfish_configure`. Weitere Informationen finden Sie unter Verwalten der Babelfish-Fehlerbehandlung mit Escape-Schraffuren.

Im Folgenden finden Sie Beispiele für die Aktivierung oder Deaktivierung der Verwendung von REPEATABLE READ und SERIALIZABLE in der aktuellen Sitzung durch Festlegen der jeweiligen

Escape-Schraffuren. Fügen Sie optional den `server` Parameter ein, um die Escape-Schraffur für die aktuelle Sitzung sowie für alle nachfolgenden neuen Sitzungen festzulegen.

So aktivieren Sie die Verwendung von SET TRANSACTION ISOLATION LEVEL REPEATABLE READ nur in der aktuellen Sitzung.

Example

```
EXECUTE sp_babelfish_configure 'isolation_level_repeatable_read', 'pg_isolation'
```

Um die Verwendung von SET TRANSACTION ISOLATION LEVEL REPEATABLE READ in der aktuellen Sitzung und allen nachfolgenden neuen Sitzungen zu aktivieren.

Example

```
EXECUTE sp_babelfish_configure 'isolation_level_repeatable_read', 'pg_isolation',
 'server'
```

So deaktivieren Sie die Verwendung von SET TRANSACTION ISOLATION LEVEL REPEATABLE READ in der aktuellen Sitzung und nachfolgenden neuen Sitzungen.

Example

```
EXECUTE sp_babelfish_configure 'isolation_level_repeatable_read', 'off', 'server'
```

So aktivieren Sie die Verwendung von SET TRANSACTION ISOLATION LEVEL SERIALIZABLE nur in der aktuellen Sitzung.

Example

```
EXECUTE sp_babelfish_configure 'isolation_level_serializable', 'pg_isolation'
```

So aktivieren Sie die Verwendung von SET TRANSACTION ISOLATION LEVEL SERIALIZABLE in der aktuellen Sitzung und allen nachfolgenden neuen Sitzungen.

Example

```
EXECUTE sp_babelfish_configure 'isolation_level_serializable', 'pg_isolation', 'server'
```

So deaktivieren Sie die Verwendung von SET TRANSACTION ISOLATION LEVEL SERIALIZABLE in der aktuellen Sitzung und nachfolgenden neuen Sitzungen.

Example

```
EXECUTE sp_babelfish_configure 'isolation_level_serializable', 'off', 'server'
```

Unterschiede zwischen Babelfish und SQL Server-Isolationsstufen

Im Folgenden finden Sie einige Beispiele für die Unterschiede bei der Implementierung der ANSI-Isolationsstufen durch SQL Server und Babelfish.

> **Note**
>
> - Wiederholbares Lesen und Snapshot der Isolationsstufe sind in Babelfish gleich.
> - Die Isolationsstufe Lesen nicht festgeschrieben und Lesen festgeschrieben ist in Babelfish gleich.

Das folgende Beispiel zeigt, wie Sie die Basistabelle für alle unten genannten Beispiele erstellen:

```
CREATE TABLE employee (
    id sys.INT NOT NULL PRIMARY KEY,
    name sys.VARCHAR(255)NOT NULL,
    age sys.INT NOT NULL
);
INSERT INTO employee (id, name, age) VALUES (1, 'A', 10);
INSERT INTO employee (id, name, age) VALUES (2, 'B', 20);
INSERT INTO employee (id, name, age) VALUES (3, 'C', 30);
```

Themen

- BABELFISH READ UNCOMMITTED IM VERGLEICH ZU SQL SERVER READ UNCOMMITTED ISOLATIONSSTUFE

- BABELFISH READ COMMIT IM VERGLEICH ZU SQL SERVER READ COMMIT ISOLATIONSSTUFE
- BABELFISH READ COMMIT IM VERGLEICH ZU SQL SERVER READ COMMIT SNAPSHOT ISOLATIONSSTUFE
- BABELFISH-ISOLATIONSSTUFE FÜR WIEDERHOLBARE LESEVORGÄNGE IM VERGLEICH ZUM SQL-SERVER
- SERIALISIERBARE ISOLATIONSSTUFE VON BABELFISH IM VERGLEICH ZU SQL SERVER SERIALISIERBARE ISOLATIONSSTUFE

BABELFISH READ UNCOMMITTED IM VERGLEICH ZU SQL SERVER READ UNCOMMITTED ISOLATIONSSTUFE

LÖSCHEN VON READS IN SQL SERVER

Transaktion 1	Transaktion 2	SQL Server-Lesevorgang nicht festgeschrieben	Babelfish – Lesen nicht festgeschrieben
BEGIN TRANSACTION	BEGIN TRANSACTION		
SET TRANSACTION ISOLATION LEVEL READ UNCOMMITTED;	SET TRANSACTION ISOLATION LEVEL READ UNCOMMITTED;		
	UPDATE Mitarbeiter SET Alter=0;	Aktualisierung erfolgreich.	Aktualisierung erfolgreich.
	INSERT INTO-MitarbeiterWERTE (4, „D“, 40);	Einfügen erfolgreich.	Einfügen erfolgreich.
SELECT * FROM Mitarbeiter;		Transaktion 1 kann nicht festgeschriebene Änderungen aus Transaktion 2 sehen.	Entspricht dem in Babelfish festgeschriebenen Lesen. Nicht festgeschriebene Änderungen von

Transaktion 1	Transaktion 2	SQL Server-Lesevorgang nicht festgeschrieben	Babelfish – Lesen nicht festgeschrieben
			Transaktion 2 sind für Transaktion 1 nicht sichtbar.
	COMMIT		
SELECT * FROM Mitarbeiter;		Zeigt die von Transaktion 2 festgeschriebenen Änderungen an.	Zeigt die von Transaktion 2 festgeschriebenen Änderungen an.

BABELFISH READ COMMIT IM VERGLEICH ZU SQL SERVER READ COMMIT ISOLATIONSSTUFE

READ – WRITE BLOCKING

Transaktion 1	Transaktion 2	SQL Server – Lese-Committed	Babelfish-Lese-Committed
BEGIN TRANSACTION	BEGIN TRANSACTION		
SET TRANSACTION ISOLATION LEVEL READ COMMITTED;	SET TRANSACTION ISOLATION LEVEL READ COMMITTED;		
SELECT * FROM Mitarbeiter;			
	UPDATE Mitarbeiter SET Alter=100 WHERE id = 1;	Aktualisierung erfolgreich.	Aktualisierung erfolgreich.

Transaktion 1	Transaktion 2	SQL Server – Lese-Committed	Babelfish-Lese-Committed
UPDATE Mitarbeiter SET age = 0 WHERE age IN (SELECT MAX(alter) FROM Mitarbeiter);		Schritt blockiert, bis Transaktion 2 ein Commit ausführt.	Änderungen an Transaktion 2 sind noch nicht sichtbar. Aktualisiert die Zeile mit id=3.
	COMMIT	Transaktion 2 wird erfolgreich übergeben. Transaktion 1 ist jetzt entsperrt und sieht das Update von Transaktion 2.	Transaktion 2 wird erfolgreich übergeben.
SELECT * FROM Mitarbeiter;		Transaktion 1 aktualisiert Zeile mit id = 1.	Transaktion 1 aktualisiert Zeile mit id = 3.

BABELFISH READ COMMIT IM VERGLEICH ZU SQL SERVER READ COMMIT SNAPSHOT ISOLATIONSSTUFE

BLOCKIERENDES VERHALTEN FÜR NEUE EINGEFÜGTE ZEILEN

Transaktion 1	Transaktion 2	Snapshot mit festgeschriebenem SQL Server-Lesevorgang	Babelfish-Lese-Committed
BEGIN TRANSACTION	BEGIN TRANSACTION		
SET TRANSACTION ISOLATION LEVEL READ COMMITTED;	SET TRANSACTION ISOLATION LEVEL READ COMMITTED;		

Transaktion 1	Transaktion 2	Snapshot mit festgeschriebenem SQL Server-Lesevorgang	Babelfish-Lese-Committed
INSERT INTO-MitarbeiterWERTE (4, „D“, 40);			
	UPDATE Mitarbeiter SET Alter = 99;	Schritt wird blockiert, bis Transaktion 1 ein Commit ausführt. Die eingefügte Zeile wird durch Transaktion 1 gesperrt.	Drei Zeilen wurden aktualisiert. Die neu eingefügte Zeile ist noch nicht sichtbar.
COMMIT		Commit erfolgreich. Transaktion 2 ist jetzt entsperrt.	Commit erfolgreich.
	SELECT * FROM Mitarbeiter;	Alle 4 Zeilen haben ein Alter von 99.	Die Zeile mit der ID = 4 hat den Alterswert 40, da sie während der Aktualisierungsabfrage für Transaktion 2 nicht sichtbar war. Andere Zeilen werden auf age=99 aktualisiert.

BABELFISH-ISOLATIONSSTUFE FÜR WIEDERHOLBARE LESEVORGÄNGE IM VERGLEICH ZUM SQL-SERVER

LESE-/SCHREIBBLOCKIERUNGSVERHALTEN

Transaktion 1	Transaktion 2	Wiederholbares Lesen in SQL Server	Wiederholbare Lesung in Babelfish
BEGIN TRANSACTION	BEGIN TRANSACTION		
WIEDERHOLBARES LESEN DER TRANSAKTIONSISOLATIONSSTUFE FESTLEGEN;	WIEDERHOLBARES LESEN DER TRANSAKTIONSISOLATIONSSTUFE FESTLEGEN;		
SELECT * FROM Mitarbeiter;			
UPDATE Mitarbeiter SET name='A_TXN1' WHERE id=1;			
	SELECT * FROM Mitarbeiter WHERE id != 1;		
	SELECT * FROM Mitarbeiter;	Transaktion 2 wird blockiert, bis Transaktion 1 ein Commit ausführt.	Transaktion 2 läuft normal ab.
COMMIT			
	SELECT * FROM Mitarbeiter;	Das Update von Transaktion 1 ist sichtbar.	Das Update von Transaktion 1 ist nicht sichtbar.

Transaktion 1	Transaktion 2	Wiederholbares Lesen in SQL Server	Wiederholbare Lesung in Babelfish
COMMIT			
	SELECT * FROM Mitarbeiter;	sieht das Update aus Transaktion 1.	sieht das Update aus Transaktion 1.

VERHALTEN BEIM SCHREIBEN/SCHREIBEN BLOCKIEREN

Transaktion 1	Transaktion 2	Wiederholbares Lesen in SQL Server	Wiederholbare Lesung in Babelfish
BEGIN TRANSACTION	BEGIN TRANSACTION		
WIEDERHOLBARES LESEN DER TRANSAKTIONSISOLATIONSSTUFE FESTLEGEN;	WIEDERHOLBARES LESEN DER TRANSAKTIONSISOLATIONSSTUFE FESTLEGEN;		
UPDATE Mitarbeiter SET name='A_TXN1' WHERE id=1;			
	UPDATE Mitarbeiter SET name='A_TXN2' WHERE id=1;	Transaktion 2 blockiert.	Transaktion 2 blockiert.
COMMIT		Commit erfolgreich und Transaktion 2 wurde entsperrt.	Erfolgreich bestätigen und Transaktion 2 schlägt mit Fehler fehl und konnte den Zugriff aufgrund gleichzeitiger Updates nicht serialisieren.

Transaktion 1	Transaktion 2	Wiederholbares Lesen in SQL Server	Wiederholbare Lesung in Babelfish
	COMMIT	Commit erfolgreich.	Transaktion 2 wurde bereits abgebrochen.
	SELECT * FROM Mitarbeiter;	Zeile mit id=1 hat name='A_TX2'.	Zeile mit id=1 hat name='A_TX1'.

PHANTOM READ

Transaktion 1	Transaktion 2	Wiederholbares Lesen in SQL Server	Wiederholbare Lesung in Babelfish
BEGIN TRANSACTION	BEGIN TRANSACTION		
WIEDERHOLBARES LESEN DER TRANSAKTIONSISOLATIONSSTUFE FESTLEGEN;	WIEDERHOLBARES LESEN DER TRANSAKTIONSISOLATIONSSTUFE FESTLEGEN;		
SELECT * FROM Mitarbeiter;			
	INSERT INTO-MitarbeiterWERTE (4, NewRowName', 20);	Transaktion 2 wird ohne Blockierung fortgesetzt.	Transaktion 2 wird ohne Blockierung fortgesetzt.
	SELECT * FROM Mitarbeiter;	Neu eingefügte Zeile ist sichtbar.	Neu eingefügte Zeile ist sichtbar.
	COMMIT		
SELECT * FROM Mitarbeiter;		Neue Zeile, die von Transaktion 2	Neue Zeile, die von Transaktion 2

Transaktion 1	Transaktion 2	Wiederholbares Lesen in SQL Server	Wiederholbare Lesung in Babelfish
		eingefügt wurde, ist sichtbar.	eingefügt wurde, ist nicht sichtbar.
COMMIT			
SELECT * FROM Mitarbeiter;		Neu eingefügte Zeile ist sichtbar.	Neu eingefügte Zeile ist sichtbar.

VERSCHIEBENDE FINALIFIZIERUNGEN

Transaktion 1	Transaktion 2	Wiederholbares Lesen in SQL Server	Wiederholbare Lesung in Babelfish
BEGIN TRANSACTION	BEGIN TRANSACTION		
WIEDERHOLBARES LESEN DER TRANSAKTIONSISOLATIONSSTUFE FESTLEGEN;	WIEDERHOLBARES LESEN DER TRANSAKTIONSISOLATIONSSTUFE FESTLEGEN;		
UPDATE Mitarbeiter SET age = 100 WHERE age IN (SELECT MIN(alter) FROM Mitarbeiter);		Transaktion 1 aktualisiert Zeile mit der ID 1.	Transaktion 1 aktualisiert Zeile mit der ID 1.
	UPDATE Mitarbeiter SET age = 0 WHERE age IN (SELECT MAX(alter) FROM Mitarbeiter);	Transaktion 2 ist blockiert, da die SELECT-Anweisung versucht, Zeilen zu lesen, die von der UPDATE-Abfrage	Transaktion 2 wird ohne Blockierung fortgesetzt, da der Lesevorgang nie blockiert ist, die SELECT-Anweisung

Transaktion 1	Transaktion 2	Wiederholbares Lesen in SQL Server	Wiederholbare Lesung in Babelfish
		in Transaktion 1 gesperrt wurden.	wird ausgeführt und schließlich wird die Zeile mit der ID = 3 aktualisiert, da die Änderungen an Transaktion 1 noch nicht sichtbar sind.
	SELECT * FROM Mitarbeiter;	Dieser Schritt wird ausgeführt, nachdem Transaktion 1 ein Commit ausgeführt hat. Zeile mit id = 1 wird von Transakti on 2 im vorherigen Schritt aktualisiert und ist hier sichtbar.	Zeile mit id = 3 wird durch Transaktion 2 aktualisiert.
COMMIT		Transaktion 2 ist jetzt entsperrt.	Commit erfolgreich.
	COMMIT		
SELECT * FROM Mitarbeiter;		Beide Transaktionen führen Aktualisierung für Zeile mit id = 1 aus.	Verschiedene Zeilen werden durch Transaktion 1 und 2 aktualisiert.

SERIALISIERBARE ISOLATIONSSTUFE VON BABELFISH IM VERGLEICH ZU SQL SERVER SERIALISIERBARE ISOLATIONSSTUFE

BEREICHSLOCKS IN SQL SERVER

Transaktion 1	Transaktion 2	Serialisierbarer SQL Server	Serialisierbar für Babelfish
BEGIN TRANSACTION	BEGIN TRANSACTION		
LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;	LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;		
SELECT * FROM Mitarbeiter;			
	INSERT INTO-MitarbeiterWERTE (4, „D“, 35);	Transaktion 2 wird blockiert, bis Transaktion 1 festgeschrieben wird.	Transaktion 2 wird ohne Blockierung fortgesetzt.
	SELECT * FROM Mitarbeiter;		
COMMIT		Transaktion 1 wird erfolgreich übergeben. Transaktion 2 ist jetzt entsperrt.	Transaktion 1 wird erfolgreich übergeben.
	COMMIT		
SELECT * FROM Mitarbeiter;		Neu eingefügte Zeile ist sichtbar.	Neu eingefügte Zeile ist sichtbar.

VERSCHIEDERTE FINAL-AbkürzungEN

Transaktion 1	Transaktion 2	Serialisierbarer SQL Server	Serialisierbar für Babelfish
BEGIN TRANSACTION	BEGIN TRANSACTION		
LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;	LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;		
	INSERT INTO-MitarbeiterWERTE (4, „D“, 40);		
UPDATE Mitarbeiter SET Alter =99 WHERE id = 4;		Transaktion 1 wird blockiert, bis Transaktion 2 ein Commit ausführt.	Transaktion 1 wird ohne Blockierung fortgesetzt.
	COMMIT	Transaktion 2 wird erfolgreich übergeben. Transaktion 1 ist jetzt entsperrt.	Transaktion 2 wird erfolgreich übergeben.
COMMIT			
SELECT * FROM Mitarbeiter;		Die neu eingefügte Zeile ist mit dem Alterswert = 99 sichtbar.	Die neu eingefügte Zeile ist mit einem Alterswert von = 40 sichtbar.

EINFÜGEN IN EINE TABELLE MIT EINDEUTIGER EINSCHRÄNKUNG

Transaktion 1	Transaktion 2	Serialisierbarer SQL Server	Serialisierbar für Babelfish
BEGIN TRANSACTION	BEGIN TRANSACTION		
LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;	LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;		
	INSERT INTO-MitarbeiterWERTE (4, „D“, 40);		
INSERT INTO employee VALUES ((SELECT MAX(id)+1 FROM Mitarbeiter), 'E', 50);		Transaktion 1 wird blockiert, bis Transaktion 2 ein Commit ausführt.	Transaktion 1 wird blockiert, bis Transaktion 2 ein Commit ausführt.
	COMMIT	Transaktion 2 wird erfolgreich übergeben. Transaktion 1 ist jetzt entsperrt.	Transaktion 2 wird erfolgreich übergeben. Transaktion 1, die mit einem doppelten Fehlerschlüsselwert abgebrochen wurde, verstößt gegen eine eindeutige Einschränkung.
COMMIT		Transaktion 1 wird erfolgreich übergeben.	Transaktion 1-Commits schlagen mit fehl und konnten den Zugriff aufgrund von

Transaktion 1	Transaktion 2	Serialisierbarer SQL Server	Serialisierbar für Babelfish
			Lese-/Schreibabhängigkeiten zwischen Transaktionen nicht serialisieren.
SELECT * FROM Mitarbeiter;		Zeile (5, „E“, 50) wird eingefügt.	Es sind nur 4 Zeilen vorhanden.

In Babelfish schlagen gleichzeitige Transaktionen, die mit serialisierbarer Isolationsstufe ausgeführt werden, mit einem Serialisierungsanomaliefehler fehl, wenn die Ausführung dieser Transaktion mit allen möglichen seriellen (jeweils einer) Ausführungen dieser Transaktionen inkonsistent ist.

SERIALISIERUNG ANOMALY

Transaktion 1	Transaktion 2	Serialisierbarer SQL Server	Serialisierbar für Babelfish
BEGIN TRANSACTION	BEGIN TRANSACTION		
LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;	LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;		
SELECT * FROM Mitarbeiter;			
UPDATE Mitarbeiter SET Alter=5 WHERE Alter=10;			

Transaktion 1	Transaktion 2	Serialisierbarer SQL Server	Serialisierbar für Babelfish
	SELECT * FROM Mitarbeiter;	Transaktion 2 wird blockiert, bis Transaktion 1 festgeschrieben wird.	Transaktion 2 wird ohne Blockierung fortgesetzt.
	UPDATE Mitarbeiter SET Alter=35 WHERE Alter=30;		
COMMIT		Transaktion 1 wird erfolgreich übergeben.	Transaktion 1 wird zuerst festgeschrieben und kann erfolgreich festgeschrieben werden.
	COMMIT	Transaktion 2 wird erfolgreich übergeben.	Das Commit von Transaktion 2 schlägt mit einem Serialisierungsfehler fehl, die gesamte Transaktion wurde zurückgesetzt. Wiederholen Sie Transaktion 2.
SELECT * FROM Mitarbeiter;		Änderungen von beiden Transaktionen sind sichtbar.	Transaktion 2 wurde zurückgesetzt. Es werden nur Änderungen an Transaktion 1 angezeigt.

In Babelfish ist eine Serialisierungsanomalie nur möglich, wenn alle gleichzeitigen Transaktionen auf Isolationsstufe SERIALIZABLE ausgeführt werden. Nehmen wir zum Beispiel das obige Beispiel, setzen Sie stattdessen Transaktion 2 auf REPEATABLE READ auf Isolationsstufe.

Transaktion 1	Transaktion 2	SQL Server-Isolationsstufen	Babelfish-Isolationsstufen
BEGIN TRANSACTION	BEGIN TRANSACTION		
LEGEN SIE DIE TRANSAKTIONSISOLATIONSSTUFE SERILAISIERBAR FEST;	FESTLEGEN DER TRANSAKTIONSISOLATIONSSTUFE FÜR WIEDERHOLBARES LESEN;		
SELECT * FROM Mitarbeiter;			
UPDATE Mitarbeiter SET Alter=5 WHERE Alter=10;			
	SELECT * FROM Mitarbeiter;	Transaktion 2 wird blockiert, bis Transaktion 1 ein Commit ausführt.	Transaktion 2 wird ohne Blockierung fortgesetzt.
	UPDATE Mitarbeiter SET Alter=35 WHERE Alter=30;		
COMMIT		Transaktion 1 wird erfolgreich übergeben.	Transaktion 1 wird erfolgreich übergeben.
	COMMIT	Transaktion 2 wird erfolgreich übergeben.	Transaktion 2 wird erfolgreich übergeben.

Transaktion 1	Transaktion 2	SQL Server-Isolationsstufen	Babelfish-Isolationsstufen
SELECT * FROM Mitarbeiter;		Änderungen von beiden Transaktionen sind sichtbar.	Änderungen von beiden Transaktionen sind sichtbar.

Verwenden von Babelfish-Funktionen mit eingeschränkter Implementierung

Jede neue Version von Babelfish bietet Unterstützung für weitere Funktionen, die besser auf die T-SQL-Funktionalität und das -Verhalten ausgerichtet sind. Dennoch gibt es einige nicht unterstützte Funktionen und Unterschiede in der aktuellen Implementierung. Im Folgenden finden Sie Informationen zu funktionalen Unterschieden zwischen Babelfish und T-SQL mit einigen Problemumgehungen oder Nutzungshinweisen.

Ab Version 1.2.0 von Babelfish haben die folgenden Funktionen derzeit eingeschränkte Implementierungen:

- SQL Server-Kataloge (Systemansichten) – Die Kataloge `sys.sysconfigures`, `sys.syscurconfigs` und `sys.configurations` unterstützen nur eine einzige schreibgeschützte Konfiguration. `sp_configure` wird zurzeit nicht unterstützt. Weitere Informationen zu den anderen von Babelfish implementierten SQL-Server-Ansichten finden Sie unter Abrufen von Informationen aus dem Babelfish-Systemkatalog.
- GRANT-Berechtigungen – GRANT...TO PUBLIC wird unterstützt, GRANT…TO PUBLIC WITH GRANT OPTION derzeit hingegen nicht.
- SQL-Server-Eigentumskette und Beschränkung des Berechtigungsmechanismus – In Babelfish funktioniert die SQL-Server-Eigentumskette für Ansichten, aber nicht für gespeicherte Prozeduren. Dies bedeutet, dass Prozeduren expliziten Zugriff auf andere Objekte gewährt werden muss, die demselben Eigentümer gehören wie die aufrufenden Prozeduren. In SQL Server reicht es aus, dem Aufrufer EXECUTE-Berechtigungen für die Prozedur zu erteilen, um andere Objekte aufzurufen, die demselben Eigentümer gehören. In Babelfish müssen dem Aufrufer auch Berechtigungen für die Objekte erteilt werden, auf die die Prozedur zugreift.
- Auflösung unqualifizierter (ohne Schemanamen) Objektreferenzen – Wenn ein SQL-Objekt (Prozedur, Ansicht, Funktion oder Trigger) auf ein Objekt verweist, ohne es mit einem Schemanamen zu qualifizieren, löst SQL Server den Schemanamen des Objekts unter Verwendung des Schemanamens des SQL-Objekts auf, in dem die Referenz auftritt. Derzeit weicht

die Auflösung in Babelfish davon ab. Hier wird das Standardschema des Datenbankbenutzers verwendet, der die Prozedur ausführt.

- Standardschemaänderungen, Sitzungen und Verbindungen – Wenn Benutzer ihr Standardschema mit `ALTER USER...WITH DEFAULT SCHEMA` ändern, wird die Änderung in dieser Sitzung sofort wirksam. Für andere derzeit verbundenen Sitzungen, die demselben Benutzer gehören, unterscheidet sich das Timing jedoch wie folgt:
  - Für SQL Server: Die Änderung wird für diesen Benutzer sofort über alle anderen Verbindungen wirksam.
  - Für Babelfish: Die Änderung wird für diesen Benutzer nur für neue Verbindungen wirksam.
- ROWVERSION- und TIMESTAMP-Datentypimplementierung und Escape-Schraffureinstellung – Die ROWVERSION- und TIMESTAMP-Datentypen werden jetzt in Babelfish unterstützt. Um ROWVERSION oder TIMESTAMP in Babelfish zu verwenden, müssen Sie die Einstellung für die Escape-Schraffur `babelfishpg_tsql.escape_hatch_rowversion` von seinem Standardwert (strict) in `ignore` ändern. Die Babelfish-Implementierung der ROWVERSION- und TIMESTAMP-Datentypen ist meist semantisch identisch mit SQL Server, mit folgenden Ausnahmen:
  - Die integrierte @@DBTS-Funktion verhält sich ähnlich wie SQL Server, weist jedoch kleine Unterschiede auf. Anstatt den zuletzt verwendeten Wert für `SELECT @@DBTS` zurückzugeben, generiert Babelfish aufgrund der zugrunde liegenden PostgreSQL-Datenbank-Engine und seiner Multi-Version Concurrency Control (MVCC) einen neuen Zeitstempel.
  - In SQL Server erhält jede eingefügte oder aktualisierte Zeile einen eindeutigen ROWVERSION/TIMESTAMP-Wert. In Babelfish wird jeder eingefügten Zeile, die durch dieselbe Anweisung aktualisiert wurde, derselbe ROWVERSION/TIMESTAMP-Wert zugewiesen.

    Wenn sich beispielsweise eine UPDATE- oder INSERT-SELECT-Anweisung auf mehrere Zeilen auswirkt, haben die betroffenen Zeilen in SQL Server alle unterschiedliche Werte in ihrer ROWVERSION/TIMESTAMP-Spalte. In Babelfish (PostgreSQL) haben die Zeilen denselben Wert.
  - Wenn Sie in SQL Server eine neue Tabelle mit SELECT-INTO erstellen, können Sie einen expliziten Wert (wie NULL) in eine zu erstellende ROWVERSION/TIMESTAMP-Spalte umwandeln. Wenn Sie denselben Vorgang in Babelfish ausführen, wird jeder Zeile in der neuen Tabelle von Babelfish ein tatsächlicher ROWVERSION/TIMESTAMP-Wert zugewiesen.

  Diese geringfügigen Unterschiede in ROWVERSION/TIMESTAMP-Datentypen sollten keine nachteiligen Auswirkungen auf Anwendungen haben, die in Babelfish ausgeführt werden.

Schemaerstellung, Eigentümerschaft und Berechtigungen – Berechtigungen zum Erstellen von Objekten in einem Schema, das einem Nicht-DBO-Benutzer gehört (mit `CREATE SCHEMA` *`schema name`* `AUTHORIZATION` *`user name`*), unterscheiden sich für Nicht-DBO-Benutzer von SQL Server und Babelfish, wie in der folgenden Tabelle dargestellt:

Der Datenbankbenutzer (Nicht-DBO), der Eigentümer des Schemas ist, kann folgende Vorgänge ausführen:	SQL Server	Babelfish
Objekte im Schema ohne zusätzliche Erteilungen durch den DBO erstellen?	Nein	Ja
Zugriff auf von DBO erstellte Objekte im Schema ohne zusätzliche Erteilungen?	Ja	Nein

Verbessern der Abfrageleistung in Babelfish

Mithilfe von Abfragehinweisen und dem PostgreSQL-Optimierer können Sie eine schnellere Abfrageverarbeitung in Babelfish erzielen.

Themen

- Verwenden eines Erläuterungsplans zur Verbesserung der Abfrageleistung von Babelfish
- Verwenden von T-SQL-Abfragehinweise zur Verbesserung der Abfrageleistung von Babelfish

Sie können die Abfrageleistung auch mithilfe der Prozedur `sp_babelfish_volatility` verbessern. Weitere Informationen finden Sie unter sp_babelfish_volatility.

Verwenden eines Erläuterungsplans zur Verbesserung der Abfrageleistung von Babelfish

Ab Version 2.1.0 enthält Babelfish zwei Funktionen, die den PostgreSQL-Optimierer transparent verwenden, um geschätzte und tatsächliche Abfragepläne für T-SQL-Abfragen am TDS-Port zu generieren. Diese Funktionen ähneln der Verwendung von SET STATISTICS PROFILE oder SET SHOWPLAN_ALL mit SQL-Server-Datenbanken, um langsam laufende Abfragen zu identifizieren und zu verbessern.

> **Note**
>
> Das Abrufen von Abfrageplänen von Funktionen, Kontrollflüssen und Cursor wird derzeit nicht unterstützt.

In der Tabelle finden Sie einen Vergleich der Funktionen zur Erläuterung des Abfrageplans in SQL Server, Babelfish und PostgreSQL.

SQL Server	Babelfish	PostgreSQL
SHOWPLAN_ALL	BABELFISH_SHOWPLAN_ALL	EXPLAIN
STATISTICS PROFILE	BABELFISH_STATISTICS PROFILE	EXPLAIN ANALYZE
Verwendet den SQL-Server-Optimierer	Verwendet den PostgreSQL-Optimierer	Verwendet den PostgreSQL-Optimierer
Ein- und Ausgabeformat von SQL Server	Eingabeformat von SQL Server und Ausgabeformat von PostgreSQL	Ein- und Ausgabeformat von PostgreSQL
Für die Sitzung einstellen	Für die Sitzung einstellen	Auf eine bestimmte Anweisung anwenden
Unterstützt Folgendes: • SELECT • INSERT • AKTUALISIERUNG • DELETE • CURSOR • CREATE • EXECUTE	Unterstützt Folgendes: • SELECT • INSERT • AKTUALISIERUNG • DELETE • CREATE • EXECUTE • EXEC • RAISEERROR	Unterstützt Folgendes: • SELECT • INSERT • AKTUALISIERUNG • DELETE • CURSOR • CREATE • EXECUTE

SQL Server	Babelfish	PostgreSQL
• EXEC und Funktionen, einschließlich Kontrollfluss (CASE, WHILE-BREAK-CONTINUE, WAITFOR, BEGIN-END, IF-ELSE usw.)	• THROW • PRINT • USE	

Verwenden Sie die Babelfish-Funktionen wie folgt:

- SET BABELFISH_SHOWPLAN_ALL [ON|OFF] – Legen Sie diese Funktion auf ON fest, um einen geschätzten Abfrageausführungsplan zu generieren. Diese Funktion implementiert das Verhalten des PostgreSQL-Befehls `EXPLAIN`. Verwenden Sie diesen Befehl, um den Erläuterungsplan für die angegebene Abfrage abzurufen.
- SET BABELFISH_STATISTICS PROFILE [ON|OFF] – Legen Sie diese Funktion auf ON fest, um tatsächliche Abfrageausführungspläne zu erhalten. Diese Funktion implementiert das Verhalten des PostgreSQL-Befehls `EXPLAIN ANALYZE`.

Weitere Informationen zu den PostgreSQL-Befehlen `EXPLAIN` und `EXPLAIN ANALYZE` finden Sie unter EXPLAIN in der PostgreSQL-Dokumentation.

> **Note**
>
> Ab Version 2.2.0 können Sie den Parameter `escape_hatch_showplan_all` auf Ignorieren einstellen, um die Verwendung des Präfixes BABELFISH_ in der SQL-Server-Syntax für die SET-Befehle `SHOWPLAN_ALL` und `STATISTICS PROFILE` zu vermeiden.

Die folgende Befehlssequenz aktiviert beispielsweise die Abfrageplanung und gibt dann einen geschätzten Abfrageausführungsplan für die SELECT-Anweisung zurück, ohne die Abfrage auszuführen. In diesem Beispiel wird die SQL-Server-Beispieldatenbank `northwind` mit dem `sqlcmd`-Befehlszeilentool zum Abfragen des TDS-Ports verwendet:

```
1> SET BABELFISH_SHOWPLAN_ALL ON
2> GO
1> SELECT t.territoryid, e.employeeid FROM
```

```
2> dbo.employeeterritories e, dbo.territories t
3> WHERE e.territoryid=e.territoryid ORDER BY t.territoryid;
4> GO

QUERY PLAN


------------------------------------------------------------------------------


Query Text: SELECT t.territoryid, e.employeeid FROM
dbo.employeeterritories e, dbo.territories t
WHERE e.territoryid=e.territoryid ORDER BY t.territoryid
Sort  (cost=6231.74..6399.22 rows=66992 width=10)
  Sort Key: t.territoryid NULLS FIRST
  ->  Nested Loop  (cost=0.00..861.76 rows=66992 width=10)
        ->  Seq Scan on employeeterritories e  (cost=0.00..22.70 rows=1264 width=4)
              Filter: ((territoryid)::"varchar" IS NOT NULL)
        ->  Materialize  (cost=0.00..1.79 rows=53 width=6)
              ->  Seq Scan on territories t  (cost=0.00..1.53 rows=53 width=6)
```

Wenn Sie mit der Überprüfung und Anpassung Ihrer Abfrage fertig sind, deaktivieren Sie die Funktion wie nachfolgend gezeigt:

```
1> SET BABELFISH_SHOWPLAN_ALL OFF
```

Wenn BABELFISH_STATISTICS PROFILE auf ON festgelegt ist, gibt jede ausgeführte Abfrage ihre reguläre Ergebnismenge zurück, gefolgt von einer zusätzlichen Ergebnismenge, die tatsächliche Abfrageausführungspläne anzeigt. Babelfish generiert den Abfrageplan, der die schnellste Ergebnismenge liefert, wenn die SELECT-Anweisung aufgerufen wird.

```
1> SET BABELFISH_STATISTICS PROFILE ON
1>
2> GO
1> SELECT e.employeeid, t.territoryid FROM
2> dbo.employeeterritories e, dbo.territories t
3> WHERE t.territoryid=e.territoryid ORDER BY t.territoryid;
4> GO
```

Die Ergebnismenge und der Abfrageplan werden zurückgegeben (dieses Beispiel zeigt nur den Abfrageplan).

```
QUERY PLAN


------------------------------------------------------------------------------
Query Text: SELECT e.employeeid, t.territoryid FROM
dbo.employeeterritories e, dbo.territories t
WHERE t.territoryid=e.territoryid ORDER BY t.territoryid
Sort  (cost=42.44..43.28 rows=337 width=10)
  Sort Key: t.territoryid NULLS FIRST


  ->  Hash Join  (cost=2.19..28.29 rows=337 width=10)
       Hash Cond: ((e.territoryid)::"varchar" = (t.territoryid)::"varchar")
        ->  Seq Scan on employeeterritories e  (cost=0.00..22.70 rows=1270 width=36)
        ->  Hash  (cost=1.53..1.53 rows=53 width=6)
             ->  Seq Scan on territories t  (cost=0.00..1.53 rows=53 width=6)
```

Weitere Informationen darüber, wie Sie Ihre Abfragen und die vom PostgreSQL-Optimierer zurückgegebenen Ergebnisse analysieren können, finden Sie unter explain.depesz.com. Weitere Informationen zu den PostgreSQL-Befehlen EXPLAIN und EXPLAIN ANALYZE finden Sie unter EXPLAIN in der PostgreSQL-Dokumentation.

Parameter, die Erläuterungsoptionen von Babelfish steuern

Sie können die in der folgenden Tabelle aufgeführten Parameter verwenden, um die Art der Informationen zu steuern, die in Ihrem Abfrageplan angezeigt werden.

Parameter	Beschreibung
babelfishpg_tsql.explain_buffers	Ein boolescher Wert, der Informationen zur Puffernutzung für den Optimierer ein- und ausschaltet. (Standardwert: off) (Zulässig: off, on)
babelfishpg_tsql.explain_costs	Ein boolescher Wert, der geschätzte Start- und Gesamtkosteninformationen für den Optimiere r ein- und ausschaltet. (Standardwert: on) (Zulässig: off, on)

Parameter	Beschreibung
babelfishpg_tsql.explain_format	Gibt das Ausgabeformat für den EXPLAIN-Plan an. (Standardwert: text) (Zulässig: text, xml, json, yaml)
babelfishpg_tsql.explain_settings	Ein boolescher Wert, der die Aufnahme von Informationen zu Konfigurationsparametern in die EXPLAIN-Planausgabe ein- oder ausschaltet. (Standardwert: off) (Zulässig: off, on)
babelfishpg_tsql.explain_summary	Ein boolescher Wert, der zusammenfassende Informationen wie die Gesamtzeit nach dem Abfrageplan ein- oder ausschaltet. (Standardwert: on) (Zulässig: off, on)
babelfishpg_tsql.explain_timing	Ein boolescher Wert, der die tatsächliche Startzeit und die Zeit, die in jedem Knoten in der Ausgabe verbracht wird, ein- oder ausschaltet. (Standardwert: on) (Zulässig: off, on)
babelfishpg_tsql.explain_verbose	Ein boolescher Wert, der die detaillierteste Version eines Erläuterungsplans ein- oder ausschaltet. (Standardwert: off) (Zulässig: off, on)
babelfishpg_tsql.explain_wal	Ein boolescher Wert, der die Generierung von WAL-Datensatzinformationen im Rahmen eines Erläuterungsplans aktiviert (oder deaktiviert). (Standardwert: off) (Zulässig: off, on)

Sie können die Werte aller Babelfish-bezogenen Parameter in Ihrem System überprüfen, indem Sie entweder den PostgreSQL-Client oder den SQL-Server-Client verwenden. Führen Sie den folgenden Befehl aus, um Ihre aktuellen Parameterwerte abzurufen:

```
1> execute sp_babelfish_configure '%explain%';
```

```
2> GO
```

In der folgenden Ausgabe sehen Sie, dass alle Einstellungen für diesen speziellen Babelfish-DB-Cluster auf ihre Standardwerte festgelegt sind. In diesem Beispiel wird nicht die gesamte Ausgabe gezeigt.

```
             name                    setting                     short_desc
--------------------------------- --------
 ---------------------------------------------------------
babelfishpg_tsql.explain_buffers   off      Include information on buffer usage
babelfishpg_tsql.explain_costs     on       Include information on estimated startup
 and total cost
babelfishpg_tsql.explain_format    text     Specify the output format, which can be
 TEXT, XML, JSON, or YAML
babelfishpg_tsql.explain_settings  off      Include information on configuration
 parameters
babelfishpg_tsql.explain_summary   on       Include summary information (e.g.,totaled
 timing information) after the query plan
babelfishpg_tsql.explain_timing    on       Include actual startup time and time spent
 in each node in the output
babelfishpg_tsql.explain_verbose   off      Display additional information regarding
 the plan
babelfishpg_tsql.explain_wal       off      Include information on WAL record
 generation

(8 rows affected)
```

Sie können die Einstellung für diese Parameter mit `sp_babelfish_configure` ändern, wie im folgenden Beispiel veranschaulicht.

```
1> execute sp_babelfish_configure 'explain_verbose', 'on';
2> GO
```

Wenn Sie die Einstellung auf einer clusterweiten Ebene dauerhaft festlegen möchten, schließen Sie das Schlüsselwort Server ein, wie im folgenden Beispiel gezeigt.

```
1> execute sp_babelfish_configure 'explain_verbose', 'on', 'server';
2> GO
```

Verwenden von T-SQL-Abfragehinweise zur Verbesserung der Abfrageleistung von Babelfish

Ab Version 2.3.0 unterstützt Babelfish die Verwendung von Abfragehinweisen mit `pg_hint_plan`. In Aurora PostgreSQL ist `pg_hint_plan` standardmäßig installiert. Weitere Informationen zur PostgreSQL-Erweiterung `pg_hint_plan` finden Sie unter https://github.com/ossc-db/pg_hint_plan. Weitere Informationen zu der Version dieser Erweiterung, die von Aurora PostgreSQL unterstützt wird, finden Sie unter Versionen der Erweiterungen für Amazon Aurora PostgreSQL in den Versionshinweisen für Aurora PostgreSQL.

Mit dem Abfrageoptimierer kann für jede SQL-Anweisung der bestmögliche Ausführungsplans ermittelt werden. Bei der Auswahl eines Plans berücksichtigt der Abfrageoptimierer sowohl das Kostenmodell der Engine als auch die Spalten- und Tabellenstatistiken. Der vorgeschlagene Plan entspricht jedoch möglicherweise nicht den Anforderungen Ihrer Datensätze. Daher werden mit Abfragehinweisen die Leistungsprobleme angesprochen, um die Ausführungspläne zu verbessern. Ein `query hint` ist Syntax, die dem SQL-Standard hinzugefügt wurde und die Datenbank-Engine anweist, wie die Abfrage auszuführen ist. Beispielsweise kann ein Hinweis die Engine anweisen, einem sequenziellen Scan zu folgen und jeden Plan zu überschreiben, den der Abfrageoptimierer ausgewählt hat.

Aktivieren von T-SQL-Abfragehinweisen in Babelfish

Derzeit ignoriert Babelfish standardmäßig alle T-SQL-Hinweise. Wenn Sie T-SQL-Hinweise anwenden möchten, führen Sie den Befehl `sp_babelfish_configure` mit dem Wert enable_pg_hint auf ON (EIN) aus.

```
EXECUTE sp_babelfish_configure 'enable_pg_hint', 'on' [, 'server']
```

Sie können die Einstellungen auf einer clusterweiten Ebene dauerhaft festlegen, indem Sie das Schlüsselwort Server einschließen. Verwenden Sie „Server“ nicht, wenn Sie die Einstellung nur für die aktuelle Sitzung festlegen möchten.

Nach Einstellung von `enable_pg_hint` auf ON (EIN) wendet Babelfish die folgenden T-SQL-Hinweise an.

- INDEX-Hinweise
- JOIN-Hinweise
- FORCE ORDER-Hinweis
- MAXDOP-Hinweis

Mit der folgenden Befehlssequenz wird beispielsweise `pg_hint_plan` aktiviert.

```
1> CREATE TABLE t1 (a1 INT PRIMARY KEY, b1 INT);
2> CREATE TABLE t2 (a2 INT PRIMARY KEY, b2 INT);
3> GO
1> EXECUTE sp_babelfish_configure 'enable_pg_hint', 'on';
2> GO
1> SET BABELFISH_SHOWPLAN_ALL ON;
2> GO
1> SELECT * FROM t1 JOIN t2 ON t1.a1 = t2.a2; --NO HINTS (HASH JOIN)
2> GO
```

Auf die SELECT-Anweisung wird kein Hinweis angewendet. Der Abfrageplan wird ohne Hinweis zurückgegeben.

```
QUERY PLAN


------------------------------------------------------------------------------
Query Text: SELECT * FROM t1 JOIN t2 ON t1.a1 = t2.a2
Hash Join (cost=60.85..99.39 rows=2260 width=16)
 Hash Cond: (t1.a1 = t2.a2)
 -> Seq Scan on t1 (cost=0.00..32.60 rows=2260 width=8)
 -> Hash (cost=32.60..32.60 rows=2260 width=8)
 -> Seq Scan on t2 (cost=0.00..32.60 rows=2260 width=8)
```

```
1> SELECT * FROM t1 INNER MERGE JOIN t2 ON t1.a1 = t2.a2;
2> GO
```

Der Abfragehinweis wird auf die SELECT-Anweisung angewendet. Die folgende Ausgabe zeigt, dass der Abfrageplan mit Merge Join zurückgegeben wird.

```
QUERY PLAN


------------------------------------------------------------------------------
Query Text: SELECT/*+ MergeJoin(t1 t2) Leading(t1 t2)*/ * FROM t1 INNER JOIN t2 ON
 t1.a1 = t2.a2
```

```
Merge Join (cost=0.31..190.01 rows=2260 width=16)
 Merge Cond: (t1.a1 = t2.a2)
 -> Index Scan using t1_pkey on t1 (cost=0.15..78.06 rows=2260 width=8)
 -> Index Scan using t2_pkey on t2 (cost=0.15..78.06 rows=2260 width=8)
```

```
1> SET BABELFISH_SHOWPLAN_ALL OFF;
2> GO
```

Einschränkungen

Beachten Sie bei der Verwendung der Abfragehinweise die folgenden Einschränkungen:

- Wenn ein Abfrageplan zwischengespeichert wird, bevor `enable_pg_hint` aktiviert wird, werden in derselben Sitzung keine Hinweise angewendet. Sie werden in der neuen Sitzung angewendet.
- Wenn Schemanamen explizit angegeben werden, können keine Hinweise angewendet werden. Sie können Tabellenaliase als Problemumgehung verwenden.
- Ein Abfragehinweis kann nicht auf Ansichten und Unterabfragen angewendet werden.
- Hinweise funktionieren nicht für UPDATE/DELETE-Anweisungen mit JOINs.
- Ein Indexhinweis für einen nicht existierenden Index oder eine Tabelle wird ignoriert.
- Der FORCE ORDER-Hinweis funktioniert nicht für HASH JOINs und Nicht-ANSI JOINS.

Verwenden von Aurora PostgreSQL-Erweiterungen mit Babelfish

Aurora PostgreSQL bietet Erweiterungen für die Arbeit mit anderen AWS Diensten. Dies sind optionale Erweiterungen, die verschiedene Anwendungsfälle unterstützen, z. B. die Verwendung von Amazon S3 mit Ihrem DB-Cluster zum Importieren oder Exportieren von Daten.

- Wenn Sie Daten aus einem Amazon S3 Bucket in Ihren Babelfish-DB-Cluster importieren möchten, richten Sie die Aurora-PostgreSQL-Erweiterung `aws_s3` ein. Mit dieser Erweiterung können Sie auch Daten aus Ihrem Aurora-PostgreSQL-DB-Cluster in einen Amazon S3 Bucket exportieren.
- AWS Lambda ist ein Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Sie können Lambda-Funktionen verwenden, um zum Beispiel Ereignisbenachrichtigungen von Ihrer DB-Instance zu verarbeiten. Weitere Informationen zu Lambda finden Sie unter Was ist AWS Lambda? im AWS Lambda -Entwicklerhandbuch. Zum Aufrufen von Lambda-Funktionen aus Ihrem Babelfish-DB-Cluster richten Sie die Aurora-PostgreSQL-Erweiterung `aws_lambda` ein.

Um diese Erweiterungen für Ihren Babelfish-Cluster einzurichten, müssen Sie zuerst dem internen Babelfish-Benutzer die Erlaubnis erteilen, die Erweiterungen zu laden. Nachdem Sie die Berechtigung erteilt haben, können Sie dann Aurora-PostgreSQL-Erweiterungen laden.

Aktivieren von Aurora-PostgreSQL-Erweiterungen in Ihrem Babelfish-DB-Cluster

Bevor Sie die `aws_s3`- oder `aws_lambda`-Erweiterungen laden können, müssen Sie Ihrem Babelfish-DB-Cluster die erforderlichen Berechtigungen gewähren.

In der folgenden Vorgehensweise wird das `psql`-PostgreSQL-Befehlszeilen-Tool für die Verbindung mit dem DB-Cluster verwendet. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrem psql. Sie können auch pgAdmin verwenden. Details hierzu finden Sie unter Herstellen einer Verbindung mit dem DB-Cluster mit pgAdmin.

Dieses Verfahren lädt sowohl `aws_s3` als auch `aws_lambda` nacheinander. Sie müssen nicht beides laden, wenn Sie nur eine dieser Erweiterungen verwenden möchten. Die `aws_commons`-Erweiterung wird von beiden Optionen benötigt und wird standardmäßig geladen, wie in der Ausgabe gezeigt.

Richten Sie Babelfish-DB-Cluster mit Berechtigungen für die Aurora-PostgreSQL-Erweiterungen ein

1. Stellen Sie eine Verbindung mit Ihrem Babelfish-DB-Cluster her. Verwenden Sie den Namen für den „Hauptbenutzer“ (-U), den Sie beim Erstellen des Babelfish-DB-Clusters angegeben haben. In den Beispielen wird der Standard (`postgres`) dargestellt.

   Für LinuxmacOS, oderUnix:

   ```
   psql -h your-Babelfish.cluster.444455556666-us-east-1.rds.amazonaws.com \
   -U postgres \
   -d babelfish_db \
   -p 5432
   ```

   Windows:

   ```
   psql -h your-Babelfish.cluster.444455556666-us-east-1.rds.amazonaws.com ^
   -U postgres ^
   -d babelfish_db ^
   -p 5432
   ```

   Der Befehl antwortet mit einer Aufforderung zur Eingabe des Passworts für den Benutzernamen (-U).

```
Password:
```

Geben Sie das Passwort für den Benutzernamen (-U) für den DB-Cluster ein. Wenn die Verbindung erfolgreich ist, wird eine Ausgabe ähnlich der Folgenden angezeigt.

```
psql (13.4)
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256,
 compression: off)
Type "help" for help.

postgres=>
```

2. Erteilen Sie dem internen Babelfish-Benutzer Berechtigungen zum Erstellen und Laden von Erweiterungen.

```
babelfish_db=> GRANT rds_superuser TO master_dbo;
GRANT ROLE
```

3. Erstellen und laden Sie die `aws_s3`-Erweiterung. Die `aws_commons`-Erweiterung ist erforderlich und wird automatisch mit `aws_s3` installiert.

```
babelfish_db=> create extension aws_s3 cascade;
NOTICE:  installing required extension "aws_commons"
CREATE EXTENSION
```

4. Erstellen und laden Sie die `aws_lambda`-Erweiterung.

```
babelfish_db=> create extension aws_lambda cascade;
CREATE EXTENSION
babelfish_db=>
```

Verwenden von Babelfish mit Amazon S3

Wenn Sie noch keinen Amazon-S3-Bucket für Ihren Babelfish-DB-Cluster haben, können Sie einen erstellen. Gewähren Sie Zugriff für jeden Amazon-S3-Bucket, den Sie verwenden möchten.

Bevor Sie versuchen, Daten mit einem Amazon-S3-Bucket zu importieren oder zu exportieren, führen Sie die folgenden einmaligen Schritte aus.

Gewähren Sie Ihrer Babelfish-DB-Instance Zugriff auf Ihren Amazon-S3-Bucket

1. Erstellen Sie bei Bedarf einen Amazon-S3-Bucket für Ihre Babelfish-Instance. Befolgen Sie dazu die Anweisungen unter Erstellen eines Buckets im Benutzerhandbuch zum Amazon Simple Storage Service.
2. Laden Sie Dateien in Ihren Amazon-S3-Bucket hoch. Befolgen Sie dazu die Schritte unter Hinzufügen eines Objekts zu einem Bucket im Benutzerhandbuch zum Amazon Simple Storage Service.
3. Richten Sie Berechtigungen nach Bedarf ein:

   - Zum Importieren von Daten aus Amazon S3 benötigt der Babelfish-DB-Cluster die Berechtigung für den Zugriff auf den Bucket. Wir empfehlen, eine AWS Identity and Access Management (IAM-) Rolle zu verwenden und dieser Rolle für Ihren Cluster eine IAM-Richtlinie zuzuordnen. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Verwenden einer IAM-Rolle für den Zugriff auf einen Amazon S3-Bucket.
   - Wenn Sie Daten aus Ihrem Babelfish-DB-Cluster exportieren möchten, muss Ihrem Cluster Zugriff auf den Amazon S3 Bucket gewährt werden. Wie beim Importieren empfehlen wir die Verwendung einer IAM-Rolle und -Richtlinie. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Einrichten des Zugriffs auf einen Amazon S3-Bucket.

Sie können Amazon S3 jetzt mit der `aws_s3`-Erweiterung mit Ihrem Babelfish-DB-Cluster verwenden.

Importieren von Daten aus Amazon S3 nach Babelfish und exportieren von Babelfish-Daten nach Amazon S3

1. Verwenden Sie die `aws_s3`-Erweiterung mit Ihrem Babellfish-DB-Cluster.

   Verweisen Sie in diesem Fall auf die Tabellen, wie sie in PostgreSQL existieren. Das heißt, beim Import in eine Babelfish-Tabelle namens `[database].[schema].[tableA]` bezeichnen Sie diese Tabelle in der `aws_s3`-Funktion als `database_schema_tableA`:

   - Ein Beispiel für die Verwendung einer `aws_s3`-Funktion zum Importieren von Daten finden Sie unter Importieren von Daten aus Amazon S3 in Ihren Aurora PostgreSQL DB-Cluster.
   - Beispiele für die Verwendung von `aws_s3`-Funktionen zum Exportieren von Daten finden Sie unter Exportieren von Abfragedaten mithilfe der Funktion aws_s3.query_export_to_s3.
2. Verweisen Sie mit der PostgreSQL-Benennung auf Babelfish-Tabellen, wenn Sie die `aws_s3`-Erweiterung und Amazon S3 wie in folgender Tabelle verwenden.

Babelfish-Tabelle	Aurora PostgreSQL-Tabelle
database.*schema*.*table*	*database*_*schema*_*table*

Weitere Informationen zur Verwendung von Amazon S3 mit Aurora PostgreSQL finden Sie unter Importieren von Amazon S3 in einen Aurora-PostgreSQL-DB-Cluster und Exportieren von Daten aus einem/einer Aurora PostgreSQL-DB-Cluster zu Amazon S3.

Verwenden Sie Babelfish mit AWS Lambda

Nach dem die `aws_lambda`-Erweiterung in Ihrem Babelfish-DB-Cluster geladen ist und bevor Sie Lambda-Funktionen aufrufen, gewähren Sie Lambda wie folgt Zugriff auf Ihren DB-Cluster.

Richten Sie den Zugriff für Ihren Babelfish-DB-Cluster zur Funktion mit Lambda ein

Dieses Verfahren verwendet die AWS CLI , um die IAM-Richtlinie und -Rolle zu erstellen und diese dem Babelfish-DB-Cluster zuzuordnen.

1. Erstellen Sie eine IAM-Richtlinie, die den Zugriff auf Lambda von Ihrem Babelfish-DB-Cluster aus erlaubt.

```
aws iam create-policy  --policy-name rds-lambda-policy --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "AllowAccessToExampleFunction",
        "Effect": "Allow",
        "Action": "lambda:InvokeFunction",
        "Resource": "arn:aws:lambda:aws-region:444455556666:function:my-function"
        }
    ]
}'
```

2. Erstellen Sie eine IAM-Rolle, die die Richtlinie zur Laufzeit annehmen kann.

```
aws iam create-role  --role-name rds-lambda-role --assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal": {
```

```
            "Service": "rds.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
        }
    ]
}'
```

3. Fügen Sie der Rolle die -Richtlinie an.

```
aws iam attach-role-policy \
    --policy-arn arn:aws:iam::444455556666:policy/rds-lambda-policy \
    --role-name rds-lambda-role --region aws-region
```

4. Hängen Sie die Rolle an Ihren Babelfish-DB-Cluster an.

```
aws rds add-role-to-db-cluster \
       --db-cluster-identifier my-cluster-name \
       --feature-name Lambda \
       --role-arn  arn:aws:iam::444455556666:role/rds-lambda-role   \
       --region aws-region
```

Nachdem Sie diese Aufgaben durchgeführt haben, können Sie Ihre Lambda-Funktionen aufrufen. Weitere Informationen und Beispiele für die Einrichtung AWS Lambda des Aurora PostgreSQL-DB-Clusters mit AWS Lambda finden Sie unter. Schritt 2: Konfigurieren Sie IAM für Ihren Aurora PostgreSQL-DB-Cluster, und AWS Lambda

Aufrufen einer Lambda-Funktion aus Ihrem Babelfish-DB-Cluster

AWS Lambda unterstützt Funktionen, die in Java, Node.js, Python, Ruby und anderen Sprachen geschrieben wurden. Wenn die Funktion beim Aufruf Text zurückgibt, können Sie sie von Ihrem Babelfish-DB-Cluster aus aufrufen. Das folgende Beispiel ist eine Platzhalter-Python-Funktion, die eine Begrüßung zurückgibt.

```
lambda_function.py
import json
def lambda_handler(event, context):
    #TODO implement
    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
```

Derzeit wird JSON von Babelfish nicht unterstützt. Wenn Ihre Funktion JSON zurückgibt, verwenden Sie einen Wrapper, um den JSON-Code zu behandeln. Angenommen, die vorher gezeigte `lambda_function.py` ist in Lambda als `my-function` gespeichert.

1. Stellen Sie mit Hilfe des `psql`-Clients (oder des pgAdmin-Clients) eine Verbindung zu Ihrem Babelfish-DB-Cluster her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrem psql.
2. Erstellen Sie den Wrapper. In diesem Beispiel wird die prozedurale Sprache von PostgreSQL für SQL verwendet, `PL/pgSQL`. Weitere Informationen hierzu finden Sie unter PL/pgSQL-SQL Procedural Language.

   ```
   create or replace function master_dbo.lambda_wrapper()
   returns text
   language plpgsql
   as
   $$
   declare
      r_status_code integer;
      r_payload text;
   begin
      SELECT payload INTO r_payload
        FROM aws_lambda.invoke(  aws_commons.create_lambda_function_arn('my-function',
    'us-east-1')
                               ,'{"body": "Hello from Postgres!"}'::json );
      return r_payload ;
   end;
   $$;
   ```

   Die Funktion kann jetzt vom Babelfish-TDS-Port (1433) oder vom PostgreSQL-Port (5433) aus ausgeführt werden.

   a. So rufen Sie diese Funktion von Ihrem PostgreSQL-Port aus auf:

      ```
      SELECT * from aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-
      function', 'us-east-1'), '{"body": "Hello from Postgres!"}'::json );
      ```

      Die Ausgabe sieht folgendermaßen oder ähnlich aus:

```
status_code |                         payload                          |
 executed_version | log_result
-------------+----------------------------------------------------------
+-----------------+------------
         200 | {"statusCode": 200, "body": "\"Hello from Lambda!\""} | $LATEST
         |
(1 row)
```

b. Um diese Funktion vom TDS-Port aus aufzurufen, stellen Sie eine Verbindung mit dem Port über den `sqlcmd`-Befehlszeilen-Client von SQL Server her. Details hierzu finden Sie unter Verbinden mit Ihrem DB-Cluster mithilfe eines SQL Server-Clients. Wenn eine Verbindung hergestellt ist, führen Sie Folgendes aus:

```
1> select lambda_wrapper();
2> go
```

Daraufhin erhalten Sie ein Ergebnis, das dem hier dargestellten entspricht:

```
{"statusCode": 200, "body": "\"Hello from Lambda!\""}
```

Weitere Informationen zur Verwendung von Lambda mit Aurora PostgreSQL finden Sie unter Aufrufen einer AWS Lambda Funktion aus einem Aurora PostgreSQL-DB-Cluster (PostgreSQL-DB-Instance). Weitere Informationen über die Nutzung von Lambda-Funktionen finden Sie unter Erste Schritte mit Lambda im AWS Lambda -Entwicklerhandbuch.

Verwenden von pg_stat_statements in Babelfish

Babelfish für Aurora PostgreSQL unterstützt die `pg_stat_statements`-Erweiterung ab 3.3.0. Weitere Informationen finden Sie unter pg_stat_statements.

Einzelheiten zur von Aurora PostgreSQL unterstützten Version dieser Erweiterung finden Sie unter Erweiterungsversionen.

Erstellen der pg_stat_statements-Erweiterung

Zum Aktivieren von `pg_stat_statements` müssen Sie die Berechnung der Abfrage-ID aktivieren. Dies erfolgt automatisch, wenn `compute_query_id` auf on oder `auto` in der Parametergruppe gesetzt ist. Der Standardwert für den `compute_query_id`-Parameter ist `auto`. Sie müssen auch

diese Erweiterung erstellen, um diese Funktion zu aktivieren. Verwenden Sie den folgenden Befehl, um die Erweiterung vom T-SQL-Endpunkt aus zu installieren:

```
1>EXEC sp_execute_postgresql 'CREATE EXTENSION pg_stat_statements WITH SCHEMA sys';
```

Sie können mit der folgenden Abfrage auf die Abfragestatistiken zugreifen:

```
postgres=>select * from pg_stat_statements;
```

> **Note**
>
> Wenn Sie während der Installation den Schemanamen für die Erweiterung nicht angeben, wird dieser standardmäßig im öffentlichen Schema erstellt. Um darauf zuzugreifen, müssen Sie eckige Klammern mit Schemaqualifizierer verwenden, wie unten gezeigt:

```
postgres=>select * from [public].pg_stat_statements;
```

Sie können die Erweiterung auch vom PSQL-Endpunkt aus erstellen.

Autorisieren der Erweiterung

Standardmäßig können Sie die Statistiken für Abfragen sehen, die in Ihrer T-SQL-Datenbank ausgeführt wurden, ohne dass eine Autorisierung erforderlich ist.

Um auf Abfragestatistiken zugreifen zu können, die von anderen erstellt wurden, benötigen Sie eine `pg_read_all_stats`-PostgreSQL-Rolle. Folgen Sie den unten genannten Schritten, um den Befehl GRANT pg_read_all_stats zu erstellen.

1. Verwenden Sie in T-SQL die folgende Abfrage, die den internen PG-Rollennamen zurückgibt.

   ```
   SELECT rolname FROM pg_roles WHERE oid = USER_ID();
   ```

2. Stellen Sie mit der Berechtigung rds_superuser eine Verbindung mit der Babelfish-für-Aurora-PostgreSQL-Datenbank her und verwenden Sie den folgenden Befehl:

```
GRANT pg_read_all_stats TO <rolname_from_above_query>
```

Beispiel

Vom T-SQL-Endpunkt aus:

```
1>SELECT rolname FROM pg_roles WHERE oid = USER_ID();
2>go
```

```
rolname
-------
master_dbo
(1 rows affected)
```

Vom PSQL-Endpunkt aus:

```
babelfish_db=# grant pg_read_all_stats to master_dbo;
```

```
GRANT ROLE
```

Sie können mit der Ansicht pg_stat_statements auf die Abfragestatistiken zugreifen:

```
1>create table t1(cola int);
2>go
1>insert into t1 values (1),(2),(3);
2>go
```

```
(3 rows affected)
```

```
1>select userid, dbid, queryid, query from pg_stat_statements;
2>go
```

```
userid dbid queryid             query
------ ---- -------             -----
```

```
37503 34582 6487973085327558478 select * from t1
37503 34582 6284378402749466286 SET QUOTED_IDENTIFIER OFF
37503 34582 2864302298511657420 insert into t1 values ($1),($2),($3)
10    34582 NULL                <insufficient privilege>
37503 34582 5615368793313871642 SET TEXTSIZE 4096
37503 34582 639400815330803392  create table t1(cola int)
(6 rows affected)
```

Zurücksetzen der Abfragestatistiken

Sie können `pg_stat_statements_reset()` verwenden, um die bisher von pg_stat_statements erfassten Statistiken zurückzusetzen. Weitere Informationen finden Sie unter pg_stat_statements. Dies wird derzeit nur über den PSQL-Endpunkt unterstützt. Stellen Sie mit der `rds_superuser`-Berechtigung eine Verbindung zu Babelfish für Aurora PostgreSQL her und verwenden Sie den folgenden Befehl:

```
SELECT pg_stat_statements_reset();
```

Einschränkungen

- Derzeit wird `pg_stat_statements()` nicht über den T-SQL-Endpunkt unterstützt. `pg_stat_statements`-View ist die empfohlene Methode zum Erfassen von Statistiken.
- Einige der Abfragen werden möglicherweise vom T-SQL-Parser neu geschrieben, der von der Aurora PostgreSQL-Engine implementiert wurde. In der `pg_stat_statements`-Ansicht wird die neu geschriebene Abfrage und nicht die ursprüngliche Abfrage angezeigt.

  Beispiel

  ```
  select next value for [dbo].[newCounter];
  ```

  Die obige Abfrage wird in der Ansicht pg_stat_statements wie folgt umgeschrieben.

  ```
  select nextval($1);
  ```

- Aufgrund des Ausführungsablaufs der Anweisungen werden einige Abfragen möglicherweise nicht von pg_stat_statements verfolgt und sind daher in der Ansicht nicht sichtbar. Dazu gehören die

folgenden Anweisungen: `use dbname`, `goto`, `print`, `raise error`, `set`, `throw`, `declare cursor`.

- Bei den Anweisungen CREATE LOGIN und ALTER LOGIN werden Abfrage und Abfrage-ID nicht angezeigt. Es werden unzureichende Berechtigungen angezeigt.
- Die `pg_stat_statements`-Ansicht enthält immer die folgenden zwei Einträge, da diese intern vom `sqlcmd`-Client ausgeführt werden.
  - SET QUOTED_IDENTIFIER OFF
  - SET TEXTSIZE 4096

Verwendung von pgvector in Babelfish

Mit pgvector, einer Open-Source-Erweiterung, können Sie direkt in Ihrer Postgres-Datenbank nach ähnlichen Daten suchen. Babelfish unterstützt diese Erweiterung jetzt ab den Versionen 15.6 und 16.2. Weitere Informationen finden Sie in der Open-Source-Dokumentation von pgvector.

Voraussetzungen

Um die PGVector-Funktionalität zu aktivieren, installieren Sie die Erweiterung im sys-Schema mit einer der folgenden Methoden:

- Führen Sie den folgenden Befehl im sqlcmd-Client aus:

```
exec sys.sp_execute_postgresql 'CREATE EXTENSION vector WITH SCHEMA sys';
```

- Connect zum PSQL-Client her `babelfish_db` und führen Sie den folgenden Befehl aus:

```
CREATE EXTENSION vector WITH SCHEMA sys;
```

> **Note**
>
> Nach der Installation der Erweiterung pgvector ist der Vektor-Datentyp nur in neuen Datenbankverbindungen verfügbar, die Sie einrichten. Bestehende Verbindungen erkennen den neuen Datentyp nicht.

Unterstützte Funktionalität

Babelfish erweitert die T-SQL-Funktionalität um die folgenden Funktionen:

- Speichern

  Babelfish unterstützt jetzt eine mit Vektor-Datentypen kompatible Syntax und verbessert so die T-SQL-Kompatibilität. Weitere Informationen zum Speichern von Daten mit pgvector finden Sie unter Speichern.

- Abfragen

  Babelfish erweitert die Unterstützung von T-SQL-Ausdrücken um Vektor-Ähnlichkeitsoperatoren. Für alle anderen Abfragen ist jedoch weiterhin die standardmäßige T-SQL-Syntax erforderlich.

  > **Note**
  >
  > T-SQL unterstützt den Array-Typ nicht, und die Datenbanktreiber haben keine Schnittstelle, um sie zu handhaben. Um dieses Problem zu umgehen, verwendet Babelfish Textzeichenfolgen (varchar/nvarchar) zum Speichern von Vektordaten. Wenn Sie beispielsweise einen Vektorwert [1,2,3] anfordern, gibt Babelfish als Antwort die Zeichenfolge '[1,2,3]' zurück. Sie können diese Zeichenfolge auf Anwendungsebene nach Ihren Bedürfnissen analysieren und aufteilen.

  Weitere Informationen zum Abfragen von Daten mit pgvector finden Sie unter Abfragen.

- Indizierung

  T-SQL unterstützt `Create Index USING INDEX_METHOD` jetzt Syntax. Sie können jetzt einen Ähnlichkeitssuchoperator definieren, der bei der Erstellung eines Indexes für eine bestimmte Spalte verwendet wird.

  Die Grammatik wurde auch erweitert, um Operationen zur Vektorähnlichkeit für die benötigte Spalte zu unterstützen (überprüfen Sie die column_name_list_with_order_for_vector-Grammatik).

```
CREATE [UNIQUE] [clustered] [COLUMNSTORE] INDEX <index_name> ON <table_name> [USING
 vector_index_method] (<column_name_list_with_order_for_vector>)
Where column_name_list_with_order_for_vector is:
```

```
    <column_name> [ASC | DESC] [VECTOR_COSINE_OPS | VECTOR_IP_OPS | VECTOR_L2_OPS]
(COMMA simple_column_name [ASC | DESC] [VECTOR_COSINE_OPS | VECTOR_IP_OPS |
VECTOR_L2_OPS])
```

Weitere Informationen zur Indizierung von Daten mit pgvector finden Sie unter Indizierung.

- Leistung
  - Wird `SET BABELFISH_STATISTICS PROFILE ON` zum Debuggen von Abfrageplänen vom T-SQL-Endpunkt aus verwendet.
  - Erhöhen `max_parallel_workers_get_gather` Sie die Anzahl mithilfe der in `set_config` T-SQL unterstützten Funktion.
  - Wird `IVFFlat` für ungefähre Suchanfragen verwendet. Weitere Informationen finden Sie unter IVFFlat.

  Informationen zur Verbesserung der Leistung mit pgvector finden Sie unter Leistung.

Einschränkungen

- Babelfish unterstützt keine Volltextsuche für die Hybridsuche. Weitere Informationen finden Sie unter Hybridsuche.
- Babelfish unterstützt derzeit keine Neuindizierungsfunktionen. Sie können den PostgreSQL-Endpunkt jedoch weiterhin für die Neuindizierung verwenden. Weitere Informationen finden Sie unter Staubsaugen.

Verwenden von Amazon Aurora Machine Learning mit Babelfish

Sie können die Funktionen Ihres Babelfish for Aurora PostgreSQL-DB-Clusters erweitern, indem Sie ihn in Amazon Aurora Machine Learning integrieren. Diese nahtlose Integration gewährt Ihnen Zugriff auf eine Reihe leistungsstarker Dienste wie Amazon Comprehend oder Amazon SageMaker oder Amazon Bedrock, die jeweils auf unterschiedliche Anforderungen im Bereich maschinelles Lernen zugeschnitten sind.

Als Babelfish-Benutzer können Sie bei der Arbeit mit Aurora Machine Learning vorhandenes Wissen über T-SQL-Syntax und -Semantik nutzen. Folgen Sie den Anweisungen in der AWS Dokumentation für Aurora PostgreSQL. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora PostgreSQL.

Voraussetzungen

- Bevor Sie versuchen, Ihren Babelfish for Aurora PostgreSQL-DB-Cluster für die Nutzung von Aurora Machine Learning einzurichten, müssen Sie die entsprechenden Anforderungen und Voraussetzungen verstehen. Weitere Informationen finden Sie unter Voraussetzungen für die Verwendung von Aurora Machine Learning mit Aurora PostgreSQL.
- Stellen Sie sicher, dass Sie die `aws_ml` Erweiterung entweder mithilfe des Postgres-Endpunkts oder der Store-Prozedur installieren. `sp_execute_postgresql`

```
exec sys.sp_execute_postgresql 'Create Extension aws_ml'
```

> **Note**
>
> Derzeit unterstützt Babelfish keine Kaskadenoperationen in Babelfish. `sp_execute_postgresql` Da es `aws_ml` darauf angewiesen ist`aws_commons`, müssen Sie es separat mithilfe des Postgres-Endpunkts installieren.

```
create extension aws_common;
```

Umgang mit T-SQL-Syntax und -Semantik mit Funktionen **`aws_ml`**

In den folgenden Beispielen wird erklärt, wie T-SQL-Syntax und -Semantik auf die Amazon ML-Services angewendet werden:

Example : aws_bedrock.invoke_model — Eine einfache Abfrage mit Amazon Bedrock-Funktionen

```
aws_bedrock.invoke_model(
   model_id      varchar,
   content_type  text,
   accept_type   text,
   model_input   text)
Returns Varchar(MAX)
```

Das folgende Beispiel zeigt, wie Sie mithilfe von invoke_model ein Anthropic Claude 2-Modell für Bedrock aufrufen.

```
SELECT aws_bedrock.invoke_model (
    'anthropic.claude-v2', -- model_id
    'application/json', -- content_type
    'application/json', -- accept_type
    '{"prompt": "\n\nHuman:
    You are a helpful assistant that answers questions directly
    and only using the information provided in the context below.
    \nDescribe the answerin detail.\n\nContext: %s \n\nQuestion:
    %s \n\nAssistant:","max_tokens_to_sample":4096,"temperature"
    :0.5,"top_k":250,"top_p":0.5,"stop_sequences":[]}' -- model_input
);
```

Example : aws_comprehend.detect_sentiment — Eine einfache Abfrage mit Amazon Comprehend Comprehend-Funktionen

```
aws_comprehend.detect_sentiment(
   input_text varchar,
   language_code varchar,
   max_rows_per_batch int)
Returns table (sentiment varchar, confidence real)
```

Das folgende Beispiel zeigt, wie der Amazon Comprehend Service aufgerufen wird.

```
select sentiment from aws_comprehend.detect_sentiment('This is great', 'en');
```

Example : aws_sagemaker.invoke_endpoint — Eine einfache Abfrage mit Amazon-Funktionen SageMaker

```
aws_sagemaker.invoke_endpoint(
  endpoint_name varchar,
  max_rows_per_batch int,
  VARIADIC model_input "any") -- Babelfish inherits PG's variadic parameter type
Rerurns Varchar(MAX)
```

Da model_input als VARIADIC markiert ist und den Typ „any“ hat, können Benutzer eine Liste mit beliebiger Länge und beliebigem Datentyp an die Funktion übergeben, die als Eingabe für das Modell dient. Das folgende Beispiel zeigt, wie der SageMaker Amazon-Service aufgerufen wird.

```
SELECT CAST (aws_sagemaker.invoke_endpoint(
    'sagemaker_model_endpoint_name',
    NULL,
    arg1, arg2 -- model inputs are separate arguments )
AS INT) -- cast the output to INT
```

Ausführlichere Informationen zur Verwendung von Aurora Machine Learning mit Aurora PostgreSQL finden Sie unter. Verwendung von Amazon Aurora Machine Learning mit Aurora PostgreSQL

Einschränkungen

- Babelfish erlaubt zwar nicht die Erstellung von Arrays, kann aber dennoch Daten verarbeiten, die Arrays repräsentieren. Wenn du solche Funktionen verwendest`aws_bedrock.invoke_model_get_embeddings`, die Arrays zurückgeben, werden die Ergebnisse als Zeichenfolge geliefert, die die Array-Elemente enthält.

Babelfish unterstützt verknüpfte Server

Babelfish für Aurora PostgreSQL unterstützt verknüpfte Server mithilfe der PostgreSQL-Erweiterung `tds_fdw` in Version 3.1.0. Sie müssen die Erweiterung `tds_fdw` installieren, um mit verknüpften Servern arbeiten zu können. Weitere Informationen über die Erweiterung `tds_fdw` finden Sie unter Arbeiten mit den unterstützten Fremddaten-Wrapper für Amazon Aurora PostgreSQL.

Installieren der Erweiterung **`tds_fdw`**

Sie können die Erweiterung `tds_fdw` mit den folgenden Methoden installieren.

Verwendung von CREATE EXTENSION vom PostgreSQL-Endpunkt aus

1. Stellen Sie in der Babelfish-Datenbank im PostgreSQL-Port eine Verbindung mit Ihrer PostgreSQL-DB-Instance her. Verwenden Sie ein Konto, das über die Rolle rds_superuser verfügt.

```
psql --host=your-DB-instance.aws-region.rds.amazonaws.com --port=5432 --
username=test --dbname=babelfish_db --password
```

2. Installieren Sie die `tds_fdw`-Erweiterung. Dies ist ein einmaliger Installationsvorgang. Sie müssen keine erneute Installation vornehmen, wenn der DB-Cluster neu gestartet wird.

```
babelfish_db=> CREATE EXTENSION tds_fdw;
CREATE EXTENSION
```

Aufruf der gespeicherten Prozedur **`sp_execute_postgresql`** vom TDS-Endpunkt aus

Babelfish unterstützt die Installation der Erweiterung `tds_fdw` durch Aufrufen der Prozedur `sp_execute_postgresql` ab Version 3.3.0. Sie können PostgreSQL-Anweisungen vom T-SQL-Endpunkt aus ausführen, ohne den T-SQL-Port zu verlassen. Weitere Informationen finden Sie unter Referenz zu Verfahren für Babelfish für Aurora PostgreSQL.

1. Stellen Sie in der Babelfish-Datenbank im T-SQL-Port eine Verbindung zu Ihrer PostgreSQL-DB-Instance her.

```
sqlcmd -S your-DB-instance.aws-region.rds.amazonaws.com -U test -P password
```

2. Installieren Sie die `tds_fdw`-Erweiterung.

```
1>EXEC sp_execute_postgresql N'CREATE EXTENSION tds_fdw';
2>go
```

Unterstützte Funktionen

Babelfish unterstützt das Hinzufügen von Remote-Endpunkten von RDS für SQL Server oder Babelfish für Aurora PostgreSQL als verknüpften Server. Sie können auch andere Remote-Instances von SQL Server als verknüpfte Server hinzufügen. Verwenden Sie dann `OPENQUERY()`, um Daten von diesen verknüpften Servern abzurufen. Ab Babelfish Version 3.2.0 werden auch vierteilige Namen unterstützt.

Die folgenden gespeicherten Prozeduren und Katalogansichten werden unterstützt, um die verknüpften Server zu verwenden.

Gespeicherte Prozeduren

- sp_addlinkedserver – Babelfish unterstützt den Parameter `@provstr` nicht.
- sp_addlinkedsrvlogin
  - Sie müssen einen expliziten Remote-Benutzernamen und ein Passwort angeben, um eine Verbindung zu der Remote-Datenquelle herzustellen. Sie können keine Verbindung mit den eigenen Anmeldeinformationen des Benutzers herstellen. Babelfish unterstützt nur `@useself = false`.
  - Babelfish unterstützt den Parameter `@locallogin` nicht, da die Konfiguration des Remote-Serverzugriffs für die lokale Anmeldung nicht unterstützt wird.
- sp_linkedservers
- sp_helplinkedsrvlogin
- sp_dropserver
- sp_droplinkedsrvlogin – Babelfish unterstützt den Parameter `@locallogin` nicht, da die Konfiguration des Remote-Serverzugriffs für die lokale Anmeldung nicht unterstützt wird.
- sp_serveroption – Babelfish unterstützt die folgenden Serveroptionen:
  - Abfrage-Timeout (ab Babelfish-Version 3.2.0)
  - Verbindungs-Timeout (ab Babelfish-Version 3.3.0)
- sp_testlinkedserver (ab Babelfish-Version 3.3.0)
- sp_enum_oledb_providers (ab Babelfish-Version 3.3.0)

Katalogansichten

- sys.servers
- sys.linked_logins

Verwenden der Verschlüsselung während der Übertragung für die Verbindung

Die Verbindung vom Quellserver von Babelfish für Aurora PostgreSQL mit dem Remote-Zielserver verwendet je nach Datenbankkonfiguration des Remote-Servers die Verschlüsselung während der Übertragung (TLS/SSL). Wenn der Remote-Server nicht für die Verschlüsselung konfiguriert ist, bleibt der Babelfish-Server, der die Anforderung an die Remote-Datenbank stellt, unverschlüsselt.

So erzwingen Sie die Verbindungsverschlüsselung

- Wenn der verknüpfte Zielserver eine Instance von RDS für SQL Server ist, legen Sie `rds.force_ssl = on` für die Ziel-Instance von SQL Server fest. Weitere Informationen zur SSL/TLS-Konfiguration für RDS für SQL Server finden Sie unter Verwenden von SSL mit einer Microsoft-SQL-Server-DB-Instance.
- Wenn es sich bei dem verknüpften Zielserver um einen Cluster von Babelfish für Aurora PostgreSQL handelt, legen Sie `babelfishpg_tsql.tds_ssl_encrypt = on` und `ssl = on` für den Zielserver fest. Weitere Informationen zu SSL/TLS finden Sie unter SSL-Einstellungen und Clientverbindungen für Babelfish.

Hinzufügen von Babelfish als verknüpften Server über SQL Server

Babelfish für Aurora PostgreSQL kann über einen SQL Server als verknüpfter Server hinzugefügt werden. In einer SQL-Server-Datenbank können Sie Babelfish als verknüpften Server hinzufügen, indem Sie den Anbieter von Microsoft OLE DB für ODBC verwenden: MSDASQL.

Es gibt zwei Möglichkeiten, Babelfish mithilfe des Anbieters MSDASQL über SQL Server als verknüpften Server zu konfigurieren:

- Angeben der ODBC-Verbindungszeichenfolge als Anbieterzeichenfolge
- Angeben des System-DSN der ODBC-Datenquelle, während der verknüpfte Server hinzugefügt wird

Einschränkungen

- OPENQUERY() funktioniert nur für SELECT und nicht für DML.
- Vierteilige Objektnamen funktionieren nur zum Lesen und nicht zum Ändern der entfernten Tabelle. Ein UPDATE kann in der FROM-Klausel auf eine entfernte Tabelle verweisen, ohne sie zu ändern.
- Die Ausführung von gespeicherten Prozeduren auf mit Babelfish verknüpften Servern wird nicht unterstützt.
- Das Upgrade der Hauptversion von Babelfish funktioniert möglicherweise nicht, wenn Objekte von `OPENQUERY()` abhängig sind oder Objekte durch vierteilige Namen referenziert werden. Sie müssen sicherstellen, dass alle Objekte, die auf `OPENQUERY()` oder vierteilige Namen verweisen, vor einem Upgrade der Hauptversion gelöscht werden.
- Die folgenden Datentypen funktionieren auf dem Babelfish-Remote-Server nicht wie erwartet: `nvarchar(max)`, `varchar(max)`, `varbinary(max)`, `binary(max)` und `time`. Wir empfehlen, die CAST-Funktion zu verwenden, um diese in unterstützte Datentypen zu konvertieren.

Beispiel

Im folgenden Beispiel stellt eine Babelfish-für-Aurora-PostgreSQL-Instance eine Verbindung zu einer Instance von RDS für SQL Server in der Cloud her.

```
EXEC master.dbo.sp_addlinkedserver @server=N'rds_sqlserver', @srvproduct=N'',
 @provider=N'SQLNCLI', @datasrc=N'myserver.CB2XKFSFFMY7.US-WEST-2.RDS.AMAZONAWS.COM';
EXEC master.dbo.sp_addlinkedsrvlogin
 @rmtsrvname=N'rds_sqlserver',@useself=N'False',@locallogin=NULL,@rmtuser=N'username',@rmtpassw
```

Wenn der verbundene Server eingerichtet ist, können Sie T-SQL OPENQUERY() oder eine vierteilige Standardbenennung verwenden, um auf eine Tabelle, Ansicht oder andere unterstützte Objekte auf dem Remote-Server zu verweisen:

```
SELECT * FROM OPENQUERY(rds_sqlserver, 'SELECT * FROM TestDB.dbo.t1');
SELECT * FROM rds_sqlserver.TestDB.dbo.t1;
```

So löschen Sie den verbundenen Server und alle verbundenen Logins:

```
EXEC master.dbo.sp_dropserver @server=N'rds_sqlserver', @droplogins=N'droplogins';
```

Fehlerbehebung

Sie können für Quell- und Remoteserver dieselbe Sicherheitsgruppe verwenden, um eine Kommunikation beider Server zu ermöglichen. Die Sicherheitsgruppe sollte nur eingehenden Datenverkehr am TDS-Port (standardmäßig 1433) zulassen und die Quell-IP in der Sicherheitsgruppe kann als Sicherheitsgruppen-ID selbst festgelegt werden. Weitere Informationen zum Einrichten der Regeln für die Verbindung zu einer Instance von einer anderen Instance mit derselben Sicherheitsgruppe finden Sie unter Regeln für die Verbindung mit Instances von einer Instance mit der gleichen Sicherheitsgruppe aus.

Wenn der Zugriff nicht richtig konfiguriert ist, wird eine Fehlermeldung ähnlich wie das folgende Beispiel angezeigt, wenn Sie versuchen, den Remote-Server abzufragen.

```
TDS client library error: DB #: 20009, DB Msg: Unable to connect: server is unavailable
 or does not exist (mssql2019.aws-region.rds.amazonaws.com), OS #: 110, OS Msg:
 Connection timed out, Level: 9
```

Volltextsuche in Babelfish verwenden

Ab Version 4.0.0 bietet Babelfish eingeschränkte Unterstützung für die Volltextsuche (FTS). FTS ist eine leistungsstarke Funktion in relationalen Datenbanken, die eine effiziente Suche und Indizierung von textlastigen Daten ermöglicht. Es ermöglicht Ihnen, komplexe Textsuchen durchzuführen und relevante Ergebnisse schnell abzurufen. FTS ist besonders wertvoll für Anwendungen, die mit großen Mengen an Textdaten umgehen, wie Content-Management-Systeme, E-Commerce-Plattformen und Dokumentenarchive.

Grundlegendes zu den von Babelfish Full Text Search unterstützten Funktionen

Babelfish unterstützt die folgenden Funktionen der Volltextsuche:

- CONTAINS-Klausel:
  - Grundlegende Unterstützung für die CONTAINS-Klausel.

    ```
    CONTAINS (
         {
            column_name
         }
         , '<contains_search_condition>'
    )
    ```

    > **Note**
    >
    > Derzeit wird nur die englische Sprache unterstützt.

  - Umfassende Bearbeitung und Übersetzung von `simple_term` Suchbegriffen.
- `FULLTEXT INDEX`Klausel:
  - Unterstützt nur die `CREATE FULLTEXT INDEX ON table_name(column_name [...n]) KEY INDEX index_name` Aussage.
  - Unterstützt die vollständige `DROP FULLTEXT INDEX` Aussage.

> **Note**
>
> Um den Volltextindex neu zu indizieren, müssen Sie den Volltextindex löschen und einen neuen Index für dieselbe Spalte erstellen.

- Sonderzeichen in der Suchbedingung:
  - Babelfish stellt sicher, dass einzelne Vorkommen von Sonderzeichen in Suchzeichenfolgen effektiv behandelt werden.

    > **Note**
    >
    > Babelfish identifiziert zwar jetzt Sonderzeichen in der Suchzeichenfolge, es ist jedoch wichtig zu wissen, dass die erzielten Ergebnisse von denen mit T-SQL abweichen können.

- Tabellenalias in column_name:
  - Dank der Unterstützung von Tabellenalias können Benutzer präzisere und lesbarere SQL-Abfragen für die Volltextsuche erstellen.

Einschränkungen bei der Babelfish-Volltextsuche

- Derzeit werden die folgenden Optionen in Babelfish for Clause nicht unterstützt. `CONTAINS`
  - Sonderzeichen und andere Sprachen als Englisch werden nicht unterstützt. Sie erhalten die allgemeine Fehlermeldung für nicht unterstützte Zeichen und Sprachen

    ```
    Full-text search conditions with special characters or languages other than English
     are not currently supported in Babelfish
    ```

  - Mehrere Spalten wie `column_list`
  - EIGENSCHAFTS-Attribut
  - `prefix_term`, `generation_term`, `generic_proximity_term`, `custom_proximity_term`, und `weighted_term`
  - Boolesche Operatoren werden nicht unterstützt und Sie erhalten die folgende Fehlermeldung, wenn Sie sie verwenden:

```
boolean operators not supported
```

  - Bezeichnernamen mit Punkten werden nicht unterstützt.
- Derzeit werden die folgenden Optionen in Babelfish for `CREATE FULLTEXT INDEX` Clause nicht unterstützt.
  - [TYP SPALTE type_column_name]
  - [SPRACHE language_term]
  - [STATISTISCHE_SEMANTIK]
  - Optionen für Katalogdateigruppen
  - mit Optionen
- Das Erstellen eines Volltextkatalogs wird nicht unterstützt. Für die Erstellung eines Volltextindexes ist kein Volltextkatalog erforderlich.
- `CREATE FULLTEXT INDEX`unterstützt keine Bezeichnernamen mit Punkten.
- Babelfish unterstützt derzeit keine aufeinanderfolgenden Sonderzeichen in Suchzeichenfolgen. Sie erhalten die folgende Fehlermeldung, wenn Sie es verwenden:

```
Consecutive special characters in the full-text search condition are not currently
 supported in Babelfish
```

Babelfish unterstützt Geospatial-Datentypen

Ab den Versionen 3.5.0 und 4.1.0 bietet Babelfish Unterstützung für die folgenden zwei räumlichen Datentypen:

- Geometrischer Datentyp — Dieser Datentyp ist für die Speicherung planarer oder euklidischer (flacher Erdboden) Daten vorgesehen.
- Geografischer Datentyp — Dieser Datentyp ist für die Speicherung ellipsoidförmiger oder erdnaher Daten wie GPS-Längen- und Breitengradkoordinaten vorgesehen.

Diese Datentypen ermöglichen die Speicherung und Bearbeitung von Geodaten, allerdings mit Einschränkungen.

Die Geodatentypen in Babelfish verstehen

- Geospatiale Datentypen werden in verschiedenen Datenbankobjekten wie Ansichten, Prozeduren und Tabellen unterstützt.

- Unterstützt den 2D-Punktdatentyp zum Speichern von Ortsdaten als Punkte, die durch Breitengrad, Längengrad und einen gültigen Spatial Reference System Identifier (SRID) definiert sind.
- Anwendungen, die über Treiber wie JDBC, ODBC, DOTNET und PYTHON eine Verbindung zu Babelfish herstellen, können diese Geospatial-Funktion nutzen.

Funktionen des Datentyps „Geometrie“, die in Babelfish unterstützt werden

- ST GeomFromText (***geometry_tagged_text***, SRID) — Erzeugt eine Geometrieinstanz unter Verwendung der WKT-Darstellung (Well-known Text).
- ST PointFromText (***point_tagged_text***, SRID) — Erzeugt eine Punktinstanz mithilfe der WKT-Darstellung.
- Point (X, Y, SRID) — Erzeugt eine Punktinstanz unter Verwendung von Gleitkommawerten der X- und Y-Koordinaten.
- .ST AsText () <geometry_instance>— Extrahiert die WKT-Darstellung aus einer Geometrieinstanz.
- .stDistance (other_geometry) <geometry_instance>— Berechnet den Abstand zwischen zwei Geometrieinstanzen.
- .STX — Extrahiert die X-Koordinate <geometry_instance>(Längengrad) für die Geometrieinstanz.
- .STY <geometry_instance>— Extrahiert die Y-Koordinate (Breitengrad) für die Geometrieinstanz.

Funktionen des Datentyps „Geografie“, die in Babelfish unterstützt werden

- ST GeomFromText (***geography_tagged_text***, SRID) — Erzeugt eine geografische Instanz mithilfe der WKT-Darstellung.
- ST PointFromText (***point_tagged_text***, SRID) — Erzeugt eine Punktinstanz mithilfe der WKT-Darstellung.
- Point (Lat, Long, SRID) — Erzeugt eine Punktinstanz unter Verwendung von Gleitkommawerten für Breitengrad und Längengrad.
- .ST AsText () <geography_instance>— Extrahiert die WKT-Darstellung aus der Geography-Instanz.

- .stDistance (other_geography) <geography_instance>— Berechnet die Entfernung zwischen zwei Geography-Instanzen.
- .Lat <geography_instance>— Extrahiert den Latitude-Wert für die Geography-Instanz.
- .Long <geography_instance>— Extrahiert den Längengradwert für die Geography-Instanz.

Einschränkungen in Babelfish für Geodatentypen

- Derzeit unterstützt Babelfish keine erweiterten Funktionen wie Z-M-Flags für Punktinstanzen von Geodatentypen.
- Andere Geometrietypen als Punktinstanzen werden derzeit nicht unterstützt:
  - LineString
  - CircularString
  - CompoundCurve
  - Polygon
  - CurvePolygon
  - MultiPoint
  - MultiLineString
  - MultiPolygon
  - GeometryCollection
- Derzeit wird die räumliche Indizierung für Geodatentypen nicht unterstützt.
- Derzeit werden nur die aufgelisteten Funktionen für diese Datentypen unterstützt. Weitere Informationen finden Sie unter Funktionen des Datentyps „Geometrie“, die in Babelfish unterstützt werden und Funktionen des Datentyps „Geografie“, die in Babelfish unterstützt werden.
- Die Ausgabe der STDistance-Funktion für Geographiedaten kann im Vergleich zu T-SQL geringfügige Genauigkeitsabweichungen aufweisen. Dies ist auf die zugrunde liegende PostGIS-Implementierung zurückzuführen. Weitere Informationen finden Sie unter ST_Distance
- Für eine optimale Leistung sollten Sie integrierte Geospatial-Datentypen verwenden, ohne zusätzliche Abstraktionsebenen in Babelfish zu erstellen.

> **Tip**
>
> Sie können zwar benutzerdefinierte Datentypen erstellen, es wird jedoch nicht empfohlen, diese zusätzlich zu Geodaten zu erstellen. Dies könnte zu Komplexität führen und aufgrund der begrenzten Unterstützung möglicherweise zu unerwartetem Verhalten führen.

- In Babelfish werden Geospatial-Funktionsnamen als Schlüsselwörter verwendet und führen räumliche Operationen nur dann durch, wenn sie in der vorgesehenen Weise verwendet werden.

> **Tip**
>
> Vermeiden Sie bei der Erstellung benutzerdefinierter Funktionen und Prozeduren in Babelfish die Verwendung derselben Namen wie bei integrierten Geospatial-Funktionen. Wenn Sie bereits Datenbankobjekte mit denselben Namen haben, verwenden Sie diese`sp_rename`, um sie umzubenennen.

Fehlerbehebung bei Babelfish

Im Folgenden finden Sie Tipps zur Fehlerbehebung und Workarounds für einige Probleme mit Babelfish-DB-Clustern.

Themen

Verbindungsfehler

Häufige Ursachen für Verbindungsfehler mit einem neuen Aurora-DB-Cluster umfassen Folgende:

- Sicherheitsgruppe lässt keinen Zugriff zu — Wenn Sie Probleme haben, sich mit einem Babelfish zu verbinden, stellen Sie sicher, dass Sie Ihre IP-Adresse der Amazon EC2-Sicherheitsgruppe hinzugefügt haben. Sie können https://checkip.amazonaws.com/ nutzen, um Ihre IP-Adresse zu ermitteln und sie dann Ihrer Inbound-Regel für den TDS-Port und den PostgreSQL-Port hinzuzufügen. Weitere Informationen finden Sie unter Hinzufügen von Regeln zur Sicherheitsgruppe im Amazon EC2-Benutzerhandbuch.
- Nicht übereinstimmende SSL-Konfigurationen – Wenn der `rds.force_ssl`-Parameter in Aurora PostgreSQL aktiviert (auf 1 eingestellt) ist, dann müssen sich Clients über SSL mit Babelfish verbinden. Wenn Ihr Client nicht richtig eingerichtet ist, wird Ihnen eine Fehlermeldung angezeigt, z. B. die folgende:

  ```
  Cannot connect to your-Babelfish-DB-cluster, 1433
  ---------------------
  ADDITIONAL INFORMATION:
  no pg_hba_conf entry for host "256.256.256.256", user "your-user-name",
  "database babelfish_db", SSL off (Microsoft SQL Server, Error: 33557097)
  ...
  ```

  Dieser Fehler weist auf ein mögliches SSL-Konfigurationsproblem zwischen Ihrem lokalen Client und dem Babelfish-DB-Cluster hin und darauf, dass der Cluster von Clients die Verwendung von SSL verlangt (der zugehörige `rds.force_ssl`-Parameter ist auf 1 festgelegt). Weitere Informationen zum Konfigurieren von SSL finden Sie unter Verwenden von SSL mit einer PostgreSQL-DB-Instance im Amazon RDS-Benutzerhandbuch.

  Wenn Sie SQL Server Management Studio (SSMS) verwenden, um eine Verbindung mit Babelfish herzustellen und dieser Fehler angezeigt wird, können Sie die Verbindungsoptionen Encrypt

connection (Verbindung verschlüsseln) und Trust server certificate (Trust-Serverzertifikat) im Bereich „Connection Properties“ (Verbindungseigenschaften) auswählen und es erneut versuchen. Diese Einstellungen übernehmen die SSL-Verbindungsanforderung für SSMS.

Weitere Informationen zur Fehlerbehebung von Aurora-DB-Verbindungsproblemen finden Sie unter Verbindung zur Amazon RDS-DB-Instance kann nicht hergestellt werden.

Deaktivieren von Babelfish

Wenn Sie Babelfish nicht mehr benötigen, können Sie die Babelfish-Funktionalität deaktivieren.

Achten Sie auf einige Überlegungen:

- In einigen Fällen können Sie Babelfish deaktivieren, bevor Sie eine Migration zu Aurora PostgreSQL abschließen. Wenn Sie dies tun und Ihre DDL von SQL Server-Datentypen abhängt oder Sie eine T-SQL-Funktionalität in Ihrem Code verwenden, schlägt Ihr Code fehl.
- Wenn Sie nach der Bereitstellung einer Babelfish-Instanz die Babelfish-Erweiterung deaktivieren, können Sie dieselbe Datenbank nicht erneut auf demselben Cluster bereitstellen.

Um Babelfish zu deaktivieren, ändern Sie Ihre Parametergruppe und stellen Sie `rds.babelfish_status` auf `OFF`. Sie können Ihre SQL Server-Datentypen weiterhin mit Babelfish off verwenden, indem Sie `rds.babelfish_status` auf `datatypeonly` stellen.

Wenn Sie Babelfish in der Parametergruppe deaktivieren, verlieren alle Cluster, die diese Parametergruppe verwenden, die Babelfish-Funktionalität.

Weitere Informationen zu Aurora-Parametergruppen finden Sie unter Arbeiten mit Parametergruppen. Informationen zum Festlegen von Babelfish-spezifischen Parametern finden Sie unter Einstellungen der DB-Cluster-Parametergruppe für Babelfish.

Babelfish-Versions-Updates

Babelfish ist eine Option, die mit Aurora PostgreSQL Version 13.4 und höher verfügbar ist. Updates für Babelfish werden mit bestimmten neuen Versionen der Aurora-PostgreSQL-Datenbank-Engine verfügbar. Weitere Informationen finden Sie unter Versionshinweise für Aurora PostgreSQL.

> **Note**
>
> Babelfish-DB-Cluster, die auf einer beliebigen Version von Aurora PostgreSQL 13 ausgeführt werden, können nicht auf Aurora PostgreSQL 14.3, 14.4 und 14.5 aktualisiert werden. Außerdem unterstützt Babelfish kein direktes Upgrade von 13.x auf 15.x. Sie müssen zuerst Ihren 13.x-DB-Cluster auf 14.6 und höher und dann auf die 15.x-Version aktualisieren.

Eine Liste der unterstützten Funktionen für verschiedene Babelfish-Versionen finden Sie unter Unterstützte Funktionalität in Babelfish nach Version.

Eine Liste der nicht unterstützten Funktionen finden Sie unter Nicht unterstützte Funktionalität in Babelfish.

Sie können den describe-db-engine-versions AWS CLI Befehl verwenden, um eine Liste der Aurora-PostgreSQL-Versionen in Ihrem abzurufenAWS-Region, die Babelfish unterstützen, wie im folgenden Beispiel gezeigt.

Für Linux, macOSoder Unix:

```
$ aws rds describe-db-engine-versions --region us-east-1 \
    --engine aurora-postgresql \
    --query '*[]|[?SupportsBabelfish==`true`].[EngineVersion]' \
    --output text
13.4
13.5
13.6
13.7
13.8
14.3
14.4
14.5
14.6
14.7
14.8
```

```
14.9
14.10
15.2
15.3
15.4
15.5
16.1
```

Weitere Informationen finden Sie unter describe-db-engine-versions in der Referenz zum AWS CLI-Befehl.

In den folgenden Themen erfahren Sie, wie Sie die Version von Babelfish identifizieren, die auf Ihrem DB-Cluster von Aurora PostgreSQL ausgeführt wird, und wie Sie auf eine neue Version aktualisieren.

Inhalt

Identifizieren Ihrer Babelfish-Version

Sie können Babelfish abfragen, um Details zur Babelfish-Version, der Aurora-PostgreSQL-Version und der kompatiblen Microsoft SQL Server-Version zu finden. Sie können den TDS-Port oder den PostgreSQL-Port verwenden.

So fragen Sie Versionsinformationen mit dem TDS-Port ab

1. Verwenden Sie `sqlcmd` oder `ssms`, um eine Verbindung mit dem Endpunkt Ihres Babelfish-DB-Clusters herzustellen.

```
sqlcmd -S bfish_db.cluster-123456789012.aws-region.rds.amazonaws.com,1433 -U
    login-id -P password -d db_name
```

2. Um die Babelfish-Version zu identifizieren, führen Sie die folgende Abfrage aus:

```
1> SELECT CAST(serverproperty('babelfishversion') AS VARCHAR)
2> GO
```

   Die Abfrage gibt Ergebnisse wie die Folgenden zurück:

```
serverproperty
------------------------------
3.4.0

(1 rows affected)
```

3. Um die Version des Aurora-PostgreSQL-DB-Clusters zu identifizieren, führen Sie die folgende Abfrage aus:

```
1> SELECT aurora_version() AS aurora_version
2> GO
```

   Die Abfrage gibt Ergebnisse wie die Folgenden zurück:

```
aurora_version


-----------------------------------------------
15.5.0

(1 rows affected)
```

4. Führen Sie die folgende Abfrage aus, um die kompatible Microsoft SQL Server-Version zu identifizieren:

```
1> SELECT @@VERSION AS version
```

```
2> GO
```

Die Abfrage gibt Ergebnisse wie die Folgenden zurück:

```
Babelfish for Aurora PostgreSQL with SQL Server Compatibility - 12.0.2000.8
Dec 7 2023 09:43:06
Copyright (c) Amazon Web Services
PostgreSQL 15.5 on x86_64-pc-linux-gnu (Babelfish 3.4.0)

(1 rows affected)
```

Als Beispiel für einen kleinen Unterschied zwischen Babelfish und Microsoft SQL Server können Sie die folgende Abfrage ausführen. Bei Babelfish gibt die Abfrage 1 und auf Microsoft SQL Server `NULL` zurück.

```
SELECT CAST(serverproperty('babelfish') AS VARCHAR) AS runs_on_babelfish
```

Sie können auch den PostgreSQL-Port verwenden, um Versionsinformationen abzurufen, wie im Folgenden beschrieben.

So fragen Sie Versionsinformationen mit dem PostgreSQL-Port ab

1. Verwenden Sie `psql` oder `pgAdmin`, um eine Verbindung mit dem Endpunkt Ihres Babelfish-DB-Clusters herzustellen.

   ```
   psql host=bfish_db.cluster-123456789012.aws-region.rds.amazonaws.com
        port=5432 dbname=babelfish_db user=sa
   ```

2. Schalten Sie das erweiterte Feature (`\x`) von `psql` ein, damit die Ausgabe besser lesbar ist.

   ```
   babelfish_db=> \x
   babelfish_db=> SELECT
   babelfish_db=> aurora_version() AS aurora_version,
   babelfish_db=> version() AS postgresql_version,
   babelfish_db=> sys.version() AS Babelfish_compatibility,
   babelfish_db=> sys.SERVERPROPERTY('BabelfishVersion') AS Babelfish_Version;
   ```

   Die Abfrage gibt dann eine Ausgabe ähnlich der folgenden zurück:

```
-[ RECORD 1 ]-----------
+-------------------------------------------------------------------------------------------
aurora_version          | 15.5.0
postgresql_version      | PostgreSQL 15.5 on x86_64-pc-linux-gnu, compiled by
 x86_64-pc-linux-gnu-gcc (GCC) 9.5.0, 64-bit
babelfish_compatibility | Babelfish for Aurora Postgres with SQL Server
 Compatibility - 12.0.2000.8                    +
                         | Dec 7 2023 09:43:06
                                    +
                         | Copyright (c) Amazon Web Services
                                     +
                         | PostgreSQL 15.5 on x86_64-pc-linux-gnu (Babelfish 3.4.0)
babelfish_version       | 3.4.0
```

Durchführen eines Upgrades Ihres Babelfish-Clusters auf eine neue Version

Neue Versionen von Babelfish werden mit einigen neuen Versionen der Datenbank-Engine von Aurora PostgreSQL-Datenbank nach Version 13.4 verfügbar. Jede neue Version von Babelfish hat eine eigene Versionsnummer. Wie bei Aurora PostgreSQL verwendet Babelfish das Benennungsschema *major*.*minor*.*patch* für Versionen. Zum Beispiel wurde die erste Babelfish-Version, Babelfish Version 1.0.0, im Rahmen von Aurora PostgreSQL 13.4.0 verfügbar.

Babelfish benötigt keinen separaten Installationsvorgang. Wie unter Erstellen eines DB-Clusters von Babelfish for Aurora PostgreSQL beschrieben, wählen Sie die Option Turn on Babelfish (Babelfish aktivieren) aus, wenn Sie einen DB-Cluster von Aurora PostgreSQL erstellen.

Dementsprechend können Sie Babelfish nicht unabhängig vom unterstützenden Aurora-DB-Cluster aktualisieren. Wenn Sie einen vorhandenen DB-Cluster von Babelfish für Aurora PostgreSQL auf eine neue Version von Babelfish aktualisieren möchten, führen Sie ein Upgrade des DB-Clusters von Aurora PostgreSQL auf eine neue Version durch, die die Version von Babelfish unterstützt, die Sie verwenden möchten. Das Verfahren, das Sie für das Upgrade befolgen, hängt wie folgt von der Version von Aurora PostgreSQL ab, die Ihre Babelfish-Bereitstellung unterstützt.

Hauptversions-Upgrades

Sie müssen die folgenden Aurora-PostgreSQL-Versionen vor dem Upgrade auf Aurora PostgreSQL 15.2 und höher zunächst auf Aurora PostgreSQL 14.6 und höher aktualisieren.

- Aurora PostgreSQL 13.8 und alle höheren Versionen

- Aurora PostgreSQL 13.7.1 und alle höheren Nebenversionen
- Aurora PostgreSQL 13.6.4 und alle höheren Nebenversionen

Sie können Aurora PostgreSQL 14.6 und höhere Versionen auf Aurora PostgreSQL 15.2 und höhere Versionen aktualisieren.

Das Upgrade eines DB-Clusters von Aurora PostgreSQ auf eine neue Hauptversion erfordert mehrere vorbereitende Aufgaben. Weitere Informationen finden Sie unter Durchführen eines Hauptversions-Upgrades. Damit Sie Ihren DB-Cluster von Babelfish für Aurora PostgreSQL erfolgreich aktualisieren können, müssen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe für die neue Aurora-PostgreSQL-Version erstellen. Diese neue Parametergruppe muss dieselben Babelfish-Parametereinstellungen enthalten wie die des Clusters, den Sie aktualisieren. Weitere Informationen und eine Tabelle mit Quellen und Zielen für das Upgrade von Hauptversionen finden Sie unter Durchführen von Upgrades von Babelfish auf eine neue Hauptversion.

Nebenversions-Upgrades und -Patches

Für das Upgrade von Nebenversionen und Patches muss keine neue DB-Cluster-Parametergruppe erstellt werden. Nebenversionen und Patches können den Upgrade-Prozess für Nebenversionen verwenden, unabhängig davon, ob dieser automatisch oder manuell erfolgt. Weitere Informationen und eine Tabelle mit Versionsquellen und -zielen finden Sie unter Durchführen eines Upgrades von Babelfish auf eine neue Nebenversion.

> **Note**
>
> Bevor Sie ein Haupt- oder Nebenversions-Upgrade durchführen, führen Sie alle ausstehenden Wartungsaufgaben für Ihren Cluster von Babelfish für Aurora PostgreSQL aus.

Themen

- Durchführen eines Upgrades von Babelfish auf eine neue Nebenversion
- Durchführen von Upgrades von Babelfish auf eine neue Hauptversion

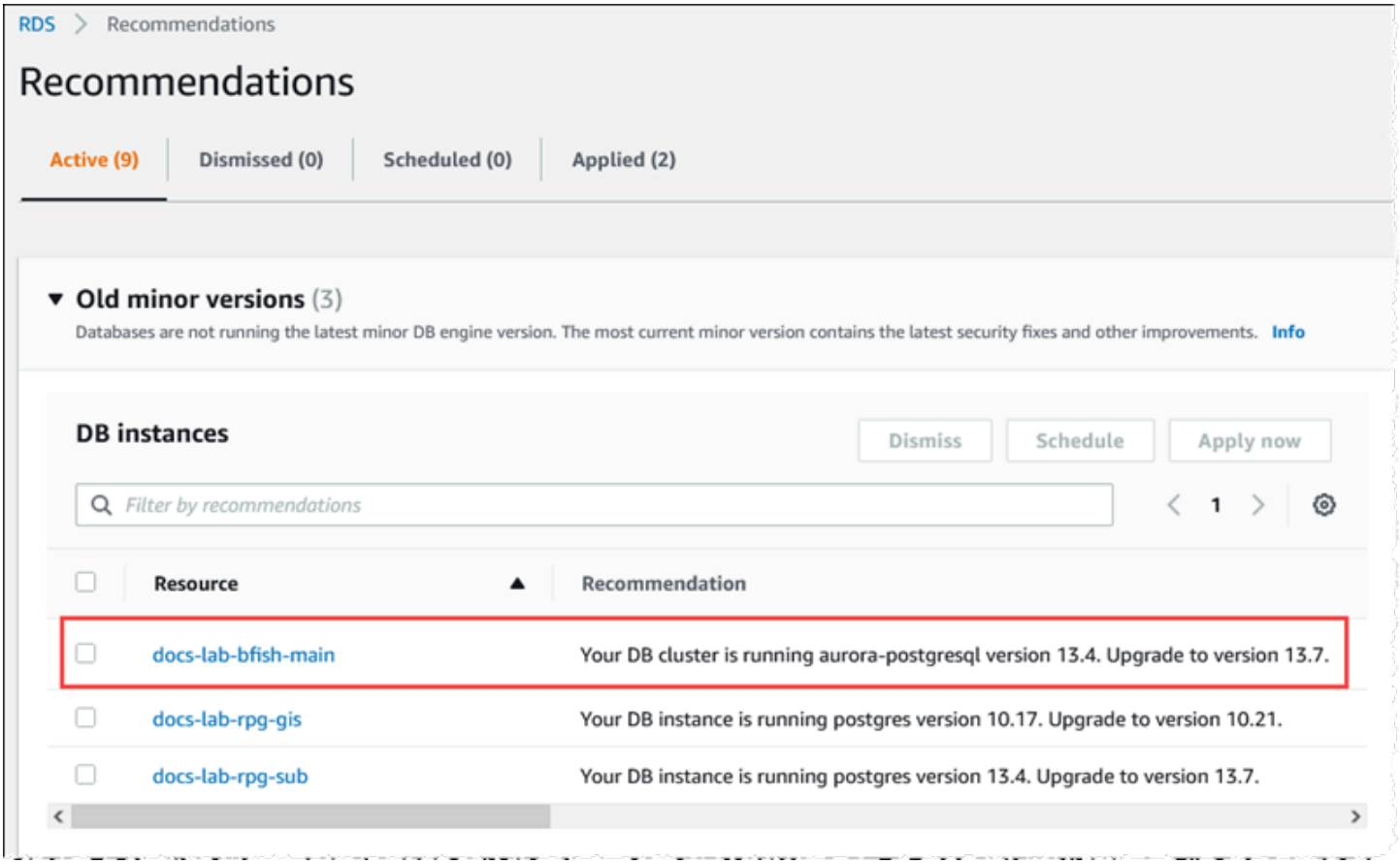
Durchführen eines Upgrades von Babelfish auf eine neue Nebenversion

Eine neue Nebenversion enthält nur Änderungen, die abwärtskompatibel sind. Eine Patch-Version enthält wichtige Korrekturen, die einer Nebenversion nach ihrer Veröffentlichung hinzugefügt werden.

Die Versionsbezeichnung für die erste Version von Aurora PostgreSQL 13.4 lautete beispielsweise Aurora PostgreSQL 13.4.0. Bisher wurden mehrere Patches für diese Nebenversion veröffentlicht, darunter Aurora PostgreSQL 13.4.1, 13.4.2 und 13.4.4. Die für jede Aurora-PostgreSQL-Version verfügbaren Patches finden Sie in der Liste Patch releases (Patch-Versionen) oben in den Versionshinweisen von Aurora PostgreSQL für die entsprechende Version. Ein Beispiel finden Sie unter PostgreSQL 14.3 in den Versionshinweisen für Aurora PostgreSQL.

Wenn Ihr DB-Cluster von Aurora PostgreSQL mit der Option Auto minor version upgrade (Automatisches Unterversion-Upgrade) konfiguriert ist, wird Ihr DB-Cluster von Babelfish für Aurora PostgreSQL während des Wartungsfensters des Clusters automatisch aktualisiert. Weitere Informationen zum automatischen Nebenversions-Upgrade (AmVU) und wie Sie es verwenden, finden Sie unter Automatische Nebenversions-Upgrades für Aurora-DB-Cluster. Wenn Ihr Cluster AmVU nicht verwendet, können Sie Ihren DB-Cluster von Babelfish für Aurora PostgreSQL auf neue Nebenversionen manuell aktualisieren, indem Sie entweder auf Wartungsaufgaben reagieren oder den Cluster so ändern, dass er die neue Version verwendet.

Wenn Sie eine Aurora-PostgreSQL-Version zur Installation auswählen und einen vorhandenen DB-Cluster von Aurora PostgreSQL in der AWS Management Console anzeigen, zeigt die Version nur die *major*.*minor*-Ziffern an. In der folgenden Abbildung aus der Konsole wird für einen vorhandenen DB-Cluster von Babelfish für Aurora PostgreSQL mit Aurora PostgreSQL 13.4 beispielsweise ein Upgrade des Clusters auf Version 13.7 empfohlen, eine neue Nebenversion von Aurora PostgreSQL.



Um vollständige Versionsdetails, einschließlich der *Patch*-Ebene, zu erhalten, können Sie den DB-Cluster von Aurora PostgreSQL mithilfe der Aurora-PostgreSQL-Funktion `aurora_version` abfragen. Weitere Informationen finden Sie unter aurora_version im Aurora-PostgreSQL-Funktionsreferenz. Ein Beispiel für die Verwendung der Funktion finden Sie in der Prozedur To use the PostgreSQL port to query for version information unter Identifizieren Ihrer Babelfish-Version.

Die folgende Tabelle zeigt die Versionen von Aurora PostgreSQL und Babelfish sowie die verfügbaren Zielversionen, die den Upgrade-Prozess für Nebenversionen unterstützen können.

Aktuelle Quellversionen		Neuestes Upgrade-Ziele		Sonstige verfügbare Upgrade-Versionen			
Aurora PostgreSQL	Babelfish	Aurora PostgreSQL	Babelfish	Aurora-PostgreSQL-Versionen mit Babelfish-Option			
15.4	3.3.0	15.5	3.4.0				

Aktuelle Quellversionen		Neuestes Upgrade-Ziele		Sonstige verfügbare Upgrade-Versionen			
15.3.2	3.2.1	15.5	3.4.0	15.4			
15.2.4	3.1.3	15.5	3.4.0	15.4	15.3		
14.9.1	2.6.0	14.10	2.7.0				
14.8.2	2.5.1	14.10	2.7.0	14.9.1			
14.7.4	2.4.3	14.10	2.7.0	14.9.1	14.8.2		
14.6.4	2.3.3	14.10	2.7.0	14.9.1	14.8.2	14.7.4	
14.5.3	2.2.3	14.10	2.7.0	14.9.1	14.8.2	14.7.4	14.6.4
14.3.1	2.1.1	14.6	2.3.0				
14.3.0	2.1.0	14.6	2.3.0	14.3.1			
13.8	1.4.0	13.9	1.5				
13.7.1	1.3.1	13.9	1.5	13.8			
13.7.0	1.3.0	13.9	1.5	13.7.1			
13.6.4	1.2.4	13.9	1.5	13.7			
13.6.3	1.2.1	13.9	1.5	13.7	13.6.4		
13.6.2	1.2.1	13.9	1.5	13.7	13.6.4		
13.6.1	1.2.0	13.9	1.5	13.7	13.6.4		
13.6.0	1.2.0	13.9	1.5	13.7	13.6.4		
13.5	1.1.0	13.9	1.5	13.7	13.6		
13.4	1.0.0	13.9	1.5	13.7	13.6	13.5	

Durchführen von Upgrades von Babelfish auf eine neue Hauptversion

Für ein Hauptversions-Upgrade müssen Sie zuerst Ihren DB-Cluster von Babelfish für Aurora PostgreSQL auf eine Version aktualisieren, die das Hauptversions-Upgrade unterstützt. Wenden Sie dazu Patch-Updates oder Nebenversions-Upgrades auf Ihren DB-Cluster an. Weitere Informationen finden Sie unter Durchführen eines Upgrades von Babelfish auf eine neue Nebenversion.

Die folgende Tabelle zeigt die Versionen von Aurora PostgreSQL und Babelfish, die ein Hauptversions-Upgrade unterstützen können.

Aktuelle Quellversionen		Neuestes verfügbares Upgrade-Ziel		Andere verfügbare Versionen (Nebenversions-Upgrades)		
Aurora PostgreSQL	Babelfish	Aurora PostgreSQL	Babelfish	Aurora-PostgreSQL-Version (Babelfish-Version)		
15.5	3.4.0	16.1	4.0.0			
15.4	3.3.0	16.1	4.0.0			
15.3	3.2.0	16.1	4.0.0			
15.2	3.1.0	16.1	4.0.0			
14.10	2.7.0	15.5	3.4.0			
14.9	2.6.0	15.5	3.4.0	15.4 (3.3.0)		
14.8	2.5.0	15.5	3.4.0	15.4 (3.3.0)	15.3 (3.2.0)	
14.7	2.4.0	15.5	3.4.0	15.4 (3.3.0)	15.3 (3.2.0)	15.2(3.1.0)
14.6	2.3.0	15.5	3.4.0	15.4 (3.3.0)	15.3 (3.2.0)	15.2(3.1.0)
13.9	1.5.0	14.6	2.3.0			
13.8	1.4.0	14.6	2.3.0			
13.7.1	1.3.1	14.6	2.3.0	13.8 (1.4)		

Aktuelle Quellversionen		Neuestes verfügbares Upgrade-Ziel		Andere verfügbare Versionen (Nebenversions-Upgrades)		
13.6.4	1.2.2	14.6	2.3.0	13.8 (1.4)	13.7 (1.3)	

Vor dem Durchführen von Upgrades von Babelfish auf eine neue Hauptversion

Ein Upgrade kann zu kurzen Ausfällen führen. Aus diesem Grund empfehlen wir, dass Sie Upgrades während Ihres Wartungsfensters oder in anderen Zeiträumen geringer Auslastung durchführen oder planen.

Vor dem Durchführen eines Hauptversions-Upgrades

1. Ermitteln Sie die Babelfish-Version Ihres vorhandenen DB-Clusters von Aurora PostgreSQL mithilfe der unter Identifizieren Ihrer Babelfish-Version beschriebenen Befehle. Die Versionsinformationen von Aurora PostgreSQL und Babelfish werden von PostgreSQL verarbeitet. Folgen Sie daher den im Verfahren To use the PostgreSQL port to query for version information beschriebenen Schritten, um die Details zu erhalten.
2. Überprüfen Sie, ob Ihre Version das Hauptversions-Upgrade unterstützt. Eine Liste der Versionen, die die Funktion zum Upgraden der Hauptversion unterstützen, finden Sie unter Durchführen eines Upgrades von Babelfish auf eine neue Nebenversion. Führen Sie außerdem die vor dem Upgrade erforderlichen Aufgaben durch.

   Wenn Ihre Babelfish-Version beispielsweise auf einem DB-Cluster von Aurora PostgreSQL 13.5 läuft und Sie ein Upgrade auf Aurora PostgreSQL 15.2 durchführen möchten, wenden Sie zuerst alle Nebenversionen und Patches an, um Ihren Cluster auf Aurora PostgreSQL 14.6 zu aktualisieren. Wenn Ihr Cluster Version 14.6. oder höher ausführt, fahren Sie mit dem Upgrade der Hauptversion fort.
3. Erstellen Sie einen manuellen Snapshot Ihres aktuellen Babelfish-DB-Clusters als Backup. Mit dem Backup können Sie den Cluster auf seine Aurora-PostgreSQL- und Babelfish-Version zurücksetzen und alle Daten auf den Zustand vor dem Upgrade wiederherstellen. Weitere Informationen finden Sie unter Erstellen eines DB-Cluster-Snapshots. Stellen Sie sicher, dass Sie Ihre vorhandene benutzerdefinierte DB-Cluster-Parametergruppe beibehalten, um sie erneut zu verwenden, wenn Sie diesen Cluster auf den Zustand vor dem Upgrade wiederherstellen möchten. Weitere Informationen finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot und Überlegungen zu Parametergruppen.

4. Bereiten Sie eine benutzerdefinierte DB-Cluster-Parametergruppe für die DB-Zielversion von Aurora PostgreSQL vor. Duplizieren Sie die Einstellungen für die Babelfish-Parameter aus Ihrem aktuellen DB-Cluster von Babelfish für Aurora PostgreSQL. Eine Liste aller Babelfish-Parameter finden Sie unter Einstellungen der DB-Cluster-Parametergruppe für Babelfish. Für ein Upgrade der Hauptversion sind für die folgenden Parameter dieselben Einstellungen wie für den Quell-DB-Cluster erforderlich. Damit das Upgrade erfolgreich ist, müssen alle Einstellungen identisch sein.

   - rds.babelfish_status
   - babelfishpg_tds.tds_default_numeric_precision
   - babelfishpg_tds.tds_default_numeric_scale
   - babelfishpg_tsql.database_name
   - babelfishpg_tsql.default_locale
   - babelfishpg_tsql.migration_mode
   - babelfishpg_tsql.server_colation_name

   > **Warning**
   >
   > Wenn die Einstellungen für die Babelfish-Parameter in der benutzerdefinierten DB-Cluster-Parametergruppe für die neue Aurora-PostgreSQL-Version nicht mit den Parameterwerten des Clusters übereinstimmen, den Sie aktualisieren, schlägt die Operation `ModifyDBCluster` fehl. Die Fehlermeldung `InvalidParameterCombination` erscheint in der AWS Management Console oder in der Ausgabe des AWS CLI-Befehls `modify-db-cluster`.

5. Verwenden Sie die AWS Management Console oder die AWS CLI, um die benutzerdefinierte Parametergruppe für den DB-Cluster zu erstellen. Wählen Sie die entsprechende Aurora-PostgreSQL-Familie für die Version von Aurora PostgreSQL aus, die Sie für das Upgrade benötigen.

   > **Tip**
   >
   > Parametergruppen werden auf der Ebene der AWS-Region verwaltet. Wenn Sie mit der AWS CLI arbeiten, können Sie eine Standardregion für die Konfiguration verwenden, anstatt `--region` im Befehl anzugeben. Weitere Informationen zur Verwendung

der AWS CLI finden Sie unter Schnelleinrichtung im AWS Command Line Interface-Benutzerhandbuch.

Durchführen eines Hauptversions-Upgrades

1. Führen Sie ein Upgrade des DB-Clusters von Aurora PostgreSQL auf eine neue Hauptversion durch. Weitere Informationen finden Sie unter Upgrade der Aurora-PostgreSQL-Engine auf eine neue Hauptversion.
2. Starten Sie die Writer-Instance des Clusters neu, damit die Parametereinstellungen wirksam werden.

Nach dem Durchführen von Upgrades auf eine neue Hauptversion

Nach einem Upgrade der Hauptversion auf eine neue Aurora-PostgreSQL-Version ist der `IDENTITY`-Wert in Tabellen mit einer `IDENTITY`-Spalte möglicherweise größer (+32) als vor dem Upgrade. Wenn die nächste Zeile in solche Tabellen eingefügt wird, springt der generierte Identitätsspaltenwert demzufolge zur Zahl +32 und die Sequenz beginnt von dort aus. Dieser Zustand wirkt sich nicht negativ auf die Funktionen Ihres Babelfish-DB-Clusters aus. Wenn Sie möchten, können Sie das Sequenzobjekt jedoch auf der Grundlage des Maximalwerts der Spalte zurücksetzen. Stellen Sie dazu eine Verbindung zum T-SQL-Port auf Ihrer Babelfish-Writer-Instance mit `sqlcmd` oder einem anderen SQL-Server-Client her. Weitere Informationen finden Sie unter Verbinden mit Ihrem DB-Cluster mithilfe eines SQL Server-Clients.

```
sqlcmd -S bfish-db.cluster-123456789012.aws-region.rds.amazonaws.com,1433 -U
     sa -P ******** -d dbname
```

Wenn die Verbindung hergestellt ist, verwenden Sie den folgenden SQL-Befehl, um Anweisungen zu generieren, mit denen Sie das zugehörige Sequenzobjekt als Ausgangswert verwenden können. Dieser SQL-Befehl funktioniert sowohl für Babelfish-Konfigurationen mit einer einzelnen Datenbank als auch mit mehreren Datenbanken. Weitere Informationen zu diesen beiden Bereitstellungsmodellen finden Sie unter Verwenden von Babelfish mit einer einzigen Datenbank oder mehreren Datenbanken.

```
DECLARE @schema_prefix NVARCHAR(200) = ''
IF current_setting('babelfishpg_tsql.migration_mode') = 'multi-db'
    SET @schema_prefix = db_name() + '_'
```

```
SELECT 'SELECT setval(pg_get_serial_sequence(''' + @schema_prefix +
 schema_name(tables.schema_id)
    + '.' + tables.name + ''', ''' + columns.name + '''),(select max(' + columns.name +
 ')
    FROM ' + schema_name(tables.schema_id) + '.' + tables.name + '));
    'FROM sys.tables tables JOIN sys.columns
    columns ON tables.object_id = columns.object_id
    WHERE columns.is_identity = 1
GO
```

Die Abfrage generiert eine Reihe von SELECT-Anweisungen, die Sie dann ausführen können, um den maximalen IDENTITY-Wert zurückzusetzen und etwaige Lücken zu schließen. Im Folgenden wird die Ausgabe gezeigt, wenn die SQL-Server-Beispieldatenbank Northwind verwendet wird, die auf einem Babelfish-Cluster ausgeführt wird.

```
------------------------------------------------------
SELECT setval(pg_get_serial_sequence('northwind_dbo.categories', 'categoryid'),(select
 max(categoryid)
    FROM dbo.categories));

SELECT setval(pg_get_serial_sequence('northwind_dbo.orders', 'orderid'),(select
 max(orderid)
    FROM dbo.orders));


SELECT setval(pg_get_serial_sequence('northwind_dbo.products', 'productid'),(select
 max(productid)
    FROM dbo.products));


SELECT setval(pg_get_serial_sequence('northwind_dbo.shippers', 'shipperid'),(select
 max(shipperid)
    FROM dbo.shippers));


SELECT setval(pg_get_serial_sequence('northwind_dbo.suppliers', 'supplierid'),(select
 max(supplierid)
    FROM dbo.suppliers));


(5 rows affected)
```

Führen Sie die Anweisungen nacheinander aus, um die Sequenzwerte zurückzusetzen.

Beispiel: Durchführen eines Upgrades des Babelfish-DB-Clusters auf eine Hauptversion

In diesem Beispiel finden Sie eine Reihe von AWS CLI-Befehlen, die erklären, wie ein DB-Cluster von Aurora PostgreSQL 13.6.4, auf dem Babelfish Version 1.2.2 ausgeführt wird, zu Aurora PostgreSQL 14.6 aktualisiert wird. Zunächst erstellen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe für Aurora PostgreSQL 14. Als Nächstes ändern Sie die Parameterwerte so, dass sie denen von Aurora PostgreSQL Version 13 als Quelle entsprechen. Schließlich führen Sie das Upgrade durch, indem Sie den Quell-Cluster ändern. Weitere Informationen finden Sie unter Einstellungen der DB-Cluster-Parametergruppe für Babelfish. In diesem Thema finden Sie auch Informationen zur Verwendung der AWS Management Console zur Durchführung des Upgrades.

Verwenden Sie den CLI-Befehl create-db-cluster-parameter-group, um die DB-Cluster-Parametergruppe für die neue Version zu erstellen.

Für Linux, macOSoder Unix:

```
aws rds create-db-cluster-parameter-group \
    --db-cluster-parameter-group-name docs-lab-babelfish-apg-14 \
    --db-parameter-group-family aurora-postgresql14 \
    --description 'New custom parameter group for upgrade to new major version' \
    --region us-west-1
```

Wenn Sie diesen Befehl ausführen, wird die benutzerdefinierte DB-Cluster-Parametergruppe in der AWS-Region erstellt. Die Ausgabe entspricht weitgehend der folgenden.

```
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "docs-lab-babelfish-apg-14",
        "DBParameterGroupFamily": "aurora-postgresql14",
        "Description": "New custom parameter group for upgrade to new major version",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-west-1:111122223333:cluster-
pg:docs-lab-babelfish-apg-14"
    }
}
```

Weitere Informationen finden Sie unter Erstellen einer DB-Cluster-Parametergruppe.

Verwenden Sie den CLI-Befehl modify-db-cluster-parameter-group, um die Einstellungen so zu ändern, dass sie mit dem Quell-Cluster übereinstimmen.

Windows:

```
aws rds modify-db-cluster-parameter-group --db-cluster-parameter-group-name docs-lab-
babelfish-apg-14 ^
  --parameters
 "ParameterName=rds.babelfish_status,ParameterValue=on,ApplyMethod=pending-reboot" ^
 "ParameterName=babelfishpg_tds.tds_default_numeric_precision,ParameterValue=38,ApplyMethod=pen
reboot" ^
 "ParameterName=babelfishpg_tds.tds_default_numeric_scale,ParameterValue=8,ApplyMethod=pending-
reboot" ^
 "ParameterName=babelfishpg_tsql.database_name,ParameterValue=babelfish_db,ApplyMethod=pending-
reboot" ^
 "ParameterName=babelfishpg_tsql.default_locale,ParameterValue=en-
US,ApplyMethod=pending-reboot" ^
 "ParameterName=babelfishpg_tsql.migration_mode,ParameterValue=single-
db,ApplyMethod=pending-reboot" ^
 "ParameterName=babelfishpg_tsql.server_collation_name,ParameterValue=sql_latin1_general_cp1_ci
reboot"
```

Die Antwort sieht in etwa so aus:

```
{
    "DBClusterParameterGroupName": "docs-lab-babelfish-apg-14"
}
```

Verwenden Sie den modify-db-cluster CLI-Befehl , um den Cluster so zu ändern, dass er die neue Version und die neue benutzerdefinierte DB-Cluster-Parametergruppe verwendet. Sie geben auch das Argument `--allow-major-version-upgrade` an, wie im folgenden Beispiel gezeigt.

```
aws rds modify-db-cluster \
--db-cluster-identifier docs-lab-bfish-apg-14 \
--engine-version 14.6 \
--db-cluster-parameter-group-name docs-lab-babelfish-apg-14 \
--allow-major-version-upgrade \
--region us-west-1 \
--apply-immediately
```

Verwenden Sie den reboot-db-instance -CLI-Befehl, um die Writer-Instance des Clusters neu zu starten, damit die Parametereinstellungen wirksam werden können.

```
aws rds reboot-db-instance \
--db-instance-identifier docs-lab-bfish-apg-14-instance-1\
--region us-west-1
```

Verwenden des Babelfish-Produktversionsparameters

Ein neuer Grand Unified Configuration (GUC)-Parameter namens `babelfishpg_tds.product_version` wird in den Versionen Babelfish 2.4.0 und 3.1.0 eingeführt. Mit diesem Parameter können Sie die Versionsnummer des SQL-Server-Produkts als Ausgabe von Babelfish festlegen.

Der Parameter ist eine 4-teilige Versions-ID-Zeichenfolge und jeder Teil sollte durch „.“ getrennt werden.

Syntax

```
Major.Minor.Build.Revision
```

- Hauptversion: Eine Zahl zwischen 11 und 16.
- Nebenversion: Eine Zahl zwischen 0 und 255.
- Build-Version: Eine Zahl zwischen 0 und 65535.
- Revision: 0 und eine beliebige positive Zahl.

Konfigurieren des Babelfish-Produktversionsparameters

Sie müssen die Cluster-Parametergruppe verwenden, um den Parameter babelfishpg_tds.product_version in der Konsole festzulegen. Weitere Informationen zum Ändern des DB-Cluster-Parameters finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe.

Wenn Sie den Produktversionsparameter auf einen ungültigen Wert festlegen, wird die Änderung nicht wirksam. Die Konsole zeigt Ihnen möglicherweise den neuen Wert an, der Parameter behält jedoch den vorherigen Wert bei. Details zu den Fehlermeldungen können Sie der Engine-Protokolldatei entnehmen.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group \
--db-cluster-parameter-group-name mydbparametergroup \
--parameters
 "ParameterName=babelfishpg_tds.product_version,ParameterValue=15.2.4000.1,ApplyMethod=immediat
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
--db-cluster-parameter-group-name mydbparametergroup ^
--parameters
 "ParameterName=babelfishpg_tds.product_version,ParameterValue=15.2.4000.1,ApplyMethod=immediat
```

Betroffene Abfragen und Parameter

Abfrage/Parameter	Ergebnis	Wirksamkeit
SELECT @@VERSION	Gibt die benutzerdefinierte SQL-Server-Version zurück (babelfishpg_tsql.version value = Standard)	Sofort
SELECT SERVERPROPERTY microSDProductVersion')	Gibt die benutzerdefinierte SQL-Server-Version zurück	Sofort
SELECT SERVERPROPERTY microSDProductMajorVersion')	Gibt die Hauptversion der benutzerdefinierte SQL-Server-Version zurück	Sofort
VERSION-Token in der PRELOGIN-Antwortnachricht	Der Server gibt PRELOGIN-Nachrichten mit der benutzerdefinierten SQL-Server-Version zurück	Wird wirksam, wenn ein Benutzer eine neue Sitzung erstellt
SQL ServerVersion in LoginAck bei Verwendung von JDBC	DatabaseMetaData.getDatabaseProductVersion()	Wird wirksam, wenn ein Benutzer eine neue Sitzung erstellt

Abfrage/Parameter	Ergebnis	Wirksamkeit
	gibt eine benutzerdefinierte SQL Server-Version zurück	

Schnittstelle mit dem Parameter babelfishpg_tsql.version

Sie können die Ausgabe von @@VERSION mit den Parametern babelfishpg_tsql.version und babelfishpg_tds.product_version festlegen. In den folgenden Beispielen wird gezeigt, wie sich diese beiden Parameter zueinander verhalten.

- Wenn der Parameter babelfishpg_tsql.version „default“ ist und der Parameter babelfishpg_tds.product_version 15.0.2000.8 lautet.
  - Ausgabe von @@version – 15.0.2000.8.
- Wenn der Parameter babelfishpg_tsql.version auf 13.0.2000.8 festgelegt ist und der Parameter babelfishpg_tds.product_version 15.0.2000.8 lautet.
  - Ausgabe von @@version – 13.0.2000.8.

Referenz für Babelfish for Aurora PostgreSQL

Themen

Nicht unterstützte Funktionalität in Babelfish

In den folgenden Tabellen und Listen finden Sie Funktionen, die derzeit in Babelfish nicht unterstützt werden. Updates für Babelfish sind in Aurora-PostgreSQL-Versionen enthalten. Weitere Informationen finden Sie unter Versionshinweise für Aurora PostgreSQL.

Themen

Derzeit nicht unterstützte Funktionen

In der Tabelle finden Sie Informationen zu bestimmten Funktionen, die derzeit nicht unterstützt werden.

Funktionalität oder Syntax	Beschreibung
Assembly-Module und SQL Common Language Runtime (CLR)-Routinen	Funktionen im Zusammenhang mit Baugruppenmodulen und CLR-Routinen werden nicht unterstützt.

Funktionalität oder Syntax	Beschreibung
Spalten-Attribute	ROWGUIDCOL, SPARSE, FILESTREAM und MASKED werden nicht unterstützt.
Eingeschlossene	Enthaltene Datenbanken mit Logins, die auf Datenbankebene und nicht auf Serverebene authentifiziert sind, werden nicht unterstützt.
Cursoren (aktualisierbar)	Aktualisierbare Cursor werden nicht unterstützt.
Cursoren (global)	GLOBALE Cursor werden nicht unterstützt.
Cursor (Verhalten abrufen)	Die folgenden Cursor-Abrufverhalten werden nicht unterstützt: FETCH PRIOR, FIRST, LAST, ABSOLUTE, und RELATIVE
Cursor-typisierte Ausgabepa rameter	Variablen und Parameter vom Cursor-Typ werden für Ausgabeparameter nicht unterstützt (ein Fehler wird ausgelöst).
Cursor-Optionen	SCROLL, KEYSET, DYNAMIC, FAST_FORWARD, SCROLL_LOCKS, OPTIMISTIC, TYPE_WARNING und FOR UPDATE
Datenverschlüsselung	Die Datenverschlüsselung wird nicht unterstützt.
Datenschichtanwendungen (DAC)	Import- oder Exportvorgänge für Datenschichtanwendungen (DAC) mit DAC-Paketdateien (.dacpac) oder DAC-Backu pdateien (.bacpac) werden nicht unterstützt.
DBCC-Befehle	Microsoft SQL Server Database Console Commands (DBCC) werden nicht unterstützt. DBCC CHECKIDENT wird in Babelfish 3.4.0 und höheren Versionen unterstützt.
DROP FALLS VORHANDEN	Diese Syntax wird für USER- und SCHEMA-Objekte nicht unterstützt. Es wird für die Objekte TABLE, VIEW, PROCEDURE, FUNCTION und DATABASE unterstützt.
Verschlüsselung	Eingebaute Funktionen und Anweisungen unterstützen keine Verschlüsselung.

Funktionalität oder Syntax	Beschreibung
ENCRYPT_CLIENT_CERT-Verbindungen	Verbindungen mit Clientzertifikaten werden nicht unterstützt.
EXECUTE AS-Anweisung	Diese Aussage wird nicht unterstützt.
EXECUTE AS SELF-Klausel	Diese Klausel wird in Funktionen, Prozeduren oder Triggern nicht unterstützt.
EXECUTE AS USER-Klausel	Diese Klausel wird in Funktionen, Prozeduren oder Triggern nicht unterstützt.
Fremdschlüsseleinschränkungen, die auf den Datenbank namen verweisen	Fremdschlüsseleinschränkungen, die auf den Datenbanknamen verweisen, werden nicht unterstützt.
FORMAT	Benutzerdefinierte Typen werden nicht unterstützt.
Funktionsdeklarationen mit mehr als 100 Parametern	Funktionsdeklarationen, die mehr als 100 Parameter enthalten, werden nicht unterstützt.
Funktionsaufrufe, die DEFAULT als Parameterwert enthalten	DEFAULT ist kein unterstützter Parameterwert für einen Funktionsaufruf. DEFAULT als Parameterwert für einen Funktionsaufruf wird ab Babelfish 3.4.0 und höheren Versionen unterstützt.
Funktionen, extern definiert	Externe Funktionen, einschließlich SQL CLR-Funktionen, werden nicht unterstützt.
Globale temporäre Tabellen (Tabellen mit Namen, die mit ## beginnen)	Globale temporäre Tabellen werden nicht unterstützt.
Graph-Funktion	Alle SQL-Graph-Funktionalität werden nicht unterstützt.
Bezeichner (Variablen oder Parameter) mit mehreren führenden @ Zeichen	Identifikatoren, die mit mehr als einem führenden @ beginnen, werden nicht unterstützt.

Funktionalität oder Syntax	Beschreibung
Bezeichner, Tabellen- oder Spaltennamen, welche die Zeichen @ oder]] enthalten	Tabellen- oder Spaltennamen, die ein @- Zeichen oder eckige Klammern enthalten, werden nicht unterstützt.
Eingebreitete Indizes	Inline-Indizes werden nicht unterstützt.
Aufrufen einer Prozedur, deren Name in einer Variablen enthalten ist	Die Verwendung einer Variablen als Prozedurnamen wird nicht unterstützt.
Materialisierte Ansichten	Materialisierte Ansichten werden nicht unterstützt.
NICHT FÜR REPLICATION-Klausel	Diese Syntax wird akzeptiert und ignoriert.
ODBC Escape-Funktionen	ODBC-Escape-Funktionen werden nicht unterstützt.
Partitionierung	Tabellen- und Indexpartitionierung wird nicht unterstützt.
Prozeduraufrufe mit DEFAULT als Parameterwert	DEFAULT ist kein unterstützter Parameterwert. DEFAULT als Parameterwert für einen Funktionsaufruf wird ab Babelfish 3.4.0 und höheren Versionen unterstützt.
Verfahrenserklärungen mit mehr als 100 Parametern	Deklarationen mit mehr als 100 Parametern werden nicht unterstützt.
Prozeduren, extern definiert	Extern definierte Prozeduren, einschließlich SQL CL), werden nicht unterstützt.
Versionierung der Prozedur	Prozedur Versionierung wird nicht unterstützt.
Prozeduren MIT RECOMPILE	WITH RECOMPILE (wenn es in Verbindung mit den Anweisungen DECLARE und EXECUTE verwendet wird) wird nicht unterstützt.

Funktionalität oder Syntax	Beschreibung
Remote-Objektreferenzen	Die Ausführung von Prozeduren und Funktionen mit vierteiligen Namen wird nicht unterstützt. Unterstützt in entfernten Objekten vierteilige Objektnamen für ausgewählte Abfragen. Weitere Informationen finden Sie unter Einstellungen der DB-Cluster-Parametergruppe für Babelfish.
Sicherheit auf Zeilenebene	Die Sicherheit auf Zeilenebene mit CREATE SECURITY POLICY und Funktionen mit Inline-Tabellenwert wird nicht unterstützt.
Service-Broker-Funktionalität	Die Service-Broker-Funktionalität wird nicht unterstützt.
SESSIONPROPERTY	Nicht unterstützte Eigenschaften: ANSI_NULLS, ANSI_PADDING, ANSI_WARNINGS, ARITHABORT, CONCAT_NULL_YIELDS_NULL und NUMERIC_ROUNDABORT
SET-LANGUAGE	Diese Syntax wird mit keinem anderen Wert als `english` oder `us_english` unterstützt.
SP_CONFIGURE	Diese gespeicherte Systemprozedur wird nicht unterstützt.
SQL-Schlüsselwort `SPARSE`	Das Schlüsselwort SPARSE wird akzeptiert und ignoriert.
Syntax des Tabellenwert-Konstruktors (FROM-Klausel)	Die nicht unterstützte Syntax gilt für eine abgeleitete Tabelle, die mit der FROM-Klausel erstellt wurde.
Temporäre Tabellen	Temporäre Tabellen werden nicht unterstützt.
Temporäre Verfahren werden nicht automatisch gelöscht	Diese Funktion wird nicht unterstützt.
Trigger, extern definiert	Diese Trigger werden nicht unterstützt, einschließlich SQL Common Language Runtime (CLR).

Funktionalität oder Syntax	Beschreibung
Ohne SCHEMABINDING-Klausel	Das Erstellen einer Ansicht ohne SCHEMABINDING wird nicht unterstützt, die Ansicht wird jedoch erstellt, als ob WITH SCHEMABINDING angegeben wurde. Die Verwendung von SCHEMABINDING beim Erstellen von Funktionen, Prozeduren und Triggern wird stillschweigend ignoriert.

Nicht unterstützte Einstellungen

Die folgenden Einstellungen werden nicht unterstützt:

- SETZE ANSI_NULL_DFLT_OFF EIN
- SETZE ANSI_NULL_DFLT_ON AUS
- SETZE ANSI_PADDING AUS
- SETZE ANSI_WARNINGS AUS
- AKTIVIEREN SIE ARITHABORT AUS
- SETZE ARITHIGNORE AUF
- SETZE CURSOR_CLOSE_ON_COMMIT AUF
- SET NUMERIC_ROUNDABORT ON
- SET PARSEONLY ON (Befehl funktioniert nicht wie erwartet)
- SET FMTONLY ON (Der Befehl funktioniert nicht wie erwartet. Er unterdrückt nur die Ausführung von SELECT-Anweisungen, von anderen jedoch nicht.)

Befehle, die nicht unterstützt werden

Für folgende Befehle werden bestimmte Funktionen nicht unterstützt:

- SIGNATURE HINZUFÜGEN
- DATENBANK ÄNDERN, DATENBANK ÄNDERN
- BACKUP/RESTORE DATABASE/LOG
- BACPAC und DACPAC FILES RESTORE
- AUTORISIERUNG ERSTELLEN, ÄNDERN, LÖSCHEN. ALTER AUTHORIZATION wird für Datenbankobjekte unterstützt.

- ERSTELLE, ÄNDERUNG, DROP VERFÜGBARKEITSGRUPPE
- BROKER-PRIORITÄT ERSTELLEN, ÄNDERN, LÖSCHEN
- SPALTENVERSCHLÜSSELUNGSSCHLÜSSEL ERSTELLEN, ÄNDERN, LÖSCHEN
- DATENBANK-VERSCHLÜSSELUNGSSCHLÜSSEL ERSTELLEN, ÄNDERN, LÖSCHEN
- ZERTIFIKAT ERSTELLEN, ÄNDERN, LÖSCHEN, SICHERN
- CREATE AGGREGATE
- VERTRAG ERSTELLEN
- CHECKPOINT

Nicht unterstützte Spaltennamen oder Attribute

Die folgenden Spaltennamen werden nicht unterstützt:

- $IDENTITY
- $ROWGUID
- IDENTITYCOL

Nicht unterstützte Datentypen

Die folgenden Datentypen werden nicht unterstützt:

- Geospatial (GEOGRAPHY und GEOMETRY)
- HIERARCHYID

Nicht unterstützte Objekttypen

Die folgenden Objekttypen werden nicht unterstützt:

- SPALTEN-MASTERSCHLÜSSEL
- EXTERNE DATENQUELLE ERSTELLEN, ÄNDERN
- DATENBANK-AUDIT-SPEZIFIKATION ERSTELLEN, ÄNDERN, LÖSCHEN
- EXTERNE BIBLIOTHEK ERSTELLEN, ÄNDERN, LÖSCHEN
- SERVER-AUDIT ERSTELLEN, ÄNDERN, LÖSCHEN
- ERSTELLEN, ÄNDERN, LÖSCHEN DER SERVER-AUDIT-SPEZIFIKATION

- SYMMETRISCHEN SCHLÜSSEL ERSTELLEN, ÄNDERN, LÖSCHEN, ÖFFNEN/SCHLIESSEN
- CREATE, DROP DEFAULT
- ANMELDEINFORMATION
- KRYPTOGRAFISCHER ANBIETER
- DIAGNOSESITZUNG
- Indizierte Ansichten
- SERVICE-MASTERSCHLÜSSELS
- SYNONYM

Nicht unterstützte Funktionen

Folgende integrierte Funktionen werden nicht unterstützt:

Aggregationsfunktionen

- APPROX_COUNT_DISTINCT
- CHECKSUM_AGG
- GROUPING_ID
- STRING_AGG unter Verwendung der WITHIN GROUP-Klausel

Kryptografische Funktionen

- CERTENCODED-Funktion
- CERTID-Funktion
- CERTPROPERTY-Funktion

Metadatenfunktionen

- COLUMNPROPERTY
- TYPEPROPERTY
- SERVERPROPERTY-Funktion – Die folgenden Eigenschaften werden nicht unterstützt:
  - BuildClrVersion
  - ComparisonStyle
  - ComputerNamePhysicalNetBIOS

- HadrManagerStatus
- InstanceDefaultDataPath
- InstanceDefaultLogPath
- IsClustered
- IsHadrAktiviert
- LCID
- NumLicenses
- ProcessID
- ProductBuild
- ProductBuildTyp
- ProductUpdateReferenz
- ResourceLastUpdateDateZeit
- ResourceVersion
- ServerName
- SqlCharEingestellt
- SqlCharSetName
- SqlSortBestellung
- SqlSortOrderName
- FilestreamShareName
- FilestreamConfiguredStufe
- FilestreamEffectiveStufe

Sicherheitsfunktionen

- CERTPRIVATEKEY
- LOGINPROPERTY

Anweisungen, Operatoren, andere Funktionen

- EVENTDATA-Funktion
- GET_TRANSMISSION_STATUS
- OPENXML

Nicht unterstützte Syntax

Die folgende Syntax wird nicht unterstützt:

- ALTER DATABASE
- ALTER DATABASE SCOPED CONFIGURATION
- ALTER DATABASE SCOPED CREDENTIAL
- ALTER DATABASE SET HADR
- ALTER FUNCTION
- ALTER INDEX
- ALTER PROCEDURE statement
- ALTER SCHEMA
- ALTER SERVER CONFIGURATION
- ALTER SERVICE, BACKUP/RESTORE SERVICE MASTER KEY-Klausel
- ALTER VIEW
- BEGIN CONVERSATION TIMER
- STARTEN SIE VERTEILTE TRANSAKTION
- BEGIN DIALOG CONVERSATION
- BULK INSERT
- CREATE COLUMNSTORE INDEX
- CREATE EXTERNAL FILE FORMAT
- CREATE EXTERNAL TABLE
- ANWENDUNGSROLLE ERSTELLEN, ÄNDERN, LÖSCHEN
- BAUGRUPPE ERSTELLEN, ÄNDERN, LÖSCHEN
- ASYMMETRISCHEN SCHLÜSSEL ERSTELLEN, ÄNDERN, LÖSCHEN
- CREATE, ALTER, DROP CREDENTIAL
- CREATE, ALTER, DROP CRYPTOGRAPHIC PROVIDER
- CREATE, ALTER, DROP ENDPOINT
- EVENT-SITZUNG ERSTELLEN, ÄNDERN, LÖSCHEN
- CREATE, ALTER, DROP EXTERNAL LANGUAGE
- EXTERNEN RESSOURCENPOOL ERSTELLEN, ÄNDERN, LÖSCHEN
- ERSTELLEN, ÄNDERN, LÖSCHEN VOLLTEXTKATALOG

- ERSTELLEN, ÄNDERN, LÖSCHEN VOLLTEXTINDEX
- ERSTELLEN, ÄNDERN, LÖSCHEN VOLLTEXT-STOPLIST
- CREATE, ALTER, DROP MESSAGE TYPE
- ERSTELLEN, ÄNDERN, LÖSCHEN, ÖFFNEN/SCHLIESSEN, HAUPTSCHLÜSSEL SICHERN/WIEDERHERSTELLEN
- CREATE, ALTER, DROP PARTITION FUNCTION
- CREATE, ALTER, DROP PARTITION SCHEME
- CREATE, ALTER, DROP QUEUE
- RESSOURCENGOUVERNEUR ERSTELLEN, ÄNDERN, LÖSCHEN
- CREATE, ALTER, DROP RESOURCE POOL
- ERSTELLEN, ÄNDERN, BENUTZER LÖSCHEN
- CREATE, ALTER, DROP SEARCH PROPERTY LIST
- CREATE, ALTER, DROP SECURITY POLICY
- CREATE, ALTER, DROP SELECTIVE XML INDEX clause
- CREATE, ALTER, DROP SERVICE
- CREATE, ALTER, DROP SPATIAL INDEX
- CREATE, ALTER, DROP TYPE
- CREATE, ALTER, DROP XML INDEX
- CREATE, ALTER, DROP XML SCHEMA COLLECTION
- REGEL ERSTELLEN/LÖSCHEN
- CREATE, DROP WORKLOAD CLASSIFIER
- WORKLOAD-GRUPPE ERSTELLEN, ÄNDERN, LÖSCHEN
- ALTER TRIGGER
- TABELLE ERSTELLEN… GRANT-Klausel
- TABELLE ERSTELLEN… IDENTITY-Klausel
- CREATE USER – Diese Syntax wird nicht unterstützt. Die PostgreSQL-Anweisung CREATE USER erstellt keinen Benutzer, der der SQL Server CREATE USER Syntax entspricht. Weitere Informationen finden Sie unter T-SQL-Unterschiede bei Babelfish.
- DENY
- END, MOVE CONVERSATION
- EXECUTE with AS LOGIN or AT option

- GET CONVERSATION GROUP
- GROUP BY ALL clause
- GROUP BY CUBE clause
- GROUP BY ROLLUP clause
- INSERT... DEFAULT VALUES
- MERGE
- READTEXT
- REVERT
- SELECT PIVOT (wird ab Version 3.4.0 und höher unterstützt, außer wenn es in einer Viewdefinition, einem allgemeinen Tabellenausdruck oder einer Verknüpfung verwendet wird) / UNPIVOT
- SELECT TOP x PERCENT WHERE x **<>** 100
- SELECT TOP... WITH TIES
- SELECT... FOR BROWSE
- WÄHLEN VON… FOR XML AUTO
- SELECT... FOR XML EXPLICIT
- SEND
- SET DATEFORMAT
- SET DEADLOCK_PRIORITY
- SET FMTONLY
- SET FORCEPLAN
- SET NUMERIC_ROUNDABORT ON
- SET OFFSETS
- SET REMOTE_PROC_TRANSACTIONS
- SET SHOWPLAN_TEXT
- SET SHOWPLAN_XML
- SET STATISTICS
- SET STATISTICS PROFILE
- SET STATISTICS TIME
- SET STATISTICS XML
- SHUTDOWN statement

- UPDATE STATISTICS
- UPDATETEXT
- Using EXECUTE to call a SQL function
- VIEW... CHECK OPTION clause
- VIEW... VIEW_METADATA clause
- WAITFOR DELAY
- WAITFOR TIME
- WAITFOR, RECEIVE
- WITH XMLNAMESPACES construct
- WRITETEXT
- XPATH expressions

Unterstützte Funktionalität in Babelfish nach Version

In der folgenden Tabelle finden Sie T-SQL-Funktionen, die von verschiedenen Babelfish-Versionen unterstützt werden. Listen der nicht unterstützten Funktionen finden Sie unter Nicht unterstützte Funktionalität in Babelfish. Weitere Informationen zu verschiedenen Babelfish-Versionen finden Sie unter Versionshinweise für Aurora PostgreSQL.

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
4-teilige Objektnamenreferenzen für SELECT-Anweisungen	✓	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–
AS-Schlüsselwort in CREATE FUNCTION	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
ALTER AUTHORIZATION-Syntax	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
zum Ändern des Datenbankbesitzers															
ALTER ROLE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
BENUTZER ÄNDERN... MIT ANMELDUNG	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
AT TIME ZONE-Klausel	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
Babelfish-Instanz als Verbindungsserver	✓	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–

	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
T-SQL-Funktionalität oder -Syntax															
Vergleichsoperatoren !< und !>	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
CREATE statt Trigger (DML) in SQL Server-Ansichten	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
CREATE ROLE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CREATE TRIGGER	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Erstellen Sie eindeutige Indizes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
T-SQL-Funktionalität oder -Syntax															
Datenbank übergreifende Ausführung von Prozeduren	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Datenbank übergreifende Verweise SELECT, SELECT.. INTO, INSERT, UPDATE, DELETE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
T-SQL-Funktionalität oder -Syntax															
Vom Cursor eingegebene Parameter nur für Eingabeparameter (nicht für die Ausgabe)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Datenmigration mit dem bcp-Client-Hilfsprogramm	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
Datentyp TIMESTAMP, ROWVERSION (Informationen zur Verwendung finden Sie unter Funktionen mit eingeschränkter Implementierung)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
DEFAULT-Schlüsselwort bei Aufrufen von gespeicherten Prozeduren und Funktionen	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
DBCC PRÜFNUMMER	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
DROP DATABASE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
DROP IF EXISTS (für SCHEMA-, DATABASE- und USER-Objekte)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
INDEX INDEX AUF schema.table LÖSCHEN	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–
INDEX LÖSCHEN schema.table.index	–	✓	–	–	–	–	–	–	–	–	–	–	–	–	–
DROP ROLE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
T-SQL-Funktionalität oder -Syntax															
ENABLE/DISABLE TRIGGER	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
VOLLTEXTSUCHE	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Volltextsuche mit CONTAINS-Klausel	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–
GRANT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Räumliche Datentypen für Geometrie und Geografie	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
GUC babelfish pg_tds.product_version	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
Bezeichner mit führendem Punktzeichen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
STATT-Trigger für Tabellen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
STATT-Triggern für Ansichten	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	–
KILL	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–

	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
T-SQL-Funktionalität oder -Syntax															
PIVOT (wird ab 3.4.0 und höheren Versionen unterstützt, außer wenn es in einer Ansichtsdefinition, einem allgemeinen Tabellenausdruck oder einer Verknüpfung	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax verwendet wird)	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
REVOKE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SELECT... OFFSET... FETCH-Klauseln	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
WÄHLEN SIE FÜR JSON-AUTO	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
STELLEN SIE BABELFISH_SHOWPLAN_ALL EIN (und AUS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
SETZEN DAS PROFIL BABELFISH_STATISTICS EIN (AUS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SET CONTEXT_INFO	✓	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–
SET LOCK_TIMEOUT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SET NO_BROWSETABLE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
ZEILENANZAHL FESTLEGEN	✓	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–
SET SHOWPLAN_ALL	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
SET STATISTICS IO	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
SET TRANSACTION ISOLATION LEVEL REPEATABLE READ	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
SET TRANSACTION ISOLATION LEVEL SERIALIZABLE	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
DIE SYNTAX DER TRANSAKTIONSISOLATIONSSTUFE	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–

	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
T-SQL-Funktionalität oder -Syntax															
SSMS-Verbindung mit dem Verbindungsdialogfeld des Objekt-Explorers herstellen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SSMS-Datenmigration mit dem Import/Export Wizard	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
SSMS: Teilweise Unterstützung für den Objekt-Explorer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
STDEV	✓	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–
STDEVP	✓	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–
Trigger mit mehreren DML-Aktionen können auf Übergangstabellen verweisen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
T-SQL-Funktionalität oder -Syntax															
T-SQL-Hinweise (Join-Methoden, Indexverwendung, MAXDOP)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
T-SQL-Syntax mit eckigen Klammern und dem LIKE-Prädikat	✓	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
Zeichenfolgenwerte ohne Anführungszeichen in Aufrufen von gespeicherten Prozeduren und Standardwerten	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
VAR	✓	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–
VARP	✓	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–
Aurora and PostgreSQL features:															
Aurora ML-Dienste	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–

	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
T-SQL-Funktionalität oder -Syntax															
Datenbankauthentifizierung mit Kerberos unter Verwendung AWS Directory Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
Speicherauszug und Wiederherstellung	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Erweiterung pg_stat_statement	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	–
pgvector	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
Zero-Downtime-Patching (ZDP) (Patchen ohne Ausfallzeiten)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
T-SQL Built-in functions:															
ANWENDUNGSNAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
ATN2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
CHARINDEX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CHOOSE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SPALTENLÄNGE	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
SPALTENNAME	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
COLUMNS_UPDATED	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
COLUMNPROPERTY (nur Len) CharMaxAllowsNull	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CONCAT_WS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CONTEXT_INFO	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–	–
CURSOR_STATUS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DATABASE_PRINCIPAL_ID	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–	–
DATEADD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
DATEDIFF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
DATEDIFF_BIG	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
DATEFROMPARTS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
DATENAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
DATEPART	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
DATETIMEFROMPARTS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DATETIME2FROMPARTS	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–	–
DATETIMEOFFSETFROMPARTS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
DATETRUNC	✓	✓	✓	✓	–	–	–	✓	–	–	–	–	–	–	–
DATUM_BUCKET	✓	✓	✓	✓	–	–	–	✓	–	–	–	–	–	–	–
EOMONTH	✓	✓	✓	✓	–	–	–	✓	–	–	–	–	–	–	–
ALS AUFRUFER AUSFÜHREN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
erweiterte Eigenschaft fn_list	✓	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
FÜR JSON	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
FULLTEXTSERVICEPROPERTY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HAS_DBACCESS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HAS_PERMS_BY_NAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HOST_NAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
HOST_ID	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	–
IDENTITY	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
IS_MEMBER	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IS_ROLEMEMBER	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IS_SRVROLEMEMBER	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ISJSON	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
JSON_MODIFY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
JSON_QUERY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
JSON_VALUE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NÄCHSTER WERT FÜR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
OBJECTDEFINITION	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
OBJECTSCHEMANAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
JSON ÖFFNEN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OPENQUERY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ORIGINAL_LOGIN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PARSENAME	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	–
PATINDEX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ROWCOUNT_BIG	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
SCHEMA_NAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SITZUNGSKONTEXT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
SESSION_USER	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SID_BINARY (gibt immer NULL zurück)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
SMALLDATETIMEFROMPARTS	✓	✓	✓	✓	✓	–	–	✓	✓	✓	–	–	–	–	–
SQUARE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
STR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
STRING_AGG	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–
STRING_SPLIT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
SUSER_SID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SUSER_SNAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SWITCHOFFSET	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
SYSTEM_USER	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
TIMEFROMPARTS	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–	–
TODATETIMEOFFSET	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
TO_CHAR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
TRIGGER_NESTLEVEL (nur ohne Argumente)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TRY_CONVERT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
TYPE_ID	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
TYPNAME	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
UPDATE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T-SQL INFORMATION_SCHEMA catalogs															
CHECK_CONSTRAINTS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
VERWENDUNG VON COLUMN_DOMAIN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
COLUMNS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
COLUMN_USAGE EINSCHRÄNKEN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOMAINS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VERWENDUNG VON SCHLÜSSEL SPALTEN	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
ROUTINES	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
TABLES	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TABLE_CONSTRAINTS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ANSICHTEN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T-SQL System-defined @@ variables:															
@@CURSOR_ROWS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@DATEFIRST	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@DBTS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@ERROR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@ERROR =213	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@FETCH_STATUS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@IDENTITY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
@@LANGUAGE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@LOCK_TIMEOUT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@MAX_CONNECTIONS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@MAX_PRECISION	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@MICROSOFTVERSION	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@NESTLEVEL	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@PROCID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@ROWCOUNT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@SERVERNAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@SERVICENAME	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@SPID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
@@TRANCOUNT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
@@VERSION (Beachten Sie den Formatunterschied wie unter beschrieben [T-SQL-Unterschiede bei Babelfish]).	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T-SQL System stored procedures:															
sp_addextended-Eigenschaft	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sp_addLinkedServer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sp_addlinkedsrvlogin	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sp_addrolle	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
sp_addrolemember	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
sp_babelfish_volatility	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sp_column_privileges	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_columns	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_columns_100	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_columns_managed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sp_cursor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursor_list	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursorclose	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursorexecute	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursorfetch	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursoropen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursoroption	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursorprepare	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursorprepexec	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_cursorunprepare	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sp_databases	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_datatype_info	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_datatype_info_100	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_describe_cursor	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_describe_first_result_set	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_describe_undeclared_parameters	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
erweiterte Eigenschaft sp_drop	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sp_dropobverknüpfte SRV-Anmeldung	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sp_dropobjrol	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
sp_dropobjrole Mitglied	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
sp_dropobjserver	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sp_enumoledb_providers	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	–
sp_executeobj	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sp_execute_postgresql (ERSTELLEN, ÄNDERN, LÖSCHEN)	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	
sp_executesql	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_fkeys	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_getapplock	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_helpdb	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_helpdb hat die Rolle repariert	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
sp_helplinkedsrvlogin	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sp_helprole	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_helprole Mitglied	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_helpsrv-Rollenmitglied	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
sp_helpuser	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_linkedservers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sp_oledb_ro_usrname	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_pkeys	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_prefix	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
sp_prepare	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sp_procedure_params_100_managed	✓	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
sp_releaseapplock	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_rename	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sp_serveroption (Option connect_timeout)	✓	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–
sp_set_session_context	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sp_special_columns	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_sproc_columns	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_sproc_columns_100	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sp_statistics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_statistics_100	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_stored_procedures	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_table_privileges	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_tablecollations_100	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sp_tables	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Verbindungsserver sp_test	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	–
sp_unprepare	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
erweiterte Eigenschaft sp_update	✓	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–
sp_wer	✓	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–
xp_qv	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T-SQL Properties supported on the CONNECTIONPROPERTY system function															
auth_scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
client_net_address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
lokale_Netzadresse	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
lokaler_TCP-Port	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
net_transport	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
protokoll typ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
physical_net_transport	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T-SQL Properties supported on the OBJECTPROPERTY system function															
IsInlineFunktion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsScalarFunktion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsTableFunktion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T-SQL Properties supported on the SERVERPROPERTY function															
Babelfish	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kollation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sortierungs-ID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Edition	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
EditionID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
EngineEdition	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
InstanceName	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
IsAdvancedAnalyticsInstalled	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsBigDataCluster	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsFullTextInstalled	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsIntegratedSecurityOnly	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsLocalDB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsPolyBaseInstalled	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsSingleUtzer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IsXTPSupported	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
Japanese_CI_AI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Japanese_CI_AS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Japanese_CS_AS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LicenseType	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MachineName	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
ProductLevel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
ProductMajorAusführung	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ProductMinorAusführung	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ProductUpdateLevel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
ProductVersion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ServerName	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SQL Server views supported by Babelfish															
information_schema.key_column_usage	✓	✓	✓	–	–	–	✓	–	–	–	–	–	–	–	
information_schema.routinen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	
information_schema.schemata	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	
information_schema.sequenzen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–	
sys.all_columns	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sys.all_objects	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.all_parameters	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–
sys.all_sql_modules	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.all_views	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.columns	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.configurations	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.data_spaces	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.database_files	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.database_mirroring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sys.database_principals	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.database_role_members	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.databases	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.dm_exec_connections	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.dm_exec_sessions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.dm_hadr_database_replica_states	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.dm_os_host_info	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sys.endpoints	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.extended_properties	✓	✓	✓	✓	–	–	✓	✓	–	–	–	–	–	–	–
sys.indexes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.schemas	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.server_principals	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.server_role_members	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
sys.sql_modules	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.sysconfigures	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.syscurconfigs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

T-SQL-Funktionalität oder -Syntax	4.1.0	4.0.0	3.5.0	3.4.0	3.3.0	3.2.0	3.1.0	2.8.0	2.7.0	2.6.0	2.5.0	2.4.0	2.3.0	2.2.0	2.1.0
sys.syslogins	✓	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–
sys.sysprocesses	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.sys-B enutzer	✓	✓	✓	✓	✓	✓	–	✓	✓	–	–	–	–	–	–
sys.table_types	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.tables	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sys.types	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–	–
sys.xml_schema_collections	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sys-Sprachen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sysobjects.crdate	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–	–

Referenz zu Verfahren für Babelfish für Aurora PostgreSQL

Übersicht

Sie können das folgende Verfahren für DB-Instances von Amazon RDS verwenden, auf denen Babelfish für Aurora PostgreSQL ausgeführt wird, um eine bessere Abfrageleistung zu erzielen:

- sp_babelfish_volatility
- sp_execute_postgresql

sp_babelfish_volatility

Die Volatilität von PostgreSQL-Funktionen hilft dem Optimierer bei der Ausführung von Abfragen. Dies hat bei Verwendung in bestimmten Klauseln erhebliche Auswirkungen auf die Abfrageleistung.

Syntax

```
sp_babelfish_volatility 'function_name', 'volatility'
```

Argumente

function_name (optional)

Sie können den Wert dieses Arguments entweder mit einem zweiteiligen Namen wie `schema_name.function_name` oder nur mit `function_name` angeben. Wenn Sie nur `function_name` angeben, ist der Schemaname das Standardschema für den aktuellen Benutzer.

volatility (optional)

Die gültigen PostgreSQL-Werte für die Volatilität sind `stable`, `volatile` oder `immutable`. Weitere Informationen finden Sie unter https://www.postgresql.org/docs/current/xfunc-volatility.html.

> **Note**
>
> Wenn `sp_babelfish_volatility` mit `function_name` aufgerufen wird und dieser mehrere Definitionen hat, wird ein Fehler ausgegeben.

Ergebnismenge

Wenn die Parameter nicht angegeben werden, wird die Ergebnismenge unter den folgenden Spalten angezeigt: `schemaname`, `functionname`, `volatility`.

Nutzungshinweise

Die Volatilität von PostgreSQL-Funktionen hilft dem Optimierer bei der Ausführung von Abfragen. Dies hat bei Verwendung in bestimmten Klauseln erhebliche Auswirkungen auf die Abfrageleistung.

Beispiele

Die folgenden Beispielen veranschaulichen das Erstellen einfacher Funktionen und die Anwendung von `sp_babelfish_volatility` auf diese Funktionen mit verschiedenen Methoden.

```
1> create function f1() returns int as begin return 0 end
2> go
```

```
1> create schema test_schema
2> go
```

```
1> create function test_schema.f1() returns int as begin return 0 end
2> go
```

Das folgende Beispiel zeigt die Volatilität der Funktionen:

```
1> exec sp_babelfish_volatility
2> go

schemaname  functionname volatility
----------- ------------ ----------
dbo         f1           volatile
test_schema f1           volatile
```

Das folgende Beispiel zeigt, wie Sie die Volatilität der Funktionen ändern können:

```
1> exec sp_babelfish_volatility 'f1','stable'
2> go
1> exec sp_babelfish_volatility 'test_schema.f1','immutable'
2> go
```

Wenn Sie nur function_name angeben, werden der Schemaname, der Funktionsname und die Volatilität dieser Funktion angezeigt. Das folgende Beispiel zeigt die Volatilität der Funktionen nach Änderung der Werte:

```
1> exec sp_babelfish_volatility 'test_schema.f1'
2> go

schemaname  functionname volatility
----------- ------------ ----------
test_schema f1           immutable
```

```
1> exec sp_babelfish_volatility 'f1'
2> go

schemaname  functionname volatility
----------- ------------ ----------
dbo         f1           stable
```

Wenn Sie kein Argument angeben, wird eine Liste der Funktionen (Schemaname, Funktionsname, Volatilität der Funktionen) angezeigt, die in der aktuellen Datenbank vorhanden sind:

```
1> exec sp_babelfish_volatility
2> go

schemaname  functionname volatility
----------- ------------ ----------
dbo         f1           stable
test_schema f1           immutable
```

sp_execute_postgresql

Sie können PostgreSQL-Anweisungen vom T-SQL-Endpunkt aus ausführen. Dies vereinfacht Ihre Anwendungen, da Sie den T-SQL-Port nicht verlassen müssen, um diese Anweisungen auszuführen.

Syntax

```
sp_execute_postgresql [ @stmt = ] statement
```

Argumente

[@stmt]-Anweisung

Das Argument hat den Datentyp „varchar“. Dieses Argument akzeptiert Anweisungen im PG-Dialekt.

> **Note**
>
> Sie können nur eine Anweisung im PG-Dialekt als Argument übergeben, andernfalls wird der folgende Fehler ausgelöst.

```
1>exec sp_execute_postgresql 'create extension pg_stat_statements; drop extension
 pg_stat_statements'
2>go
```

```
Msg 33557097, Level 16, State 1, Server BABELFISH, Line 1
expected 1 statement but got 2 statements after parsing
```

Nutzungshinweise

CREATE EXTENSION

Erstellt eine neue Erweiterung und lädt diese in die aktuelle Datenbank.

```
1>EXEC sp_execute_postgresql 'create extension [ IF NOT EXISTS ] <extension name>
 [ WITH ] [SCHEMA schema_name] [VERSION version]';
2>go
```

Im folgenden Beispiel sehen Sie, wie eine Erweiterung erstellt wird:

```
1>EXEC sp_execute_postgresql 'create extension pg_stat_statements with schema sys
 version "1.10"';
```

```
2>go
```

Verwenden Sie den folgenden Befehl für den Zugriff auf Erweiterungsobjekte:

```
1>select * from pg_stat_statements;
2>go
```

> **Note**
>
> Wenn der Schemaname bei der Erstellung der Erweiterung nicht explizit angegeben wird, werden die Erweiterungen standardmäßig im öffentlichen Schema installiert. Sie müssen den Schemaqualifizierer angeben, um auf die Erweiterungsobjekte zuzugreifen, wie unten dargestellt:

```
1>select * from [public].pg_stat_statements;
2>go
```

Unterstützte Erweiterungen

Die folgenden mit Aurora PostgreSQL verfügbaren Erweiterungen können mit Babelfish verwendet werden.

- `pg_stat_statements`
- `tds_fdw`
- `fuzzystrmatch`

Einschränkungen

- Benutzer müssen in T-SQL über die Rolle „sysadmin“ und in Postgres über die Rolle „rds_superuser“ verfügen, um die Erweiterungen installieren zu können.
- Es ist nicht möglich, Erweiterungen in vom Benutzer erstellten Schemas sowie in dbo- und Gastschemas für die Masterdatenbank, die Datenbank „tempdb“ und die Datenbank „msdb“ zu installieren.
- Die Option CASCADE wird nicht unterstützt.

ALTER EXTENSION

Mit ALTER EXTENSION können Sie eine Aktualisierung auf eine neue Erweiterungsversion vornehmen.

```
1>EXEC sp_execute_postgresql 'alter extension <extension name> UPDATE TO
 <new_version>';
2>go
```

Einschränkungen

- Sie können die Version Ihrer Erweiterung nur mit der Anweisung ALTER EXTENSION aktualisieren. Andere Operationen werden nicht unterstützt.

DROP EXTENSION

Löscht die angegebene Erweiterung. Sie können auch die Optionen `if exists` oder `restrict` verwenden, um die Erweiterung zu löschen.

```
1>EXEC sp_execute_postgresql 'drop extension <extension name>';
2>go
```

Einschränkungen

- Die Option CASCADE wird nicht unterstützt.

Verwalten von Amazon Aurora PostgreSQL

Im folgenden Abschnitt werden die Verwaltung der Performance und Skalierung für einen Amazon-Aurora-PostgreSQL-DB-Cluster erläutert. Es umfasst auch Informationen über andere Wartungsaufgaben.

Themen

- Anzeigen des Volume-Status für einen Aurora PostgreSQL-DB-Cluster
- RAM-Datenträger für das stats_temp_directory
- Verwalten temporärer Dateien mit PostgreSQL

Skalierung von Aurora PostgreSQL-DB-Instances

Sie können Aurora PostgreSQL-DB-Instances auf zwei Arten skalieren, durch Skalierung der Instance oder durch Skalierung der Lesevorgänge. Weitere Informationen zur Lese-Skalierung finden Sie unter Skalierung von Lesevorgängen.

Sie können Ihr Aurora-PostgreSQL-DB-Cluster skalieren, indem Sie die DB-Instance-Klasse für jede DB-Instance im DB-Cluster ändern. Aurora PostgreSQL unterstützt mehrere DB-Instance-Klassen, die für Aurora optimiert sind. Verwenden Sie nicht die Instance-Klasse db.t2 oder db.t3 für größere Aurora-Cluster mit einer Größe von mehr als 40 Terabyte (TB).

> **Note**
>
> Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs- und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Einzelheiten zu den T-Instance-Klassen finden Sie unter DB-Instance-Klassenarten.

Die Skalierung erfolgt nicht augenblicklich. Es kann 15 Minuten oder länger dauern, bis die Änderung zu einer anderen DB-Instance-Klasse abgeschlossen ist. Wenn Sie diesen Ansatz zum Ändern der DB-Instance-Klasse verwenden, sollten Sie die Änderung während des nächsten geplanten Wartungsfensters (und nicht sofort) anwenden, um Auswirkungen auf die Benutzer zu vermeiden.

Alternativ zur direkten Änderung der DB-Instance-Klasse können Sie Ausfallzeiten minimieren, indem Sie die Hochverfügbarkeitsfunktionen von Amazon Aurora verwenden. Fügen Sie Ihrem Cluster zuerst ein Aurora-Replikat hinzu. Wählen Sie beim Erstellen des Replikats die DB-Instance-Klassengröße, die Sie für Ihren Cluster verwenden möchten. Wenn das Aurora Replica mit dem Cluster synchronisiert wird, können Sie das neu hinzugefügte Replikat ausfallen. Weitere Informationen hierzu finden Sie unter Aurora-Replikate und Schnelles Failover mit Amazon Aurora PostgreSQL.

Detaillierte Angaben zu den von Aurora PostgreSQL unterstützten DB-Instance-Klassen finden Sie unter Unterstützte DB-Engines für DB-Instance-Klassen.

Maximale Verbindungen zu einer Aurora PostgreSQL-DB-Instance

Ein Aurora-PostgreSQL-DB-Cluster weist Ressourcen basierend auf der DB-Instance-Klasse und ihrem verfügbaren Speicher zu. Jede Verbindung mit dem DB-Cluster verbraucht inkrementelle Mengen dieser Ressourcen wie Speicher und CPU. Der pro Verbindung verbrauchte Speicher variiert je nach Abfragetyp, Anzahl und der Tatsache, ob temporäre Tabellen verwendet werden. Selbst eine inaktive Verbindung verbraucht Speicher und CPU. Das liegt daran, dass bei Abfragen für eine Verbindung mehr Speicher für jede Abfrage zugewiesen wird und der Speicher nicht vollständig freigegeben wird, auch wenn die Verarbeitung beendet wird. Daher empfehlen wir Ihnen, sicherzustellen, dass Ihre Anwendungen keine inaktiven Verbindungen aufrechterhalten: Jede dieser Verbindungen verschwendet Ressourcen und wirkt sich negativ auf die Leistung aus. Weitere Informationen finden Sie unter Ressourcen, die von inaktiven PostgreSQL-Verbindungen verbraucht werden.

Die maximale Anzahl der zulässigen Verbindungen einer Aurora-PostgreSQL-DB-Instance wird durch den Wert des Parameters `max_connections` in der Parametergruppe für diese DB-Instance festgelegt. Die ideale Einstellung für den `max_connections` Parameter ist eine, die alle Client-Verbindungen unterstützt, die Ihre Anwendung benötigt, ohne zu viele ungenutzte Verbindungen, plus mindestens 3 weitere Verbindungen zur Unterstützung der AWS Automatisierung. Vor dem Ändern des Parameters `max_connections` sollten Sie Folgendes berücksichtigen:

- Wenn der Wert von `max_connections` zu niedrig ist, verfügt die Aurora-PostgreSQL-DB-Instance möglicherweise nicht über ausreichende Verbindungen, wenn Clients versuchen, eine Verbindung herzustellen. In diesem Fall werden durch Verbindungsversuche mit `psql` Fehlermeldungen wie die folgenden ausgelöst:

  ```
  psql: FATAL: remaining connection slots are reserved for non-replication superuser
   connections
  ```

- Wenn der Wert von `max_connections` die Anzahl der benötigten Verbindungen übersteigt, können die nicht verwendeten Verbindungen die Leistung beeinträchtigen.

Der Standardwert von `max_connections` wird von der folgenden Aurora-PostgreSQL–FunktionLEAST abgeleitet:

`LEAST({DBInstanceClassMemory/9531392},5000)`.

Wenn Sie den Wert für `max_connections` ändern möchten, müssen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe erstellen und dort ihren Wert ändern. Wenn Sie Ihre benutzerdefinierte

DB-Parametergruppe auf Ihren Cluster angewendet haben, müssen Sie die primäre Instance neu starten, damit der neue Wert wirksam wird. Weitere Informationen finden Sie unter Amazon-Aurora-PostgreSQL-Parameter und Erstellen einer DB-Cluster-Parametergruppe.

> **Tip**
>
> Wenn Ihre Anwendungen häufig Verbindungen öffnen und schließen oder langlebige Verbindungen in großer Zahl offen lassen, empfehlen wir Ihnen, Amazon-RDS-Proxy zu verwenden. RDS-Proxy ist ein vollständig verwalteter, hochverfügbarer Datenbank-Proxy, der Datenbankverbindungen sicher und effizient per Verbindungspooling freigibt. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

Weitere Informationen dazu, wie Aurora Serverless v2-Instances diesen Parameter behandeln, finden Sie unter Maximale Anzahl der Verbindungen für Aurora Serverless v2.

Temporäre Speicherlimits für Aurora PostgreSQL

Aurora PostgreSQL speichert Tabellen und Indizes im Aurora-Speichersubsystem. Aurora PostgreSQL verwendet separaten temporären Speicher für nicht persistente temporäre Dateien. Dazu gehören Dateien, die für Zwecke wie das Sortieren großer Datensätze während der Abfrageverarbeitung oder für Indexerstellungsvorgänge verwendet werden. Weitere Informationen finden Sie im Artikel Wie kann ich lokale Speicherprobleme in Aurora-PostgreSQL-kompatiblen Instances beheben?.

Diese lokalen Speicher-Volumes werden von Amazon Elastic Block Store gestützt und können durch Einsatz einer größeren DB-Instance-Klasse erweitert werden. Weitere Informationen über Speicher finden Sie unter Amazon Aurora-Speicher und -Zuverlässigkeit. Sie können Ihren lokalen Speicher für temporäre Objekte auch vergrößern, indem Sie einen NVMe-fähigen Instance-Typ und Aurora Optimized Reads-fähige temporäre Objekte verwenden. Weitere Informationen finden Sie unter Verbesserung der Abfrageleistung für Aurora PostgreSQL mit Aurora-optimierten Lesevorgängen.

> **Note**
>
> Beim Skalieren von DB-Instances, z. B. von db.r5.2xlarge auf db.r5.4xlarge, treten unter Umständen `storage-optimization`-Ereignisse auf.

Die folgende Tabelle zeigt die maximale Menge an temporärem Speicher, die für jede Aurora PostgreSQL-DB-Instance-Klasse verfügbar ist. Informationen zur Unterstützung der DB-Instance-Klasse für Aurora finden Sie unter Aurora DB-Instance-Klassen.

DB-Instance-Klasse	Maximal verfügbarer temporärer Speicher (GiB)
db.x2g.16xlarge	1829
db.x2g.12xlarge	1606
db.x2g.8xlarge	1071
db.x2g.4xlarge	535
db.x2g.2xlarge	268
db.x2g.xlarge	134
db.x2g.large	67
db.r7g.16xlarge	1008
db.r7g.12xlarge	756
db.r7g.8xlarge	504
db.r7g.4xlarge	252
db.r7g.2xlarge	126
db.r7g.xlarge	63
db.r7g.large	32
db.r6g.16xlarge	1008
db.r6g.12xlarge	756
db.r6g.8xlarge	504
db.r6g.4xlarge	252

DB-Instance-Klasse	Maximal verfügbarer temporärer Speicher (GiB)
db.r6g.2xlarge	126
db.r6g.xlarge	63
db.r6g.large	32
db.r6i.32xlarge	1829
db.r6i.24xlarge	1500
db.r6i.16xlarge	1008
db.r6i.12xlarge	748
db.r6i.8xlarge	504
db.r6i.4xlarge	249
db.r6i.2xlarge	124
db.r6i.xlarge	62
db.r6i.large	31
db.r5.24xlarge	1500
db.r5.16xlarge	1008
db.r5.12xlarge	748
db.r5.8xlarge	504
db.r5.4xlarge	249
db.r5.2xlarge	124
db.r5.xlarge	62
db.r5.large	31

DB-Instance-Klasse	Maximal verfügbarer temporärer Speicher (GiB)
db.r4.16xlarge	960
db.r4.8xlarge	480
db.r4.4xlarge	240
db.r4.2xlarge	120
db.r4.xlarge	60
db.r4.large	30
db.t4g.large	16,5
db.t4g.medium	8,13
db.t3.large	16
db.t3.medium	7,5

> **Note**
>
> NVMe-fähige Instanztypen können den verfügbaren temporären Speicherplatz um bis zur gesamten NVMe-Größe erhöhen. Weitere Informationen finden Sie unter Verbesserung der Abfrageleistung für Aurora PostgreSQL mit Aurora-optimierten Lesevorgängen.

Sie können den für eine DB-Instance verfügbaren temporären Speicher mit der `FreeLocalStorage` CloudWatch Metrik --> überwachen, die unter beschrieben ist. CloudWatch Amazon-Metriken für Amazon Aurora (Dies gilt nicht für Aurora Serverless v2.)

Bei einigen Workloads können Sie die Menge an temporärem Speicher reduzieren, indem Sie den Prozessen, die die Operation ausführen, mehr Arbeitsspeicher zuweisen. Um den für einen Vorgang verfügbaren Speicher zu erhöhen, erhöhen Sie die PostgreSQL-Werte der Parameter work_mem oder maintenance_work_mem.

Huge Pages für PostgreSQL

Huge Pages ist eine Arbeitsspeicher-Verwaltungsfunktion, die den Overhead reduziert, wenn eine DB-Instance mit großen, zusammenhängenden Arbeitsspeicherblöcken arbeitet, wie sie von gemeinsam genutzten Puffern verwendet werden. Diese PostgreSQL-Funktion wird von allen derzeit verfügbaren Versionen von Aurora PostgreSQL unterstützt.

Der Parameter `Huge_pages` ist standardmäßig für alle DB-Instance-Klassen aktiviert, außer t3.medium, db.t3.large, db.t4g.medium, db.t4g.large. In den unterstützten Instance-Klassen von Aurora PostgreSQL können Sie den Parameterwert `huge_pages` nicht ändern oder diese Funktion deaktivieren.

Testen von Amazon Aurora PostgreSQL unter Verwendung von Fehlersimulationsabfragen

Sie können die Fehlertoleranz Ihres Aurora PostgreSQL-DB-Clusters testen, indem Sie Fehlersimulationsabfragen verwenden. Fehlersimulationsabfragen werden als SQL-Befehle an eine Amazon Aurora-Instance ausgegeben. Mit Fehlersimulationsabfragen können Sie die Instance zum Absturz bringen, sodass Sie Failover und Wiederherstellung testen können. Sie können auch Aurora Replica-Ausfall, Festplattenausfall und Datenträgerüberlastung simulieren. Fehlersimulationsabfragen werden von allen verfügbaren Aurora-PostgreSQL-Versionen wie folgt unterstützt.

- Aurora PostgreSQL 12, 13, 14 und höhere Versionen
- Aurora PostgreSQL 11.7 und höhere Versionen
- Aurora PostgreSQL 10.11 und höhere Versionen

Themen

Wenn eine Fehlersimulationsabfrage einen Absturz angibt, erzwingt sie einen Absturz der Aurora PostgreSQL-DB-Instance. Die anderen Fehler-Injection-Abfragen erzeugen Simulationen von Ausfallereignissen, lösen aber keine Ereignisse aus. Wenn Sie eine Fehlersimulationsabfrage senden, geben Sie auch einen Zeitraum vor, in dem die Fehlerereignissimulation ablaufen soll.

Sie können eine Fehlersimulationsabfrage an eine Ihrer Aurora Replica-Instances senden, indem Sie eine Verbindung mit dem Endpunkt der Aurora Replica herstellen. Weitere Informationen finden Sie unter Amazon Aurora-Verbindungsverwaltung.

Testen eines Instance-Ausfalls

Sie können den Absturz einer Aurora PostgreSQL-Instance erzwingen, indem Sie die Fehlersimulationsabfrage-Funktion verwende `aurora_inject_crash()`.

Für diese Fehlersimulationsabfrage tritt kein Failover auf. Wenn Sie ein Failover testen möchten, können Sie die Aktion Failover-Instance für Ihren DB-Cluster in der RDS-Konsole auswählen oder den failover-db-cluster AWS CLI Befehl oder die RDS-API-Operation FailoverDBCluster verwenden.

Syntax

```
SELECT aurora_inject_crash ('instance' | 'dispatcher' | 'node');
```

Optionen

Diese Fehlersimulationsabfrage löst einen der folgenden Ausfalltypen aus. Bei der Absturzart wird die Groß-/Kleinschreibung nicht berücksichtigt:

'instance'

Es wird ein Absturz der PostgreSQL-kompatiblen Datenbank für die Amazon Aurora-Instance simuliert.

'Disponent'

Es wird ein Absturz des Dispatchers auf primären Instance für das Aurora-DB-Cluster simuliert. Der Dispatcher schreibt Updates zum Cluster-Volume für ein Amazon Aurora-DB-Cluster.

'Knoten'

Es wird ein Absturz sowohl der PostgreSQL-kompatiblen Datenbank als auch des Dispatchers für die Amazon Aurora-Instance simuliert.

Testen eines Aurora-Replikatausfalls

Sie können den Ausfall eines Aurora-Replikats mittels der Fehlersimulationsabfrage-Funktion simuliere `aurora_inject_replica_failure()`.

EinAurora Replikatfehler blockiert die Replikation auf dasAurora Replikat oder alle Aurora-Replikate im DB-Cluster um den angegebenen Prozentsatz für das angegebene Zeitintervall. Wenn das Zeitintervall abgeschlossen ist, sind die betroffenen Aurora-Replikate automatisch mit der primären Instance synchronisiert.

Syntax

```
SELECT aurora_inject_replica_failure(
   percentage_of_failure,
   time_interval,
   'replica_name'
);
```

Optionen

Diese Fehlersimulationsabfrage verwendet die folgenden Parameter:

prozent_an_ausfällen

Der Prozentsatz der Replikate, die während des Ausfallereignisses blockiert werden sollen. Dieser Wert kann ein Duplikat zwischen 0 und 100 sein. Wenn Sie 0 angeben, wird keine Replikation blockiert. Wenn Sie 100 angeben, wird die gesamte Replikation blockiert.

time_intervall

Die Zeitspanne für die Simulation des Ausfalls des Aurora-Replikats. Das Intervall ist in Sekunden. Wenn der Wert beispielsweise 20 ist, wird die Simulation 20 Sekunden lang ausgeführt.

> **Note**
>
> Seien Sie vorsichtig bei der Angabe des Zeitintervalls für das Ausfallereignis in Ihrem Aurora-Replikat. Wenn Sie ein zu langes Intervall festlegen und Ihre Writer-Instance eine große Datenmenge während des Ausfallereignisses schreibt, könnte Ihr Aurora-DB-Cluster annehmen, dass Ihr Aurora-Replikat ausgefallen ist, und es ersetzen.

replica_name

Das Aurora-Replikat, in das die Ausfallsimulation injiziert werden soll. Geben Sie den Namen eines Aurora-Replikats an, um einen Ausfall des einzelnen Aurora-Replikats zu simulieren. Geben Sie eine leere Zeichenfolge an, um Ausfälle für alle Aurora-Replikate im DB-Cluster zu simulieren.

Informationen zur Identifizierung von Replikatnamen finden Sie in der Spalte `server_id` der Funktion `aurora_replica_status()`. Zum Beispiel:

```
postgres=> SELECT server_id FROM aurora_replica_status();
```

Testen eines Festplattenausfalls

Sie können einen Festplattenausfall für einen Aurora PostgreSQL-DB-Cluster mittels der Fehlersimulationsabfrage-Funktion simuliere `aurora_inject_disk_failure()`.

Während einer Simulation eines Festplattenausfalls markiert der Aurora PostgreSQL-DB-Cluster zufällige Festplattensegmente als fehlerhaft. Anfragen an diese Segmente werden für die Dauer der Simulation blockiert.

Syntax

```
SELECT aurora_inject_disk_failure(
   percentage_of_failure,
   index,
   is_disk,
   time_interval
);
```

Optionen

Diese Fehlersimulationsabfrage verwendet die folgenden Parameter:

prozent_an_ausfällen

Der Prozentsatz des Datenträgers, der während des Ausfallereignisses als ausgefallen markiert werden soll. Dieser Wert kann ein Duplikat zwischen 0 und 100 sein. Wenn Sie 0 festlegen, wird kein Segment der Festplatte als fehlerhaft markiert. Wenn Sie 100 festlegen, wird die gesamte Festplatte als fehlerhaft markiert.

index

Ein spezifischer logischer Datenblock, in dem das Ausfallereignis simuliert werden soll. Wenn Sie den Bereich der verfügbaren logischen Blöcke oder Speichernodedaten überschreiten, erhalten Sie eine Fehlermeldung, in der Ihnen der maximal festlegbare Indexwert angezeigt wird. Informationen zur Vermeidung dieses Fehlers finden Sie unter Anzeigen des Volume-Status für einen Aurora PostgreSQL-DB-Cluster.

ist_festplatte

Gibt an, ob der Injektionsfehler auf einen logischen Block oder einen Speicherknoten zurückzuführen ist. Die Angabe von „true“ bedeutet, dass Injektionsfehler auf einen logischen Block zurückzuführen sind. Die Angabe von „false“ bedeutet, dass Injektionsfehler auf einen Speicherknoten zurückzuführen sind.

time_intervall

Die Zeit, die zum Simulieren des Festplattenausfalls benötigt wird. Das Intervall ist in Sekunden. Wenn der Wert beispielsweise 20 ist, wird die Simulation 20 Sekunden lang ausgeführt.

Testen einer Festplattenüberlastung

Sie können eine Festplattenüberlastung für einen Aurora-PostgreSQL-DB-Cluster simulieren, indem Sie die Fehlersimulationsabfragefunktion verwenden`aurora_inject_disk_congestion()`.

Während einer Simulation einer Festplattenüberlastung markiert der Aurora PostgreSQL-DB-Cluster zufällige Festplattensegmente als überlastet. Anfragen an diese Segmente werden für die Dauer der angegebenen minimalen und maximalen Verzögerungszeit während der Simulation verzögert.

Syntax

```
SELECT aurora_inject_disk_congestion(
   percentage_of_failure,
   index,
   is_disk,
   time_interval,
   minimum,
   maximum
);
```

Optionen

Diese Fehlersimulationsabfrage verwendet die folgenden Parameter:

prozent_an_ausfällen

Der Prozentsatz des Datenträgers, der während des Ausfallereignisses als überlastet markiert werden soll. Dies ist ein doppelter Wert zwischen 0 und 100. Wenn Sie 0 festlegen, wird kein

Segment der Festplatte als überlastet markiert. Wenn Sie 100 festlegen, wird die gesamte Festplatte als überlastet markiert.

index

Ein spezifischer logischer Datenblock oder Speicherknoten, der zum Simulieren des Ausfallereignisses verwendet werden soll.

Wenn Sie den Bereich der verfügbaren logischen Datenblöcke oder Speichernodes überschreiten, erhalten Sie eine Fehlermeldung, die Ihnen den maximalen Indexwert angibt, den Sie angeben können. Informationen zur Vermeidung dieses Fehlers finden Sie unter Anzeigen des Volume-Status für einen Aurora PostgreSQL-DB-Cluster.

ist_festplatte

Gibt an, ob der Injektionsfehler auf einen logischen Block oder einen Speicherknoten zurückzuführen ist. Die Angabe von „true“ bedeutet, dass Injektionsfehler auf einen logischen Block zurückzuführen sind. Die Angabe von „false“ bedeutet, dass Injektionsfehler auf einen Speicherknoten zurückzuführen sind.

time_intervall

Die Zeit, die für die Simulation der Festplattenüberlastung benötigt wird. Das Intervall ist in Sekunden. Wenn der Wert beispielsweise 20 ist, wird die Simulation 20 Sekunden lang ausgeführt.

Minimum, Maximum

Der Mindest- und Höchstwert in Millisekunden für die Überlastungsverzögerung. Gültige Werte reichen von 0,0 bis 100,0 Millisekunden. Festplattensegmente, die als überlastet gekennzeichnet sind, werden für die Dauer der Simulation um eine zufällige Zeit innerhalb des minimalen und maximalen Bereichs verzögert. Der Höchstwert muss größer als der Mindestwert sein.

Anzeigen des Volume-Status für einen Aurora PostgreSQL-DB-Cluster

In Amazon Aurora besteht ein DB-Cluster-Volume aus einer Sammlung von logischen Blöcken. Jeder von ihnen stellt 10 Gigabyte des zugeteilten Arbeitsspeichers bereit. Diese Blöcke werden als Schutzgruppen bezeichnet.

Die Daten in den einzelnen Schutzgruppen werden über sechs physische Speichereinheiten, so genannte Speicherknoten, repliziert. Diese Speicherknoten werden in drei Availability Zones (AZs) in der Region zugeteilt, in der sich das DB-Cluster befindet. Jeder Speicherknoten wiederum besteht

aus einem oder mehreren logischen Datenblöcken für das DB-Cluster-Volume. Weitere Informationen zu Schutzgruppen und Speicherknoten finden Sie unter Introducing the Aurora Storage Engine im AWS Database Blog. Weitere Informationen über Aurora-Cluster-Volumes im Allgemeinen finden Sie unter Amazon Aurora-Speicher und -Zuverlässigkeit.

Verwenden Sie die Funktion `aurora_show_volume_status()`, um die folgenden Serverstatusvariablen zurückzugeben:

- `Disks` – Die Gesamtanzahl der logischen Datenblöcke für das DB-Cluster-Volume.
- `Nodes` — Die Gesamtanzahl der Speicherknoten für das DB-Cluster-Volume.

Sie können die Funktion `aurora_show_volume_status()` verwenden, um einen Fehler zu vermeiden, wenn Sie die Fehlersimulationsfunktion `aurora_inject_disk_failure()` verwenden. Die Fehlersimulationsfunktion `aurora_inject_disk_failure()` simuliert den Ausfall eines gesamten Speicherknotens oder eines einzelnen logischen Datenblocks innerhalb eines Speicherknotens. In der Funktion geben Sie den Indexwert eines spezifischen logischen Datenblocks oder Speicherknotens an. Die Anweisung gibt jedoch einen Fehler zurück, wenn Sie einen Indexwert angeben, der größer ist als die Anzahl der logischen Datenblöcke oder Speicherknoten, die vom DB-Cluster-Volume verwendet werden. Weitere Informationen über Fehlersimulationsabfragen finden Sie unter Testen von Amazon Aurora PostgreSQL unter Verwendung von Fehlersimulationsabfragen.

> **Note**
>
> Die Funktion `aurora_show_volume_status()` steht für Aurora PostgreSQL-Version 10.11 zur Verfügung. Weitere Informationen zu den Aurora PostgreSQL-Versionen erhalten Sie unter Amazon Aurora PostgreSQL Releases und Engine Versionen.

Syntax

```
SELECT * FROM aurora_show_volume_status();
```

Beispiel

```
customer_database=> SELECT * FROM aurora_show_volume_status();
 disks | nodes
-------+-------
    96 |    45
```

RAM-Datenträger für das stats_temp_directory

Sie können den Aurora-PostgreSQL-Parameter `rds.pg_stat_ramdisk_size` verwenden, um den Systemspeicher anzugeben, der einer RAM-Disk für die Speicherung von PostgreSQL `stats_temp_directory`. Der RAM-Disk-Parameter ist für alle Aurora-PostgreSQL-14-Versionen und niedriger verfügbar.

Bei bestimmten Workloads kann durch die Einstellung dieses Parameters die Leistung verbessert und die I/O-Anforderungen können gesenkt werden. Weitere Informationen über `stats_temp_directory` finden Sie unter Laufzeitstatistik in der PostgreSQL-Dokumentation. Ab PostgreSQL Version 15 hat die PostgreSQL-Community auf die Verwendung von dynamischem gemeinsam genutztem Speicher Memory umgestellt. Eine Einstellung von `stats_temp_directory` ist also nicht erforderlich.

Um einen RAM-Datenträger für Ihr `stats_temp_directory` zu aktivieren, legen Sie den Parameter `rds.pg_stat_ramdisk_size` in der von Ihrer DB-Cluster verwendeten Parametergruppe auf einen Wert ungleich Null fest. Dieser Parameter wird in MB angegeben, daher müssen Sie einen ganzzahligen Wert verwenden. Ausdrücke, Formeln und Funktionen sind für den Parameter `rds.pg_stat_ramdisk_size` nicht gültig. Stellen Sie sicher, dass Sie den DB-Cluster neu starten, damit die Änderungen wirksam werden. Weitere Informationen zum Festlegen von Parametern finden Sie unter Arbeiten mit Parametergruppen. Weitere Informationen zum Neustart einer Verbindung mit dem DB-Cluster finden Sie unter Neustart eines Amazon Aurora DB-Clusters oder einer Amazon Aurora DB-Instance.

Mit dem folgenden AWS CLI-Befehl wird beispielsweise der RAM-Datenträgerparameter auf 256 MB festgelegt.

```
aws rds modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name db-cl-pg-ramdisk-testing \
    --parameters "ParameterName=rds.pg_stat_ramdisk_size, ParameterValue=256,
 ApplyMethod=pending-reboot"
```

Nachdem Sie den DB-Cluster neu gestartet haben, führen Sie den folgenden Befehl aus, um den Status des 1:`stats_temp_directory`

```
postgres=> SHOW stats_temp_directory;
```

Der Befehl sollte Folgendes zurückgeben:

```
stats_temp_directory
---------------------------
/rdsdbramdisk/pg_stat_tmp
(1 row)
```

Verwalten temporärer Dateien mit PostgreSQL

In PostgreSQL verwendet eine Abfrage, die Sortier- und Hash-Operationen ausführt, den Instance-Speicher, um Ergebnisse bis zu dem im Parameter `work_mem` angegebenen Wert zu speichern. Wenn der Instance-Speicher nicht ausreicht, werden temporäre Dateien erstellt, um die Ergebnisse zu speichern. Diese werden auf die Festplatte geschrieben, um die Abfrageausführung abzuschließen. Später werden diese Dateien automatisch entfernt, nachdem die Abfrage abgeschlossen ist. In In Aurora PostgreSQL teilen sich diese Dateien den lokalen Speicher mit anderen Protokolldateien. Sie können den lokalen Speicherplatz Ihres DB-Clusters von Aurora PostgreSQL überwachen, indem Sie sich die Amazon-CloudWatch-Metrik für `FreeLocalStorage` ansehen. Weitere Informationen finden Sie unter Behebung lokaler Speicherprobleme.

Sie können die folgenden Parameter und Funktionen verwenden, um die temporären Dateien in Ihrer Instance zu verwalten.

- **`temp_file_limit`** – Dieser Parameter bricht jede Abfrage ab, die die Größe von temp_files in KB überschreitet. Dieses Limit verhindert, dass Abfragen endlos ausgeführt werden und Speicherplatz mit temporären Dateien belegen. Sie können den Wert anhand der Ergebnisse des Parameters `log_temp_files` schätzen. Es hat sich bewährt, das Workload-Verhalten zu untersuchen und das Limit der Schätzung entsprechend festzulegen. Das folgende Beispiel zeigt, wie eine Abfrage abgebrochen wird, wenn sie das Limit überschreitet.

  ```
  postgres=> select * from pgbench_accounts, pg_class, big_table;
  ```

  ```
  ERROR: temporary file size exceeds temp_file_limit (64kB)
  ```

- **`log_temp_files`** – Dieser Parameter sendet Nachrichten an die Datei postgresql.log, wenn die temporären Dateien einer Sitzung entfernt werden. Dieser Parameter erstellt Protokolle, nachdem eine Abfrage erfolgreich abgeschlossen wurde. Daher ist er bei der Fehlerbehebung aktiver, lang andauernder Abfragen möglicherweise nicht hilfreich.

Das folgende Beispiel zeigt, dass nach erfolgreichem Abschluss der Abfrage die Einträge in der Datei postgresql.log protokolliert werden, während die temporären Dateien bereinigt werden.

```
2023-02-06 23:48:35 UTC:205.251.233.182(12456):adminuser@postgres:[31236]:LOG:
 temporary file: path "base/pgsql_tmp/pgsql_tmp31236.5", size 140353536
2023-02-06 23:48:35 UTC:205.251.233.182(12456):adminuser@postgres:[31236]:STATEMENT:
  select a.aid from pgbench_accounts a, pgbench_accounts b where a.bid=b.bid order by
 a.bid limit 10;
2023-02-06 23:48:35 UTC:205.251.233.182(12456):adminuser@postgres:[31236]:LOG:
 temporary file: path "base/pgsql_tmp/pgsql_tmp31236.4", size 180428800
2023-02-06 23:48:35 UTC:205.251.233.182(12456):adminuser@postgres:[31236]:STATEMENT:
  select a.aid from pgbench_accounts a, pgbench_accounts b where a.bid=b.bid order by
 a.bid limit 10;
```

- **pg_ls_tmpdir** – Diese Funktion, die von RDS für PostgreSQL 13 und höher verfügbar ist, bietet Einblick in die aktuelle Nutzung temporärer Dateien. Die abgeschlossene Abfrage erscheint nicht in den Ergebnissen der Funktion. Im folgenden Beispiel können Sie sich die Ergebnisse dieser Funktion ansehen.

```
postgres=> select * from pg_ls_tmpdir();
```

```
      name       |    size    |      modification
-----------------+------------+------------------------
 pgsql_tmp8355.1 | 1072250880 | 2023-02-06 22:54:56+00
 pgsql_tmp8351.0 | 1072250880 | 2023-02-06 22:54:43+00
 pgsql_tmp8327.0 | 1072250880 | 2023-02-06 22:54:56+00
 pgsql_tmp8351.1 |  703168512 | 2023-02-06 22:54:56+00
 pgsql_tmp8355.0 | 1072250880 | 2023-02-06 22:54:00+00
 pgsql_tmp8328.1 |  835031040 | 2023-02-06 22:54:56+00
 pgsql_tmp8328.0 | 1072250880 | 2023-02-06 22:54:40+00
(7 rows)
```

```
postgres=> select query from pg_stat_activity where pid = 8355;

query
```

```
-------------------------------------------------------------------------------------------
select a.aid from pgbench_accounts a, pgbench_accounts b where a.bid=b.bid order by
 a.bid
(1 row)
```

Der Dateiname enthält die Verarbeitungs-ID (PID) der Sitzung, die die temporäre Datei generiert hat. Eine komplexere Abfrage, wie im folgenden Beispiel, führt eine Summenberechnung der temporären Dateien für jede PID durch.

```
postgres=> select replace(left(name, strpos(name, '.')-1),'pgsql_tmp','') as pid,
 count(*), sum(size) from pg_ls_tmpdir() group by pid;
```

```
 pid  | count |   sum
------+-------+------------------
 8355 |     2 | 2144501760
 8351 |     2 | 2090770432
 8327 |     1 | 1072250880
 8328 |     2 | 2144501760
(4 rows)
```

- **pg_stat_statements** – Wenn Sie den Parameter pg_stat_statements aktivieren, können Sie die durchschnittliche Nutzung temporärer Dateien pro Aufruf einsehen. Sie können die query_id der Abfrage identifizieren und verwenden, um die Nutzung temporärer Dateien zu untersuchen, wie im folgenden Beispiel gezeigt.

```
postgres=> select queryid from pg_stat_statements where query like 'select a.aid from
 pgbench%';
```

```
       queryid
----------------------
 -7170349228837045701
(1 row)
```

```
postgres=> select queryid, substr(query,1,25), calls, temp_blks_read/calls
 temp_blks_read_per_call, temp_blks_written/calls temp_blks_written_per_call from
 pg_stat_statements where queryid = -7170349228837045701;
```

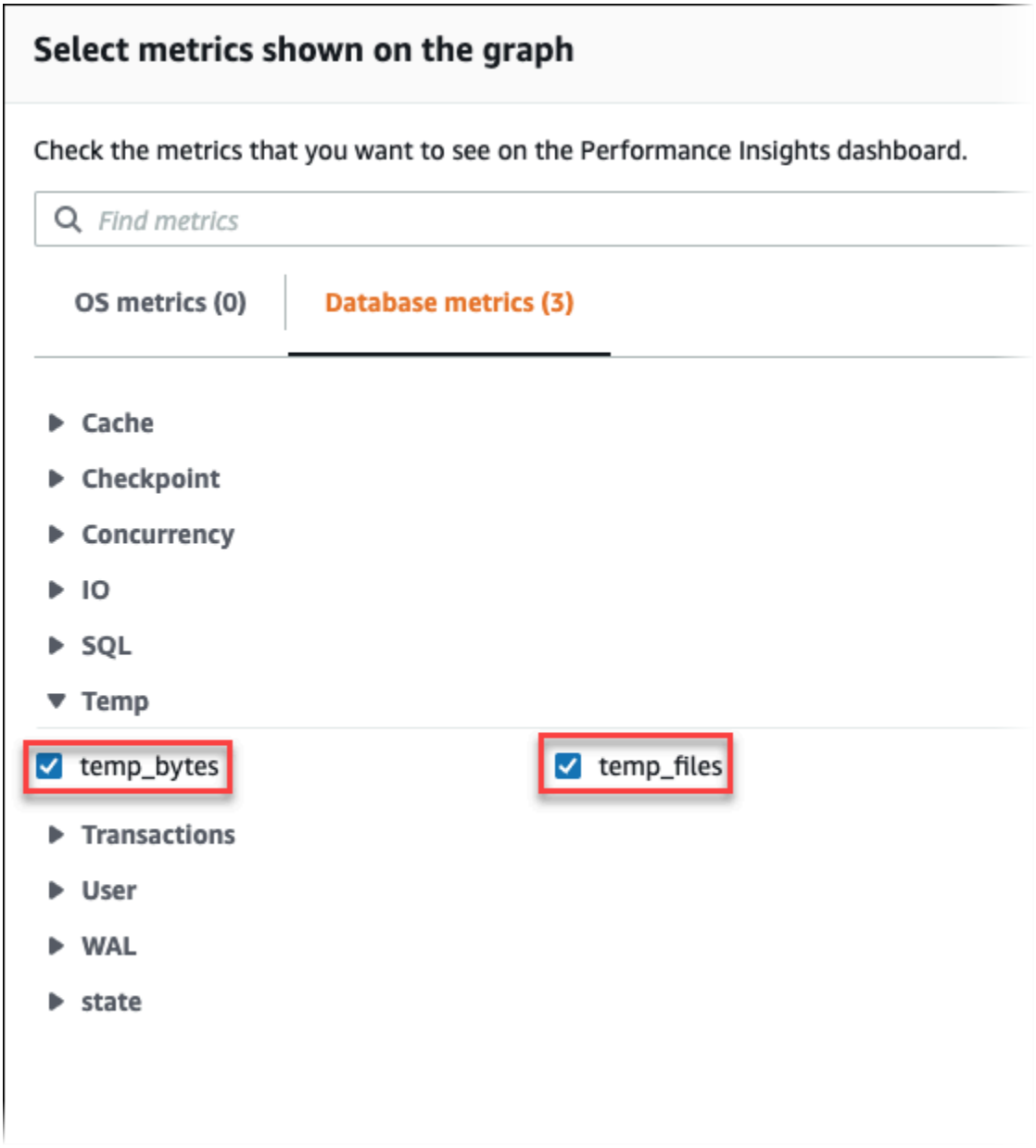
```
       queryid        |          substr           | calls | temp_blks_read_per_call |
 temp_blks_written_per_call
----------------------+---------------------------+-------+-------------------------
+---------------------------
 -7170349228837045701 | select a.aid from pgbench |    50 |                  239226 |
                     388678
(1 row)
```

- **Performance Insights** – Im Performance-Insights-Dashboard können Sie die Nutzung temporärer Dateien einsehen, indem Sie die Metriken temp_bytes und temp_files aktivieren. Anschließend können Sie den Durchschnitt dieser beiden Metriken sehen und feststellen, wie sie dem Abfrage-Workload entsprechen. In der Ansicht in Performance Insights werden nicht speziell die Abfragen angezeigt, die die temporären Dateien generieren. Wenn Sie jedoch Performance Insights mit der für `pg_ls_tmpdir` angezeigten Abfrage kombinieren, können Sie Fehler in Ihrem Abfrage-Workload beheben, analysieren und die Änderungen ermitteln.

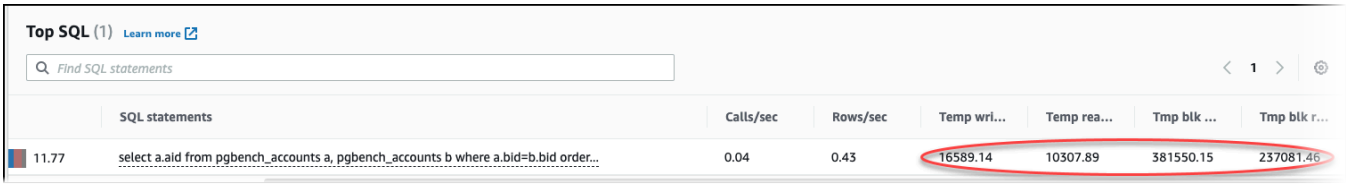
  Weitere Informationen zur Analyse von Metriken und Abfragen mit Performance Insights finden Sie unter Analyse der Metriken mit dem Performance Insights-Dashboard.

  So zeigen Sie die Nutzung temporärer Dateien mit Performance Insights an

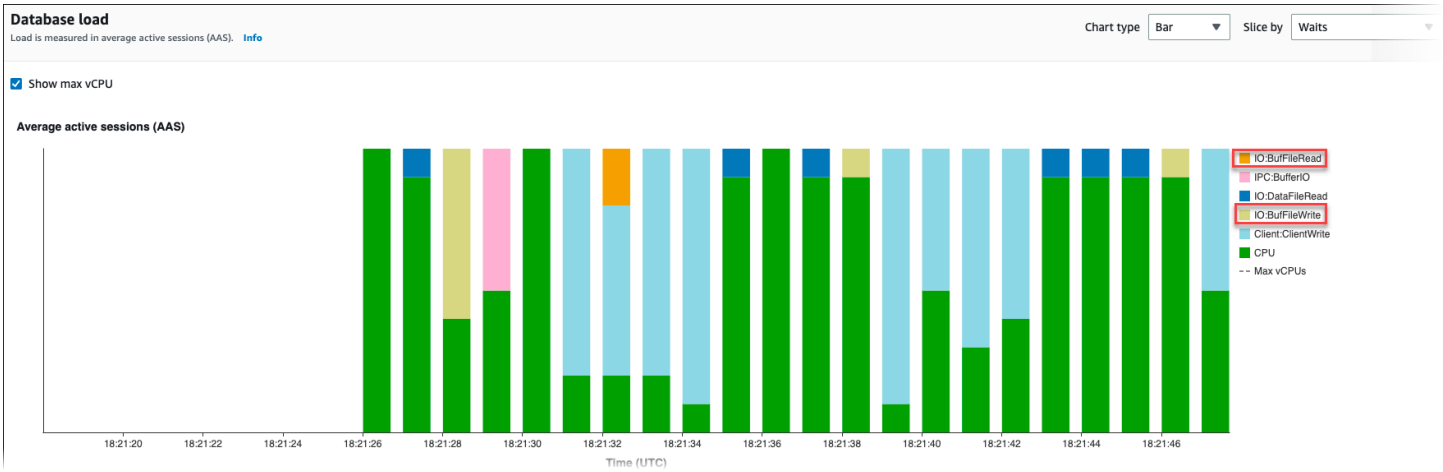
  1. Wählen Sie im Performance-Insights-Dashboard Metriken verwalten aus.
  2. Wählen Sie Datenbankmetriken und die Metriken temp_bytes und temp_files aus, wie im folgenden Screenshot gezeigt.



3. Wählen Sie auf der Registerkarte Top SQL das Symbol Einstellungen aus.
4. Schalten Sie im Fenster Einstellungen die folgenden Statistiken ein, damit sie auf der Registerkarte Top SQL angezeigt werden, und wählen Sie Weiter aus.
   - Temporäre Schreibvorgänge pro Sekunde
   - Temporäre Lesevorgänge pro Sekunde
   - Temporäre Massenschreibvorgänge/Aufruf
   - Temporäre Massenlesevorgänge/Aufruf
5. Die temporäre Datei wird aufgegliedert, wenn sie mit der für `pg_ls_tmpdir` gezeigten Abfrage kombiniert wird, wie im folgenden Beispiel gezeigt.



Die `IO:BufFileRead`- und `IO:BufFileWrite`-Ereignisse treten auf, wenn die häufigsten Abfragen in Ihrem Workload häufig temporäre Dateien erstellen. Mit Performance Insights können Sie die häufigsten Abfragen identifizieren, die auf `IO:BufFileRead` und `IO:BufFileWrite` warten, indem Sie die Abschnitte Durchschnittliche aktive Vorträge (AAS) in Datenbanklast und Top SQL überprüfen.



Weitere Informationen zur Analyse von Top-Abfragen und Last nach Warteereignis mit Performance Insights finden Sie unter Überblick über die Registerkarte „Top SQL“. Sie sollten die Abfragen identifizieren und optimieren, die zu einer erhöhten Nutzung temporärer Dateien und damit verbundenen Warteereignissen führen. Weitere Informationen zu diesen Warteereignissen und deren Behebung finden Sie unter IO:BufFileRead und IO:BufFileWrite.

> **Note**
>
> Der Parameter `work_mem` steuert, wann der Sortiervorgang nicht mehr genügend Speicherplatz hat und die Ergebnisse in temporäre Dateien geschrieben werden. Wir empfehlen, die Einstellung dieses Parameters nicht höher als auf den Standardwert festzulegen, da dadurch jede Datenbanksitzung mehr Speicher belegen würde. Außerdem kann eine einzelne Sitzung, die komplexe Verknüpfungen und Sortierungen durchführt, parallele Operationen ausführen, bei denen jeder Vorgang Speicherplatz belegt.
> Wenn Sie einen umfangreichen Bericht mit mehreren Verknüpfungen und Sortierungen haben, empfiehlt es sich, diesen Parameter mit dem Befehl `SET work_mem` auf

Sitzungsebene festzulegen. Dann wird die Änderung nur auf die aktuelle Sitzung angewendet und der Wert nicht global geändert.

Optimierung mit Warteereignissen für Aurora PostgreSQL

Warteereignisse sind ein wichtiges Optimierungs-Tool für Aurora PostgreSQL. Wenn Sie herausfinden können, warum Sitzungen auf Ressourcen warten und was sie tun, können Sie Engpässe besser reduzieren. Anhand der Informationen in diesem Abschnitt können Sie mögliche Ursachen und Abhilfemaßnahmen ermitteln. Bevor Sie sich mit diesem Abschnitt befassen, empfehlen wir Ihnen dringend, die grundlegenden Aurora-Konzepte zu verstehen, insbesondere die folgenden Themen:

- Amazon Aurora-Speicher und -Zuverlässigkeit
- Verwalten von Performance und Skalierung für einen Aurora-DB-Cluster

Important

Die Warteereignisse in diesem Abschnitt gelten speziell für Aurora PostgreSQL. Verwenden Sie die Informationen in diesem Abschnitt, um nur Amazon Aurora zu optimieren, nicht RDS für PostgreSQL.
Einige Warteereignisse in diesem Abschnitt haben keine Entsprechungen in den Open-Source-Versionen dieser Datenbank-Engines. Andere Warteereignisse haben dieselben Namen wie Ereignisse in Open-Source-Engines, verhalten sich jedoch anders. Beispielsweise funktioniert Amazon-Aurora-Speicher anders als Open-Source-Speicher, sodass speicherbezogene Warteereignisse auf unterschiedliche Ressourcenbedingungen hinweisen.

Themen

- io:BuffileRead und io:BuffileWrite
- IO:DataFileRead
- IO:XactSync
- IPC:DamRecordTxAck
- Lock:advisory
- Lock:extend
- Lock:Relation
- Lock:transactionid
- Lock:tuple
- LWLock:buffer_content (BufferContent)
- LWLock:buffer_mapping
- LWLock:BufferIO (IPC:BufferIO)
- LWLock:lock_manager
- LWLockMultiXact:
- Timeout:PgSleep

Grundlegende Konzepte für Aurora PostgreSQL-Optimierung

Bevor Sie Ihre Aurora PostgreSQL-Datenbank optimieren, sollten Sie wissen, was Warteereignisse sind und warum sie auftreten. Sehen Sie sich auch die grundlegende Speicher- und Festplattenarchitektur von Aurora PostgreSQL an. Ein hilfreiches Architekturdiagramm finden Sie im PostgreSQL-Wikibook.

Themen

- Aurora PostgreSQL-Warteereignisse
- Aurora PostgreSQL-Speicher
- Aurora PostgreSQL-Prozesse

Aurora PostgreSQL-Warteereignisse

Ein Warteereignis zeigt eine Ressource an, auf die eine Sitzung wartet. Das Warteereignis `Client:ClientRead` tritt beispielsweise ein, wenn Aurora PostgreSQL darauf wartet, Daten von

der client.emory- und Festplattenarchitektur von Aurora PostgreSQL zu empfangen. Zu den typischen Ressourcen, auf die eine Sitzung wartet, gehören die folgenden:

- Singlethread-Zugriff auf einen Puffer, beispielsweise wenn eine Sitzung versucht, einen Puffer zu ändern
- Eine Zeile, die derzeit von einer anderen Sitzung gesperrt ist
- Eine gelesene Datendatei
- Eine geschriebene Protokolldatei

Um beispielsweise eine Abfrage zu erfüllen, kann die Sitzung einen vollständigen Tabellenscan durchführen. Wenn sich die Daten noch nicht im Arbeitsspeicher befinden, wartet die Sitzung, bis die Datenträger-I/O abgeschlossen ist. Wenn die Puffer in den Speicher gelesen werden, muss die Sitzung möglicherweise warten, da andere Sitzungen auf dieselben Puffer zugreifen. Die Datenbank zeichnet die Wartezeiten unter Verwendung eines vordefinierten Warteereignisses auf. Diese Ereignisse sind in Kategorien eingeteilt.

Ein Wait-Ereignis allein zeigt kein Leistungsproblem an. Wenn sich beispielsweise die angeforderten Daten nicht im Speicher befinden, müssen die Daten von der Festplatte gelesen werden. Wenn eine Sitzung eine Zeile für eine Aktualisierung sperrt, wartet eine andere Sitzung darauf, dass die Zeile entsperrt wird, damit sie sie aktualisieren kann. Bei einem Commit muss gewartet werden, bis der Schreibvorgang in eine Protokolldatei abgeschlossen ist. Wartezeiten sind ein wesentlicher Bestandteil des normalen Funktionierens einer Datenbank.

Eine große Anzahl von Warteereignissen weist normalerweise auf ein Leistungsproblem hin. In solchen Fällen können Sie Warteereignisdaten verwenden, um zu bestimmen, wo die Sitzungen Zeit verbringen. Wenn beispielsweise ein Bericht, der normalerweise in Minuten ausgeführt wird, jetzt stundenlang ausgeführt wird, können Sie die Warteereignisse identifizieren, die am meisten zur Gesamtwartezeit beitragen. Wenn Sie die Ursachen für die häufigsten Warteereignisse ermitteln können, können Sie manchmal Änderungen vornehmen, die die Leistung verbessern. Wenn Ihre Sitzung beispielsweise auf eine Zeile wartet, die von einer anderen Sitzung gesperrt wurde, können Sie die Sperrsitzung beenden.

Aurora PostgreSQL-Speicher

Aurora PostgreSQL-Speicher ist in freigegeben und lokal unterteilt.

Themen

- Gemeinsamer Speicher in Aurora PostgreSQL

- Lokaler Speicher in Aurora PostgreSQL

Gemeinsamer Speicher in Aurora PostgreSQL

Aurora PostgreSQL weist beim Start der Instance gemeinsam genutzten Speicher zu. Shared Memory ist in mehrere Teilbereiche unterteilt. Nachfolgend finden Sie eine Beschreibung der wichtigsten.

Themen

- Freigegebene Puffer
- Write-Ahead-Protokoll (WAL)-Puffer

Freigegebene Puffer

Der freigegebene Pufferpool ist ein Aurora PostgreSQL-Speicherbereich, der alle Seiten enthält, die von Anwendungsverbindungen verwendet werden oder verwendet wurden. Eine Seite ist die Speicherversion eines Plattenblocks. Der gemeinsam genutzte Pufferpool zwischenspeichert die von der Platte gelesenen Datenblöcke. Der Pool reduziert die Notwendigkeit, Daten erneut von der Festplatte zu lesen, wodurch die Datenbank effizienter arbeitet.

Jede Tabelle und jeder Index wird als Array von Seiten einer festen Größe gespeichert. Jeder Block enthält mehrere Tupel, die Zeilen entsprechen. Ein Tupel kann auf jeglicher Seite gespeichert werden.

Der gemeinsam genutzte Pufferpool hat endlichen Speicher. Wenn eine neue Anforderung eine Seite erfordert, die sich nicht im Speicher befindet und kein Speicher mehr vorhanden ist, entfernt Aurora PostgreSQL eine weniger häufig verwendete Seite, um die Anforderung aufzunehmen. Die Räumungsrichtlinie wird durch einen Takt-Sweep-Algorithmus implementiert.

Der Parameter `shared_buffers` bestimmt, wie viel Speicher der Server für das Caching von Daten bereitstellt.

Write-Ahead-Protokoll (WAL)-Puffer

Ein Write-Ahead-Protokoll(WAL)-Puffer enthält Transaktionsdaten, die Aurora PostgreSQL später in den persistenten Speicher schreibt. Mithilfe des WAL-Mechanismus kann Aurora PostgreSQL Folgendes tun:

- Daten nach einem Fehler wiederherstellen

- Reduzieren Sie die Festplatten–I/O indem Sie häufige Schreibvorgänge auf die Festplatte vermeiden

Wenn ein Client Daten ändert, schreibt Aurora PostgreSQL die Änderungen in den WAL-Puffer. Wenn der Client einen `COMMIT` ausgibt, schreibt der WAL-Writerprozess Transaktionsdaten in die WAL-Datei.

Der Parameter `wal_level` bestimmt, wie viele Informationen in das WAL geschrieben werden.

Lokaler Speicher in Aurora PostgreSQL

Jeder Backend-Prozess weist lokalen Speicher für die Abfrageverarbeitung zu.

Themen

- Arbeitsspeicherbereich
- Wartungs-Arbeitsspeicherbereich
- Temporärer Pufferbereich

Arbeitsspeicherbereich

Der Arbeitsspeicherbereich enthält temporäre Daten für Abfragen, die Sortierungen und Hashes durchführen. Beispielsweise führt eine Abfrage mit einer `ORDER BY`-Klausel eine Sortierung durch. Abfragen verwenden Hash-Tabellen in Hash-Joins und Aggregationen.

Der `work_mem`-Parameter die Speichermenge, die von internen Sortiervorgängen und Hash-Tabellen verwendet werden soll, bevor in temporäre Plattendateien geschrieben wird. Der Standardwert lautet 4 MB. Mehrere Sitzungen können gleichzeitig ausgeführt werden, und jede Sitzung kann Wartungsvorgänge parallel ausführen. Aus diesem Grund kann der gesamte verwendete Arbeitsspeicher ein Vielfaches der Einstellung `work_mem` betragen.

Wartungs-Arbeitsspeicherbereich

Der Wartungsarbeitsspeicherbereich speichert Daten für Wartungsvorgänge zwischen. Zu diesen Vorgängen gehören das Vakuumieren, das Erstellen eines Index und das Hinzufügen von Fremdschlüsseln.

Der Parameter `maintenance_work_mem` gibt die maximale Speichermenge an, die von Wartungsvorgängen verwendet werden soll. Der Standardwert lautet 64 MB. In einer Datenbanksitzung kann jeweils nur ein Wartungsvorgang ausgeführt werden.

Temporärer Pufferbereich

Der temporäre Pufferbereich speichert temporäre Tabellen für jede Datenbanksitzung zwischen.

Jede Sitzung weist temporäre Puffer nach Bedarf bis zu dem von Ihnen angegebenen Limit zu. Wenn die Sitzung endet, löscht der Server die Puffer.

Der Parameter `temp_buffers` legt die maximale Anzahl temporärer Puffer fest, die von jeder Sitzung verwendet werden. Vor der ersten Verwendung temporärer Tabellen innerhalb einer Sitzung können Sie den `temp_buffers`-Wert ändern.

Aurora PostgreSQL-Prozesse

Aurora PostgreSQL verwendet mehrere Prozesse.

Themen

Postmaster-Prozess

Der Postmaster-Prozess ist der erste Prozess, der beim Starten von Aurora PostgreSQL gestartet wird. Der Postmaster-Prozess hat die folgenden Hauptaufgaben:

- Hintergrundprozesse teilen und überwachen
- Empfangen Sie Authentifizierungsanfragen von Clientprozessen und authentifizieren Sie sie, bevor Sie der Datenbank erlauben, Anfragen zu bearbeiten

Backend-Prozesse

Wenn der Postmaster eine Client-Anfrage authentifiziert, forkisiert der Postmaster einen neuen Backend-Prozess, auch Postgres-Prozess genannt. Ein Client-Prozess verbindet sich mit genau einem Backend-Prozess. Der Client-Prozess und der Backend-Prozess kommunizieren direkt ohne Eingriff des Postmaster-Prozesses.

Hintergrundprozesse

Der Postmaster-Prozess teilt mehrere Prozesse, die unterschiedliche Backend-Aufgaben ausführen. Einige der wichtigeren sind die folgenden:

- WAL-Writer

  Aurora PostgreSQL schreibt Daten im WAL-Puffer (Write Ahead Logging) in die Protokolldateien. Das Prinzip der Write-Ahead-Protokollierung besteht darin, dass die Datenbank keine Änderungen in die Datendateien schreiben kann, bis die Datenbank Protokolldatensätze geschrieben hat, die diese Änderungen auf die Festplatte beschreiben. Der WAL-Mechanismus reduziert Festplatten-I/O und ermöglicht Aurora PostgreSQL, die Protokolle zu verwenden, um die Datenbank nach einem Fehler wiederherzustellen.

- Hintergrund-Autor

  Dieser Prozess schreibt regelmäßig schmutzige (modifizierte) Seiten aus den Speicherpuffern in die Datendateien. Eine Seite wird schmutzig, wenn ein Backend-Prozess sie im Speicher ändert.

- Autovacuum-Daemon

  Der Daemon besteht aus Folgendem:

  - Der Autovacuum-Launcher
  - Die Autovacuum-Worker-Prozesse

  Wenn Autovacuum aktiviert ist, sucht es nach Tabellen mit einer großen Anzahl eingefügter, aktualisierter oder gelöschter Tupel. Der Daemon hat folgende Aufgaben:

  - Wiederherstellen oder Wiederverwenden von Speicherplatz, der von aktualisierten oder gelöschten Zeilen belegt ist
  - Vom Planer verwendete Statistiken aktualisieren
  - Schutz vor Verlust alter Daten durch Transaktions-ID-Wraparound

  Die Autovacuum-Funktion automatisiert die Ausführung von `VACUUM`- und `ANALYZE`-Befehlen. `VACUUM` hat folgende Varianten: Standard und Voll. Standardvakuum läuft parallel zu anderen Datenbankvorgängen. `VACUUM FULL` erfordert eine exklusive Sperre für die Tabelle, an der es arbeitet. Daher kann es nicht parallel zu Vorgänge ausgeführt werden, die auf dieselbe Tabelle zugreifen. `VACUUM` erzeugt eine beträchtliche Menge an I/O-Datenverkehr, was zu einer schlechten Leistung anderer aktiver Sitzungen führen kann.

Aurora PostgreSQL-Warteereignisse

Die folgende Tabelle listet die Warteereignisse für Aurora PostgreSQL auf, die am häufigsten auf Leistungsprobleme hinweisen, und fasst die häufigsten Ursachen und Korrekturmaßnahmen

zusammen. Die folgenden Warteereignisse sind eine Teilmenge der Liste in Amazon-Aurora-PostgreSQL-Warteereignisse.

Warteereignis	Definition
Kunde: ClientRead	Dieses Ereignis tritt ein, wenn Aurora PostgreSQL darauf wartet, Daten vom Client zu empfangen.
Kunde: ClientWrite	Dieses Ereignis tritt ein, wenn Aurora PostgreSQL darauf wartet, Daten an den Client zu schreiben.
CPU	Dieses Ereignis tritt auf, wenn ein Thread in der CPU aktiv ist oder auf die CPU wartet.
io:BuffileRead und io:BuffileWrite	Diese Ereignisse treten auf, wenn Aurora PostgreSQL temporäre Dateien erstellt.
IO:DataFileRead	Dieses Ereignis tritt auf, wenn eine Verbindung darauf wartet, dass ein Backend-Prozess eine erforderliche Seite aus dem Speicher liest, da die Seite nicht im gemeinsam genutzten Speicher verfügbar ist.
IO:XactSync	Dieses Ereignis tritt ein, wenn die Datenbank darauf wartet, dass das Aurora-Storage-Subsystem den Commit einer regulären Transaktion bzw. den Commit oder Rollback einer vorbereiteten Transaktion ausführt.
IPC:DamRecordTxAck	Dieses Ereignis tritt auf, wenn Aurora PostgreSQL in einer Sitzung, die Datenbank-Aktivitätsstreams verwendet, ein Aktivitätsstream-Ereignis erzeugt und dann wartet, bis dieses Ereignis dauerhaft wird
Lock:advisory	Dieses Ereignis tritt auf, wenn eine PostgreSQL-Anwendung eine Sperre verwendet, um Aktivitäten über mehrere Sitzungen hinweg zu koordinieren.

Warteereignis	Definition
Lock:extend	Dieses Ereignis tritt ein, wenn ein Backend-Prozess darauf wartet, eine Beziehung zu sperren, um sie zu erweitern, während ein anderer Prozess diese Beziehung für denselben Zweck gesperrt hat.
Lock:Relation	Dieses Ereignis tritt ein, wenn eine Abfrage darauf wartet, eine Sperre für eine Tabelle oder Ansicht zu erhalten, die derzeit von einer anderen Transaktion gesperrt ist.
Lock:transactionid	Dieses Ereignis tritt ein, wenn eine Transaktion auf eine Sperre auf Zeilenebene wartet.
Lock:tuple	Dieses Ereignis tritt ein, wenn ein Backend-P rozess darauf wartet, eine Sperre für ein Tupel zu erlangen.
LWLock:buffer_content (BufferContent)	Dieses Ereignis tritt ein, wenn eine Sitzung darauf wartet, eine Datenseite im Speicher zu lesen oder zu schreiben, während eine andere Sitzung diese Seite zum Schreiben gesperrt hat.
LWLock:buffer_mapping	Dieses Ereignis tritt ein, wenn eine Sitzung darauf wartet, einen Datenblock einem Puffer im gemeinsam genutzten Pufferpool zuzuordnen.
LWLock:BufferIO (IPC:BufferIO)	Dieses Ereignis tritt auf, wenn Aurora PostgreSQ L oder RDS for PostgreSQL darauf wartet, dass andere Prozesse ihre Eingabe-/Ausgabe-(I/O)-Vorg änge beenden, wenn sie gleichzeitig versuchen, auf eine Seite zuzugreifen.

Warteereignis	Definition
LWLock:lock_manager	Dieses Ereignis tritt ein, wenn die Aurora PostgreSQL-Engine den Speicherbereich der gemeinsam genutzten Sperre verwaltet, um eine Sperre zuzuweisen, zu überprüfen und aufzuheben, wenn eine Fast-Path-Sperre nicht möglich ist.
LWLockMultiXact:	Diese Art von Ereignis tritt auf, wenn Aurora PostgreSQL eine Sitzung offen hält, um mehrere Transaktionen abzuschließen, die dieselbe Zeile in einer Tabelle betreffen. Das Warteereignis gibt an, welcher Aspekt der Verarbeitung mehrerer Transaktionen das Warteereignis generiert, d. h. LWLock:MultiXactOffsetSLRU, LWLock:MultiXactOffsetBuffer, LWLock:MultiXactMemberSLRU oder LWLock:MultiXactMemberBuffer.
Timeout:PgSleep	Dieses Ereignis tritt ein, wenn ein Serverprozess die Funktion `pg_sleep` aufgerufen hat und darauf wartet, dass das Sleep-Timeout abläuft.

Kunde: ClientRead

Das Ereignis `Client:ClientRead` tritt ein, wenn Aurora PostgreSQL darauf wartet, Daten vom Client zu empfangen.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für Aurora PostgreSQL Version 10 und höher unterstützt.

Kontext

Ein Aurora PostgreSQL DB-Cluster wartet darauf, Daten vom Client zu empfangen. Der Aurora PostgreSQL-DB-Cluster muss die Daten vom Client empfangen, bevor er weitere Daten an den Client senden kann. Die Zeit, die der Cluster wartet, bevor er Daten vom Client empfängt, ist ein `Client:ClientRead`-Ereignis.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Häufige Gründe dafür, dass das `Client:ClientRead`-Ereignis in den Top-Wartezeiten angezeigt wird, sind die folgenden:

Erhöhte Netzwerklatenz

Es kann zu einer erhöhten Netzwerklatenz zwischen dem Aurora PostgreSQL-DB-Cluster und dem Client kommen. Eine höhere Netzwerklatenz erhöht die Zeit, die der DB-Cluster benötigt, um Daten vom Client zu empfangen.

Erhöhte Belastung des Clients

Auf dem Client kann es zu CPU-Druck oder Netzwerksättigung kommen. Eine Zunahme der Last auf dem Client kann die Übertragung von Daten vom Client zum Aurora PostgreSQL-DB-Cluster verzögern.

Übermäßige Netzwerkrundfahrten

Eine große Anzahl von Netzwerk-Roundtrips zwischen dem Aurora PostgreSQL-DB-Cluster und dem Client kann die Datenübertragung vom Client zum Aurora PostgreSQL-DB-Cluster verzögern.

Großer Kopiervorgang

Während eines Kopiervorgangs werden die Daten vom Dateisystem des Clients in den Aurora PostgreSQL DB-Cluster übertragen. Das Senden einer großen Datenmenge an den DB-Cluster kann die Übertragung von Daten vom Client zum DB-Cluster verzögern.

Verbindung von Clients im Leerlauf

Eine Verbindung mit einer DB-Instance von Aurora PostgreSQL befindet sich im Transaktionsstatus im Leerlauf und wartet darauf, dass ein Client weitere Daten sendet oder einen Befehl ausgibt. Dieser Status kann zu einer Zunahme von `Client:ClientRead`-Ereignissen führen.

PgBouncer wird für das Verbindungspooling verwendet

PgBouncer hat eine Netzwerkkonfigurationseinstellung auf niedriger Ebene aufgerufen`pkt_buf`, die standardmäßig auf 4.096 gesetzt ist. Wenn der Workload Abfragepakete mit mehr als 4.096 Byte durchsendet, empfehlen wir PgBouncer, die Einstellung auf 8.192 zu erhöhen. `pkt_buf` Wenn die neue Einstellung die Anzahl der `Client:ClientRead`-Ereignisse nicht verringert, empfehlen wir, die `pkt_buf`-Einstellung auf höhere Werte zu erhöhen, z. B. 16.384 oder 32.768. Wenn der Abfragetext groß ist, kann die größere Einstellung besonders hilfreich sein.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Themen

- Platzieren Sie die Clients im selben Availability Zone- und VPC-Subnetz wie der Cluster
- Skalieren Sie Ihren -C
- Instances der aktuellen Generation verwenden
- Erhöhung der Netzwerkbandbreite
- Überwachen Sie Maximen für die Netzwerkleistung
- Überwachen Sie auf Transaktionen im Status „Leerlauf in Transaktion“

Platzieren Sie die Clients im selben Availability Zone- und VPC-Subnetz wie der Cluster

Um die Netzwerklatenz zu reduzieren und den Netzwerkdurchsatz zu erhöhen, platzieren Sie Clients in dieselbe Availability Zone und Virtual Private Cloud (VPC) -Subnetz wie der Aurora PostgreSQL DB-Cluster. Stellen Sie sicher, dass sich die Clients so geografisch wie möglich am DB-Cluster befinden.

Skalieren Sie Ihren -C

Ermitteln Sie anhand von Amazon CloudWatch oder anderen Host-Metriken, ob Ihr Client derzeit durch CPU- oder Netzwerkbandbreite oder beides eingeschränkt ist. Wenn der Kunde eingeschränkt ist, skalieren Sie Ihren Kunden entsprechend.

Instances der aktuellen Generation verwenden

In einigen Fällen verwenden Sie möglicherweise keine DB-Instance-Klasse, die Jumbo-Frames unterstützt. Wenn Sie Ihre Anwendung auf Amazon EC2 ausführen, sollten Sie eine Instance

der aktuellen Generation für den Client verwenden. Konfigurieren Sie außerdem die maximale Übertragungseinheit (MTU) im Kundenvorgangssystem Diese Technik könnte die Anzahl der Netzläufe reduzieren und den Netzwerkdurchsatz erhöhen. Weitere Informationen finden Sie unter Jumbo Frames (9001 MTU) im Amazon EC2 EC2-Benutzerhandbuch.

Weitere Informationen zu DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen. Um die DB-Instance-Klasse zu bestimmen, die einem Amazon EC2-Instance-Typ entspricht, platzieren Sie `db.` vor dem Namen des Amazon EC2-Instance-Typs. Beispielsweise entspricht die `r5.8xlarge`-Amazon EC2-Instance der `db.r5.8xlarge`-DB-Instance-Klasse.

Erhöhung der Netzwerkbandbreite

Verwenden Sie `NetworkReceiveThroughput` und `NetworkTransmitThroughput` CloudWatch Amazon-Metriken, um den eingehenden und ausgehenden Netzwerkverkehr auf dem DB-Cluster zu überwachen. Diese Metriken können Ihnen helfen festzustellen, ob die Netzwerkbandbreite für Ihre Workload ausreicht.

Wenn Ihre Netzwerkbandbreite nicht ausreicht, erhöhen Sie sie. Wenn der AWS Client oder Ihre DB-Instance die Netzwerkbandbreitenlimits erreicht, besteht die einzige Möglichkeit, die Bandbreite zu erhöhen, darin, Ihre DB-Instance-Größe zu erhöhen.

Weitere Informationen zu CloudWatch Metriken finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora.

Überwachen Sie Maximen für die Netzwerkleistung

Wenn Sie Amazon EC2-Clients verwenden, bietet Amazon EC2 Maximum für Netzwerkleistungsmetriken, einschließlich der aggregierten eingehenden und ausgehenden Netzwerkbandbreite. Es bietet auch Verbindungsverfolgung, um sicherzustellen, dass Pakete wie erwartet zurückgegeben werden, und Zugriff auf Link-lokale Dienste für Dienste wie das Domain Name System (DNS). Um diese Maximen zu überwachen, verwenden Sie einen aktuell erweiterten Netzwerktreiber und überwachen Sie die Netzwerkleistung für Ihren Client.

Weitere Informationen finden Sie unter Überwachen der Netzwerkleistung für Ihre Amazon EC2 EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch und Überwachen der Netzwerkleistung für Ihre Amazon EC2 EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch.

Überwachen Sie auf Transaktionen im Status „Leerlauf in Transaktion“

Überprüfen Sie, ob Sie eine steigende Anzahl von `idle in transaction`-Verbindungen haben. Beobachten Sie dazu die `state`-Spalte in der `pg_stat_activity`-Tabelle. Möglicherweise können Sie die Verbindungsquelle identifizieren, indem Sie eine Abfrage ähnlich der folgenden ausführen.

```
select client_addr, state, count(1) from pg_stat_activity
where state like 'idle in transaction%'
group by 1,2
order by 3 desc
```

Kunde: ClientWrite

Das `Client:ClientWrite`-Ereignis tritt auf, wenn Aurora PostgreSQL darauf wartet, Daten an den Client zu schreiben.

Themen

- Unterstützte Engine-Versionen
- Kontext
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für Aurora PostgreSQL Version 10 und höher unterstützt.

Kontext

Ein Clientprozess muss alle Daten lesen, die von einem Aurora PostgreSQL DB-Cluster empfangen wurden, bevor der Cluster weitere Daten senden kann. Die Zeit, die der Cluster wartet, bevor weitere Daten an den Client gesendet werden, ist ein `Client:ClientWrite`-Ereignis.

Ein reduzierter Netzwerkdurchsatz zwischen dem Aurora PostgreSQL DB-Cluster und dem Client kann dieses Ereignis verursachen. CPU-Druck und Netzwerksättigung auf dem Client können dieses Ereignis ebenfalls verursachen. CPU-Druck liegt vor, wenn die CPU voll ausgelastet ist und Aufgaben auf CPU-Zeit warten. Eine Netzwerksättigung liegt vor, wenn das Netzwerk zwischen Datenbank und Client mehr Daten überträgt, als es verarbeiten kann.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Häufige Gründe dafür, dass das `Client:ClientWrite`-Ereignis in den Top-Wartezeiten angezeigt wird, sind die folgenden:

Erhöhte Netzwerklatenz

Es kann zu einer erhöhten Netzwerklatenz zwischen dem Aurora PostgreSQL-DB-Cluster und dem Client kommen. Eine höhere Netzwerklatenz erhöht die Zeit, die der Client benötigt, um die Daten zu empfangen.

Erhöhte Belastung des Clients

Auf dem Client kann es zu CPU-Druck oder Netzwerksättigung kommen. Eine Erhöhung der Belastung des Clients verzögert den Empfang von Daten aus dem Aurora PostgreSQL DB-Cluster.

Große Datenmenge, die an den Kunden gesendet werden

Der Aurora PostgreSQL DB-Cluster sendet möglicherweise eine große Datenmenge an den Client. Ein Client kann die Daten möglicherweise nicht so schnell empfangen, wie der Cluster sie sendet. Aktivitäten wie das Kopieren einer großen Tabelle können zu einer Zunahme von `Client:ClientWrite`-Ereignissen führen.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Themen

- Platzieren Sie die Clients im selben Availability Zone- und VPC-Subnetz wie der Cluster
- Instances der aktuellen Generation verwenden
- Reduzieren Sie die an den Kunden gesendeten Daten
- Skalieren Sie Ihren -C

Platzieren Sie die Clients im selben Availability Zone- und VPC-Subnetz wie der Cluster

Um die Netzwerklatenz zu reduzieren und den Netzwerkdurchsatz zu erhöhen, platzieren Sie Clients in dieselbe Availability Zone und Virtual Private Cloud (VPC) -Subnetz wie der Aurora PostgreSQL DB-Cluster.

Instances der aktuellen Generation verwenden

In einigen Fällen verwenden Sie möglicherweise keine DB-Instance-Klasse, die Jumbo-Frames unterstützt. Wenn Sie Ihre Anwendung auf Amazon EC2 ausführen, sollten Sie eine Instance der aktuellen Generation für den Client verwenden. Konfigurieren Sie außerdem die maximale Übertragungseinheit (MTU) im Kundenvorgangssystem Diese Technik könnte die Anzahl der Netzläufe reduzieren und den Netzwerkdurchsatz erhöhen. Weitere Informationen finden Sie unter Jumbo Frames (9001 MTU) im Amazon EC2 EC2-Benutzerhandbuch.

Weitere Informationen zu DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen. Um die DB-Instance-Klasse zu bestimmen, die einem Amazon EC2-Instance-Typ entspricht, platzieren Sie `db.` vor dem Namen des Amazon EC2-Instance-Typs. Beispielsweise entspricht die `r5.8xlarge`-Amazon EC2-Instance der `db.r5.8xlarge`-DB-Instance-Klasse.

Reduzieren Sie die an den Kunden gesendeten Daten

Passen Sie Ihre Anwendung nach Möglichkeit an, um die Datenmenge zu reduzieren, die der Aurora PostgreSQL DB-Cluster an den Client sendet. Solche Anpassungen entlasten die CPU- und Netzwerkkonflikte auf dem Client.

Skalieren Sie Ihren -C

Ermitteln Sie anhand von Amazon CloudWatch oder anderen Host-Metriken, ob Ihr Client derzeit durch CPU- oder Netzwerkbandbreite oder beides eingeschränkt ist. Wenn der Kunde eingeschränkt ist, skalieren Sie Ihren Kunden entsprechend.

CPU

Dieses Ereignis tritt auf, wenn ein Thread in der CPU aktiv ist oder auf die CPU wartet.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen sind für Aurora PostgreSQL Version 9.6 und höher relevant.

Context

Die Zentrale Verarbeitungseinheit (CPU) ist die Komponente eines Computers, die Anweisungen ausführt. Beispielsweise führen CPU-Anweisungen arithmetische Vorgänge aus und tauschen Daten im Speicher aus. Wenn eine Abfrage die Anzahl der Anweisungen erhöht, die sie über das Datenbank-Engine ausführt, erhöht sich der Zeitaufwand für die Ausführung der Abfrage. CPU-Scheduling gibt einem Prozess CPU-Zeit. Die Planung wird vom Kernel des Betriebssystems orchestriert.

Themen

Wie kann man sagen, wann diese Wartezeit stattfindet

Dieses CPU-Warteereignis zeigt an, dass ein Backend-Prozess in der CPU aktiv ist oder auf die CPU wartet. Sie wissen, dass es passiert, wenn eine Abfrage die folgenden Informationen anzeigt:

- Die Spalte `pg_stat_activity.state` hat den Wert `active`.
- Die Spalten `wait_event_type` und `wait_event` in `pg_stat_activity` sind beide `null`.

Führen Sie die folgende Abfrage aus, um die Backend-Prozesse anzuzeigen, die auf der CPU verwenden oder auf dieser warten.

```
SELECT *
FROM   pg_stat_activity
WHERE  state = 'active'
AND    wait_event_type IS NULL
AND    wait_event IS NULL;
```

DbloadCPU-Metrik

Die Performance Insights-Metrik für CPU ist `DBLoadCPU`. Der Wert für `DBLoadCPU` kann vom Wert für die Amazon CloudWatch-Metrik `CPUUtilization` abweichen. Die letztere Metrik wird vom HyperVisor für eine Datenbank-Instance gesammelt.

Metriken für Os.cPuUtilization

Performance Insights Betriebssystem-Metriken liefern detaillierte Informationen zur CPU-Auslastung. Sie können beispielsweise die folgenden Metriken anzeigen:

- `os.cpuUtilization.nice.avg`
- `os.cpuUtilization.total.avg`
- `os.cpuUtilization.wait.avg`
- `os.cpuUtilization.idle.avg`

Performance Insights meldet die CPU-Auslastung durch die Datenbank-Engine als `os.cpuUtilization.nice.avg`.

Wahrscheinliche Ursache für CPU-Planung

Aus Sicht des Betriebssystems ist die CPU aktiv, wenn der Leerlauf-Thread nicht ausgeführt wird. Die CPU ist aktiv, während sie eine Berechnung durchführt, aber sie ist auch aktiv, wenn sie auf Speicher-I/O wartet. Diese Art von I/O dominiert eine typische Datenbank-Workload.

Wenn die folgenden Bedingungen erfüllt sind, werden Prozesse wahrscheinlich warten, bis die folgenden Bedingungen erfüllt sind:

- Die CloudWatch `CPUUtilization`-Metrik liegt nahe bei 100 Prozent.
- Die durchschnittliche Belastung ist größer als die Anzahl der vCPUs, was auf eine hohe Last hinweist. Sie finden die `loadAverageMinute`-Metrik im Abschnitt Betriebssystemmetriken in Performance Insights.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das CPU-Warteereignis mehr als normal auftritt und möglicherweise auf ein Leistungsproblem hinweist, sind typische Ursachen die folgenden.

Themen

- Wahrscheinliche Ursachen für plötzliche Stacheln
- Wahrscheinliche Ursachen für langfristige Hochfrequenz
- Corner Cases

Wahrscheinliche Ursachen für plötzliche Stacheln

Die wahrscheinlichsten Ursachen für plötzliche Stacheln sind wie folgt:

- Ihre Anwendung hat zu viele gleichzeitige Verbindungen zur Datenbank geöffnet. Dieses Szenario wird als „Verbindungssturm“ bezeichnet.
- Ihre Anwendungs-Workload hat sich auf eine der folgenden Weisen geändert:
  - Neue Anfragen
  - Eine Zunahme der Größe Ihres Datensatzes
  - Indexpflege oder -erstellung
  - Neue Funktionen
  - Neue Betreiber
  - Eine Zunahme der parallelen Abfrageausführung
- Ihre Abfrageausführungspläne haben sich geändert. In einigen Fällen kann eine Änderung zu einem Anstieg der Puffer führen. Beispielsweise verwendet die Abfrage jetzt einen sequentiellen Scan, als sie zuvor einen Index verwendet hat. In diesem Fall benötigen die Abfragen mehr CPU, um dasselbe Ziel zu erreichen.

Wahrscheinliche Ursachen für langfristige Hochfrequenz

Die wahrscheinlichsten Ursachen für Ereignisse, die über einen langen Zeitraum auftreten:

- Zu viele Backend-Prozesse laufen gleichzeitig auf der CPU. Diese Prozesse können parallele Arbeiter sein.
- Abfragen funktionieren suboptimal, da sie eine große Anzahl von Puffern benötigen.

Corner Cases

Wenn sich herausstellt, dass keine der wahrscheinlichen Ursachen tatsächliche Ursachen ist, können folgende Situationen auftreten:

- Die CPU tauscht Prozesse ein- und aus.
- Der CPU-Kontextwechsel hat zugenommen.
- Aurora PostgreSQL-Code fehlen Warteereignisse.

Aktionen

Wenn das CPU-Wait-Ereignis die Datenbankaktivität dominiert, weist dies nicht unbedingt auf ein Leistungsproblem hin. Reagieren Sie auf dieses Ereignis nur, wenn sich die Leistung verschlechtert.

Themen

Untersuchen Sie, ob die Datenbank den CPU-Anstieg verursacht

Untersuchen Sie die `os.cpuUtilization.nice.avg`-Metrik in Performance Insights. Wenn dieser Wert weit unter der CPU-Auslastung liegt, tragen Nicht-Datenbankprozesse den Hauptbeitrag zur CPU bei.

Bestimmen Sie, ob die Anzahl der Verbindungen gestiegen ist

Untersuchen Sie die Metrik `DatabaseConnections` in Amazon CloudWatch. Ihre Aktion hängt davon ab, ob die Zahl während des Zeitraums erhöhter CPU-Warteereignisse erhöht oder gesunken ist.

Die Verbindungen nahmen zu

Wenn die Anzahl der Verbindungen gestiegen ist, vergleichen Sie die Anzahl der Backend-Prozesse, die CPU verbrauchen, mit der Anzahl der vCPUs. Die folgenden Szenarien sind möglich:

- Die Anzahl der Backend-Prozesse, die CPU verbrauchen, ist geringer als die Anzahl der vCPUs.

  In diesem Fall ist die Anzahl der Verbindungen kein Problem. Möglicherweise versuchen Sie jedoch weiterhin, die CPU-Auslastung zu reduzieren.
- Die Anzahl der Backend-Prozesse, die CPU verbrauchen, ist größer als die Anzahl der vCPUs.

  Ziehen Sie in diesem Fall die folgenden Optionen in Betracht:
  - Verringern Sie die Anzahl der Backend-Prozesse, die mit Ihrer Datenbank verbunden sind. Implementieren Sie beispielsweise eine Verbindungs-Pooling-Lösung wie RDS Proxy. Weitere Informationen hierzu finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.
  - Aktualisieren Sie Ihre Instance-Größe, um eine höhere Anzahl von vCPUs zu erhalten.
  - Leiten Sie ggf. einige schreibgeschützte Workloads auf Reader-Knoten um.

Die Verbindungen haben nicht zugenommen

Untersuchen Sie die `blks_hit`-Metriken in Performance Insights. Suchen Sie nach einer Korrelation zwischen einem Anstieg von `blks_hit` und der CPU-Auslastung. Die folgenden Szenarien sind möglich:

- CPU-Auslastung und `blks_hit` sind korreliert.

  Suchen Sie in diesem Fall die wichtigsten SQL-Anweisungen, die mit der CPU-Auslastung verknüpft sind, und suchen Sie nach Planänderungen. Sie können eine der folgenden Techniken verwenden:

  - Erklären Sie die Pläne manuell und vergleichen Sie sie mit dem erwarteten Ausführungsplan.
  - Achten Sie auf eine Zunahme der Blocktreffer pro Sekunde und lokalen Blocktreffern pro Sekunde. Wählen Sie im Abschnitt Top-SQL des Performance Insights-Dashboards Einstellungen aus.
- CPU-Auslastung und `blks_hit` sind nicht korreliert.

  Stellen Sie in diesem Fall fest, ob einer der folgenden Fälle auftritt:

  - Die Anwendung stellt schnell eine Verbindung zur Datenbank her und trennt sie von dieser.

    Diagnostizieren Sie dieses Verhalten, indem Sie `log_connections` und `log_disconnections` aktivieren und dann die PostgreSQL-Protokolle analysieren. Ziehen Sie in Erwägung, den `pgbadger`-Protokoll-Analyzer zu verwenden. Weitere Informationen finden Sie unter https://github.com/darold/pgbadger.
  - Das Betriebssystem ist überlastet.

    In diesem Fall zeigt Performance Insights, dass Backend-Prozesse länger CPU verbrauchen als gewöhnlich. Suchen Sie in den Metriken von Performance Insights `os.cpuUtilization` oder der Metrik CloudWatch `CPUUtilization` nach Beweisen. Wenn das Betriebssystem überlastet ist, sehen Sie sich Enhanced Monitoring-Metriken an, um eine weitere Diagnose zu erhalten. Schauen Sie sich insbesondere die Prozessliste und den Prozentsatz der CPU an, die von jedem Prozess verbraucht wird.
  - Top SQL-Anweisungen verbrauchen zu viel CPU.

    Untersuchen Sie Anweisungen, die mit der CPU-Auslastung verknüpft sind, um festzustellen, ob sie weniger CPU verbrauchen können. Führen Sie einen `EXPLAIN`-Befehl aus und konzentrieren Sie sich auf die Planknoten, die die größte Auswirkung haben. Erwägen Sie, einen Visualizer

für PostgreSQL-Ausführungspläne zu verwenden. Um dieses Tool auszuprobieren, siehe http://explain.dalibo.com/.

Reagieren auf Workload-Änderungen

Wenn sich Ihre Workload geändert hat, suchen Sie nach folgenden Arten von Änderungen:

Neue Anfragen

Überprüfen Sie, ob die neuen Abfragen erwartet werden. Stellen Sie in diesem Fall sicher, dass ihre Ausführungspläne und die Anzahl der Ausführungen pro Sekunde erwartet werden.

Eine Zunahme der Größe des Datensatzes

Bestimmen Sie, ob die Partitionierung, falls sie noch nicht implementiert ist, helfen könnte. Diese Strategie könnte die Anzahl der Seiten verringern, die eine Abfrage abrufen muss.

Indexpflege oder -erstellung

Überprüfen Sie, ob der Zeitplan für die Wartung erwartet wird. Eine bewährte Methode besteht darin, Wartungsarbeiten außerhalb der Hauptverkehrszeiten zu planen.

Neue Funktionen

Überprüfen Sie, ob diese Funktionen während des Tests erwartungsgemäß funktionieren. Überprüfen Sie insbesondere, ob die Anzahl der Ausführungen pro Sekunde erwartet wird.

Neue Betreiber

Überprüfen Sie, ob sie während des Tests erwartungsgemäß funktionieren.

Eine Zunahme der laufenden parallelen Abfragen

Stellen Sie fest, ob eine der folgenden Situationen aufgetreten ist:

- Die beteiligten Relationen oder Indizes sind plötzlich so groß geworden, dass sie sich deutlich von `min_parallel_table_scan_size` oder `min_parallel_index_scan_size` unterscheiden.
- Die letzten Änderungen wurden an `parallel_setup_cost` oder `parallel_tuple_cost` vorgenommen.
- Die letzten Änderungen wurden an `max_parallel_workers` oder `max_parallel_workers_per_gather` vorgenommen.

io:BuffileRead und io:BuffileWrite

Die Ereignisse `IO:BufFileRead` und `IO:BufFileWrite` treten auf, wenn Aurora PostgreSQL temporäre Dateien erstellt. Wenn Vorgänge mehr Arbeitsspeicher benötigen, als die derzeit definierten Arbeitsspeicherparameter definieren, schreiben sie temporäre Daten in persistenten Speicher. Dieser Vorgang wird manchmal als „Verschütten auf die Festplatte“ bezeichnet.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Context

`IO:BufFileRead` und `IO:BufFileWrite` beziehen sich auf den Arbeitsspeicherbereich und den Wartungsarbeitsspeicherbereich. Weitere Informationen zu diesen lokalen Speicherbereichen finden Sie unter Arbeitsspeicherbereich und Wartungs-Arbeitsspeicherbereich.

Der Standardwert für `work_mem` ist 4 MB. Wenn eine Sitzung parallel Vorgänge ausführt, verwendet jeder Worker, der die Parallelität bearbeitet, 4 MB Speicher. Stellen Sie `work_mem` daher sorgfältig ein. Wenn Sie den Wert zu stark erhöhen, verbraucht eine Datenbank mit vielen Sitzungen möglicherweise zu viel Speicher. Wenn Sie den Wert zu niedrig festlegen, erstellt Aurora PostgreSQL temporäre Dateien im lokalen Speicher. Die Festplatten-I/O für diese temporären Dateien kann die Leistung verringern.

Wenn Sie die folgende Ereignisfolge beobachten, generiert Ihre Datenbank möglicherweise temporäre Dateien:

1. Plötzlicher und starker Rückgang der Verfügbarkeit
2. Schnelle Erholung für den freien Speicherplatz

Möglicherweise sehen Sie auch ein „Kettensäge“ -Muster. Dieses Muster kann darauf hinweisen, dass Ihre Datenbank ständig kleine Dateien erstellt.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Im Allgemeinen werden diese Warteereignisse durch Vorgänge verursacht, die mehr Speicher verbrauchen, als die Parameter `work_mem` oder `maintenance_work_mem` zuweisen. Um dies zu kompensieren, schreiben die Vorgänge in temporäre Dateien. Häufige Ursachen für die `IO:BufFileRead`- und `IO:BufFileWrite`-Ereignisse sind die folgenden:

Abfragen, die mehr Speicher benötigen als im Arbeitsspeicherbereich vorhanden

Abfragen mit den folgenden Merkmalen verwenden den Arbeitsspeicherbereich:

- Hash-Verknüpfungen
- `ORDER BY`-Klausel
- `GROUP BY`-Klausel
- `DISTINCT`
- Fensterfunktionen
- `CREATE TABLE AS SELECT`
- Aktualisierung der materialisierten Ansicht

Anweisungen, die mehr Speicher benötigen als im Arbeitsspeicherbereich für Wartungsarbeiten vorhanden

Die folgenden Anweisungen verwenden den Arbeitsspeicherbereich für Wartungsarbeiten:

- `CREATE INDEX`
- `CLUSTER`

Aktionen

Abhängig von den Ursachen Ihres Wait-Ereignisses empfehlen wir verschiedene Aktionen.

Themen

- Erwägen Sie, Fensterfunktionen anstelle von GROUP-BY-Funktionen zu verwenden
- Untersuchen Sie materialisierte Ansichten und CTAS-Aussagen
- Verwenden Sie pg_repack, wenn Sie Indizes erstellen
- Erhöhen Sie maintenance work_mem, wenn Sie Tabellen clustern
- Optimieren Sie den Speicher, um io:BuffileRead und io:BuffileWrite zu verhindern

Identifizieren Sie das Problem

Nehmen Sie an, dass Performance Insights nicht aktiviert ist und Sie vermuten, dass `IO:BufFileRead` und `IO:BufFileWrite` häufiger als normal auftreten. Gehen Sie wie folgt vor:

1. Untersuchen Sie die Metrik `FreeLocalStorage` in Amazon CloudWatch.
2. Suchen Sie nach einem Kettensägenmuster, bei dem es sich um eine Reihe von gezackten Stacheln handelt.

Ein Kettensägenmuster weist auf einen schnellen Verbrauch und die Freigabe von Speicher hin, die häufig mit temporären Dateien verbunden sind. Wenn Sie dieses Muster bemerken, aktivieren Sie Performance Insights. Wenn Sie Performance Insights verwenden, können Sie feststellen, wann die Wait-Ereignisse auftreten und welche Abfragen mit ihnen verknüpft sind. Ihre Lösung hängt von der spezifischen Abfrage ab, die die Ereignisse verursacht.

Oder stellen Sie den Parameter `log_temp_files` ein. Dieser Parameter protokolliert alle Abfragen, die mehr als Schwellenwert für temporäre Dateien erzeugen. Wenn der Wert `0` ist, protokolliert Aurora PostgreSQL alle temporären Dateien. Wenn der Wert `1024` ist, protokolliert Aurora PostgreSQL alle Abfragen, die temporäre Dateien erzeugen, die größer als 1 MB sind. Weitere Informationen zu `log_temp_files` finden Sie unter Fehlerberichte und -protokollierung in der PostgreSQL-Dokumentation.

Untersuchen Sie Ihre Join-Anfragen

Ihre Anwendung verwendet wahrscheinlich Joins. Die folgende Abfrage verbindet beispielsweise vier Tabellen.

```
SELECT *
       FROM order
 INNER JOIN order_item
       ON (order.id = order_item.order_id)
```

```
 INNER JOIN customer
       ON (customer.id = order.customer_id)
 INNER JOIN customer_address
       ON (customer_address.customer_id = customer.id AND
           order.customer_address_id = customer_address.id)
 WHERE customer.id = 1234567890;
```

Eine mögliche Ursache für Spitzen bei der Verwendung temporärer Dateien ist ein Problem in der Abfrage selbst. Beispielsweise filtert eine defekte Klausel die Joins möglicherweise nicht richtig. Betrachten Sie den zweiten inneren Join im folgenden Beispiel.

```
SELECT *
       FROM order
 INNER JOIN order_item
       ON (order.id = order_item.order_id)
 INNER JOIN customer
       ON (customer.id = customer.id)
 INNER JOIN customer_address
       ON (customer_address.customer_id = customer.id AND
           order.customer_address_id = customer_address.id)
 WHERE customer.id = 1234567890;
```

Die obige Abfrage verknüpft fälschlicherweise `customer.id` mit `customer.id`, wodurch zwischen jedem Kunden und jeder Bestellung ein kartesisches Produkt generiert wird. Diese Art des versehentlichen Joins generiert große temporäre Dateien. Abhängig von der Größe der Tabellen kann eine kartesische Abfrage sogar Speicher füllen. Wenn die folgenden Bedingungen erfüllt sind, hat Ihre Anwendung möglicherweise kartesische Joins:

- Sie sehen einen großen, starken Rückgang der Speicherverfügbarkeit, gefolgt von einer schnellen Wiederherstellung.
- Es werden keine Indizes erstellt.
- Es werden keine `CREATE TABLE FROM SELECT`-Anweisungen ausgegeben.
- Es werden keine materialisierten Ansichten aktualisiert.

Um festzustellen, ob die Tabellen mit den richtigen Schlüsseln verbunden werden, überprüfen Sie Ihre Abfrage- und objektrelationalen Mapping-Anweisungen. Denken Sie daran, dass bestimmte Abfragen Ihrer Anwendung nicht ständig aufgerufen werden und einige Abfragen dynamisch generiert werden.

Überprüfen Sie Ihre ORDER BY- und GROUP BY Anfragen

In einigen Fällen kann eine `ORDER BY`-Klausel zu übermäßig vielen temporären Dateien führen. Berücksichtigen Sie die folgenden Hinweise:

- Schließen Sie Spalten nur dann in eine `ORDER BY`-Klausel ein, wenn sie sortiert werden müssen. Diese Richtlinie ist besonders wichtig für Abfragen, die Tausende von Zeilen zurückgeben und viele Spalten in der `ORDER BY`-Klausel angeben.
- Ziehen Sie in Betracht, Indizes zu erstellen, um `ORDER BY`-Klauseln zu beschleunigen, wenn sie mit Spalten übereinstimmen, die dieselbe aufsteigende oder absteigende Reihenfolge aufweisen. Partielle Indizes sind vorzuziehen, da sie kleiner sind. Kleinere Indizes werden schneller gelesen und durchquert.
- Wenn Sie Indizes für Spalten erstellen, die Nullwerte akzeptieren können, überlegen Sie, ob die Nullwerte am Ende oder am Anfang der Indizes gespeichert werden sollen.

  Reduzieren Sie nach Möglichkeit die Anzahl der Zeilen, die sortiert werden müssen, indem Sie die Ergebnismenge filtern. Wenn Sie `WITH`-Klausel-Anweisungen oder Unterabfragen verwenden, denken Sie daran, dass eine innere Abfrage eine Ergebnismenge generiert und an die äußere Abfrage übergibt. Je mehr Zeilen eine Abfrage herausfiltern kann, desto weniger muss die Abfrage erledigen.
- Wenn Sie nicht die vollständige Ergebnismenge abrufen müssen, verwenden Sie die `LIMIT`-Klausel. Wenn Sie beispielsweise nur die obersten fünf Zeilen benötigen, generiert eine Abfrage mit der `LIMIT`-Klausel keine Ergebnisse. Auf diese Weise benötigt die Abfrage weniger Speicher und temporäre Dateien.

Eine Abfrage, die eine `GROUP BY`-Klausel verwendet, kann auch temporäre Dateien erfordern. `GROUP BY`-Abfragen fassen Werte mithilfe von Funktionen wie den folgenden zusammen:

- `COUNT`
- `AVG`
- `MIN`
- `MAX`
- `SUM`
- `STDDEV`

Befolgen Sie zum Optimieren von `GROUP BY`-Abfragen die Empfehlungen für `ORDER BY`-Abfragen.

Verwenden Sie den DISTINCT-Vorgang nicht

Vermeiden Sie nach Möglichkeit die Verwendung des `DISTINCT`-Vorgangs, um doppelte Zeilen zu entfernen. Je mehr unnötige und doppelte Zeilen Ihre Abfrage zurückgibt, desto teurer wird der `DISTINCT`-Vorgang. Fügen Sie nach Möglichkeit Filter in der `WHERE`-Klausel hinzu, auch wenn Sie dieselben Filter für verschiedene Tabellen verwenden. Das Filtern der Abfrage und der korrekte Beitritt verbessern Ihre Leistung und reduziert den Ressourcennutzung. Es verhindert auch falsche Berichte und Ergebnisse.

Wenn Sie `DISTINCT` für mehrere Zeilen derselben Tabelle verwenden müssen, sollten Sie einen zusammengesetzten Index erstellen. Das Gruppieren mehrerer Spalten in einem Index kann die Zeit zum Auswerten verschiedener Zeilen verbessern. Wenn Sie Amazon-Aurora-PostgreSQL-Version 10 oder höher verwenden, können Sie außerdem mithilfe des `CREATE STATISTICS`-Befehls Statistiken zwischen mehreren Spalten korrelieren.

Erwägen Sie, Fensterfunktionen anstelle von GROUP-BY-Funktionen zu verwenden

Mit `GROUP BY` ändern Sie die Ergebnismenge und rufen dann das aggregierte Ergebnis ab. Mithilfe von Fensterfunktionen aggregieren Sie Daten, ohne die Ergebnismenge zu ändern. Eine Fensterfunktion verwendet die `OVER`-Klausel, um Berechnungen über die von der Abfrage definierten Mengen durchzuführen und eine Zeile mit einer anderen zu korrelieren. Sie können alle `GROUP BY`-Funktionen in Fensterfunktionen verwenden, aber auch Funktionen wie die folgenden verwenden:

- `RANK`
- `ARRAY_AGG`
- `ROW_NUMBER`
- `LAG`
- `LEAD`

Um die Anzahl der temporären Dateien zu minimieren, die von einer Fensterfunktion generiert werden, entfernen Sie Duplikationen für dieselbe Ergebnismenge, wenn Sie zwei verschiedene Aggregationen benötigen. Betrachten Sie folgende Abfrage.

```
SELECT sum(salary) OVER (PARTITION BY dept ORDER BY salary DESC) as sum_salary
     , avg(salary) OVER (PARTITION BY dept ORDER BY salary ASC) as avg_salary
  FROM empsalary;
```

Sie können die Abfrage mit der `WINDOW`-Klausel wie folgt umschreiben.

```
SELECT sum(salary) OVER w as sum_salary
         , avg(salary) OVER w as_avg_salary
    FROM empsalary
  WINDOW w AS (PARTITION BY dept ORDER BY salary DESC);
```

Standardmäßig konsolidiert der Ausführungsplaner von Aurora PostgreSQL ähnliche Knoten, sodass keine Vorgänge dupliziert werden. Durch die Verwendung einer expliziten Deklaration für den Fensterblock können Sie die Abfrage jedoch einfacher pflegen. Sie können die Leistung auch verbessern, indem Sie Doppelarbeit verhindern.

Untersuchen Sie materialisierte Ansichten und CTAS-Aussagen

Wenn eine materialisierte Ansicht aktualisiert wird, wird eine Abfrage ausgeführt. Diese Abfrage kann einen Vorgang wie `GROUP BY`, `ORDER BY` oder `DISTINCT` enthalten. Während einer Aktualisierung können Sie eine große Anzahl temporärer Dateien und die Warteereignisse `IO:BufFileWrite` und `IO:BufFileRead` beobachten. Wenn Sie eine Tabelle basierend auf einer `SELECT`-Anweisung erstellen, führt die `CREATE TABLE`-Anweisung eine Abfrage aus. Um die benötigten temporären Dateien zu reduzieren, optimieren Sie die Abfrage.

Verwenden Sie pg_repack, wenn Sie Indizes erstellen

Wenn Sie einen Index erstellen, ordnet die Engine die Ergebnismenge an. Wenn Tabellen größer werden und die Werte in der indizierten Spalte vielfältiger werden, benötigen die temporären Dateien mehr Speicherplatz. In den meisten Fällen können Sie die Erstellung temporärer Dateien für große Tabellen nicht verhindern, ohne den Speicherbereich für Wartungsarbeiten zu ändern. Weitere Informationen finden Sie unter Wartungs-Arbeitsspeicherbereich.

Eine mögliche Problemumgehung beim Neuerstellen eines großen Index besteht darin, das pg_repack-Tool zu verwenden. Weitere Informationen finden Sie unter Reorganisieren von Tabellen in PostgreSQL-Datenbanken mit minimalen Sperren in der pg_repack-Dokumentation.

Erhöhen Sie maintenance work_mem, wenn Sie Tabellen clustern

Der Befehl `CLUSTER` gruppiert die durch table_name angegebene Tabelle basierend auf einem vorhandenen Index, der durch index_name angegeben wird. Aurora PostgreSQL erstellt die Tabelle physisch so neu, dass sie der Reihenfolge eines bestimmten Indexes entspricht.

Als magnetische Speicherung vorherrschend war, war Clustering üblich, da der Speicherdurchsatz begrenzt war. Jetzt, da SSD-basierter Speicher üblich ist, ist Clustering weniger beliebt. Wenn Sie

jedoch Tabellen clustern, können Sie die Leistung je nach Tabellengröße, Index, Abfrage usw. immer noch geringfügig steigern.

Wenn Sie den Befehl `CLUSTER` ausführen und die Warteereignisse `IO:BufFileWrite` und `IO:BufFileRead` beobachten, stimmen Sie `maintenance_work_mem` ab. Erhöhen Sie die Speichergröße auf einen ziemlich großen Betrag. Ein hoher Wert bedeutet, dass die Engine mehr Speicher für den Clustering-Vorgang verwenden kann.

Optimieren Sie den Speicher, um io:BuffileRead und io:BuffileWrite zu verhindern

In irgendeiner Situation müssen Sie den Speicher abstimmen. Ihr Ziel ist es, die folgenden Anforderungen auszugleichen:

- Der `work_mem`-Wert (siehe Arbeitsspeicherbereich)
- Der Speicher, der nach dem Diskontieren des`shared_buffers`Wert (siehePuffer Pool)
- Die maximale Anzahl geöffneter und verwendeter Verbindungen, die durch `max_connections` begrenzt ist

Erhöhen Sie die Größe des Arbeitsspeicherbereichs

In einigen Situationen besteht Ihre einzige Möglichkeit darin, den von Ihrer Sitzung verwendeten Speicher zu erhöhen. Wenn Ihre Abfragen richtig geschrieben sind und die richtigen Schlüssel für Joins verwenden, sollten Sie den `work_mem`-Wert erhöhen. Weitere Informationen finden Sie unter Arbeitsspeicherbereich.

Um herauszufinden, wie viele temporäre Dateien eine Abfrage generiert, setzen Sie `log_temp_files` auf `0`. Wenn Sie den `work_mem`-Wert auf den in den Protokollen angegebenen Höchstwert erhöhen, verhindern Sie, dass die Abfrage temporäre Dateien generiert. `work_mem` legt jedoch das Maximum pro Planknoten für jede Verbindung oder jeden parallelen Worker fest. Wenn die Datenbank über 5.000 Verbindungen verfügt und jede 256 MiB-Speicher verwendet, benötigt die Engine 1,2 TiB RAM. Daher kann es sein, dass Ihrer Instance der Speicher knapp wird.

Reservieren Sie ausreichend Speicher für den freigegebenen Pufferpool

Ihre Datenbank verwendet Speicherbereiche wie den freigegebenen Pufferpool, nicht nur den Arbeitsspeicherbereich. Berücksichtigen Sie die Anforderungen dieser zusätzlichen Speicherbereiche, bevor Sie `work_mem` erhöhen. Weitere Informationen zum Pufferpool finden Sie unter Puffer Pool.

Angenommen, Ihre Aurora PostgreSQL-Instance-Klasse ist db.r5.2xlarge. Diese Klasse hat 64 GiB Speicher. Standardmäßig sind 75 Prozent des Arbeitsspeichers für den freigegebenen Pufferpool reserviert. Nachdem Sie den dem Shared Memory-Bereich zugewiesenen Betrag abgezogen haben, bleiben 16.384 MB übrig. Weisen Sie den verbleibenden Speicher nicht ausschließlich dem Arbeitsspeicherbereich zu, da das Betriebssystem und die Engine ebenfalls Speicher benötigen.

Der Speicher, den Sie `work_mem` zuordnen können, hängt von der Instance-Klasse ab. Wenn Sie eine größere Instance-Klasse verwenden, ist mehr Speicher verfügbar. Im vorhergehenden Beispiel können Sie jedoch nicht mehr als 16 GiB verwenden. Andernfalls ist Ihre Instance nicht verfügbar, wenn ihr der Speicher ausgeht. Um die Instance aus dem nicht verfügbaren Status wiederherzustellen, werden die Aurora PostgreSQL-Automatisierungsdienste automatisch neu gestartet.

Verwalten der Anzahl der Verbindungen

Angenommen, Ihre Datenbank-Instance hat 5.000 gleichzeitige Verbindungen. Jede Verbindung verwendet mindestens 4 MB `work_mem`. Der hohe Speicherverbrauch der Verbindungen dürfte die Leistung beeinträchtigen. Als Reaktion darauf haben Sie die folgenden Optionen:

- Aktualisieren Sie auf eine größere Instance-Klasse.
- Verringern Sie die Anzahl gleichzeitiger Datenbankverbindungen mit einem Verbindungsproxy oder Pooler.

Berücksichtigen Sie bei Proxys Amazon RDS Proxy, PGBouncer oder einen auf Ihrer Anwendung basierenden Verbindungspooler. Diese Lösung lindert die CPU-Last. Es reduziert auch das Risiko, wenn alle Verbindungen den Arbeitsspeicherbereich benötigen. Wenn weniger Datenbankverbindungen vorhanden sind, können Sie den Wert von `work_mem` erhöhen. Auf diese Weise reduzieren Sie das Auftreten der `IO:BufFileRead`- und `IO:BufFileWrite`-Warteereignisse. Auch die Abfragen, die auf den Arbeitsspeicherbereich warten, beschleunigen sich erheblich.

IO:DataFileRead

Das `IO:DataFileRead`-Ereignis tritt auf, wenn eine Verbindung darauf wartet, dass ein Backend-Prozess eine erforderliche Seite aus dem Speicher liest, da die Seite nicht im gemeinsam genutzten Speicher verfügbar ist.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Kontext

Alle Abfragen und Datenmanipulationsvorgänge (DML) greifen auf Seiten im Pufferpool zu. Zu den Anweisungen, die Lesevorgänge auslösen können, gehören `SELECT`, `UPDATE` und `DELETE`. Ein `UPDATE` kann beispielsweise Seiten aus Tabellen oder Indizes lesen. Wenn sich die angeforderte oder aktualisierte Seite nicht im gemeinsam genutzten Pufferpool befindet, kann dieser Lesevorgang zum `IO:DataFileRead`-Ereignis führen.

Da der gemeinsame Pufferpool endlich ist, kann er sich füllen. In diesem Fall zwingen Anfragen nach Seiten, die sich nicht im Speicher befinden, die Datenbank dazu, Blöcke von der Festplatte zu lesen. Wenn das `IO:DataFileRead`-Ereignis häufig auftritt, ist Ihr gemeinsam genutzter Pufferpool möglicherweise zu klein für Ihre Workload. Dieses Problem ist bei `SELECT`-Abfragen akut, die eine große Anzahl von Zeilen lesen, die nicht in den Pufferpool passen. Weitere Informationen zum Pufferpool finden Sie unter Puffer Pool.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Häufige Ursachen für das Ereignis `IO:DataFileRead` sind die folgenden:

Verbindungsspitzen

> Möglicherweise finden Sie mehrere Verbindungen, die die gleiche Anzahl von io:DataFileRead-Wait-Ereignissen erzeugen. In diesem Fall kann eine Spitze (plötzlicher und starker Anstieg) bei `IO:DataFileRead`-Ereignissen auftreten.

SELECT- und DML-Anweisungen, die sequentielle Scans durchführen

> Ihre Anwendung führt möglicherweise einen neuen Vorgang aus. Oder ein vorhandener Vorgang könnte sich aufgrund eines neuen Ausführungsplans ändern. Suchen Sie in solchen Fällen

nach Tabellen (insbesondere großen Tabellen), die einen größeren `seq_scan`-Wert haben. Finden Sie sie, indem Sie `pg_stat_user_tables` abfragen. Verwenden Sie die Erweiterung `pg_stat_statements`, um Abfragen zu verfolgen, die mehr Lesevorgänge generieren.

CTAS und CREATE INDEX für große Datensätze

Ein CTAS ist eine `CREATE TABLE AS SELECT`-Anweisung. Wenn Sie ein CTAS mit einem großen Datensatz als Quelle ausführen oder einen Index für eine große Tabelle erstellen, kann das `IO:DataFileRead`-Ereignis auftreten. Wenn Sie einen Index erstellen, muss die Datenbank möglicherweise das gesamte Objekt mithilfe eines sequentiellen Scans lesen. Ein CTAS generiert `IO:DataFile`-Reads, wenn Seiten nicht im Speicher sind.

Mehrere Vakuumarbeiter laufen gleichzeitig

Vakuumarbeiter können manuell oder automatisch ausgelöst werden. Wir empfehlen, eine aggressive Vakuumstrategie zu verabschieden. Wenn eine Tabelle jedoch viele aktualisierte oder gelöschte Zeilen enthält, erhöhen sich die `IO:DataFileRead`-Wartezeiten. Nachdem der Raum zurückgewonnen wurde, nimmt die für `IO:DataFileRead` aufgewendete Vakuumzeit ab.

Aufnahme großer Datenmengen

Wenn Ihre Anwendung große Datenmengen aufnimmt, können `ANALYZE`-Vorgänge häufiger auftreten. Der `ANALYZE`-Prozess kann durch einen Autovacuum Launcher ausgelöst oder manuell aufgerufen werden.

Der `ANALYZE`-Vorgang liest eine Teilmenge der Tabelle. Die Anzahl der zu scannenden Seiten wird berechnet, indem 30 mit dem `default_statistics_target`-Wert multipliziert wird. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation. Der Parameter `default_statistics_target` akzeptiert Werte zwischen 1 und 10.000, wobei der Standardwert 100 ist.

Hungertod

Wenn Netzwerkbandbreite oder CPU der Instance verbraucht werden, kann das `IO:DataFileRead`-Ereignis häufiger auftreten.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Themen

- Überprüfen Sie Prädikatfilter auf Abfragen, die Wartezeiten generieren
- Minimieren Sie die Auswirkungen von Wartungsvorgängen
- Reagieren Sie auf eine hohe Anzahl von Verbindungen

Überprüfen Sie Prädikatfilter auf Abfragen, die Wartezeiten generieren

Angenommen, Sie identifizieren bestimmte Abfragen, die `IO:DataFileRead`-Warteereignisse generieren. Sie können sie mit den folgenden Techniken identifizieren:

- Performance Insights
- Katalogansichten wie die der Erweiterung `pg_stat_statements`
- Die Katalogansicht `pg_stat_all_tables`, wenn sie periodisch eine erhöhte Anzahl von physischen Lesevorgängen anzeigt
- Die `pg_statio_all_tables`-Ansicht, wenn sie zeigt, dass `_read`-Zähler steigen

Wir empfehlen Ihnen, zu bestimmen, welche Filter im Prädikat (`WHERE`-Klausel) dieser Abfragen verwendet werden. Befolgen Sie diese Richtlinien:

- Führen Sie den Befehl `EXPLAIN` aus. Geben Sie in der Ausgabe an, welche Arten von Scans verwendet werden. Ein sequentieller Scan weist nicht zwangsläufig ein Problem an. Abfragen, die sequenzielle Scans verwenden, erzeugen im Vergleich zu Abfragen, die Filter verwenden, natürlich mehr `IO:DataFileRead`-Ereignisse.

  Finden Sie heraus, ob die in der `WHERE`-Klausel aufgeführte Spalte indiziert ist. Wenn nicht, erwägen Sie, einen Index für diese Spalte zu erstellen. Dieser Ansatz vermeidet die sequentiellen Scans und reduziert die `IO:DataFileRead`-Ereignisse. Wenn eine Abfrage restriktive Filter enthält und immer noch sequenzielle Scans erzeugt, bewerten Sie, ob die richtigen Indizes verwendet werden.
- Finden Sie heraus, ob die Abfrage auf eine sehr große Tabelle zugreift. In einigen Fällen kann das Partitionieren einer Tabelle die Leistung verbessern, sodass die Abfrage nur notwendige Partitionen lesen kann.
- Untersuchen Sie die Kardinalität (Gesamtzahl der Zeilen) Ihrer Join-Vorgänge. Beachten Sie, wie restriktiv die Werte sind, die Sie den Filtern für Ihre `WHERE`-Klausel übergeben. Wenn möglich, stimmen Sie Ihre Abfrage ein, um die Anzahl der Zeilen zu reduzieren, die in jedem Schritt des Plans übergeben werden.

Minimieren Sie die Auswirkungen von Wartungsvorgängen

Wartungsvorgänge wie `VACUUM` und `ANALYZE` sind wichtig. Wir empfehlen, sie nicht zu deaktivieren, da Sie `IO:DataFileRead`-Warteereignisse im Zusammenhang mit diesen Wartungsvorgängen finden. Die folgenden Ansätze können die Auswirkungen dieser Vorgänge minimieren:

- Führen Sie Wartungsvorgänge während außerhalb der Hauptverkehrszeiten manuell aus. Diese Technik verhindert, dass die Datenbank den Schwellenwert für automatische Vorgänge erreicht.
- Erwägen Sie bei sehr großen Tabellen, die Tabelle zu partitionieren. Diese Technik reduziert den Overhead von Wartungsvorgängen. Die Datenbank greift nur auf die Partitionen zu, die gewartet werden müssen.
- Wenn Sie große Datenmengen aufnehmen, sollten Sie die Funktion zur automatischen Analyse deaktivieren.

Die Auto-Vakuum-Funktion wird automatisch für eine Tabelle ausgelöst, wenn die folgende Formel zutrifft.

```
pg_stat_user_tables.n_dead_tup > (pg_class.reltuples x autovacuum_vacuum_scale_factor)
 + autovacuum_vacuum_threshold
```

Die Ansicht `pg_stat_user_tables` und der Katalog `pg_class` haben mehrere Zeilen. Eine Zeile kann einer Zeile in Ihrer Tabelle entsprechen. Diese Formel geht davon aus, dass die `reltuples` für eine bestimmte Tabelle stehen. Die Parameter `autovacuum_vacuum_scale_factor` (standardmäßig 0.20) und `autovacuum_vacuum_threshold` (standardmäßig 50 Tupel) werden normalerweise global für die gesamte Instance gesetzt. Sie können jedoch verschiedene Werte für eine bestimmte Tabelle festlegen.

Themen

- Suchen Sie nach Tabellen, die unnötigerweise Speicherplatz belegen.
- Finden Sie Indizes mit unnötigem Speicherplatz
- Finden Sie Tabellen, die für die automatische Vakuumierung berechtigt sind

Suchen Sie nach Tabellen, die unnötigerweise Speicherplatz belegen.

Um Tabellen zu finden, die mehr Speicherplatz belegen als nötig, führen Sie die folgende Abfrage aus. Wenn diese Abfrage von einer Datenbankbenutzerrolle ausgeführt wird, die nicht über die

`rds_superuser`-Rolle verfügt, gibt sie nur Informationen zu den Tabellen zurück, für die die Benutzerrolle Leserechte besitzt. Diese Abfrage wird von PostgreSQL Version 12 und späteren Versionen unterstützt.

```
WITH report AS (
   SELECT   schemaname
           ,tblname
           ,n_dead_tup
           ,n_live_tup
           ,block_size*tblpages AS real_size
           ,(tblpages-est_tblpages)*block_size AS extra_size
           ,CASE WHEN tblpages - est_tblpages > 0
              THEN 100 * (tblpages - est_tblpages)/tblpages::float
              ELSE 0
            END AS extra_ratio, fillfactor, (tblpages-est_tblpages_ff)*block_size AS
 bloat_size
           ,CASE WHEN tblpages - est_tblpages_ff > 0
              THEN 100 * (tblpages - est_tblpages_ff)/tblpages::float
              ELSE 0
            END AS bloat_ratio
           ,is_na
    FROM (
          SELECT  ceil( reltuples / ( (block_size-page_hdr)/tpl_size ) ) +
 ceil( toasttuples / 4 ) AS est_tblpages
                 ,ceil( reltuples / ( (block_size-page_hdr)*fillfactor/
(tpl_size*100) ) ) + ceil( toasttuples / 4 ) AS est_tblpages_ff
                 ,tblpages
                 ,fillfactor
                 ,block_size
                 ,tblid
                 ,schemaname
                 ,tblname
                 ,n_dead_tup
                 ,n_live_tup
                 ,heappages
                 ,toastpages
                 ,is_na
            FROM (
                  SELECT ( 4 + tpl_hdr_size + tpl_data_size + (2*ma)
                             - CASE WHEN tpl_hdr_size%ma = 0 THEN ma ELSE
 tpl_hdr_size%ma END
                             - CASE WHEN ceil(tpl_data_size)::int%ma = 0 THEN ma ELSE
 ceil(tpl_data_size)::int%ma END
```

```
                            ) AS tpl_size
                            ,block_size - page_hdr AS size_per_block
                            ,(heappages + toastpages) AS tblpages
                            ,heappages
                            ,toastpages
                            ,reltuples
                            ,toasttuples
                            ,block_size
                            ,page_hdr
                            ,tblid
                            ,schemaname
                            ,tblname
                            ,fillfactor
                            ,is_na
                            ,n_dead_tup
                            ,n_live_tup
                           FROM (
                                 SELECT  tbl.oid                       AS tblid
                                        ,ns.nspname                    AS schemaname
                                        ,tbl.relname                   AS tblname
                                        ,tbl.reltuples                 AS reltuples
                                        ,tbl.relpages                  AS heappages
                                        ,coalesce(toast.relpages, 0)   AS toastpages
                                        ,coalesce(toast.reltuples, 0)  AS toasttuples
                                        ,psat.n_dead_tup               AS n_dead_tup
                                        ,psat.n_live_tup               AS n_live_tup
                                        ,24                            AS page_hdr
                                        ,current_setting('block_size')::numeric AS
 block_size

 ,coalesce(substring( array_to_string(tbl.reloptions, ' ') FROM
 'fillfactor=([0-9]+)')::smallint, 100) AS fillfactor
                                        ,CASE WHEN version()~'mingw32' OR version()~'64-
bit|x86_64|ppc64|ia64|amd64' THEN 8 ELSE 4 END        AS ma
                                        ,23 + CASE WHEN MAX(coalesce(null_frac,0)) > 0
 THEN ( 7 + count(*) ) / 8 ELSE 0::int END              AS tpl_hdr_size
                                        ,sum( (1-coalesce(s.null_frac, 0)) *
 coalesce(s.avg_width, 1024) )                                  AS tpl_data_size
                                        ,bool_or(att.atttypid =
 'pg_catalog.name'::regtype) OR count(att.attname) <> count(s.attname)        AS is_na
                                   FROM  pg_attribute       AS att
                                   JOIN  pg_class           AS tbl    ON (att.attrelid =
 tbl.oid)
```

```
                                    JOIN  pg_stat_all_tables AS psat   ON (tbl.oid =
 psat.relid)
                                    JOIN  pg_namespace       AS ns     ON (ns.oid =
 tbl.relnamespace)
                               LEFT JOIN  pg_stats           AS s      ON
 (s.schemaname=ns.nspname AND s.tablename = tbl.relname AND s.inherited=false AND
 s.attname=att.attname)
                               LEFT JOIN  pg_class           AS toast  ON
 (tbl.reltoastrelid = toast.oid)
                                   WHERE  att.attnum > 0
                                     AND  NOT att.attisdropped
                                     AND  tbl.relkind = 'r'
                                GROUP BY  tbl.oid, ns.nspname, tbl.relname,
 tbl.reltuples, tbl.relpages, toastpages, toasttuples, fillfactor, block_size, ma,
 n_dead_tup, n_live_tup
                                ORDER BY  schemaname, tblname
                              ) AS s
                  ) AS s2
       ) AS s3
 ORDER BY bloat_size DESC
)
  SELECT *
    FROM report
   WHERE bloat_ratio != 0
 -- AND schemaname = 'public'
 -- AND tblname = 'pgbench_accounts'
;

-- WHERE NOT is_na
--   AND tblpages*((pst).free_percent + (pst).dead_tuple_percent)::float4/100 >= 1
```

Sie können in Ihrer Anwendung nach einer Überlastung von Tabellen und Indizes suchen. Weitere Informationen finden Sie unter

Sie können PostgreSQL Multiversion Concurrency Control (MVCC) verwenden, um die Datenintegrität zu wahren. PostgreSQL MVCC funktioniert, indem es eine interne Kopie aktualisierter oder gelöschter Zeilen (auch Tupel genannt) speichert, bis für eine Transaktion entweder ein Commit oder ein Rollback ausgeführt wird. Diese gespeicherte interne Kopie ist für Benutzer nicht sichtbar. Wenn diese nicht sichtbaren Kopien nicht regelmäßig von den Dienstprogrammen VACUUM oder AUTOVACUUM bereinigt werden, kann es jedoch zu einer Überlastung der Tabelle kommen. Wenn diese Option nicht aktiviert ist, kann die Überlastung der Tabelle zu erhöhten Speicherkosten führen und Ihre Verarbeitungsgeschwindigkeit verlangsamen.

In vielen Fällen reichen die Standardeinstellungen für VACUUM oder AUTOVACUUM in Aurora aus, um eine ungewollte Überlastung von Tabellen zu vermeiden. Möglicherweise möchten Sie jedoch überprüfen, ob eine Überlastung vorliegt, wenn in Ihrer Anwendung die folgenden Bedingungen vorliegen:

- Verarbeitet eine große Anzahl von Transaktionen in relativ kurzer Zeit zwischen VACUUM-Prozessen.

- Funktioniert schlecht und der Speicherplatz ist knapp.

Sammeln Sie zunächst möglichst genaue Informationen darüber, wie viel Speicherplatz tote Tupel belegen und wie viel Sie wiederherstellen können, indem Sie die Überlastung der Tabellen und Indizes bereinigen. Verwenden Sie dazu die `pgstattuple`-Erweiterung, um Statistiken über Ihren Aurora-Cluster zu sammeln. Weitere Informationen finden Sie unter pgstattuple. Die Berechtigungen zum Verwenden der `pgstattuple`-Erweiterung sind auf die Rolle `pg_stat_scan_tables` und die Datenbank-Superuser beschränkt.

Um die `pgstattuple`-Erweiterung in Aurora zu erstellen, verbinden Sie eine Client-Sitzung mit dem Cluster, z. B. psql oder pgAdmin, und verwenden Sie den folgenden Befehl:

```
CREATE EXTENSION pgstattuple;
```

Erstellen Sie die Erweiterung in jeder Datenbank, für die Sie ein Profil erstellen möchten. Verwenden Sie nach dem Erstellen der Erweiterung die Befehlszeilenschnittstelle (CLI), um zu messen, wie viel unbenutzbaren Speicherplatz Sie zurückgewinnen können. Bevor Sie Statistiken sammeln, ändern Sie die Cluster-Parametergruppe, indem Sie AUTOVACUUM auf 0 festlegen. Die Einstellung 0 verhindert, dass Aurora automatisch alle toten Tupel bereinigt, die Ihre Anwendung hinterlassen hat, was sich auf die Genauigkeit der Ergebnisse auswirken kann. Verwenden Sie den folgenden Befehl, um eine einfache Tabelle zu erstellen:

```
postgres=> CREATE TABLE lab AS SELECT generate_series (0,100000);
```

```
SELECT 100001
```

Im folgenden Beispiel führen wir die Abfrage mit aktiviertem AUTOVACUUM für den DB-Cluster aus. Der Wert `dead_tuple_count` ist 0, was bedeutet, dass AUTOVACUUM die veralteten Daten oder Tupel aus der PostgreSQL-Datenbank gelöscht hat.

Wenn Sie Informationen über die Tabelle mit `pgstattuple` sammeln möchten, geben Sie in der Abfrage den Namen einer Tabelle oder eine Objektkennung (OID) an:

```
postgres=> SELECT * FROM pgstattuple('lab');
```

```
table_len  | tuple_count | tuple_len | tuple_percent | dead_tuple_count |
 dead_tuple_len | dead_tuple_percent | free_space | free_percent
-----------+-------------+-----------+---------------+------------------
+----------------+--------------------+------------+--------------
3629056    | 100001      | 2800028   | 77.16         | 0                | 0
  | 0                 | 16616      | 0.46
(1 row)
```

In der folgenden Abfrage schalten wir AUTOVACUUM aus und geben einen Befehl ein, mit dem 25 000 Zeilen aus der Tabelle gelöscht werden. Infolgedessen steigt der Wert `dead_tuple_count` auf 25 000.

```
postgres=> DELETE FROM lab WHERE generate_series < 25000;
```

```
DELETE 25000
```

```
SELECT * FROM pgstattuple('lab');
```

Beobachten von Überlastungen ohne Unterbrechung Ihrer Anwendung

Die Einstellungen in einem Aurora-Cluster sind optimiert, um die bewährten Methoden für die meisten Workloads bereitzustellen. Möglicherweise möchten Sie jedoch einen Cluster optimieren, damit er besser zu Ihren Anwendungen und Nutzungsmustern passt. In diesem Fall können Sie die `pgstattuple`-Erweiterung verwenden, ohne eine aktive Anwendung zu unterbrechen. Führen Sie dazu die folgenden Schritte aus:

1. Klonen Sie Ihre Aurora-Instance.
2. Ändern Sie die Parameterdatei, um AUTOVACUUM im Klon zu deaktivieren.
3. Führen Sie eine `pgstattuple`-Abfrage durch, während Sie den Klon mit einem Beispiel-Workload oder mit pgbench testen, einem Programm zum Ausführen von Benchmark-Tests in PostgreSQL. Weitere Informationen finden Sie unter pgbench.

Nachdem Sie Ihre Anwendungen ausgeführt und das Ergebnis angezeigt haben, verwenden Sie pg_repack oder VACUUM FULL für die wiederhergestellte Kopie und vergleichen Sie die Unterschiede. Wenn Sie einen deutlichen Rückgang der Werte dead_tuple_count, dead_tuple_len oder dead_tuple_percent feststellen, passen Sie den Bereinigungsplan Ihres Produktions-Clusters an, um die Überlastung zu minimieren.

Vermeiden von Überlastung in temporären Tabellen

Wenn Ihre Anwendung temporäre Tabellen erstellt, vergewissern Sie sich, dass Ihre Anwendung diese temporären Tabellen entfernt, wenn sie nicht mehr benötigt werden. Automatische Bereinigungsprozesse finden keine temporären Tabellen. Wenn diese Option nicht aktiviert ist, können temporäre Tabellen schnell zu einer Überlastung der Datenbank führen. Darüber hinaus kann sich die Überlastung auf die Systemtabellen ausweiten. Hierbei handelt es sich um interne Tabellen, die PostgreSQL-Objekte und -Attribute verfolgen, wie pg_attribute und pg_depend.

Wenn eine temporäre Tabelle nicht mehr benötigt wird, können Sie eine TRUNCATE-Anweisung verwenden, um die Tabelle zu leeren und Speicherplatz freizugeben. Bereinigen Sie dann die Tabellen pg_attribute und pg_depend manuell. Durch das Bereinigen dieser Tabellen wird sichergestellt, dass durch das kontinuierliche Erstellen und Kürzen/Löschen temporärer Tabellen keine Tupel hinzugefügt werden und das System nicht überlastet wird.

Sie können dieses Problem beim Erstellen einer temporären Tabelle vermeiden, indem Sie die folgende Syntax verwenden, die die neuen Zeilen löscht, wenn für Inhalt ein Commit ausgeführt wird:

```
CREATE TEMP TABLE IF NOT EXISTS table_name(table_description) ON COMMIT DELETE ROWS;
```

Die `ON COMMIT DELETE ROWS`-Klausel kürzt die temporäre Tabelle, wenn für die Transaktion ein Commit ausgeführt wird.

Vermeiden von Überlastung in Indizes

Wenn Sie ein indiziertes Feld in einer Tabelle ändern, führt die Indexaktualisierung zu einem oder mehreren toten Tupeln in diesem Index. Standardmäßig entfernt der automatische Bereinigungsprozess überflüssige Indizes, aber diese Bereinigung erfordert einen erheblichen Zeit- und Ressourcenaufwand. Um die Einstellungen für die Indexbereinigung beim Erstellen einer Tabelle anzugeben, schließen Sie die Klausel vacuum_index_cleanup ein. Standardmäßig ist die Klausel bei der Tabellenerstellung auf AUTO gesetzt, was bedeutet, dass der Server entscheidet, ob Ihr Index bereinigt werden muss, wenn er die Tabelle bereinigt. Sie können die Klausel auf EIN einstellen, um die Indexbereinigung für eine bestimmte Tabelle zu aktivieren, oder auf AUS, um die Indexbereinigung für diese Tabelle zu deaktivieren. Denken Sie daran, dass das Deaktivieren der Indexbereinigung zwar Zeit sparen kann, aber möglicherweise zu einer Überlastung des Index führen kann.

Sie können die Indexbereinigung manuell steuern, wenn Sie eine Tabelle über die Befehlszeile bereinigen. Wenn Sie eine Tabelle bereinigen und tote Tupel aus den Indizes entfernen möchten, schließen Sie die INDEX_CLEANUP-Klausel mit dem Wert EIN und dem Tabellennamen ein:

```
acctg=> VACUUM (INDEX_CLEANUP ON) receivables;
```

```

```

```
INFO: aggressively vacuuming "public.receivables"
```

```
VACUUM
```

Wenn Sie eine Tabelle bereinigen möchten, ohne die Indizes zu bereinigen, geben Sie den Wert AUS an:

```
acctg=> VACUUM (INDEX_CLEANUP OFF) receivables;
```

```

```

```
INFO: aggressively vacuuming "public.receivables"
```



```
VACUUM
```

.

Finden Sie Indizes mit unnötigem Speicherplatz

Um Indizes zu finden, die unnötigen Speicherplatz benötigen, führen Sie die folgende Abfrage aus.

```
-- WARNING: run with a nonsuperuser role, the query inspects
-- only indexes on tables you have permissions to read.
-- WARNING: rows with is_na = 't' are known to have bad statistics ("name" type is not
 supported).
-- This query is compatible with PostgreSQL 8.2 and later.

SELECT current_database(), nspname AS schemaname, tblname, idxname,
 bs*(relpages)::bigint AS real_size,
  bs*(relpages-est_pages)::bigint AS extra_size,
  100 * (relpages-est_pages)::float / relpages AS extra_ratio,
  fillfactor, bs*(relpages-est_pages_ff) AS bloat_size,
  100 * (relpages-est_pages_ff)::float / relpages AS bloat_ratio,
  is_na
  -- , 100-(sub.pst).avg_leaf_density, est_pages, index_tuple_hdr_bm,
  -- maxalign, pagehdr, nulldatawidth, nulldatahdrwidth, sub.reltuples, sub.relpages
  -- (DEBUG INFO)
FROM (
  SELECT coalesce(1 +
       ceil(reltuples/floor((bs-pageopqdata-pagehdr)/(4+nulldatahdrwidth)::float)), 0
       -- ItemIdData size + computed avg size of a tuple (nulldatahdrwidth)
    ) AS est_pages,
    coalesce(1 +
       ceil(reltuples/floor((bs-pageopqdata-pagehdr)*fillfactor/
(100*(4+nulldatahdrwidth)::float))), 0
    ) AS est_pages_ff,
    bs, nspname, table_oid, tblname, idxname, relpages, fillfactor, is_na
    -- , stattuple.pgstatindex(quote_ident(nspname)||'.'||quote_ident(idxname)) AS
 pst,
    -- index_tuple_hdr_bm, maxalign, pagehdr, nulldatawidth, nulldatahdrwidth,
 reltuples
    -- (DEBUG INFO)
  FROM (
    SELECT maxalign, bs, nspname, tblname, idxname, reltuples, relpages, relam,
 table_oid, fillfactor,
      ( index_tuple_hdr_bm +
          maxalign - CASE -- Add padding to the index tuple header to align on MAXALIGN
            WHEN index_tuple_hdr_bm%maxalign = 0 THEN maxalign
            ELSE index_tuple_hdr_bm%maxalign
          END
```

```
       + nulldatawidth + maxalign - CASE -- Add padding to the data to align on
MAXALIGN
           WHEN nulldatawidth = 0 THEN 0
           WHEN nulldatawidth::integer%maxalign = 0 THEN maxalign
           ELSE nulldatawidth::integer%maxalign
         END
     )::numeric AS nulldatahdrwidth, pagehdr, pageopqdata, is_na
     -- , index_tuple_hdr_bm, nulldatawidth -- (DEBUG INFO)
   FROM (
     SELECT
       i.nspname, i.tblname, i.idxname, i.reltuples, i.relpages, i.relam, a.attrelid
AS table_oid,
       current_setting('block_size')::numeric AS bs, fillfactor,
       CASE -- MAXALIGN: 4 on 32bits, 8 on 64bits (and mingw32 ?)
         WHEN version() ~ 'mingw32' OR version() ~ '64-bit|x86_64|ppc64|ia64|amd64'
THEN 8
         ELSE 4
       END AS maxalign,
       /* per page header, fixed size: 20 for 7.X, 24 for others */
       24 AS pagehdr,
       /* per page btree opaque data */
       16 AS pageopqdata,
       /* per tuple header: add IndexAttributeBitMapData if some cols are null-able */
       CASE WHEN max(coalesce(s.null_frac,0)) = 0
         THEN 2 -- IndexTupleData size
         ELSE 2 + (( 32 + 8 - 1 ) / 8)
         -- IndexTupleData size + IndexAttributeBitMapData size ( max num filed per
index + 8 - 1 /8)
       END AS index_tuple_hdr_bm,
       /* data len: we remove null values save space using it fractionnal part from
stats */
       sum( (1-coalesce(s.null_frac, 0)) * coalesce(s.avg_width, 1024)) AS
nulldatawidth,
       max( CASE WHEN a.atttypid = 'pg_catalog.name'::regtype THEN 1 ELSE 0 END ) > 0
AS is_na
     FROM pg_attribute AS a
       JOIN (
         SELECT nspname, tbl.relname AS tblname, idx.relname AS idxname,
           idx.reltuples, idx.relpages, idx.relam,
           indrelid, indexrelid, indkey::smallint[] AS attnum,
           coalesce(substring(
             array_to_string(idx.reloptions, ' ')
              from 'fillfactor=([0-9]+)')::smallint, 90) AS fillfactor
         FROM pg_index
```

```
            JOIN pg_class idx ON idx.oid=pg_index.indexrelid
            JOIN pg_class tbl ON tbl.oid=pg_index.indrelid
            JOIN pg_namespace ON pg_namespace.oid = idx.relnamespace
          WHERE pg_index.indisvalid AND tbl.relkind = 'r' AND idx.relpages > 0
        ) AS i ON a.attrelid = i.indexrelid
        JOIN pg_stats AS s ON s.schemaname = i.nspname
          AND ((s.tablename = i.tblname AND s.attname =
 pg_catalog.pg_get_indexdef(a.attrelid, a.attnum, TRUE))
          -- stats from tbl
          OR  (s.tablename = i.idxname AND s.attname = a.attname))
          -- stats from functionnal cols
        JOIN pg_type AS t ON a.atttypid = t.oid
      WHERE a.attnum > 0
      GROUP BY 1, 2, 3, 4, 5, 6, 7, 8, 9
    ) AS s1
  ) AS s2
    JOIN pg_am am ON s2.relam = am.oid WHERE am.amname = 'btree'
) AS sub
-- WHERE NOT is_na
ORDER BY 2,3,4;
```

Finden Sie Tabellen, die für die automatische Vakuumierung berechtigt sind

Führen Sie die folgende Abfrage aus, um Tabellen zu finden, die für die automatische Vakuumierung berechtigt sind.

```
--This query shows tables that need vacuuming and are eligible candidates.
--The following query lists all tables that are due to be processed by autovacuum.
-- During normal operation, this query should return very little.
WITH  vbt AS (SELECT setting AS autovacuum_vacuum_threshold
              FROM pg_settings WHERE name = 'autovacuum_vacuum_threshold')
    , vsf AS (SELECT setting AS autovacuum_vacuum_scale_factor
              FROM pg_settings WHERE name = 'autovacuum_vacuum_scale_factor')
    , fma AS (SELECT setting AS autovacuum_freeze_max_age
              FROM pg_settings WHERE name = 'autovacuum_freeze_max_age')
    , sto AS (SELECT opt_oid, split_part(setting, '=', 1) as param,
                split_part(setting, '=', 2) as value
              FROM (SELECT oid opt_oid, unnest(reloptions) setting FROM pg_class) opt)
SELECT
    '"'||ns.nspname||'"."'||c.relname||'"' as relation
    , pg_size_pretty(pg_table_size(c.oid)) as table_size
    , age(relfrozenxid) as xid_age
```

```
    , coalesce(cfma.value::float, autovacuum_freeze_max_age::float)
 autovacuum_freeze_max_age
    , (coalesce(cvbt.value::float, autovacuum_vacuum_threshold::float) +
         coalesce(cvsf.value::float,autovacuum_vacuum_scale_factor::float) *
 c.reltuples)
         as autovacuum_vacuum_tuples
    , n_dead_tup as dead_tuples
FROM pg_class c
JOIN pg_namespace ns ON ns.oid = c.relnamespace
JOIN pg_stat_all_tables stat ON stat.relid = c.oid
JOIN vbt on (1=1)
JOIN vsf ON (1=1)
JOIN fma on (1=1)
LEFT JOIN sto cvbt ON cvbt.param = 'autovacuum_vacuum_threshold' AND c.oid =
 cvbt.opt_oid
LEFT JOIN sto cvsf ON cvsf.param = 'autovacuum_vacuum_scale_factor' AND c.oid =
 cvsf.opt_oid
LEFT JOIN sto cfma ON cfma.param = 'autovacuum_freeze_max_age' AND c.oid = cfma.opt_oid
WHERE c.relkind = 'r'
AND nspname <> 'pg_catalog'
AND (
    age(relfrozenxid) >= coalesce(cfma.value::float, autovacuum_freeze_max_age::float)
    or
    coalesce(cvbt.value::float, autovacuum_vacuum_threshold::float) +
      coalesce(cvsf.value::float,autovacuum_vacuum_scale_factor::float) * c.reltuples
 <= n_dead_tup
    -- or 1 = 1
)
ORDER BY age(relfrozenxid) DESC;
```

Reagieren Sie auf eine hohe Anzahl von Verbindungen

Wenn Sie Amazon CloudWatch überwachen, stellen Sie möglicherweise fest, dass die `DatabaseConnections`-Metrik ansteigt. Dieser Anstieg deutet auf eine erhöhte Anzahl von Verbindungen zu Ihrer Datenbank hin. Wir empfehlen folgende Vorgehensweise:

- Beschränken Sie die Anzahl der Verbindungen, die die Anwendung mit jeder Instance öffnen kann. Wenn Ihre Anwendung über eine eingebettete Verbindungspool-Funktion verfügt, legen Sie eine angemessene Anzahl von Verbindungen fest. Basieren Sie die Zahl darauf, was die vCPUs in Ihrer Instance effektiv parallelisieren können.

Wenn Ihre Anwendung keine Verbindungspool-Funktion verwendet, sollten Sie den Amazon RDS Proxy oder eine Alternative in Betracht ziehen. Mit diesem Ansatz können Ihre Anwendung mehrere Verbindungen mit dem Load Balancer öffnen. Der Balancer kann dann eine begrenzte Anzahl von Verbindungen mit der Datenbank öffnen. Da weniger Verbindungen parallel laufen, führt Ihre DB-Instance weniger Kontextwechsel im Kernel durch. Abfragen sollten schneller voranschreiten und zu weniger Warteereignissen führen. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

- Nutzen Sie nach Möglichkeit die Reader-Knoten für Aurora PostgreSQL und lesen Sie Replikate für RDS für PostgreSQL. Wenn Ihre Anwendung einen schreibgeschützten Vorgang ausführt, senden Sie diese Anfragen an den reader-Endpunkt. Diese Technik verbreitet Anwendungsanfragen auf alle Reader-Knoten, wodurch der I/O-Druck auf den Writer-Knoten reduziert wird.
- Ziehen Sie, Ihre DB-Instance zu skalieren. Eine Instance-Klasse mit höherer Kapazität bietet mehr Speicher, was Aurora PostgreSQL einen größeren freigegebenen Pufferpool zum Speichern von Seiten gibt. Die größere Größe gibt der DB-Instance auch mehr vCPUs für die Handhabung von Verbindungen. Mehr vCPUs sind besonders hilfreich, wenn die Vorgänge, die `IO:DataFileRead`-Warteereignisse generieren, Schreibvorgänge sind.

IO:XactSync

Das `IO:XactSync` Ereignis tritt ein, wenn die Datenbank darauf wartet, dass das Aurora-Storage-Subsystem den Commit einer regulären Transaktion bzw. den Commit oder Rollback einer vorbereiteten Transaktion ausführt. Eine vorbereitete Transaktion ist Teil des Supports von PostgreSQL für einen zweiphasigen Commit.

Themen

- Unterstützte Engine-Versionen
- Context
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Context

Das Ereignis `IO:XactSync` zeigt an, dass die Instance-Zeit damit verbringt, darauf zu warten, dass das Aurora-Speichersubsystem bestätigt, dass Transaktionsdaten verarbeitet wurden.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `IO:XactSync`-Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die folgenden typischen Ursachen:

Netzwerksättigung

Der Datenverkehr zwischen Clients und der DB-Instance oder der Datenverkehr zum Speicher-Subsystem ist möglicherweise zu hoch für die Netzwerkbandbreite.

CPU-Druck

Eine hohe Workload könnte verhindern, dass der Aurora-Speicher-Daemon genügend CPU-Zeit erhält.

Aktionen

Abhängig von den Ursachen Ihres Wait-Ereignisses empfehlen wir verschiedene Aktionen.

Themen

- Überwachen Sie Ihre Ressourcen
- Hochskalieren Sie die CPU
- Erhöhung der Netzwerkbandbreite
- Reduzieren Sie die Anzahl der Commits

Überwachen Sie Ihre Ressourcen

Um die Ursache der erhöhten `IO:XactSync`-Ereignisse zu ermitteln, überprüfen Sie die folgenden Metriken:

- `WriteThroughput` und `CommitThroughput` – Änderungen des Schreibdurchsatzes oder des Commit-Durchsatzes können eine Zunahme der Workload anzeigen.
- `WriteLatency` und `CommitLatency` – Änderungen der Schreib- oder Commit-Latenz können darauf hinweisen, dass das Speichersubsystem zu mehr Arbeit aufgefordert wird.

- `CPUUtilization` – Wenn die CPU-Auslastung der Instance über 90 Prozent liegt, erhält der Aurora-Speicher-Daemon möglicherweise nicht genügend Zeit auf der CPU. In diesem Fall verschlechtert sich die I/O-Leistung.

Informationen zu diesen Metriken finden Sie unter Metriken auf Instance-Ebene für Amazon Aurora.

Hochskalieren Sie die CPU

Um Probleme mit CPU-Hunger zu beheben, sollten Sie in Betracht ziehen, zu einem Instance-Typ mit mehr CPU-Kapazität zu wechseln. Informationen zur CPU-Kapazität für eine DB-Instance-Klasse finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.

Erhöhung der Netzwerkbandbreite

Um festzustellen, ob die Instance ihre Netzwerkbandbreitenlimits erreicht, suchen Sie nach den folgenden anderen Warteereignissen:

- `IO:DataFileRead`, `IO:BufferRead`, `IO:BufferWrite` und `IO:XactWrite` – Abfragen, die große Mengen an I/O verwenden, können mehr dieser Warteereignisse generieren.
- `Client:ClientRead` und`Client:ClientWrite` – Abfragen mit großen Mengen an Client-Kommunikation können mehr dieser Warteereignisse generieren.

Wenn die Netzwerkbandbreite ein Problem darstellt, sollten Sie erwägen, zu einem Instance-Typ mit mehr Netzwerkbandbreite zu wechseln. Informationen zur Netzwerkleistung für eine DB-Instance-Klasse finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.

Reduzieren Sie die Anzahl der Commits

Um die Anzahl der Commits zu reduzieren, kombinieren Sie Anweisungen in Transaktionsblöcken.

IPC:DamRecordTxAck

Das `IPC:DamRecordTxAck`-Ereignis tritt auf, wenn Aurora PostgreSQL in einer Sitzung, die Datenbank-Aktivitätsstreams verwendet, ein Aktivitätsstream-Ereignis generiert und dann wartet, bis dieses Ereignis dauerhaft wird.

Themen

- Relevante Engine-Versionen
- Kontext

Relevante Engine-Versionen

Diese Warteereignisinformationen sind für alle Aurora PostgreSQL 10.7 und höher 10 Versionen, 11.4 und höher 11 Versionen sowie alle 12 und 13 Versionen relevant.

Kontext

Im synchronen Modus wird die Dauerhaftigkeit von Aktivitätsstream-Ereignissen gegenüber der Datenbankleistung bevorzugt. Während auf ein dauerhaftes Schreiben des Ereignisses gewartet wird, blockiert die Sitzung andere Datenbankaktivitäten, was das `IPC:DamRecordTxAck`-Warteereignis verursacht.

Ursachen

Die häufigste Ursache für das Auftreten des `IPC:DamRecordTxAck`-Ereignisses in Top-Waits ist, dass die Funktion Database Activity Streams (DAS) ein ganzheitliches Audit ist. Eine höhere SQL-Aktivität generiert Aktivitätsstream-Ereignisse, die aufgezeichnet werden müssen.

Aktionen

Abhängig von den Ursachen Ihres Wait-Ereignisses empfehlen wir verschiedene Aktionen:

- Reduzieren Sie die Anzahl der SQL-Anweisungen oder deaktivieren Sie Datenbank-Aktivitätsströme. Dadurch wird die Anzahl der Ereignisse reduziert, die dauerhafte Schreibvorgänge erfordern.
- Wechseln Sie in den asynchronen Modus. Dadurch können Konflikte beim `IPC:DamRecordTxAck`-Warteereignis reduziert werden.

  Die DAS-Funktion kann jedoch nicht die Haltbarkeit jedes Ereignisses im asynchronen Modus garantieren.

Lock:advisory

Das `Lock:advisory`-Ereignis tritt auf, wenn eine PostgreSQL-Anwendung eine Sperre verwendet, um Aktivitäten über mehrere Sitzungen hinweg zu koordinieren.

Themen

Relevante Engine-Versionen

Diese Warteereignisinformationen sind für Aurora PostgreSQL Versionen 9.6 und höher relevant.

Context

PostgreSQL-Beratungssperren sind Anwendungsebene, kooperative Sperren werden explizit durch den Anwendungscode des Benutzers gesperrt und freigeschaltet. Eine Anwendung kann PostgreSQL-Beratungssperren verwenden, um Aktivitäten über mehrere Sitzungen hinweg zu koordinieren. Im Gegensatz zu normalen Sperren auf Objekt- oder Zeilenebene hat die Anwendung die volle Kontrolle über die Lebensdauer des Schlosses. Weitere Informationen finden Sie unter Empfohlene Sperren in der PostgreSQL-Dokumentation.

Beratungssperren können vor dem Ende einer Transaktion freigegeben werden oder von einer Sitzung über Transaktionen hinweg gehalten werden. Dies gilt nicht für implizite, vom System erzwungene Sperren, wie z. B. eine zugriffsexklusive Sperre für eine Tabelle, die von einer `CREATE INDEX`-Anweisung abgerufen wird.

Eine Beschreibung der Funktionen zum Erlangen (Sperren) und Freigeben (Entsperren) von Advisory Locks finden Sie unter Advisory Lock Functions in der PostgreSQL-Dokumentation.

Advisory Locks werden zusätzlich zum regulären PostgreSQL-Locking-System implementiert und sind in der `pg_locks`-Systemansicht sichtbar.

Ursachen

Dieser Schlosstyp wird ausschließlich von einer Anwendung gesteuert, die ihn explizit verwendet. Beratungssperren, die für jede Zeile als Teil einer Abfrage erworben werden, können zu einem Anstieg der Sperren oder zu einem langfristigen Aufbau führen.

Diese Effekte treten auf, wenn die Abfrage so ausgeführt wird, dass Sperren für mehr Zeilen erwirbt, als von der Abfrage zurückgegeben werden. Die Anwendung muss schließlich jede Sperre

freigeben, aber wenn Sperren für Zeilen erworben werden, die nicht zurückgegeben werden, kann die Anwendung nicht alle Sperren finden.

Das folgende Beispiel stammt aus Empfohlene Sperren in der PostgreSQL-Dokumentation.

```
SELECT pg_advisory_lock(id) FROM foo WHERE id > 12345 LIMIT 100;
```

In diesem Beispiel kann die `LIMIT`-Klausel die Ausgabe der Abfrage nur stoppen, nachdem die Zeilen bereits intern ausgewählt und ihre ID-Werte gesperrt wurden. Dies kann plötzlich passieren, wenn ein wachsendes Datenvolumen dazu führt, dass der Planer einen anderen Ausführungsplan auswählt, der während der Entwicklung nicht getestet wurde. Der Aufbau erfolgt in diesem Fall, weil die Anwendung `pg_advisory_unlock` explizit für jeden gesperrten ID-Wert aufruft. In diesem Fall kann es jedoch nicht die Sperren finden, die für Zeilen erworben wurden, die nicht zurückgegeben wurden. Da die Sperren auf Sitzungsebene erworben werden, werden sie am Ende der Transaktion nicht automatisch freigegeben.

Eine weitere mögliche Ursache für Spikes bei blockierten Sperrversuchen sind unbeabsichtigte Konflikte. In diesen Konflikten teilen sich nicht verwandte Teile der Anwendung versehentlich denselben Sperren-ID-Raum.

Aktionen

Überprüfen Sie die Anwendungsnutzung von Beratungssperren und Details, wo und wann im Anwendungsablauf jede Art von Beratungssperre erworben und freigegeben wird.

Stellen Sie fest, ob eine Sitzung zu viele Sperren erwirbt oder eine lang andauernde Sitzung keine Sperren früh genug freigibt, was zu einem langsamen Aufbau von Sperren führt. Sie können einen langsamen Aufbau von Sperren auf Sitzungsebene korrigieren, indem Sie die Sitzung mit `pg_terminate_backend(pid)` beenden.

Ein Client, der auf eine Beratungssperre wartet, erscheint in `pg_stat_activity` mit `wait_event_type=Lock` und `wait_event=advisory`. Sie können bestimmte Sperrwerte erhalten, indem Sie die `pg_locks`-Systemansicht nach demselben `pid` abfragen und nach `locktype=advisory` und `granted=f` suchen.

Sie können dann die blockierende Sitzung identifizieren, indem Sie `pg_locks` nach derselben beratenden Sperre mit `granted=t` abfragen, wie im folgenden Beispiel gezeigt.

```
SELECT blocked_locks.pid AS blocked_pid,
```

```
        blocking_locks.pid AS blocking_pid,
        blocked_activity.usename AS blocked_user,
        blocking_activity.usename AS blocking_user,
        now() - blocked_activity.xact_start AS blocked_transaction_duration,
        now() - blocking_activity.xact_start AS blocking_transaction_duration,
        concat(blocked_activity.wait_event_type,':',blocked_activity.wait_event) AS
blocked_wait_event,
        concat(blocking_activity.wait_event_type,':',blocking_activity.wait_event) AS
blocking_wait_event,
        blocked_activity.state AS blocked_state,
        blocking_activity.state AS blocking_state,
        blocked_locks.locktype AS blocked_locktype,
        blocking_locks.locktype AS blocking_locktype,
        blocked_activity.query AS blocked_statement,
        blocking_activity.query AS blocking_statement
   FROM pg_catalog.pg_locks blocked_locks
   JOIN pg_catalog.pg_stat_activity blocked_activity ON blocked_activity.pid =
blocked_locks.pid
   JOIN pg_catalog.pg_locks blocking_locks
       ON blocking_locks.locktype = blocked_locks.locktype
       AND blocking_locks.DATABASE IS NOT DISTINCT FROM blocked_locks.DATABASE
       AND blocking_locks.relation IS NOT DISTINCT FROM blocked_locks.relation
       AND blocking_locks.page IS NOT DISTINCT FROM blocked_locks.page
       AND blocking_locks.tuple IS NOT DISTINCT FROM blocked_locks.tuple
       AND blocking_locks.virtualxid IS NOT DISTINCT FROM blocked_locks.virtualxid
       AND blocking_locks.transactionid IS NOT DISTINCT FROM
blocked_locks.transactionid
       AND blocking_locks.classid IS NOT DISTINCT FROM blocked_locks.classid
       AND blocking_locks.objid IS NOT DISTINCT FROM blocked_locks.objid
       AND blocking_locks.objsubid IS NOT DISTINCT FROM blocked_locks.objsubid
       AND blocking_locks.pid != blocked_locks.pid
   JOIN pg_catalog.pg_stat_activity blocking_activity ON blocking_activity.pid =
blocking_locks.pid
   WHERE NOT blocked_locks.GRANTED;
```

Alle API-Funktionen für beratende Sperren haben zwei Sätze von Argumenten, entweder ein `bigint`-Argument oder zwei `integer`-Argumente:

- Bei den API-Funktionen mit einem `bigint`-Argument befinden sich die oberen 32 Bit in `pg_locks.classid` und die unteren 32 Bit in `pg_locks.objid`.
- Bei den API-Funktionen mit zwei `integer`-Argumenten ist das erste Argument `pg_locks.classid` und das zweite Argument ist `pg_locks.objid`.

Der `pg_locks.objsubid`-Wert gibt an, welches API-Formular verwendet wurde: 1 bedeutet ein `bigint`-Argument; 2 bedeutet zwei `integer`-Argumente.

Lock:extend

Das `Lock:extend`-Ereignis tritt ein, wenn ein Backend-Prozess darauf wartet, eine Beziehung zu sperren, um sie zu erweitern, während ein anderer Prozess diese Beziehung für denselben Zweck gesperrt hat.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Kontext

Das Ereignis `Lock:extend` zeigt an, dass ein Backend-Prozess darauf wartet, eine Beziehung zu erweitern, für die ein anderer Backend-Prozess eine Sperre hält, während er diese Beziehung erweitert. Da jeweils nur ein Prozess eine Beziehung erweitern kann, generiert das System ein `Lock:extend`-Warteereignis. `INSERT`-, `COPY`- und `UPDATE`-Vorgänge können dieses Ereignis erzeugen.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `Lock:extend`-Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die folgenden typischen Ursachen:

Anstieg der gleichzeitigen Einfügungen oder Aktualisierungen derselben Tabelle

> Es kann zu einer Zunahme der Anzahl gleichzeitiger Sitzungen mit Abfragen kommen, die in dieselbe Tabelle einfügen oder aktualisieren.

Unzureichende Netzwerkbandbreite

Die Netzwerkbandbreite auf der DB-Instance reicht möglicherweise nicht aus, um die Speicherkommunikationsanforderungen der aktuellen Workload zu gewährleisten. Dies kann zu einer Speicherlatenz führen, die zu einem Anstieg der `Lock:extend`-Ereignisse führt.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Themen

- Reduzieren Sie gleichzeitige Einfügungen und Aktualisierungen auf dieselbe Beziehung
- Erhöhung der Netzwerkbandbreite

Reduzieren Sie gleichzeitige Einfügungen und Aktualisierungen auf dieselbe Beziehung

Stellen Sie zunächst fest, ob die `tup_inserted`- und `tup_updated`-Metriken und damit auch dieses Warteereignis gestiegen ist. Überprüfen Sie in diesem Fall, welche Beziehungen für Einfüge- und Aktualisierungsvorgänge in hohem Streit stehen. Um dies zu ermitteln, fragen Sie die `pg_stat_all_tables`-Ansicht nach den Werten in den `n_tup_ins`- und `n_tup_upd`-Feldern ab. Informationen zur Ansicht `pg_stat_all_tables` finden Sie unter pg_stat_all_tables in der PostgreSQL-Dokumentation.

Um weitere Informationen über das Blockieren und blockierte Abfragen zu erhalten, fragen Sie `pg_stat_activity` wie im folgenden Beispiel ab:

```
SELECT
    blocked.pid,
    blocked.usename,
    blocked.query,
    blocking.pid AS blocking_id,
    blocking.query AS blocking_query,
    blocking.wait_event AS blocking_wait_event,
    blocking.wait_event_type AS blocking_wait_event_type
FROM pg_stat_activity AS blocked
JOIN pg_stat_activity AS blocking ON blocking.pid = ANY(pg_blocking_pids(blocked.pid))
where
blocked.wait_event = 'extend'
and blocked.wait_event_type = 'Lock';
```

```
   pid  | usename  |            query             | blocking_id |
            blocking_query                          | blocking_wait_event |
 blocking_wait_event_type
  ------+----------+------------------------------+-------------
+-------------------------------------------------------------------
+---------------------+--------------------------
   7143 |  myuser  | insert into tab1 values (1); |        4600 | INSERT INTO tab1 (a)
 SELECT s FROM generate_series(1,1000000) s; | DataFileExtend      | IO
```

Nachdem Sie Beziehungen identifiziert haben, die zur Erhöhung von `Lock:extend`-Ereignissen beitragen, verwenden Sie die folgenden Techniken, um die Konflikte zu reduzieren:

- Finden Sie heraus, ob Sie Partitionierung verwenden können, um die Konflikte für dieselbe Tabelle zu reduzieren. Das Trennen eingefügter oder aktualisierter Tupel in verschiedene Partitionen kann die Konflikte verringern. Weitere Informationen zur Partitionierung finden Sie unter Verwalten von PostgreSQL-Partitionen mit der Erweiterung pg_partman.
- Wenn das Warteereignis hauptsächlich auf Aktualisierungsaktivitäten zurückzuführen ist, sollten Sie erwägen, den Füllfaktor-Wert der Beziehung zu reduzieren. Dies kann Anfragen nach neuen Blöcken während des Updates reduzieren. Der Füllfaktor ist ein Speicherparameter für eine Tabelle, der den maximalen Speicherplatz zum Packen einer Tabellenseite bestimmt. Es wird als Prozentsatz des gesamten Speicherplatzes für eine Seite ausgedrückt. Weitere Informationen zum Parameter fillfactor finden Sie unter CREATE TABLE in der PostgreSQL-Dokumentation.

> **Important**
>
> Wir empfehlen dringend, Ihr System zu testen, wenn Sie den Füllfaktor ändern, da sich die Änderung dieses Wertes je nach Workload negativ auf die Leistung auswirken kann.

Erhöhung der Netzwerkbandbreite

Um zu sehen, ob die Schreiblatenz zunimmt, überprüfen Sie die `WriteLatency`-Metrik in CloudWatch. Wenn ja, verwenden Sie die Amazon CloudWatch-Metriken von `WriteThroughput` und `ReadThroughput`, um den speicherbezogenen Datenverkehr auf dem DB-Cluster zu überwachen. Diese Metriken können Ihnen helfen festzustellen, ob die Netzwerkbandbreite für die Speicheraktivität Ihrer Workload ausreicht.

Wenn Ihre Netzwerkbandbreite nicht ausreicht, erhöhen Sie sie. Wenn Ihre DB-Instance die Grenzen der Netzwerkbandbreite erreicht, besteht die einzige Möglichkeit, die Bandbreite zu erhöhen, darin, die Größe Ihrer DB-Instance zu erhöhen.

Weitere Informationen zu CloudWatch-Metriken finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora. Informationen zur Netzwerkleistung für jede DB-Instance-Klasse finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.

Lock:Relation

Das `Lock:Relation`-Ereignis tritt ein, wenn eine Abfrage darauf wartet, eine Sperre für eine Tabelle oder Sicht (Relation) zu erhalten, die derzeit von einer anderen Transaktion gesperrt ist.

Themen

- Unterstützte Engine-Versionen
- Context
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Context

Die meisten PostgreSQL-Befehle verwenden implizit Sperren, um den gleichzeitigen Zugriff auf Daten in Tabellen zu steuern. Sie können diese Sperren auch explizit mit dem `LOCK`-Befehl in Ihrem Anwendungscode verwenden. Viele Sperrmodi sind nicht miteinander kompatibel und können Transaktionen blockieren, wenn sie versuchen, auf dasselbe Objekt zuzugreifen. In diesem Fall generiert Aurora PostgreSQL ein `Lock:Relation`-Ereignis. Einige gängige Beispiele sind die folgenden:

- Exklusive Sperren wie `ACCESS EXCLUSIVE` können alle gleichzeitigen Zugriffe blockieren. Vorgänge in der Datendefinitionssprache (DDL) wie `DROP TABLE`, `TRUNCATE`, `VACUUM FULL` und `CLUSTER` erwerben implizit `ACCESS EXCLUSIVE`-Sperren. `ACCESS EXCLUSIVE` ist auch der Standardsperrmodus für `LOCK TABLE`-Anweisungen, die keinen Modus explizit angeben.

- Die Verwendung von `CREATE INDEX (without CONCURRENT)` für eine Tabelle steht in Konflikt mit den DML-Anweisungen `UPDATE`, `DELETE` und `INSERT`, die `ROW EXCLUSIVE`-Sperren anfordern.

Weitere Informationen zu Sperren auf Tabellenebene und widersprüchlichen Sperrmodi finden Sie unter Explizite Sperren in der PostgreSQL-Dokumentation.

Blockieren von Abfragen und Transaktionen entsperren in der Regel auf eine der folgenden Arten:

- Blockierende Abfrage — Die Anwendung kann die Abfrage abbrechen oder der Benutzer kann den Prozess beenden. Die Engine kann die Abfrage auch aufgrund des Statement-Timeouts einer Sitzung oder eines Deadlock-Erkennungsmechanismus zum Ende zwingen.
- Blockieren einer Transaktion – Eine Transaktion stoppt die Blockierung, wenn sie eine `ROLLBACK`- oder `COMMIT`-Anweisung ausführt. Rollbacks erfolgen auch automatisch, wenn Sitzungen von einem Client oder durch Netzwerkprobleme getrennt oder beendet werden. Sitzungen können beendet werden, wenn das Datenbank-Engine heruntergefahren wird, wenn das System keinen Arbeitsspeicher mehr hat usw.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `Lock:Relation`-Ereignis häufiger als normal auftritt, kann dies auf ein Leistungsproblem hinweisen. Zu den typischen Ursachen zählen auch die Folgenden:

Gleichzeitige Sitzungen mit widersprüchlichen Tabellensperren erhöht

Es kann zu einer Zunahme der Anzahl gleichzeitiger Sitzungen mit Abfragen kommen, die dieselbe Tabelle mit widersprüchlichen Sperrmodi sperren.

Wartungsvorgänge

Zustandswartungsvorgänge wie `VACUUM` und `ANALYZE` können die Anzahl widersprüchlicher Sperren erheblich erhöhen. `VACUUM FULL` erhält eine `ACCESS EXCLUSIVE`-Sperre und `ANALYSE` erhält eine `SHARE UPDATE EXCLUSIVE`-Sperre. Beide Arten von Sperren können ein `Lock:Relation`-Wait-Ereignis verursachen. Wartungsvorgänge für Anwendungsdaten wie das Aktualisieren einer materialisierten Ansicht können auch blockierte Abfragen und Transaktionen erhöhen.

Sperrt bei Reader-In

Es könnte ein Konflikt zwischen den Beziehungssperren bestehen, die vom Writer und den Readern gehalten werden. Derzeit werden nur `ACCESS EXCLUSIVE`-Beziehungssperren auf Reader-Instances repliziert. Allerdings gerät die `ACCESS EXCLUSIVE`-Beziehungssperre in Konflikt mit jeder `ACCESS SHARE`-Beziehungssperre, die vom Reader gehalten wird. Dies kann zu einer Erhöhung der Warteereignisse für die Sperrbeziehung des Readers führen.

Aktionen

Abhängig von den Ursachen Ihres Wait-Ereignisses empfehlen wir verschiedene Aktionen.

Themen

- Reduzieren Sie die Auswirkungen der Blockierung von SQL-Anweisungen
- Minimieren Sie die Auswirkungen von Wartungsvorgängen
- Auf Lesersperren überprüfen

Reduzieren Sie die Auswirkungen der Blockierung von SQL-Anweisungen

Um die Auswirkungen des Blockierens von SQL-Anweisungen zu reduzieren, ändern Sie Ihren Anwendungscode nach Möglichkeit. Es folgen zwei gängige Techniken zum Reduzieren von Blöcken:

- Verwenden Sie die Option `NOWAIT` – Einige SQL-Befehle, wie z. B. `SELECT`- und `LOCK`-Anweisungen, unterstützen diese Option. Die `NOWAIT`-Direktive bricht die Sperre anfordernde Abfrage ab, wenn die Sperre nicht sofort erworben werden kann. Diese Technik kann dazu beitragen, zu verhindern, dass eine Blockiersitzung eine Anhäufung blockierter Sitzungen dahinter verursacht.

  Beispiel: Angenommen, Transaktion A wartet auf eine Sperre, die von Transaktion B gehalten wird. Wenn B nun eine Sperre für eine Tabelle anfordert, die durch Transaktion C gesperrt ist, könnte Transaktion A blockiert werden, bis die Transaktion C abgeschlossen ist. Wenn Transaktion B jedoch ein `NOWAIT` verwendet, wenn sie die Sperre für C anfordert, kann sie schnell fehlschlagen und sicherstellen, dass Transaktion A nicht unbegrenzt warten muss.
- Verwenden Sie `SET lock_timeout` – Legen Sie einen `lock_timeout`-Wert fest, um die Zeit zu begrenzen, die eine SQL-Anweisung wartet, um eine Sperre für eine Beziehung zu erhalten. Wenn die Sperre nicht innerhalb des angegebenen Timeouts erworben wird, wird die Transaktion, die die Sperre anfordert, abgebrochen. Stellen Sie diesen Wert auf Sitzungsebene ein.

Minimieren Sie die Auswirkungen von Wartungsvorgängen

Wartungsvorgänge wie `VACUUM` und `ANALYZE` sind wichtig. Wir empfehlen, sie nicht zu deaktivieren, da Sie `Lock:Relation`-Warteereignisse im Zusammenhang mit diesen Wartungsvorgängen finden. Die folgenden Ansätze können die Auswirkungen dieser Vorgänge minimieren:

- Führen Sie Wartungsvorgänge während außerhalb der Hauptverkehrszeiten manuell aus.
- Um `Lock:Relation`-Wartezeiten zu reduzieren, die durch Autovacuum-Aufgaben verursacht werden, führen Sie alle erforderlichen Autovacuum-Optimierungen durch. Informationen zum Optimieren von Autovacuum finden Sie unter Arbeiten mit PostgreSQL Autovacuum auf Amazon RDS im Amazon RDS-Benutzerhandbuch.

Auf Lesersperren überprüfen

Sie können sehen, wie gleichzeitige Sitzungen bei einem Autor und Lesern Sperren halten, die sich gegenseitig blockieren. Eine Möglichkeit dazu besteht darin, Abfragen auszuführen, die den Sperrtyp und die Beziehung zurückgeben. Die Tabelle enthält eine Abfolge von Abfragen zu zwei solchen gleichzeitigen Sitzungen, eine Writer-Sitzung (linke Spalte) und eine Reader-Sitzung (rechte Spalte).

Der Wiedergabeprozess wartet die Dauer von `max_standby_streaming_delay` ab, bevor die Reader-Abfrage abgebrochen wird. Wie im Beispiel gezeigt, liegt das Sperr-Timeout von 100 ms deutlich unter dem standardmäßigen `max_standby_streaming_delay`-Wert von 30 Sekunden. Für die Sperre tritt ein Timeout auf, bevor ein Problem entsteht.

Writer session	Lesersitzung

`export WRITER=aurorapg1.1234567891 0.us-west-1.rds.amazonaws.com`
 	
`psql -h $WRITER`
`psql (15devel, server 10.14)`
`Type "help" for help.`
	`export READER=aurorapg2.1234567891 0.us-west-1.rds.amazonaws.com`
	
	`psql -h $READER`
	`psql (15devel, server 10.14)`
	`Type "help" for help.`

Die Writer-Sitzung erstellt die Tabelle `t1` auf der Writer-Instance. Die `ACCESS EXCLUSIVE`-Sperre wird sofort auf dem Writer erworben, vorausgesetzt, es gibt keine widersprüchlichen Abfragen für den Writer.

Writer session

```
postgres=> CREATE TABLE t1(b
 integer);
CREATE TABLE
```

Lesersitzung

Die Lesesitzung legt ein Sperr-Timeout-Intervall von 100 Millisekunden fest.

```
postgres=> SET lock_timeout=100;
SET
```

Die Reader-Session versucht, Daten aus der Tabelle `t1` auf der Reader-Instance zu lesen.

```
postgres=> SELECT * FROM t1;
 b
---
(0 rows)
```

Die Writer-Sitzung lässt `t1` fallen.

```
postgres=> BEGIN;
BEGIN
postgres=> DROP TABLE t1;
DROP TABLE
postgres=>
```

Die Abfrage ist abgelaufen und wird im Reader abgebrochen.

```
postgres=> SELECT * FROM t1;
ERROR:  canceling statement due to
 lock timeout
LINE 1: SELECT * FROM t1;
                      ^
```

Die Lesesitzung fragt `pg_locks` und `pg_stat_activity` ab, um die Fehlerursache zu ermitteln. Das Ergebnis zeigt an, dass der `aurora wal replay`-Prozess eine `ACCESS EXCLUSIVE` -Sperre für Tabelle `t1` hält.

Writer session

Lesersitzung

```
postgres=> SELECT locktype, relation,
 mode, backend_type
postgres-> FROM pg_locks l, pg_stat_a
ctivity t1
postgres-> WHERE l.pid=t1.pid AND
 relation = 't1'::regclass::oid;
 locktype | relation |        mode
    |   backend_type
----------+----------+----------
-----------+------------------
 relation | 68628525 | AccessExc
lusiveLock | aurora wal replay
(1 row)
```

Lock:transactionid

Das `Lock:transactionid`-Ereignis tritt ein, wenn eine Transaktion auf eine Sperre auf Zeilenebene wartet.

Themen

- Unterstützte Engine-Versionen
- Context
- Wahrscheinliche Ursachen für erhöhte Wartezeiten
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Context

Das Ereignis `Lock:transactionid` tritt ein, wenn eine Transaktion versucht, eine Sperre auf Zeilenebene zu erlangen, die bereits einer gleichzeitig laufenden Transaktion gewährt wurde. Die Sitzung, die das `Lock:transactionid`-Wait-Ereignis anzeigt, ist aufgrund dieser Sperre blockiert.

Nachdem die blockierende Transaktion entweder in einer COMMIT- oder ROLLBACK-Anweisung endet, kann die blockierte Transaktion fortgesetzt werden.

Die Semantik der Multiversions-Parallelität von Aurora PostgreSQL garantiert, dass Leser keine Autoren blockieren und Autoren Leser nicht blockieren. Damit Konflikte auf Zeilenebene auftreten können, müssen blockierende und blockierte Transaktionen widersprüchliche Anweisungen der folgenden Typen ausgeben:

- UPDATE
- SELECT … FOR UPDATE
- SELECT … FOR KEY SHARE

Die Anweisung SELECT … FOR KEY SHARE ist ein Sonderfall. Die Datenbank verwendet die Klausel FOR KEY SHARE, um die Leistung der referenziellen Integrität zu optimieren. Eine Sperre auf Zeilenebene für eine Zeile kann INSERT-, UPDATE- und DELETE-Befehle für andere Tabellen blockieren, die auf die Zeile verweisen.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn dieses Ereignis mehr als normal auftritt, sind die Ursache normalerweise UPDATE-, SELECT … FOR UPDATE-, SELECT … FOR KEY SHARE-Anweisungen in Kombination mit den folgenden Bedingungen.

Themen

- Hohe Gleichzeitigkeit
- Leerlauf in Transaktion
- Lang laufende Transaktionen

Hohe Gleichzeitigkeit

Aurora PostgreSQL kann eine körnige Sperrsemantik auf Zeilenebene verwenden. Die Wahrscheinlichkeit von Konflikten auf Zeilenebene steigt, wenn die folgenden Bedingungen erfüllt sind:

- Eine sehr gleichzeitige Workload beansprucht dieselben Zeilen.
- Parallelbetrieb steigt.

Leerlauf in Transaktion

Manchmal zeigt die Spalte `pg_stat_activity.state` den Wert `idle in transaction` an. Dieser Wert wird für Sitzungen angezeigt, die eine Transaktion gestartet, aber noch kein `COMMIT` oder `ROLLBACK` ausgegeben haben. Wenn der `pg_stat_activity.state`-Wert nicht `active` ist, ist die in `pg_stat_activity` angezeigte Abfrage die letzte, die ausgeführt wurde. Die blockierende Sitzung verarbeitet eine Abfrage nicht aktiv, da eine offene Transaktion eine Sperre hält.

Wenn eine Leerlauf-Transaktion eine Sperre auf Zeilenebene erworben hat, kann dies verhindern, dass andere Sitzungen sie erwerben. Diese Bedingung führt zu einem häufigen Auftreten des Warteereignisses `Lock:transactionid`. Um das Problem zu diagnostizieren, überprüfen Sie die Ausgabe von `pg_stat_activity` und `pg_locks`.

Lang laufende Transaktionen

Transaktionen, die lange laufen, erhalten lange Zeit Sperren. Diese langjährigen Sperren können die Ausführung anderer Transaktionen verhindern.

Aktionen

Zeilensperre ist ein Konflikt zwischen `UPDATE`-, `SELECT … FOR UPDATE`- oder `SELECT … FOR KEY SHARE`-Anweisungen. Bevor Sie eine Lösung versuchen, sollten Sie herausfinden, wann diese Anweisungen in derselben Zeile ausgeführt werden. Wählen Sie mit diesen Informationen eine in den folgenden Abschnitten beschriebene Strategie aus.

Themen

Reagieren auf hohe Parallelbetrieb

Wenn Parallelität das Problem darstellt, versuchen Sie eine der folgenden Techniken:

- Senken Sie die Parallelität in der Anwendung. Verringern Sie beispielsweise die Anzahl der aktiven Sitzungen.
- Implementieren Sie einen Verbindungspool. Informationen zum Poolen von Verbindungen mit RDS-Proxy finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

- Entwerfen Sie die Anwendung oder das Datenmodell, um konkurrierende `UPDATE`- und `SELECT … FOR UPDATE`-Anweisungen zu vermeiden. Sie können auch die Anzahl der Fremdschlüssel verringern, auf die von `SELECT … FOR KEY SHARE`-Anweisungen zugegriffen wird.

Reagieren Sie auf ungenutzte Transaktionen

Wenn `pg_stat_activity.state idle in transaction` anzeigt, verwenden Sie die folgenden Strategien:

- Schalten Sie nach Möglichkeit Autocommit ein. Dieser Ansatz verhindert, dass Transaktionen andere Transaktionen blockieren, während sie auf ein `COMMIT` oder `ROLLBACK` warten.
- Suchen Sie nach Codepfaden, denen `COMMIT`, `ROLLBACK` oder `END` fehlt.
- Stellen Sie sicher, dass die Ausnahmebehandlungslogik in Ihrer Anwendung immer einen Pfad zu einem gültigen `end of transaction` hat.
- Stellen Sie sicher, dass Ihre Anwendung Abfrageergebnisse verarbeitet, nachdem die Transaktion mit `COMMIT` oder `ROLLBACK` beendet wurde.

Reagieren Sie auf lang andauernde Transaktionen

Wenn Transaktionen mit langer Laufzeit das häufige Auftreten von `Lock:transactionid` verursachen, versuchen Sie die folgenden Strategien:

- Halten Sie Zeilensperren von lang andauernden Transaktionen fern.
- Beschränken Sie die Länge von Abfragen, indem Sie nach Möglichkeit Autocommit implementieren.

Lock:tuple

Das `Lock:tuple`-Ereignis tritt ein, wenn ein Backend-Prozess darauf wartet, eine Sperre für ein Tupel zu erlangen.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Context

Das Ereignis `Lock:tuple` zeigt an, dass ein Back-End darauf wartet, eine Sperre für ein Tupel zu erlangen, während ein anderes Back-End eine widersprüchliche Sperre für dasselbe Tupel hält. Die folgende Tabelle veranschaulicht ein Szenario, in dem Sitzungen das `Lock:tuple`-Ereignis generieren.

Zeit	1. Sitzung	2. Sitzung	3. Sitzung
t1	Startet eine Transaktion.		
t2	Aktualisiert Zeile 1.		
t3		Aktualisiert Zeile 1. Die Sitzung erwirbt eine exklusive Sperre für das Tupel und wartet dann darauf, dass Sitzung 1 die Sperre durch Commit oder Rollback freigibt.	
t4			Aktualisiert Zeile 1. Die Sitzung wartet darauf, dass Sitzung 2 die exklusive Sperre für das Tupel freigibt.

Oder Sie können dieses Warteereignis simulieren, indem Sie das Benchmarking-Tool `pgbench` verwenden. Konfigurieren Sie eine hohe Anzahl gleichzeitiger Sitzungen, um dieselbe Zeile in einer Tabelle mit einer benutzerdefinierten SQL-Datei zu aktualisieren.

Weitere Informationen zu widersprüchlichen Sperrmodi finden Sie unter Explizite Sperren in der PostgreSQL-Dokumentation. Weitere Informationen zu `pgbench` finden Sie unter pgbench in der PostgreSQL-Dokumentation.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn dieses Ereignis mehr als normal auftritt und möglicherweise auf ein Leistungsproblem hinweist, sind typische Ursachen:

- Eine große Anzahl gleichzeitiger Sitzungen versucht, eine widersprüchliche Sperre für dasselbe Tupel zu erlangen, indem sie `UPDATE`- oder `DELETE`-Anweisungen ausführen.
- In hochgradig gleichzeitigen Sitzungen wird eine `SELECT`-Anweisung ausgeführt, die den `FOR UPDATE`- oder `FOR NO KEY UPDATE`-Sperrmodus verwendet.
- Verschiedene Faktoren veranlassen Anwendungs- oder Verbindungspools dazu, weitere Sitzungen zu öffnen, um dieselben Vorgänge auszuführen. Wenn neue Sitzungen versuchen, dieselben Zeilen zu ändern, kann die DB-Last stark ansteigen und `Lock:tuple` kann erscheinen.

Weitere Informationen finden Sie unter Sperren auf Zeilenebene in der PostgreSQL-Dokumentation.

Aktionen

Abhängig von den Ursachen Ihres Wait-Ereignisses empfehlen wir verschiedene Aktionen.

Themen

- Untersuchen Sie Ihre Anwendungslogik
- Finde die Blocker-Sitzung
- Reduzieren Sie Parallelität, wenn es hoch ist
- Beheben von Engpässen

Untersuchen Sie Ihre Anwendungslogik

Finden Sie heraus, ob sich eine Blocker-Sitzung schon lange im `idle in transaction`-Zustand befindet. Wenn ja, erwägen Sie, die Blocker-Sitzung als kurzfristige Lösung zu beenden. Sie können die Funktion `pg_terminate_backend` verwenden. Weitere Informationen zu dieser Funktion finden Sie unter Server-Signalisierungsfunktionen in der PostgreSQL-Dokumentation.

Gehen Sie für eine langfristige Lösung wie folgt vor:

- Passen Sie die Anwendungslogik an.
- Verwenden Sie den Parameter `idle_in_transaction_session_timeout`. Dieser Parameter beendet jede Sitzung mit einer offenen Transaktion, die länger als die angegebene Zeitspanne im

Leerlauf ist. Weitere Informationen finden Sie unter Standardeinstellungen für Clientverbindungen in der PostgreSQL-Dokumentation.

- Verwenden Sie Autocommit so weit wie möglich. Weitere Informationen finden Sie unter SET AUTOCOMMIT in der PostgreSQL-Dokumentation.

Finde die Blocker-Sitzung

Identifizieren Sie während des `Lock:tuple`-Wait-Ereignisses den Blocker und die blockierte Sitzung, indem Sie herausfinden, welche Sperren voneinander abhängen. Weitere Informationen finden Sie unter Informationen zur Sperrabhängigkeit im PostgreSQL-Wiki. Um vergangene `Lock:tuple`-Ereignisse zu analysieren, verwenden Sie die Aurora-Funktion `aurora_stat_backend_waits`.

Im folgenden Beispiel werden alle Sitzungen abgefragt, nach `tuple` gefiltert und nach `wait_time` sortiert.

```
--AURORA_STAT_BACKEND_WAITS
      SELECT a.pid,
             a.usename,
             a.app_name,
             a.current_query,
             a.current_wait_type,
             a.current_wait_event,
             a.current_state,
             wt.type_name AS wait_type,
             we.event_name AS wait_event,
             a.waits,
             a.wait_time
        FROM (SELECT pid,
                     usename,
                     left(application_name,16) AS app_name,
                     coalesce(wait_event_type,'CPU') AS current_wait_type,
                     coalesce(wait_event,'CPU') AS current_wait_event,
                     state AS current_state,
                     left(query,80) as current_query,
                     (aurora_stat_backend_waits(pid)).*
                FROM pg_stat_activity
               WHERE pid <> pg_backend_pid()
                 AND usename<>'rdsadmin') a
NATURAL JOIN aurora_stat_wait_type() wt
NATURAL JOIN aurora_stat_wait_event() we
```

```
WHERE we.event_name = 'tuple'
    ORDER BY a.wait_time;

  pid  | usename | app_name |                 current_query                  |
 current_wait_type | current_wait_event | current_state | wait_type | wait_event |
 waits | wait_time
-------+---------+----------+------------------------------------------------
+-------------------+--------------------+--------------+-----------+------------
+-------+-----------
 32136 | sys     | psql     | /*session3*/ update tab set col=1 where col=1; | Lock
           | tuple              | active        | Lock      | tuple      |     1 |
 1000018
 11999 | sys     | psql     | /*session4*/ update tab set col=1 where col=1; | Lock
           | tuple              | active        | Lock      | tuple      |     1 |
 1000024
```

Reduzieren Sie Parallelität, wenn es hoch ist

Das `Lock:tuple`-Ereignis kann ständig auftreten, insbesondere in einer arbeitsreichen Zeit. Erwägen Sie in dieser Situation, die hohe Parallelität für sehr belegte Reihen zu reduzieren. Oft steuern nur wenige Zeilen eine Warteschlange oder die boolesche Logik, was diese Zeilen sehr ausgelastet macht.

Sie können die Parallelität reduzieren, indem Sie verschiedene Ansätze verwenden, die auf der Geschäftsanforderung, der Anwendungslogik und dem Workload-Typ basieren. Sie können z. B. Folgendes tun:

- Gestalten Sie Ihre Tabellen- und Datenlogik neu, um hohe Parallelität zu reduzieren.
- Ändern Sie die Anwendungslogik, um die hohe Parallelität auf Zeilenebene zu reduzieren.
- Nutzen und gestalten Sie Abfragen mit Sperren auf Zeilenebene.
- Verwenden Sie die `NOWAIT`-Klausel mit Wiederholungsvorgänge.
- Erwägen Sie, optimistische und hybridsperrende Logik-Parallelitätssteuerung zu nutzen.
- Überlegen Sie, die Isolationsstufe der Datenbank zu ändern.

Beheben von Engpässen

Das `Lock:tuple` kann bei Engpässen wie CPU-Aushungerungen oder maximaler Nutzung der Amazon EBS-Bandbreite auftreten. Um Engpässe zu verringern, sollten Sie die folgenden Ansätze berücksichtigen:

- Skalieren Sie Ihren Instance-Klassentyp hoch.
- Optimieren Sie ressourcenintensive Abfragen.
- Ändern Sie die Anwendungslogik.
- Archivieren Sie Daten, die selten zugegriffen wird.

LWLock:buffer_content (BufferContent)

Das Ereignis `LWLock:buffer_content` tritt ein, wenn eine Sitzung darauf wartet, eine Datenseite im Speicher zu lesen oder zu schreiben, während eine andere Sitzung diese Seite zum Schreiben gesperrt hat. In Aurora PostgreSQL 13 und höher heißt dieses Warteereignis `BufferContent`.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Context

Um Daten zu lesen oder zu manipulieren, greift PostgreSQL über Shared Memory Puffer darauf zu. Um aus dem Puffer zu lesen, erhält ein Prozess eine leichte Sperre (LWLock) für den Pufferinhalt im freigegebenen Modus. Um in den Puffer zu schreiben, wird diese Sperre im exklusiven Modus angezeigt. Gemeinsame Sperren ermöglichen es anderen Prozessen, gleichzeitig gemeinsame Sperren für diesen Inhalt zu erwerben. Exklusive Sperren verhindern, dass andere Prozesse irgendeine Art von Sperre erhalten.

Die`LWLock:buffer_content`(`BufferContent`)-Ereignis zeigt an, dass mehrere Prozesse versuchen, den Inhalt eines bestimmten Puffers zu sperren.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `LWLock:buffer_content`(`BufferContent`)-Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die folgenden typischen Ursachen:

Die gleichzeitigen Aktualisierungen der gleichen Daten wurden erhöht

Es kann zu einer Zunahme der Anzahl gleichzeitiger Sitzungen mit Abfragen kommen, die denselben Pufferinhalt aktualisieren. Diese Behauptung kann bei Tabellen mit vielen Indizes ausgeprägter sein.

Workload-Daten befinden sich nicht im Speicher

Wenn sich Daten, die die aktive Workload verarbeitet, nicht im Speicher befinden, können diese Warteereignisse zunehmen. Dieser Effekt liegt daran, dass Prozesse, die Sperren halten, sie länger halten können, während sie Festplatten-I/O-Vorgänge ausführen.

Übermäßiger Einsatz von Fremdschlüsselbeschränkungen

Fremdschlüsseleinschränkungen können die Zeit erhöhen, die ein Prozess an einer Pufferinhaltssperre hält. Dieser Effekt liegt daran, dass Lesevorgänge eine gemeinsame Pufferinhaltssperre für den referenzierten Schlüssel erfordern, während dieser Schlüssel aktualisiert wird.

Aktionen

Abhängig von den Ursachen Ihres Wait-Ereignisses empfehlen wir verschiedene Aktionen. Sie können `LWLock:buffer_content`(`BufferContent`)-Ereignisse identifizieren, indem Sie Amazon RDS Performance Insights verwenden oder die Ansicht `pg_stat_activity` abfragen.

Themen

- Verbessern Sie die Effizienz im Speicher
- Reduzieren Sie die Verwendung von Fremdschlüsselbeschränkungen
- Entferne nicht verwendete Indizes

Verbessern Sie die Effizienz im Speicher

Um die Wahrscheinlichkeit zu erhöhen, dass sich aktive Workload-Daten im Speicher befinden, partitionieren Sie Tabellen oder skalieren Sie Ihre Instance-Klasse hoch. Weitere Informationen zu DB-Instance-Klassen finden Sie unter Aurora DB-Instance-Klassen.

Reduzieren Sie die Verwendung von Fremdschlüsselbeschränkungen

Untersuchen Sie Workloads, bei denen eine hohe Anzahl von `LWLock:buffer_content`(`BufferContent`)-Wait-Ereignissen auf die Verwendung von Fremdschlüsseleinschränkungen auftritt. Entfernen Sie unnötige Fremdschlüsselbeschränkungen.

Entferne nicht verwendete Indizes

Identifizieren Sie bei Workloads mit einer hohen Anzahl von `LWLock:buffer_content`(`BufferContent`)-Wait-Ereignissen nicht verwendete Indizes und entfernen Sie sie.

LWLock:buffer_mapping

Dieses Ereignis tritt ein, wenn eine Sitzung darauf wartet, einen Datenblock einem Puffer im gemeinsam genutzten Pufferpool zuzuordnen.

> **Note**
>
> Dieses Ereignis wird in Aurora PostgreSQL Version 12 und niedriger als `LWLock:buffer_mapping` und in Version 13 und höher als `LWLock:BufferMapping` angezeigt.

Themen

- Unterstützte Engine-Versionen
- Context
- Ursachen
- Aktionen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen sind für Aurora PostgreSQL Version 9.6 und höher relevant.

Context

Der freigegebene Pufferpool ist ein Aurora PostgreSQL-Speicherbereich, der alle Seiten enthält, die von Prozessen verwendet werden oder wurden. Wenn ein Prozess eine Seite benötigt, liest er die Seite in den freigegebenen Pufferpool. Der Parameter `shared_buffers` legt die Größe des

gemeinsam genutzten Puffers fest und reserviert einen Speicherbereich zum Speichern der Tabellen- und Indexseiten. Wenn Sie diesen Parameter ändern, stellen Sie sicher, dass Sie die Datenbank neu starten. Weitere Informationen finden Sie unter Freigegebene Puffer.

Das `LWLock:buffer_mapping`-Wait-Ereignis tritt in den folgenden Szenarien auf:

- Ein Prozess durchsucht die Puffertabelle nach einer Seite und erwirbt eine freigegebene Puffer-Mapping-Sperre.
- Ein Prozess lädt eine Seite in den Pufferpool und erwirbt eine exklusive Puffer-Mapping-Sperre.
- Ein Prozess entfernt eine Seite aus dem Pool und erwirbt eine exklusive Puffer-Mapping-Sperre.

Ursachen

Wenn dieses Ereignis mehr als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, greift die Datenbank in und aus dem freigegebenen Pufferpool aus. Zu den typischen Ursachen zählen auch die Folgenden:

- Große Abfragen
- Aufgeblähte Indizes und Tabellen
- Vollständige Tabellenscans
- Eine gemeinsame Poolgröße, die kleiner als der Arbeitssatz ist

Aktionen

Abhängig von den Ursachen Ihres Wait-Ereignisses empfehlen wir verschiedene Aktionen.

Themen

- Überwachen Sie pufferbezogene Metriken
- Bewerten Sie Ihre Indexierungsstrategie
- Reduzieren Sie die Anzahl der Puffer, die schnell zugewiesen werden müssen

Überwachen Sie pufferbezogene Metriken

Wenn `LWLock:buffer_mapping` auf Spitze wartet, untersuchen Sie die Puffertrefferquote. Sie können diese Metriken verwenden, um ein besseres Verständnis dafür zu erhalten, was im Puffer-Cache passiert. Untersuchen Sie die folgenden Metriken:

`BufferCacheHitRatio`

Diese Amazon CloudWatch-Metrik misst den Prozentsatz der Anfragen, die vom Puffer-Cache einer DB-Instance in Ihrem DB-Cluster verarbeitet werden. Möglicherweise sehen Sie diese Metrikabnahme im Vorfeld des `LWLock:buffer_mapping`-Wait-Ereignisses.

`blks_hit`

Diese Zählermetrik für Performance Insights gibt die Anzahl der Blöcke an, die aus dem freigegebenen Pufferpool abgerufen wurden. Nachdem das Wait-Ereignis `LWLock:buffer_mapping` aufgetreten ist, können Sie eine Spitze in `blks_hit` beobachten.

`blks_read`

Diese Zählermetrik für Performance Insights gibt die Anzahl der Blöcke an, für die I/O in den freigegebenen Pufferpool eingelesen werden mussten. Sie können im Vorfeld des `LWLock:buffer_mapping`-Warteereignisses eine Spitze in `blks_read` beobachten.

Bewerten Sie Ihre Indexierungsstrategie

Überprüfen Sie Folgendes, um zu bestätigen, dass Ihre Indexierungsstrategie die Leistung nicht beeinträchtigt:

Indexblähung

Stellen Sie sicher, dass Index und Tabellenaufblähungen nicht dazu führen, dass unnötige Seiten in den freigegebenen Puffer gelesen werden. Wenn Ihre Tabellen nicht verwendete Zeilen enthalten, sollten Sie die Daten archivieren und die Zeilen aus den Tabellen entfernen. Sie können dann die Indizes für die skalierten Tabellen neu erstellen.

Indizes für häufig verwendete Abfragen

Um festzustellen, ob Sie über die optimalen Indizes verfügen, überwachen Sie die Metriken der DB-Engine in Performance Insights. Die `tup_returned`-Metrik zeigt die Anzahl der gelesenen Zeilen an. Die `tup_fetched`-Metrik zeigt die Anzahl der an den Client zurückgegebenen Zeilen. Wenn `tup_returned` deutlich größer als `tup_fetched` ist, werden die Daten möglicherweise nicht richtig indiziert. Außerdem sind Ihre Tabellenstatistiken möglicherweise nicht aktuell.

Reduzieren Sie die Anzahl der Puffer, die schnell zugewiesen werden müssen

Um die `LWLock:buffer_mapping`-Warteereignisse zu reduzieren, versuchen Sie, die Anzahl der Puffer zu reduzieren, die schnell zugewiesen werden müssen. Eine Strategie besteht darin, kleinere

Batch-Vorgänge durchzuführen. Möglicherweise können Sie kleinere Batches erreichen, indem Sie Ihre Tabellen partitionieren.

LWLock:BufferIO (IPC:BufferIO)

Das `LWLock:BufferIO`-Ereignis tritt ein, wenn Aurora PostgreSQL oder RDS for PostgreSQL darauf wartet, dass andere Prozesse ihre Eingabe-/Ausgabe-(I/O)-Vorgänge beenden, wenn sie gleichzeitig versuchen, auf eine Seite zuzugreifen. Sein Zweck besteht darin, dass dieselbe Seite in den freigegebenen Puffer eingelesen wird.

Themen

Relevante Engine-Versionen

Diese Warteereignisinformationen sind für alle Versionen von Aurora PostgreSQL. Für Aurora PostgreSQL 12 und frühere Versionen wird dieses Warteereignis als lwlock:buffer_io bezeichnet, während es in der Version Aurora PostgreSQL 13 den Namen lwlock:bufferio trägt. Aus der Version Aurora PostgreSQL 14 wurde das BufferIO-Warteereignis von `LWLock` zum Warteereignistyp `IPC` (ipc:bufferio) verschoben.

Kontext

Jeder gemeinsam genutzte Puffer hat eine I/O-Sperre, die mit dem `LWLock:BufferIO`-Warteereignis verbunden ist, jedes Mal, wenn ein Block (oder eine Seite) außerhalb des gemeinsam genutzten Pufferpools abgerufen werden muss.

Diese Sperre wird verwendet, um mehrere Sitzungen zu behandeln, die alle Zugriff auf denselben Block benötigen. Dieser Block muss von außerhalb des gemeinsam genutzten Pufferpools gelesen werden, der durch den `shared_buffers`-Parameter definiert wird.

Sobald die Seite innerhalb des Shared Buffer Pool gelesen wird, wird die `LWLock:BufferIO`-Sperre freigegeben.

> **Note**
>
> Das `LWLock:BufferIO`-Wait-Ereignis geht dem IO:DataFileRead-Warteereignis voraus. Das `IO:DataFileRead`-Wait-Ereignis tritt auf, während Daten aus dem Speicher gelesen werden.

Weitere Informationen zu leichten Sperren finden Sie unter Übersicht über Sperren.

Ursachen

Häufige Gründe dafür, dass das `LWLock:BufferIO`-Ereignis in den Top-Wartezeiten angezeigt wird, sind die folgenden:

- Mehrere Backends oder Verbindungen, die versuchen, auf dieselbe Seite zuzugreifen, für die auch ein I/O-Vorgang aussteht
- Das Verhältnis zwischen der Größe des gemeinsam genutzten Pufferpools (definiert durch den `shared_buffers`-Parameter) und der Anzahl der Puffer, die von der aktuellen Workload benötigt werden
- Die Größe des freigegebenen Pufferpools ist nicht gut mit der Anzahl der Seiten, die durch andere Vorgänge geräumt werden
- Große oder aufgeblähte Indizes, bei denen die Engine mehr Seiten als nötig in den freigegebenen Pufferpool lesen muss
- Mangel an Indizes, die die DB-Engine dazu zwingen, mehr Seiten aus den Tabellen als nötig zu lesen
- Plötzliche Spitzen für Datenbankverbindungen, die versuchen, Vorgänge auf derselben Seite auszuführen

Aktionen

Abhängig von den Ursachen Ihres Wait-Ereignisses empfehlen wir verschiedene Aktionen:

- Beobachten Sie die Amazon CloudWatch-Metriken auf Korrelation zwischen starken Abnahmen der `BufferCacheHitRatio`- und `LWLock:BufferIO`-Warteereignisse. Dieser Effekt kann bedeuten, dass Sie eine kleine Einstellung für gemeinsame Puffer haben. Möglicherweise müssen Sie es erhöhen oder Ihre DB-Instance-Klasse hochskalieren. Sie können Ihre Workload in mehr Reader-Knoten aufteilen.

- Stimmen Sie `max_wal_size` und `checkpoint_timeout` basierend auf der Spitzenzeit Ihrer Workload ab, wenn Sie sehen, dass `LWLock:BufferIO` mit Einbrüchen der Metrik `BufferCacheHitRatio` zusammenfällt. Identifizieren Sie dann, welche Abfrage sie möglicherweise verursachen könnte.
- Überprüfen Sie, ob Sie nicht verwendete Indizes haben, und entfernen Sie sie dann.
- Verwenden Sie partitionierte Tabellen (die auch partitionierte Indizes haben). Dies hilft, die Neuordnung des Index niedrig zu halten und ihre Auswirkungen zu reduzieren.
- Vermeiden Sie, Spalten unnötig zu indizieren.
- Verhindern Sie plötzliche Spitzen der Datenbankverbindung, indem Sie einen Verbindungspool verwenden.
- Beschränken Sie die maximale Anzahl von Verbindungen zur Datenbank als bewährte Methode

LWLock:lock_manager

Dieses Ereignis tritt ein, wenn die Aurora PostgreSQL-Engine den Speicherbereich der gemeinsam genutzten Sperre verwaltet, um eine Sperre zuzuweisen, zu überprüfen und aufzuheben, wenn eine Fast-Path-Sperre nicht möglich ist.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen sind für Aurora PostgreSQL Version 9.6 und höher relevant.

Kontext

Wenn Sie eine SQL-Anweisung ausgeben, zeichnet Aurora PostgreSQL Sperren auf, um die Struktur, Daten und Integrität Ihrer Datenbank während gleichzeitiger Vorgänge zu schützen. Der Motor kann dieses Ziel mit einer schnellen Pfadsperre oder einer nicht schnellen Pfadsperre erreichen. Eine Pfadsperre, die nicht schnell ist, ist teurer und erzeugt mehr Overhead als eine schnelle Pfadsperre.

Schnelle Pfadsperre

Um den Overhead von Sperren zu reduzieren, die häufig genommen und freigegeben werden, aber selten in Konflikt geraten, können Backend-Prozesse eine schnelle Pfadsperrung verwenden. Die Datenbank verwendet diesen Mechanismus für Sperren, die die folgenden Kriterien erfüllen:

- Sie verwenden die STANDARD–Sperrmethode.
- Sie stellen eine Sperre für eine Datenbankbeziehung statt einer gemeinsamen Beziehung dar.
- Sie sind schwache Sperren, die wahrscheinlich nicht in Konflikt stehen.
- Die Engine kann schnell überprüfen, dass keine widersprüchlichen Sperren existieren können.

Die Engine kann keine schnelle Pfadsperre verwenden, wenn eine der folgenden Bedingungen erfüllt ist:

- Die Sperre erfüllt nicht die vorhergehenden Kriterien.
- Für den Backend-Prozess sind keine Slots mehr verfügbar.

Weitere Informationen zum Sperren von Fast Path finden Sie unter Fast Path in der README-Datei des PostgreSQL-Sperrmanagers und unter pg-locks in der PostgreSQL-Dokumentation.

Beispiel für ein Skalierungsproblem für den Sperrmanager

In diesem Beispiel speichert eine Tabelle mit dem Namen `purchases` Daten aus fünf Jahren, aufgeteilt nach Tagen. Jede Partition hat zwei Indizes. Die folgende Abfolge von Ereignissen tritt auf:

1. Sie fragen Daten für viele Tage ab, wodurch die Datenbank viele Partitionen lesen muss.
2. Die Datenbank erstellt einen Sperreintrag für jede Partition. Wenn Partitionsindizes Teil des Optimizer-Zugriffspfads sind, erstellt die Datenbank auch für sie einen Sperreintrag.
3. Wenn die Anzahl der angeforderten Sperreneinträge für denselben Backend-Prozess höher als 16 ist, was dem Wert von `FP_LOCK_SLOTS_PER_BACKEND` entspricht, verwendet der Sperrenmanager die Sperrmethode ohne Fast Path.

Moderne Anwendungen haben möglicherweise Hunderte von Sitzungen. Wenn gleichzeitige Sitzungen das übergeordnete Element ohne ordnungsgemäßen Schnitt von Partitionen abfragen, erstellt die Datenbank möglicherweise Hunderte oder sogar Tausende von nicht schnellen Pfadsperren. Wenn diese Parallelität höher als die Anzahl der vCPUs ist, wird normalerweise das `LWLock:lock_manager`-Warteereignis angezeigt.

> **Note**
>
> Das Wait-Ereignis `LWLock:lock_manager` hat nichts mit der Anzahl der Partitionen oder Indizes in einem Datenbankschema zu tun. Stattdessen hängt es mit der Anzahl der nicht schnellen Pfadsperren zusammen, die die Datenbank steuern muss.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Wenn das `LWLock:lock_manager` häufiger als normal auftritt, was möglicherweise auf ein Leistungsproblem hinweist, sind die wahrscheinlichsten Ursachen für plötzliche Spitzen wie folgt:

- Gleichzeitige aktive Sitzungen führen Abfragen aus, die keine schnellen Pfadsperren verwenden. Diese Sitzungen überschreiten auch die maximale vCPU.
- Eine große Anzahl gleichzeitiger aktiver Sitzungen greift auf eine stark partitionierte Tabelle zu. Jede Partition hat mehrere Indizes.
- Die Datenbank erlebt einen Verbindungssturm. Standardmäßig erzeugen einige Anwendungen und Connection Pool-Software mehr Verbindungen, wenn die Datenbank langsam ist. Diese Praxis verschlimmert das Problem. Optimieren Sie Ihre Connection Pool-Software so, dass keine Verbindungsstürme auftreten.
- Eine große Anzahl von Sitzungen fragt eine übergeordnete Tabelle ab, ohne Partitionen zu beschneiden.
- Eine Datendefinitionssprache (DDL), Datenmanipulationssprache (DML) oder ein Wartungsbefehl sperrt ausschließlich eine Beleg-Beziehung oder Tupel, auf die häufig zugegriffen oder geändert werden.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

Themen

- Verwenden Sie das Beschneiden von Partitionen
- Entfernen unnötiger Indizes
- Optimieren Sie Ihre Abfragen für schnelles Pfadsperren
- Tune auf andere Warteereignisse
- Reduzieren von Hardware-Engpässen

- Verwenden eines Verbindungs-Poolers
- Aktualisieren Sie Ihre Aurora PostgreSQL Version

Verwenden Sie das Beschneiden von Partitionen

Die Partitionsbereinigung ist eine Strategie zur Abfrageoptimierung, die nicht benötigte Partitionen von Tabellenscans ausschließt und dadurch die Leistung verbessert. Das Beschneiden der Partition ist standardmäßig aktiviert. Wenn es ausgeschaltet ist, schalten Sie es wie folgt ein.

```
SET enable_partition_pruning = on;
```

Abfragen können die Partitionsbereinigung nutzen, wenn ihre `WHERE`-Klausel die für die Partitionierung verwendete Spalte enthält. Weitere Informationen finden Sie unter Partitionsbereinigung in der PostgreSQL-Dokumentation.

Entfernen unnötiger Indizes

Ihre Datenbank enthält möglicherweise nicht verwendete oder selten verwendete Indizes. Wenn ja, erwägen Sie, sie zu löschen. Führen Sie eine der folgenden Aufgaben aus:

- Erfahren Sie, wie Sie unnötige Indizes finden, indem Sie Ungenutzte Indizes im PostgreSQL-Wiki lesen.
- Führen Sie PG Collector aus. Dieses SQL-Skript sammelt Datenbankinformationen und präsentiert sie in einem konsolidierten HTML-Bericht. Überprüfen Sie den Abschnitt „Unbenutzte Indizes“. Weitere Informationen finden Sie unter pg-collector im AWS-Labs GitHub-Repository.

Optimieren Sie Ihre Abfragen für schnelles Pfadsperren

Um herauszufinden, ob Ihre Abfragen Fast Path Locking verwenden, fragen Sie die `fastpath`-Spalte in der `pg_locks`-Tabelle ab. Wenn Ihre Abfragen keine schnelle Pfadsperre verwenden, versuchen Sie, die Anzahl der Beziehungen pro Abfrage auf weniger als 16 zu reduzieren.

Tune auf andere Warteereignisse

Wenn `LWLock:lock_manager` in der Liste der Top-Waits an erster oder zweiter Stelle steht, überprüfen Sie, ob die folgenden Wait-Ereignisse auch in der Liste erscheinen:

- `Lock:Relation`

- `Lock:transactionid`
- `Lock:tuple`

Wenn die vorhergehenden Ereignisse in der Liste hoch erscheinen, sollten Sie zuerst diese Warteereignisse optimieren. Diese Ereignisse können ein Treiber für `LWLock:lock_manager`.

Reduzieren von Hardware-Engpässen

Möglicherweise haben Sie einen Hardware-Engpass wie CPU-Hunger oder maximale Auslastung Ihrer Amazon EBS-Bandbreite. Ziehen Sie in diesen Fällen die Verringerung der Hardware-Engpässe in Betracht. Berücksichtigen Sie die folgenden Aktionen:

- Skalieren Sie Ihre Instance-Klasse hoch.
- Optimieren Sie Abfragen, die große Mengen an CPU und Speicher verbrauchen.
- Ändern Sie Ihre Anwendungslogik.
- Archiviere deine Daten.

Weitere Informationen zu CPU, Arbeitsspeicher und EBS-Netzwerkbandbreite finden Sie unter Amazon RDS-Instance-Typen.

Verwenden eines Verbindungs-Poolers

Wenn Ihre Gesamtzahl aktiver Verbindungen die maximale vCPU überschreitet, benötigen mehr Betriebssystemprozesse CPU, als Ihr Instance-Typ unterstützen kann. Ziehen Sie in diesem Fall die Verwendung oder Abstimmung eines Verbindungspool in Betracht. Weitere Informationen zu den vCPUs für Ihren Instance-Typ finden Sie unter Amazon RDS-Instance-Typen.

Weitere Informationen zum Verbindungspooling finden Sie in den folgenden Ressourcen:

- Verwenden von Amazon RDS Proxy für Aurora
- pgbouncer
- Verbindungspools und Datenquellen in der PostgreSQL-Dokumentation

Aktualisieren Sie Ihre Aurora PostgreSQL Version

Wenn Ihre aktuelle Version von Aurora PostgreSQL niedriger als 12 ist, aktualisieren Sie auf Version 12 oder höher. PostgreSQL Versionen 12 und 13 haben einen verbesserten Partitionsmechanismus.

Weitere Informationen zu Version 12 finden Sie in den Versionshinweisen zu PostgreSQL 12.0. Weitere Informationen zum Aktualisieren von Aurora PostgreSQL finden Sie unter Amazon Aurora PostgreSQL-Aktualisierungen.

LWLockMultiXact:

Die `LWLock:MultiXactOffsetSLRU`Warteereignisse `LWLock:MultiXactMemberBuffer`, `LWLock:MultiXactMemberSLRU`, und geben an`LWLock:MultiXactOffsetBuffer`, dass eine Sitzung darauf wartet, eine Liste von Transaktionen abzurufen, die dieselbe Zeile in einer bestimmten Tabelle ändert.

- `LWLock:MultiXactMemberBuffer` – Ein Prozess wartet auf I/O in einem einfachen, am wenigsten zuletzt verwendeten (SLRU) Puffer für ein Multixact-Mitglied.
- `LWLock:MultiXactMemberSLRU` – Ein Prozess wartet darauf, auf den einfachen, am wenigsten zuletzt verwendeten (SLRU) Cache für ein Multixact-Mitglied zuzugreifen.
- `LWLock:MultiXactOffsetBuffer` – Ein Prozess wartet auf I/O in einem einfachen, am wenigsten zuletzt verwendeten (SLRU) Puffer für ein Multixact-Offset.
- `LWLock:MultiXactOffsetSLRU` – Ein Prozess wartet darauf, auf den einfachen, am wenigsten zuletzt verwendeten (SLRU) Cache für ein Multixact-Offset zuzugreifen.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Kontext

Ein Multixact ist eine Datenstruktur, die eine Liste von Transaktions-IDs (XIDs) speichert, die dieselbe Tabellenzeile ändern. Wenn eine einzelne Transaktion auf eine Zeile in einer Tabelle verweist, wird die Transaktions-ID in der Tabellen-Header-Zeile gespeichert. Verweisen mehrere Transaktionen auf dieselbe Zeile in einer Tabelle, wird die Liste der Transaktions-IDs in der Multixact-Datenstruktur

gespeichert. Die Multixact-Warteereignisse geben an, dass eine Sitzung die Liste der Transaktionen, die sich auf eine bestimmte Zeile in einer Tabelle beziehen, aus der Datenstruktur abruft.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Drei häufige Ursachen für die Verwendung von Multixact sind die folgenden:

- Untertransaktionen von expliziten Savepoints – Wenn Sie explizit einen Savepoint in Ihren Transaktionen erstellen, werden neue Transaktionen für dieselbe Zeile generiert. Verwenden Sie beispielsweise `SELECT FOR UPDATE`, `SAVEPOINT` und dann `UPDATE`.

  Einige Treiber, objektrelationale Mappers (ORMs) und Abstraktionsschichten verfügen über Konfigurationsoptionen, um alle Operationen automatisch mit Savepoints zu umschließen. Dies kann bei einigen Workloads zu vielen Multixact-Warteereignissen führen. Die `autosave`-Option des PostgreSQL-JDBC-Treibers ist ein Beispiel dafür. Weitere Informationen finden Sie unter pgJDBC in der PostgreSQL-JDBC-Dokumentation. Ein anderes Beispiel ist der PostgreSQL-ODBC-Treiber und seine `protocol`-Option. Weitere Informationen finden Sie unter psqlODBC-Konfigurationsoptionen in der Dokumentation zu PostgreSQL-ODBC-Treibern.
- Subtransaktionen aus PL/pgSQL EXCEPTION-Klauseln – Jede `EXCEPTION` Klausel, die Sie in Ihre PL/pgSQL-Funktionen oder -Prozeduren schreiben, erstellt `SAVEPOINT` intern einen .
- Fremdschlüssel – Mehrere Transaktionen erwerben eine Freigabesperre für den übergeordneten Datensatz.

Wenn eine bestimmte Zeile in einer Operation mit mehreren Transaktionen enthalten ist, müssen für die Verarbeitung der Zeile die Transaktions-IDs aus den `multixact`-Auflistungen abgerufen werden. Wenn durch Lookups der Multixact nicht aus dem Speichercache abgerufen werden kann, muss die Datenstruktur aus der Aurora-Speicherschicht gelesen werden. Dieser I/O-Vorgang aus dem Speicher bedeutet, dass SQL-Abfragen länger dauern können. Speicher-Cache-Fehler können bei starker Auslastung aufgrund einer großen Anzahl von mehreren Transaktionen auftreten. All diese Faktoren tragen zu einer Zunahme dieses Warteereignisses bei.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen. Einige dieser Aktionen können dazu beitragen, die Warteereignisse sofort zu reduzieren. Andere benötigen jedoch möglicherweise Untersuchungen und Korrekturen, um Ihren Workload zu skalieren.

Themen

- Durchführen von Vacuum Freeze für Tabellen mit diesem Warteereignis
- Erhöhen Sie die Häufigkeit der Selbstbereinigung für Tabellen mit diesem Warteereignis
- Erhöhen der Speicherparameter
- Reduzieren Sie lang andauernde Transaktionen
- Langfristige Aktionen

Durchführen von Vacuum Freeze für Tabellen mit diesem Warteereignis

Wenn dieses Warteereignis plötzlich ansteigt und sich auf Ihre Produktionsumgebung auswirkt, können Sie eine der folgenden temporären Methoden verwenden, um die Anzahl zu reduzieren.

- Verwenden Sie VACUUM microSDZE für die betroffene Tabelle oder Tabellenpartition, um das Problem sofort zu beheben. Weitere Informationen finden Sie unter VACUUM.
- Verwenden Sie die VACUUM-Klausel (FREEZE, INDEX_CLEANUP FALSE), um eine schnelle Bereinigung durchzuführen, indem Sie die Indizes überspringen. Weitere Informationen finden Sie unter Bereinigen einer Tabelle so schnell wie möglich.

Erhöhen Sie die Häufigkeit der Selbstbereinigung für Tabellen mit diesem Warteereignis

Nach dem Scannen aller Tabellen in allen Datenbanken entfernt VACUUM schließlich Multixacts, und ihre ältesten Multixact-Werte werden erweitert. Weitere Informationen finden Sie unter Multixacts und Wraparound. Um die LWLock :MultiXact wait-Ereignisse auf ein Minimum zu beschränken, müssen Sie VACUUM so oft wie nötig ausführen. Stellen Sie dazu sicher, dass VACUUM in Ihrem DB-Cluster von Aurora PostgreSQL optimal konfiguriert ist.

Wenn die Verwendung von VACUUM microSDZE für die betroffene Tabelle oder Tabellenpartition das Warteereignisproblem löst, empfehlen wir, einen Scheduler wie zu verwendenpg_cron, um den VACUUM-Vorgang durchzuführen, anstatt die Selbstbereinigung auf Instance-Ebene anzupassen.

Damit die Selbstbereinigung häufiger erfolgt, können Sie den Wert des Speicherparameters `autovacuum_multixact_freeze_max_age` in der betroffenen Tabelle reduzieren. Weitere Informationen finden Sie unter autovacuum_multixact_freeze_max_age .

Erhöhen der Speicherparameter

Sie können die folgenden Parameter auf Clusterebene festlegen, sodass alle Instances in Ihrem Cluster konsistent bleiben. Dies trägt dazu bei, die Warteereignisse in Ihrem Workload zu reduzieren. Wir empfehlen Ihnen, diese Werte nicht so hoch einzustellen, dass Ihnen der Speicher ausgeht.

- `multixact_offsets_cache_size` bis 128
- `multixact_members_cache_size` bis 256

Sie müssen die Instance neu starten, damit die Parameteränderung wirksam wird. Mit diesen Parametern können Sie mehr des Instance-RAM verwenden, um die multixact-Struktur im Speicher zu speichern, bevor sie auf die Festplatte übertragen wird.

Reduzieren Sie lang andauernde Transaktionen

Lang andauernde Transaktionen führen dazu, dass die Bereinigung ihre Informationen beibehält, bis die Transaktion bestätigt oder die schreibgeschützte Transaktion geschlossen wird. Wir empfehlen, langlebige Transaktionen proaktiv zu überwachen und zu verwalten. Weitere Informationen finden Sie unter Datenbank läuft seit langem inaktiv in der Transaktionsverbindung . Versuchen Sie, Ihre Anwendung zu ändern, um die Verwendung von lang andauernden Transaktionen zu vermeiden oder zu minimieren.

Langfristige Aktionen

Untersuchen Sie Ihren Workload, um die Ursache für den Multixact-Spillover zu ermitteln. Sie müssen das Problem beheben, um Ihren Workload zu skalieren und das Warteereignis zu reduzieren.

- Sie müssen die DDL (Datendefinitionssprache) analysieren, die zum Erstellen Ihrer Tabellen verwendet wird. Stellen Sie sicher, dass die Tabellenstrukturen und Indizes gut konzipiert sind.
- Wenn die betroffenen Tabellen Fremdschlüssel haben, stellen Sie fest, ob sie benötigt werden oder ob es eine andere Möglichkeit gibt, die referenzielle Integrität durchzusetzen.
- Wenn eine Tabelle große ungenutzte Indizes hat, kann dies dazu führen, dass die Selbstbereinigung nicht zu Ihrem Workload passt und sie möglicherweise daran hindert, ausgeführt zu werden. Um dies zu vermeiden, suchen Sie nach ungenutzten Indizes und entfernen Sie sie vollständig. Weitere Informationen finden Sie unter Verwalten der Selbstbereinigung mit großen Indizes.
- Reduzieren Sie die Verwendung von Savepoints in Ihren Transaktionen.

Timeout:PgSleep

Das `Timeout:PgSleep`-Ereignis tritt ein, wenn ein Serverprozess die `pg_sleep`-Funktion aufgerufen hat und auf das Ablaufen des Sleep-Timeouts wartet.

Themen

Unterstützte Engine-Versionen

Diese Warteereignisinformationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Dieses Wait-Ereignis tritt auf, wenn eine Anwendung, eine gespeicherte Funktion oder ein Benutzer eine SQL-Anweisung ausgibt, die eine der folgenden Funktionen aufruft:

- `pg_sleep`
- `pg_sleep_for`
- `pg_sleep_until`

Die vorhergehenden Funktionen verzögern die Ausführung, bis die angegebene Anzahl von Sekunden verstrichen ist. Beispielsweise pausiert `SELECT pg_sleep(1)` für 1 Sekunde. Weitere Informationen finden Sie unter Ausführung verzögern in der PostgreSQL-Dokumentation.

Aktionen

Identifizieren Sie die Anweisung, die die `pg_sleep`-Funktion ausgeführt hat. Überprüfen Sie, ob die Verwendung der Funktion angemessen ist.

Optimierung von Aurora PostgreSQL mit proaktiven Einblicken von Amazon DevOps Guru

Proaktive DevOps-Guru-Einblicke erkennen Zustände auf Ihren Aurora-PostgreSQL-DB-Clustern, die Probleme verursachen können, und informiert Sie darüber, bevor diese auftreten. DevOps Guru kann Folgendes tun:

- Vermeiden vieler häufig auftretender Datenbankprobleme durch Abgleich der Datenbankkonfiguration mit den allgemein empfohlenen Einstellungen.
- Warnen vor kritischen Problemen in der Flotte, die, wenn sie nicht überprüft werden, später zu größeren Problemen führen können.

- Benachrichtigung bei neu erkannten Problemen.

Jeder proaktive Einblick beinhaltet eine Analyse der Problemursache und Empfehlungen für Korrekturmaßnahmen.

Themen

Die Datenbank läuft seit langem inaktiv in Transaktionsverbindung

Eine Verbindung zur Datenbank befindet sich sein mehr als 1800 Sekunden im Status `idle in transaction`.

Themen

Unterstützte Engine-Versionen

Diese Einblick-Informationen werden für alle Versionen von Aurora PostgreSQL unterstützt.

Kontext

Eine Transaktion im Status `idle in transaction` kann Sperren enthalten, die andere Abfragen blockieren. Sie kann auch verhindern, dass `VACUUM` (einschließlich Autovacuum) tote Zeilen bereinigt, was zu einer Überlastung von Index oder Tabellen oder zu einem Wraparound der Transaktions-ID führt.

Mögliche Ursachen für dieses Problem

Eine Transaktion, die in einer interaktiven Sitzung mit BEGIN oder START TRANSACTION initiiert wurde, wurde nicht mit einem COMMIT-, ROLLBACK- oder END-Befehl beendet. Dadurch wird die Transaktion in den Status `idle in transaction` versetzt.

Aktionen

Sie können ungenutzte Transaktionen finden, indem Sie `pg_stat_activity` abfragen.

Führen Sie in Ihrem SQL-Client die folgende Abfrage aus, um alle Verbindungen im Status `idle in transaction` aufzulisten und sie nach Dauer zu sortieren:

```
SELECT now() - state_change as idle_in_transaction_duration, now() - xact_start as
 xact_duration,*
FROM  pg_stat_activity
WHERE state  = 'idle in transaction'
AND   xact_start is not null
ORDER BY 1 DESC;
```

Abhängig von den Ursachen Ihres Einblicks empfehlen wir verschiedene Aktionen.

Themen

- Transaktion beenden
- Die Verbindung beenden
- Konfigurieren Sie den Parameter idle_in_transaction_session_timeout
- Überprüfen Sie den AUTOCOMMIT-Status
- Überprüfen Sie die Transaktionslogik in Ihrem Anwendungscode

Transaktion beenden

Wenn Sie eine Transaktion in einer interaktiven Sitzung mit BEGIN oder START TRANSACTION initiieren, wechselt sie in den Status `idle in transaction`. Sie verbleibt in diesem Status, bis Sie die Transaktion beenden, indem Sie einen COMMIT-, ROLLBACK-, END-Befehl ausführen oder die Verbindung vollständig trennen, um die Transaktion rückgängig zu machen.

Die Verbindung beenden

Beenden Sie die Verbindung mit einer inaktiven Transaktion mit der folgenden Abfrage:

```
SELECT pg_terminate_backend(pid);
```

pid ist die Prozess-ID der Verbindung.

Konfigurieren Sie den Parameter idle_in_transaction_session_timeout

Stellen Sie den Parameter `idle_in_transaction_session_timeout` in der Parametergruppe ein. Der Vorteil der Konfiguration dieses Parameters besteht darin, dass kein manueller Eingriff erforderlich ist, um die lang dauernde inaktive Transaktion zu beenden. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation.

Die folgende Meldung wird in der PostgreSQL-Protokolldatei angezeigt, nachdem die Verbindung beendet wurde, wenn sich eine Transaktion länger als die angegebene Zeit im Status idle_in_transaction befindet.

```
FATAL: terminating connection due to idle in transaction timeout
```

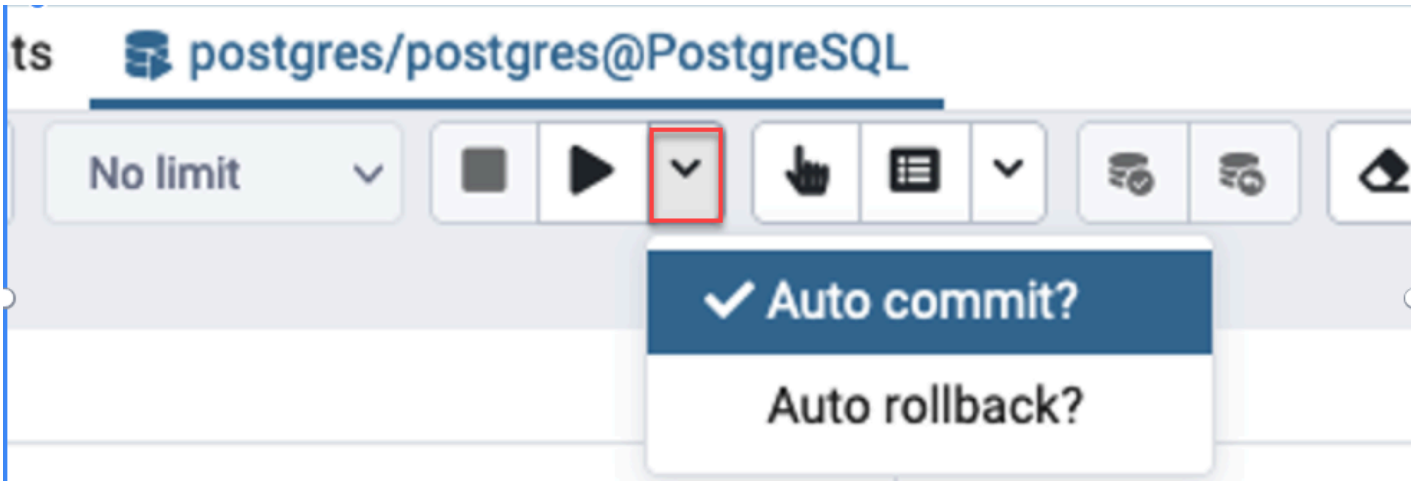
Überprüfen Sie den AUTOCOMMIT-Status

AUTOCOMMIT ist standardmäßig aktiviert. Wenn dies jedoch versehentlich im Client deaktiviert wurde, stellen Sie sicher, dass Sie es wieder aktivieren.

- Führen Sie in Ihrem psql-Client den folgenden Befehl aus:

  ```
  postgres=> \set AUTOCOMMIT on
  ```

- Schalten Sie dies in pgadmin ein, indem Sie die Option AUTOCOMMIT über den Abwärtspfeil wählen.



Überprüfen Sie die Transaktionslogik in Ihrem Anwendungscode

Untersuchen Sie Ihre Anwendungslogik auf mögliche Probleme. Berücksichtigen Sie die folgenden Aktionen:

- Prüfen Sie, ob das JDBC-Autocommit in Ihrer Anwendung auf „true“ gesetzt ist. Erwägen Sie auch, explizite `COMMIT`-Befehle in Ihrem Code zu verwenden.
- Überprüfen Sie Ihre Fehlerbehandlungslogik, um festzustellen, ob eine Transaktion nach einem Fehler geschlossen wird.
- Prüfen Sie, ob Ihre Anwendung lange braucht, um die von einer Abfrage zurückgegebenen Zeilen zu verarbeiten, während die Transaktion geöffnet ist. Wenn dies der Fall ist, erwägen Sie, die Anwendung so zu codieren, dass die Transaktion geschlossen wird, bevor die Zeilen verarbeitet werden.
- Prüfen Sie, ob eine Transaktion viele lang laufende Operationen enthält. Wenn dies der Fall ist, teilen Sie eine einzelne Transaktion in mehrere Transaktionen auf.

Relevante Metriken

Die folgenden PI-Metriken beziehen sich auf diesen Einblick:

- idle_in_transaction_count – Anzahl der Sitzungen im Status `idle in transaction`.
- idle_in_transaction_max_time – Die Dauer der am längsten laufenden Transaktion im Status `idle in transaction`.

Bewährte Methoden mit Amazon Aurora PostgreSQL

Im Folgenden finden Sie einige bewährte Methoden für die Verwaltung Ihres Amazon-Aurora-PostgreSQL-DB-Cluster. Überprüfen Sie auch die grundlegenden Wartungsaufgaben. Weitere Informationen finden Sie unter Verwalten von Amazon Aurora PostgreSQL.

Themen

- Vermeiden von Leistungseinbußen, automatischem Neustart und Failover für DB-Instances von Aurora PostgreSQL
- Diagnostizieren einer Überlastung von Tabellen und Indizes
- Verbesserte Arbeitsspeicherverwaltung in Aurora PostgreSQL
- Schnelles Failover mit Amazon Aurora PostgreSQL
- Schnelle Wiederherstellung nach Failover mit der Cluster-Cacheverwaltung für Aurora PostgreSQL
- Verwalten von Aurora PostgreSQL Verbindungsabwanderung mit Pooling
- Ändern von Speicherparametern für Aurora PostgreSQL

- Verwendung von CloudWatch Amazon-Metriken zur Analyse der Ressourcennutzung für Aurora PostgreSQL
- Verwenden der logischen Replikation, um ein Hauptversions-Upgrade für Aurora PostgreSQL durchzuführen
- Fehlerbehebung bei Speicherproblemen

Vermeiden von Leistungseinbußen, automatischem Neustart und Failover für DB-Instances von Aurora PostgreSQL

Wenn Sie hohe Workloads ausführen, die über die zugewiesenen Ressourcen Ihrer DB-Instance hinausgehen, können Sie die Ressourcen, auf denen Sie Ihre Anwendung und die Aurora-Datenbank ausführen, aufbrauchen. Wenn Sie Metriken für Ihre Datenbank-Instance wie CPU-Auslastung, Speichernutzung und Anzahl der verwendeten Datenbankverbindungen abrufen möchten, können Sie auf die von Amazon CloudWatch bereitgestellten Metriken, auf Performance-Insights und Enhanced Monitoring zurückgreifen. Informationen zur Überwachung Ihrer DB-Instance finden Sie unter Überwachung von Metriken in einem Amazon-Aurora-Cluster.

Wenn Ihre Workload die von Ihnen verwendeten Ressourcen aufbraucht, wird Ihre DB-Instance möglicherweise langsamer, neu gestartet oder es wird sogar ein Failover auf eine andere DB-Instance durchgeführt. Dies können Sie vermeiden, indem Sie Ihre Ressourcenauslastung überwachen, die Workload, die auf Ihrer DB-Instance ausgeführt wird, untersuchen und gegebenenfalls Optimierungen vornehmen. Wenn Optimierungen keine Verbesserungen der Instance-Metriken und keine Verringerung der Ressourcenauslastung ergeben, sollten Sie erwägen, Ihre DB-Instance hochzuskalieren, bevor diese an ihre Grenzen stößt. Weitere Hinweise zu verfügbaren DB-Instance-Klassen und ihren Spezifikationen finden Sie unter Aurora DB-Instance-Klassen.

Diagnostizieren einer Überlastung von Tabellen und Indizes

Sie können PostgreSQL Multiversion Concurrency Control (MVCC) verwenden, um die Datenintegrität zu wahren. PostgreSQL MVCC funktioniert, indem es eine interne Kopie aktualisierter oder gelöschter Zeilen (auch Tupel genannt) speichert, bis für eine Transaktion entweder ein Commit oder ein Rollback ausgeführt wird. Diese gespeicherte interne Kopie ist für Benutzer nicht sichtbar. Wenn diese nicht sichtbaren Kopien nicht regelmäßig von den Dienstprogrammen VACUUM oder AUTOVACUUM bereinigt werden, kann es jedoch zu einer Überlastung der Tabelle kommen. Wenn diese Option nicht aktiviert ist, kann die Überlastung der Tabelle zu erhöhten Speicherkosten führen und Ihre Verarbeitungsgeschwindigkeit verlangsamen.

In vielen Fällen reichen die Standardeinstellungen für VACUUM oder AUTOVACUUM in Aurora aus, um eine ungewollte Überlastung von Tabellen zu vermeiden. Möglicherweise möchten Sie jedoch überprüfen, ob eine Überlastung vorliegt, wenn in Ihrer Anwendung die folgenden Bedingungen vorliegen:

- Verarbeitet eine große Anzahl von Transaktionen in relativ kurzer Zeit zwischen VACUUM-Prozessen.
- Funktioniert schlecht und der Speicherplatz ist knapp.

Sammeln Sie zunächst möglichst genaue Informationen darüber, wie viel Speicherplatz tote Tupel belegen und wie viel Sie wiederherstellen können, indem Sie die Überlastung der Tabellen und Indizes bereinigen. Verwenden Sie dazu die `pgstattuple`-Erweiterung, um Statistiken über Ihren Aurora-Cluster zu sammeln. Weitere Informationen finden Sie unter pgstattuple. Die Berechtigungen zum Verwenden der `pgstattuple`-Erweiterung sind auf die Rolle `pg_stat_scan_tables` und die Datenbank-Superuser beschränkt.

Um die `pgstattuple`-Erweiterung in Aurora zu erstellen, verbinden Sie eine Client-Sitzung mit dem Cluster, z. B. psql oder pgAdmin, und verwenden Sie den folgenden Befehl:

```
CREATE EXTENSION pgstattuple;
```

Erstellen Sie die Erweiterung in jeder Datenbank, für die Sie ein Profil erstellen möchten. Verwenden Sie nach dem Erstellen der Erweiterung die Befehlszeilenschnittstelle (CLI), um zu messen, wie viel unbenutzbaren Speicherplatz Sie zurückgewinnen können. Bevor Sie Statistiken sammeln, ändern Sie die Cluster-Parametergruppe, indem Sie AUTOVACUUM auf 0 festlegen. Die Einstellung 0 verhindert, dass Aurora automatisch alle toten Tupel bereinigt, die Ihre Anwendung hinterlassen hat, was sich auf die Genauigkeit der Ergebnisse auswirken kann. Verwenden Sie den folgenden Befehl, um eine einfache Tabelle zu erstellen:

```
postgres=> CREATE TABLE lab AS SELECT generate_series (0,100000);
SELECT 100001
```

Im folgenden Beispiel führen wir die Abfrage mit aktiviertem AUTOVACUUM für den DB-Cluster aus. Der Wert `dead_tuple_count` ist 0, was bedeutet, dass AUTOVACUUM die veralteten Daten oder Tupel aus der PostgreSQL-Datenbank gelöscht hat.

Wenn Sie Informationen über die Tabelle mit `pgstattuple` sammeln möchten, geben Sie in der Abfrage den Namen einer Tabelle oder eine Objektkennung (OID) an:

```
postgres=> SELECT * FROM pgstattuple('lab');
```

```
table_len  | tuple_count | tuple_len | tuple_percent | dead_tuple_count |
 dead_tuple_len | dead_tuple_percent | free_space | free_percent
-----------+-------------+-----------+---------------+------------------
+----------------+--------------------+------------+--------------
3629056    | 100001      | 2800028   | 77.16         | 0                | 0
  | 0                  | 16616      | 0.46
(1 row)
```

In der folgenden Abfrage schalten wir AUTOVACUUM aus und geben einen Befehl ein, mit dem 25 000 Zeilen aus der Tabelle gelöscht werden. Infolgedessen steigt der Wert `dead_tuple_count` auf 25 000.

```
postgres=> DELETE FROM lab WHERE generate_series < 25000;

DELETE 25000
```

```
SELECT * FROM pgstattuple('lab');
```

```
table_len | tuple_count | tuple_len | tuple_percent | dead_tuple_count | dead_tuple_len
 | dead_tuple_percent | free_space | free_percent
-----------+-------------+-----------+---------------+------------------
+----------------+--------------------+------------+--------------
3629056 | 75001 | 2100028 | 57.87 | 25000 | 700000 | 19.29 | 16616 | 0.46
(1 row)
```

Starten Sie einen VACUUM-Prozess, um diese toten Tupel zurückzugewinnen.

Beobachten von Überlastungen ohne Unterbrechung Ihrer Anwendung

Die Einstellungen in einem Aurora-Cluster sind optimiert, um die bewährten Methoden für die meisten Workloads bereitzustellen. Möglicherweise möchten Sie jedoch einen Cluster optimieren, damit er besser zu Ihren Anwendungen und Nutzungsmustern passt. In diesem Fall können Sie die `pgstattuple`-Erweiterung verwenden, ohne eine aktive Anwendung zu unterbrechen. Führen Sie dazu die folgenden Schritte aus:

1. Klonen Sie Ihre Aurora-Instance.
2. Ändern Sie die Parameterdatei, um AUTOVACUUM im Klon zu deaktivieren.
3. Führen Sie eine `pgstattuple`-Abfrage durch, während Sie den Klon mit einem Beispiel-Workload oder mit pgbench testen, einem Programm zum Ausführen von Benchmark-Tests in PostgreSQL. Weitere Informationen finden Sie unter pgbench.

Nachdem Sie Ihre Anwendungen ausgeführt und das Ergebnis angezeigt haben, verwenden Sie pg_repack oder VACUUM FULL für die wiederhergestellte Kopie und vergleichen Sie die Unterschiede. Wenn Sie einen deutlichen Rückgang der Werte dead_tuple_count, dead_tuple_len oder dead_tuple_percent feststellen, passen Sie den Bereinigungsplan Ihres Produktions-Clusters an, um die Überlastung zu minimieren.

Vermeiden von Überlastung in temporären Tabellen

Wenn Ihre Anwendung temporäre Tabellen erstellt, vergewissern Sie sich, dass Ihre Anwendung diese temporären Tabellen entfernt, wenn sie nicht mehr benötigt werden. Automatische Bereinigungsprozesse finden keine temporären Tabellen. Wenn diese Option nicht aktiviert ist, können temporäre Tabellen schnell zu einer Überlastung der Datenbank führen. Darüber hinaus kann sich die Überlastung auf die Systemtabellen ausweiten. Hierbei handelt es sich um interne Tabellen, die PostgreSQL-Objekte und -Attribute verfolgen, wie pg_attribute und pg_depend.

Wenn eine temporäre Tabelle nicht mehr benötigt wird, können Sie eine TRUNCATE-Anweisung verwenden, um die Tabelle zu leeren und Speicherplatz freizugeben. Bereinigen Sie dann die Tabellen pg_attribute und pg_depend manuell. Durch das Bereinigen dieser Tabellen wird sichergestellt, dass durch das kontinuierliche Erstellen und Kürzen/Löschen temporärer Tabellen keine Tupel hinzugefügt werden und das System nicht überlastet wird.

Sie können dieses Problem beim Erstellen einer temporären Tabelle vermeiden, indem Sie die folgende Syntax verwenden, die die neuen Zeilen löscht, wenn für Inhalt ein Commit ausgeführt wird:

```
CREATE TEMP TABLE IF NOT EXISTS table_name(table_description) ON COMMIT DELETE ROWS;
```

Die `ON COMMIT DELETE ROWS`-Klausel kürzt die temporäre Tabelle, wenn für die Transaktion ein Commit ausgeführt wird.

Vermeiden von Überlastung in Indizes

Wenn Sie ein indiziertes Feld in einer Tabelle ändern, führt die Indexaktualisierung zu einem oder mehreren toten Tupeln in diesem Index. Standardmäßig entfernt der automatische Bereinigungsprozess überflüssige Indizes, aber diese Bereinigung erfordert einen erheblichen Zeit- und Ressourcenaufwand. Um die Einstellungen für die Indexbereinigung beim Erstellen einer Tabelle anzugeben, schließen Sie die Klausel vacuum_index_cleanup ein. Standardmäßig ist die Klausel bei der Tabellenerstellung auf AUTO gesetzt, was bedeutet, dass der Server entscheidet, ob Ihr Index bereinigt werden muss, wenn er die Tabelle bereinigt. Sie können die Klausel auf EIN einstellen, um die Indexbereinigung für eine bestimmte Tabelle zu aktivieren, oder auf AUS, um die Indexbereinigung für diese Tabelle zu deaktivieren. Denken Sie daran, dass das Deaktivieren der Indexbereinigung zwar Zeit sparen kann, aber möglicherweise zu einer Überlastung des Index führen kann.

Sie können die Indexbereinigung manuell steuern, wenn Sie eine Tabelle über die Befehlszeile bereinigen. Wenn Sie eine Tabelle bereinigen und tote Tupel aus den Indizes entfernen möchten, schließen Sie die INDEX_CLEANUP-Klausel mit dem Wert EIN und dem Tabellennamen ein:

```
acctg=> VACUUM (INDEX_CLEANUP ON) receivables;

INFO: aggressively vacuuming "public.receivables"
VACUUM
```

Wenn Sie eine Tabelle bereinigen möchten, ohne die Indizes zu bereinigen, geben Sie den Wert AUS an:

```
acctg=> VACUUM (INDEX_CLEANUP OFF) receivables;

INFO: aggressively vacuuming "public.receivables"
VACUUM
```

Verbesserte Arbeitsspeicherverwaltung in Aurora PostgreSQL

Kundenworkloads, die den in der DB-Instance verfügbaren freien Arbeitsspeicher ausschöpfen, führen zu einem Neustart der Datenbank durch das Betriebssystem, was die Nichtverfügbarkeit der Datenbank zur Folge hat. Aurora PostgreSQL hat verbesserte Funktionen zur Arbeitsspeicherverwaltung eingeführt, die Stabilitätsprobleme und Neustarts der Datenbank aufgrund von zu wenig freiem Arbeitsspeicher proaktiv verhindern. Diese Verbesserung ist standardmäßig in den folgenden Versionen verfügbar:

- 15.3 und höhere 15-Versionen
- 14.8 und höhere 14-Versionen
- 13.11 und höhere 13-Versionen
- 12.15 und höhere 12-Versionen
- 11.20 und höhere 11-Versionen

Die Arbeitsspeicherverwaltung wird auf folgende Weise verbessert:

- Datenbanktransaktionen, die mehr Arbeitsspeicher anfordern, werden abgebrochen, wenn sich das System einem kritischen Arbeitsspeicherdruck nähert.
- Das System steht unter kritischem Arbeitsspeicherdruck, wenn der gesamte physische Arbeitsspeicher bereits ausgeschöpft und auch der Swapspeicher nahezu ausgeschöpft ist. Unter diesen Umständen werden alle Transaktionen abgebrochen, die Speicher anfordern, um den Arbeitsspeicherdruck in der DB-Instance sofort zu reduzieren.
- Wichtige PostgreSQL-Launcher und Hintergrund-Worker wie Autovacuum Worker sind immer geschützt.

Konfigurieren von Speicherverwaltungsparametern

So aktivieren Sie die Speicherverwaltung

Diese Option ist standardmäßig aktiviert. Eine Fehlermeldung wird angezeigt, wenn eine Transaktion aufgrund von zu wenig Arbeitsspeicher abgebrochen wird, wie im folgenden Beispiel gezeigt:

```
ERROR: out of memory Detail: Failed on request of size 16777216.
```

So deaktivieren Sie die Speicherverwaltung

Um diese Funktion zu deaktivieren, stellen Sie mit psql eine Verbindung zum Aurora-PostgreSQL-DB-Cluster her und verwenden Sie die SET-Anweisung für die Parameterwerte, wie unten beschrieben.

Für Aurora-PostgreSQL-Versionen 11.21, 12.16, 13.12, 14.9, 15.4 und ältere Versionen:

```
postgres=>SET rds.memory_allocation_guard = true;
```

Der Standardwert des `rds.memory_allocation_guard` Parameters ist `false` in der Parametergruppe auf gesetzt.

Für Aurora PostgreSQL 12.17, 13.13, 14.10, 15.5 und höhere Versionen:

```
postgres=>rds.enable_memory_management = false;
```

Der Standardwert des `rds.enable_memory_management` Parameters ist `true` in der Parametergruppe auf gesetzt.

Das Festlegen der Werte dieser Parameter in der DB-Cluster-Parametergruppe verhindert, dass die Abfragen abgebrochen werden. Weitere Informationen zur DB-Cluster-Parametergruppe finden Sie unter Arbeiten mit Parametergruppen.

Der Wert dieser dynamischen Parameter kann auch auf Sitzungsebene festgelegt werden, um eine Sitzung in eine verbesserte Speicherverwaltung einzubeziehen oder auszuschließen.

> **Note**
>
> Wir raten davon ab, diese Funktion zu deaktivieren, da sie zu out-of-memory Fehlern führen kann, die aufgrund der Speicherauslastung im System zu einem Workload-bedingten Neustart der Datenbank führen können.

Schnelles Failover mit Amazon Aurora PostgreSQL

Im Folgenden erfahren Sie, wie Sie sicherstellen können, dass ein Failover so schnell wie möglich erfolgt. Zur schnellen Wiederherstellung nach dem Failover können Sie die Cluster-Cache-Verwaltung für Ihren Aurora-PostgreSQL-DB-Cluster verwenden. Weitere Informationen finden Sie unter Schnelle Wiederherstellung nach Failover mit der Cluster-Cacheverwaltung für Aurora PostgreSQL.

Zu den Schritten, die Sie ausführen können, um ein schnelles Failover durchzuführen, gehören die folgenden:

- Setzen Sie Transmission Control Protocol (TCP)-Keepalives mit kurzen Zeitrahmen, um länger laufende Abfragen zu stoppen, bevor das Lese-Timeout abläuft, wenn ein Fehler auftritt.
- Legen Sie strikte Timeouts für das DNS (Java Domain Name System) fest. Auf diese Weise wird sichergestellt, dass der schreibgeschützte Aurora-Endpunkt bei späteren Verbindungsversuchen ordnungsgemäß die schreibgeschützten Knoten durchlaufen kann.
- Legen Sie die Timeout-Variablen, die in der JDBC-Verbindungszeichenfolge verwendet werden, auf einen möglichst niedrigen Wert fest. Setzen Sie für kurze und lange dauernde Abfragen unterschiedliche Verbindungsobjekte ein.
- Verwenden Sie die bereitgestellten Aurora-Endpunkte für Lese- und Schreibvorgänge, um eine Verbindung zum Cluster herzustellen.
- Verwenden Sie RDS-API-Operationen, um die Anwendungsreaktion bei serverseitigen Ausfällen zu testen. Testen Sie die Anwendungsreaktionen auf clientseitige Ausfälle mithilfe eines Packet-Dropping-Tool.
- Verwenden Sie den AWS JDBC-Treiber, um die Failover-Funktionen von Aurora PostgreSQL in vollem Umfang zu nutzen. Weitere Informationen zum AWS JDBC-Treiber und vollständige Anweisungen zu seiner Verwendung finden Sie im Amazon Web Services (AWS) JDBC-Treiber-Repository. GitHub

Diese werden im Folgenden ausführlicher erläutert.

Themen

Einstellen von TCP-Keepalive-Parametern

Wenn Sie eine TCP-Verbindung einrichten, wird ein Satz von Timern mit der Verbindung verknüpft. Wenn der Keepalive-Timer den Wert null erreicht, wird ein Keepalive-Prüfpaket an den Endpunkt der Verknüpfung gesendet. Wenn das Prüfpaket eine Antwort erhält, können Sie davon ausgehen, dass die Verbindung nach wie vor aktiv ist.

Indem Sie TCP-Keepalive-Parameter aktivieren und auf strikte Werte festlegen, können Sie sicherstellen, dass im Falle, dass der Client keine Verbindung zur Datenbank herstellen kann, alle aktiven Verbindungen schnell beendet werden. Die Anwendung kann dann eine Verbindung zu einem neuen Endpunkt herstellen.

Die folgenden TCP-Keepalive-Parameter müssen festgelegt werden:

- `tcp_keepalive_time` gibt die Zeitspanne in Sekunden an, nach der ein Keepalive-Paket gesendet wird, wenn keine Daten vom Socket gesendet wurden. ACKs werden nicht als Daten betrachtet. Wir empfehlen die folgende Einstellung:

  ```
  tcp_keepalive_time = 1
  ```

- `tcp_keepalive_intvl` gibt die Zeitspanne in Sekunden an, die zwischen dem ersten gesendeten Paket und dem Senden von nachfolgenden Keepalive-Paketen verstreicht. Stellen Sie diese Zeit ein, indem Sie die `tcp_keepalive_time`-Parameter verwenden. Wir empfehlen die folgende Einstellung:

  ```
  tcp_keepalive_intvl = 1
  ```

- `tcp_keepalive_probes` gibt die Anzahl von unbeantworteten Keepalive-Prüfpaketen an, nach denen die Anwendung benachrichtigt wird. Wir empfehlen die folgende Einstellung:

  ```
  tcp_keepalive_probes = 5
  ```

Mit diesen Einstellungen sollte die Anwendung innerhalb von fünf Sekunden benachrichtigt werden, wenn die Datenbank nicht mehr antwortet. Falls die Keepalive-Pakete innerhalb des Anwendungsnetzwerks häufig verworfen werden, können Sie einen höheren `tcp_keepalive_probes`-Wert angegeben. Dies ermöglicht mehr Puffer in weniger zuverlässigen Netzwerken, erhöht jedoch die Zeit, die benötigt wird, um einen tatsächlichen Ausfall zu erkennen.

Einrichten von TCP-Keepalive-Parametern in Linux

1. Testen Sie, wie Sie Ihre TCP-Keealive-Parameter konfigurieren.

   Wir empfehlen, dies über die Befehlszeile mit den folgenden Befehlen zu tun. Diese vorgeschlagene Konfiguration ist systemweit. Mit anderen Worten, es wirkt sich auch auf alle anderen Anwendungen aus, die Sockets mit der `SO_KEEPALIVE`-Option erstellen.

   ```
   sudo sysctl net.ipv4.tcp_keepalive_time=1
   sudo sysctl net.ipv4.tcp_keepalive_intvl=1
   ```

```
sudo sysctl net.ipv4.tcp_keepalive_probes=5
```

2. Nachdem Sie eine geeignete Konfiguration für Ihre Anwendung gefunden haben, schreiben Sie diese Einstellungen fest, indem Sie die folgenden Zeilen zu `/etc/sysctl.conf` hinzufügen, einschließlich aller vorgenommenen Änderungen:

```
tcp_keepalive_time = 1
tcp_keepalive_intvl = 1
tcp_keepalive_probes = 5
```

Konfigurieren Ihrer Anwendung für schnelles Failover

Im Folgenden finden Sie eine Beschreibung verschiedener Konfigurationsänderungen für Aurora PostgreSQL, die Sie für ein schnelles Failover vornehmen können. Weitere Informationen zur Einrichtung und Konfiguration des PostgreSQL-JDBC-Treibers finden Sie in der Dokumentation zum PostgreSQL-JDBC-Treiber.

Themen

- Reduzieren von DNS-Cache-Timeouts
- Einstellen einer Aurora PostgreSQL-Verbindungszeichenfolge für ein schnelles Failover
- Weitere Optionen zum Abrufen der Hostzeichenfolge

Reduzieren von DNS-Cache-Timeouts

Wenn Ihre Anwendung versucht, eine Verbindung nach einem Failover aufzubauen, wird der neue Aurora-PostgreSQL-Writer ein früherer Reader sein. Sie können ihn finden, indem Sie den schreibgeschützten Aurora-Endpunkt verwenden, bevor DNS-Updates vollständig verbreitet wurden. Den Java DNS-TTL–(time to live)-Wert niedrig festzulegen, z. B. unter 30 Sekunden, sorgt dafür, dass bei späteren Verbindungsversuchen die Reader-Knoten durchlaufen werden können.

```
// Sets internal TTL to match the Aurora RO Endpoint TTL
java.security.Security.setProperty("networkaddress.cache.ttl" , "1");
// If the lookup fails, default to something like small to retry
java.security.Security.setProperty("networkaddress.cache.negative.ttl" , "3");
```

Einstellen einer Aurora PostgreSQL-Verbindungszeichenfolge für ein schnelles Failover

Für die Verwendung eines schnellen Failover in Aurora PostgreSQL stellen Sie sicher, dass die Verbindungszeichenfolge Ihrer Anwendung eine Liste mit Hosts statt einen einzelnen Host enthält. Im Folgenden eine beispielhafte Verbindungszeichenfolge, die Sie verwenden können, um sich mit einem Aurora-PostgreSQL-Cluster zu verbinden. In diesem Beispiel sind die Hosts fett dargestellt.

```
jdbc:postgresql://myauroracluster.cluster-c9bfei4hjlrd.us-east-1-
beta.rds.amazonaws.com:5432,
myauroracluster.cluster-ro-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432
/postgres?user=<primaryuser>&password=<primarypw>&loginTimeout=2
&connectTimeout=2&cancelSignalTimeout=2&socketTimeout=60
&tcpKeepAlive=true&targetServerType=primary
```

Für die bestmögliche Verfügbarkeit und um eine Abhängigkeit von der RDS-API zu vermeiden, empfehlen wir, eine Datei zu pflegen, mit der Sie eine Verbindung herstellen können. Diese Datei enthält eine Hostzeichenfolge, aus der die Anwendung Daten lesen kann, wenn Sie eine Verbindung zur Datenbank herstellen. Die Hostzeichenfolge enthält alle für das Cluster verfügbaren Aurora-Endpunkte. Weitere Informationen zu Aurora-Endpunkten finden Sie unter Amazon Aurora-Verbindungsverwaltung.

Beispielsweise können Sie Ihre Endpunkte wie folgt in einer lokalen Datei speichern.

```
myauroracluster.cluster-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432,
myauroracluster.cluster-ro-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432
```

Ihre Anwendung liest aus dieser Datei. um den Hostdatenabschnitt der JDBC-Verbindungzeichenfolge mit Daten füllen. Das Umbenennen des DB-Clusters bewirkt eine Änderung dieser Endpunkte. Stellen Sie sicher, dass Ihre Anwendung dieses Ereignis behandelt, falls es auftritt.

Eine weitere Option ist die Verwendung einer Liste mit DB-Instance-Knoten wie folgt.

```
my-node1.cksc6xlmwcyw.us-east-1-beta.rds.amazonaws.com:5432,
my-node2.cksc6xlmwcyw.us-east-1-beta.rds.amazonaws.com:5432,
my-node3.cksc6xlmwcyw.us-east-1-beta.rds.amazonaws.com:5432,
my-node4.cksc6xlmwcyw.us-east-1-beta.rds.amazonaws.com:5432
```

Der Vorteil dieses Ansatzes besteht darin, dass der PostgreSQL-JDBC-Verbindungstreiber alle Knoten dieser Liste in einer Schleife durchläuft, um eine gültige Verbindung zu finden. Im Gegensatz dazu werden bei Verwendung der Aurora-Endpunkte bei jedem Verbindungsversuch nur zwei Knoten

ausprobiert. Die Verwendung von DB-Instance-Knoten hat jedoch einen Nachteil. Wenn Sie Knoten zum Cluster hinzufügen oder daraus entfernen und dadurch die Liste der Instance-Endpunkte nicht mehr aktuell ist, findet der Verbindungstreiber möglicherweise keinen geeigneten Host mehr für einen Verbindungsaufbau.

Um sicherzustellen, dass die Anwendung mit dem Verbindungsaufbau zu einem Host nicht zu lange wartet, legen Sie für die folgenden Parameter strikte Werte fest:

- `targetServerType` – Steuert, ob der Treiber eine Verbindung zu einem Schreib- oder Leseknoten herstellt. Um sicherzustellen, dass Ihre Anwendungen nur eine Verbindung zu einem Schreibknoten herstellen, legen Sie den `targetServerType` auf `primary` fest.

  Werte für den Parameter `targetServerType` sind `primary`, `secondary`, `any` und `preferSecondary`. Der `preferSecondary`-Wert versucht, zuerst die Verbindung zu einem Lese-Knoten herzustellen. Er stellt eine Verbindung zum Schreiber her, wenn keine Leser-Verbindung hergestellt werden kann.
- `loginTimeout` – Steuert, wie lange Ihre Anwendung auf die Anmeldung bei der Datenbank wartet, nachdem eine Socket-Verbindung hergestellt wurde.
- `connectTimeout` – Steuert, wie lange der Socket wartet, um eine Verbindung zur Datenbank herzustellen.

Sie können weitere Anwendungsparameter ändern, um den Verbindungsvorgang zu beschleunigen, anhängig davon, wie strikt die Anwendung sein soll:

- `cancelSignalTimeout` – In einigen Anwendungen soll möglicherweise ein Best-Effort-Abbruchsignal für eine abgelaufene Abfrage gesendet werden. Falls dieses Abbruchsignal in Ihrem Failover-Pfad ist, ziehen Sie dafür eine strikte Einstellung in Erwägung, damit dieses Signal nicht an inaktiven Host gesendet wird.
- `socketTimeout` – Dieser Parameter steuert, wie lange vom Socket auf Lesevorgänge gewartet wird. Er kann als globales Abfrage-Timeout genutzt werden, um sicherzustellen, dass eine Abfrage nicht länger als für diesen Wert wartet. Eine gute Praxis ist es, zwei Verbindungs-Handler zu haben. Ein Verbindungs-Handler führt kurzlebige Abfragen aus und legt diesen Wert niedriger fest. Bei einem anderen Verbindungs-Handler für Abfragen mit langer Ausführungsdauer ist dieser Wert viel höher festgelegt. Auf diese Weise können Sie sich sicher sein, dass TCP-Keepalive-Parameter im Falle eines Serverausfalls Abfragen beenden, die über eine lange Zeit ausgeführt werden.
- `tcpKeepAlive` – Aktivieren Sie diesen Parameter, um sicherzustellen, dass die festgelegten TCP-Keepalive-Parameter angewendet werden.

- `loadBalanceHosts` – Ist der Wert dieses Parameters auf `true` gesetzt, stellt die Anwendung die Verbindung zu einem zufällig aus der Liste der Host-Kandidaten ausgewählten Host her.

Weitere Optionen zum Abrufen der Hostzeichenfolge

Sie können die Hostzeichenfolge aus mehreren Quellen erhalten, einschließlich der `aurora_replica_status`-Funktion und durch Verwenden der Amazon RDS-API.

In vielen Fällen müssen Sie bestimmen, wer Schreiber im Cluster ist oder um weitere Leseknoten im Cluster zu finden. Dazu kann sich Ihre Anwendung mit einer beliebigen DB-Instance im DB-Cluster verbinden und die `aurora_replica_status`-Funktion abfragen. Sie können diese Funktion verwenden, um die Dauer für das Auffinden eines Host für eine Verbindung zu reduzieren. In bestimmten Netzwerkausfallszenarien zeigt out-of-date die `aurora_replica_status` Funktion jedoch möglicherweise Informationen an oder ist unvollständig.

Eine gute Möglichkeit, um sicherzustellen, dass Ihre Anwendung einen Knoten findet, zu dem eine Verbindung hergestellt werden kann, besteht darin, zu versuchen, eine Verbindung zum Cluster-Schreiber-Endpunkt und dann zum Cluster-Reader-Endpunkt herzustellen. Sie tun dies, bis Sie eine lesbare Verbindung herstellen können. Diese Endpunkte ändern sich nur, wenn Sie Ihren DB-Cluster umbenennen. Sie können diese daher normalerweise als statische Elemente Ihrer Anwendung beibehalten oder in einer Ressourcendatei speichern, aus der Ihre Anwendung liest.

Nachdem Sie eine Verbindung zu einem dieser Endpunkte hergestellt haben, können Sie Informationen über den Rest des Clusters erhalten. Dazu rufen Sie die `aurora_replica_status`-Funktion auf. Der folgende Befehl ruft z. B. Informationen mit `aurora_replica_status` ab.

```
postgres=> SELECT server_id, session_id, highest_lsn_rcvd, cur_replay_latency_in_usec,
 now(), last_update_timestamp
FROM aurora_replica_status();

server_id | session_id | highest_lsn_rcvd | cur_replay_latency_in_usec | now |
 last_update_timestamp
-----------+--------------------------------------+-----------------
+---------------------------+-------------------------------+-----------------------
mynode-1 | 3e3c5044-02e2-11e7-b70d-95172646d6ca | 594221001 | 201421 | 2017-03-07
 19:50:24.695322+00 | 2017-03-07 19:50:23+00
mynode-2 | 1efdd188-02e4-11e7-becd-f12d7c88a28a | 594221001 | 201350 | 2017-03-07
 19:50:24.695322+00 | 2017-03-07 19:50:23+00
mynode-3 | MASTER_SESSION_ID | | | 2017-03-07 19:50:24.695322+00 | 2017-03-07
 19:50:23+00
```

```
(3 rows)
```

Beispielsweise könnte der Host-Abschnitt Ihrer Verbindungszeichenfolge sowohl mit den Schreiber- als auch den Reader-Cluster-Endpunkten, wie im Folgenden dargestellt, beginnen.

```
myauroracluster.cluster-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432,
myauroracluster.cluster-ro-c9bfei4hjlrd.us-east-1-beta.rds.amazonaws.com:5432
```

In diesem Szenario versucht die Anwendung, eine Verbindung zu einem beliebigen Knotentyp (primärer oder sekundärer) herzustellen. Wenn Ihre Anwendung verbunden ist, empfiehlt es sich, zuerst den Lese-/Schreibstatus des Knotens zu untersuchen. Fragen Sie dazu das Ergebnis des Befehls `SHOW transaction_read_only` ab.

Gibt die Abfrage den Wert `OFF` zurück, haben Sie erfolgreich eine Verbindung zum primären Knoten hergestellt. Angenommen, der Rückgabewert ist jedoch `ON` und Ihre Anwendung benötigt eine Lese-/Schreibverbindung. In diesem Fall können Sie die `aurora_replica_status`-Funktion aufrufen, um festzustellen, ob `server_id session_id='MASTER_SESSION_ID'` enthält. Diese Funktion gibt Ihnen den Namen des primären Knotens zurück. Sie können dies mit dem `endpointPostfix` verwenden, das wie folgt beschrieben ist.

Stellen Sie sicher, dass Sie wissen, wenn Sie eine Verbindung zu einem Replica herstellen, das veraltete Daten enthält. In diesem Fall zeigt die `aurora_replica_status` Funktion möglicherweise out-of-date Informationen an. Sie können einen Schwellenwert für Alterung auf Anwendungsebene festlegen. Um dies zu überprüfen, können Sie den Unterschied zwischen der Serverzeit und dem `last_update_timestamp`-Wert betrachten. Im Allgemeinen sollte Ihre Anwendung es vermeiden, aufgrund widersprüchlicher Informationen, die von der Funktion `aurora_replica_status` zurückgegeben werden, zwischen zwei Hosts hin- und herzuschalten. Ihre Anwendung sollte zuerst alle bekannten Hosts ausprobieren, anstatt den von `aurora_replica_status` zurückgegebenen Daten zu folgen.

Java-Beispiel zum Auflisten von Instances, die den Vorgang DescribeDBClusters-API verwenden

Sie können programmgesteuert mit AWS SDK for Java nach der Instance-Liste suchen, genauer gesagt, mit dem Vorgang DescribeDBClusters-API.

Hier ist ein kleines Beispiel, wie Sie dies in Java 8 durchführen können.

```
AmazonRDS client = AmazonRDSClientBuilder.defaultClient();
```

```
DescribeDBClustersRequest request = new DescribeDBClustersRequest()
   .withDBClusterIdentifier(clusterName);
DescribeDBClustersResult result =
rdsClient.describeDBClusters(request);

DBCluster singleClusterResult = result.getDBClusters().get(0);

String pgJDBCEndpointStr =
singleClusterResult.getDBClusterMembers().stream()
   .sorted(Comparator.comparing(DBClusterMember::getIsClusterWriter)
   .reversed()) // This puts the writer at the front of the list
   .map(m -> m.getDBInstanceIdentifier() + endpointPostfix + ":" +
 singleClusterResult.getPort()))
   .collect(Collectors.joining(","));
```

Hier enthält `pgJDBCEndpointStr` eine formatierte Liste mit Endpunkten, wie im Folgenden.

```
my-node1.cksc6xlmwcyw.us-east-1-beta.rds.amazonaws.com:5432,
my-node2.cksc6xlmwcyw.us-east-1-beta.rds.amazonaws.com:5432
```

Die Variable `endpointPostfix` kann eine Konstante sein, die Ihre Anwendung festlegt. Oder Ihre Anwendung kann es erhalten, indem sie den `DescribeDBInstances`-API-Vorgang für eine einzelne Instance in Ihrem Cluster abfragt. Dieser Wert bleibt innerhalb eines AWS-Region und für einen einzelnen Kunden konstant. Es wird also ein API-Aufruf gespeichert, um diese Konstante in einer Ressourcendatei zu speichern, aus der Ihre Anwendung liest. Im vorherigen Beispiel ist es auf den folgenden festgelegt.

```
.cksc6xlmwcyw.us-east-1-beta.rds.amazonaws.com
```

Eine gute Methode zur Gewährleistung der Verfügbarkeit ist die standardmäßige Nutzung der Aurora-Endpunkte Ihres DB-Clusters für den Fall, dass die API nicht oder zu langsam reagiert. Diese Endpunkte sind garantiert auf dem aktuellen Stand – im Zeitraum, der für das Update eines DNS-Datensatzes benötigt wird. Das Aktualisieren des DNS-Eintrags mit einem Endpunkt dauert in der Regel weniger als 30 Sekunden. Sie können den Endpunkt in einer Ressourcendatei speichern, die von Ihrer Anwendung verwendet wird.

Testen eines Failovers

In allen Fällen müssen Sie einen DB-Cluster mit zwei oder mehr DB-Instances haben.

Serverseitig können bestimmte API-Vorgänge einen Ausfall verursachen, anhand dessen Sie testen können, wie Ihre Anwendungen reagieren:

- FailoverDBCluster – Dieser Vorgang versucht, eine neue DB-Instance in Ihrem DB-Cluster an den Scrhreiber weiterzuleiten.

  Das folgende Codebeispiel zeigt, wie Sie mit `failoverDBCluster` einen Ausfall verursachen können. Weitere Informationen zur Einrichtung eines Amazon RDS-Clients finden Sie unter Verwenden des AWS SDK for Java.

  ```
  public void causeFailover() {

      final AmazonRDS rdsClient = AmazonRDSClientBuilder.defaultClient();

      FailoverDBClusterRequest request = new FailoverDBClusterRequest();
      request.setDBClusterIdentifier("cluster-identifier");

      rdsClient.failoverDBCluster(request);
  }
  ```

- RebootDBInstance – Failover ist nicht in diesem API-Vorgang garantiert. Es fährt jedoch die Datenbank auf dem Schreiber herunter. Sie können es verwenden, um zu testen, wie Ihre Anwendung auf das Abbrechen von Verbindungen reagiert. Der `ForceFailover`-Parameter gilt nicht für Aurora-Engines. Verwenden Sie stattdessen den `FailoverDBCluster`-API-Vorgang.
- ModifyDBCluster – Das Modifizieren des `Port`-Parameters wird einen Nutzungsausfall verursachen, wenn die Knoten im Cluster über einen neuen Port kommunizieren. Im Allgemeinen kann Ihre Anwendung zuerst auf diesen Fehler reagieren, indem sie sicherstellt, dass nur Ihre Anwendung die Portänderungen kontrolliert. Stellen Sie außerdem sicher, dass die Endpunkte, von denen es abhängig ist, ordnungsgemäß aktualisiert werden können. Sie können dies tun, indem Sie jemanden beauftragen, den Port manuell zu aktualisieren, wenn er Änderungen auf API-Ebene vornimmt. Oder Sie können dies tun, indem Sie die RDS-API in Ihrer Anwendung verwenden, um festzustellen, ob sich der Port geändert hat.
- ModifyDBInstance – Ändern des `DBInstanceClass`-Parameters verursacht einen Ausfall.
- DeleteDBInstance – Das Löschen des primären (Schreibers) wird eine Weiterleitung einer neuen DB-Instance an den Schreiber in Ihrem DB-Cluster verursachen.

Wenn Sie Linux verwenden, können Sie auf Anwendungs- oder Clientseite testen, wie die Anwendung auf plötzliche Paketverluste reagiert. Sie können dies basierend darauf tun, ob Port, Host

oder ob TCP-Keepalive-Pakete gesendet oder empfangen werden, indem Sie den Befehl „iptables“ verwenden.

Beispiel für schnelles Java-Failover

Der folgende Beispiel-Code zeigt, wie eine Anwendung einen Aurora-PostgreSQL-Treibermanager einrichten kann.

Die Anwendung ruft die `getConnection`-Funktion auf, wenn eine Verbindung hergestellt werden soll. Ein Anruf bei `getConnection` kann möglicherweise keinen gültigen Host finden. Ein Beispiel ist, wenn kein Schreiber gefunden wird, aber der `targetServerType`-Parameter auf `primary` festgelegt ist. In diesem Fall sollte die aufrufende Anwendung einfach erneut versuchen, die Funktion aufzurufen.

Um zu vermeiden, dass das Wiederholungsverhalten auf die Anwendung geschoben wird, können Sie diesen Wiederholungsaufruf in einen Verbindungspooler verpacken. Bei den meisten Verbindungspoolern können Sie eine JDBC-Verbindungszeichenfolge angeben. Ihre Anwendung ewerbung kann sich also bei `getJdbcConnectionString` einwählen und das an den Verbindungspooler weitergeben. Dadurch können Sie ein schnelleres Failover mit Aurora PostgreSQL verwenden.

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.SQLException;
import java.sql.Statement;
import java.util.ArrayList;
import java.util.List;
import java.util.stream.Collectors;
import java.util.stream.IntStream;

import org.joda.time.Duration;

public class FastFailoverDriverManager {
   private static Duration LOGIN_TIMEOUT = Duration.standardSeconds(2);
   private static Duration CONNECT_TIMEOUT = Duration.standardSeconds(2);
   private static Duration CANCEL_SIGNAL_TIMEOUT = Duration.standardSeconds(1);
   private static Duration DEFAULT_SOCKET_TIMEOUT = Duration.standardSeconds(5);

   public FastFailoverDriverManager() {
       try {
            Class.forName("org.postgresql.Driver");
       } catch (ClassNotFoundException e) {
```

```
            e.printStackTrace();
      }

      /*
        * RO endpoint has a TTL of 1s, we should honor that here. Setting this
aggressively makes sure that when
        * the PG JDBC driver creates a new connection, it will resolve a new different
RO endpoint on subsequent attempts
        * (assuming there is > 1 read node in your cluster)
        */
       java.security.Security.setProperty("networkaddress.cache.ttl" , "1");
      // If the lookup fails, default to something like small to retry
      java.security.Security.setProperty("networkaddress.cache.negative.ttl" , "3");
  }

  public Connection getConnection(String targetServerType) throws SQLException {
      return getConnection(targetServerType, DEFAULT_SOCKET_TIMEOUT);
  }

  public Connection getConnection(String targetServerType, Duration queryTimeout)
throws SQLException {
       Connection conn =
DriverManager.getConnection(getJdbcConnectionString(targetServerType, queryTimeout));

      /*
        * A good practice is to set socket and statement timeout to be the same thing
since both
        * the client AND server will stop the query at the same time, leaving no
running queries
        * on the backend
        */
       Statement st = conn.createStatement();
       st.execute("set statement_timeout to " + queryTimeout.getMillis());
       st.close();

      return conn;
  }

  private static String urlFormat = "jdbc:postgresql://%s"
          + "/postgres"
          + "?user=%s"
          + "&password=%s"
          + "&loginTimeout=%d"
          + "&connectTimeout=%d"
```

```
            + "&cancelSignalTimeout=%d"
            + "&socketTimeout=%d"
            + "&targetServerType=%s"
            + "&tcpKeepAlive=true"
            + "&ssl=true"
            + "&loadBalanceHosts=true";
    public String getJdbcConnectionString(String targetServerType, Duration
 queryTimeout) {
        return String.format(urlFormat,
                getFormattedEndpointList(getLocalEndpointList()),
                CredentialManager.getUsername(),
                CredentialManager.getPassword(),
                LOGIN_TIMEOUT.getStandardSeconds(),
                CONNECT_TIMEOUT.getStandardSeconds(),
                CANCEL_SIGNAL_TIMEOUT.getStandardSeconds(),
                queryTimeout.getStandardSeconds(),
                targetServerType
        );
    }

    private List<String> getLocalEndpointList() {
        /*
          * As mentioned in the best practices doc, a good idea is to read a local
 resource file and parse the cluster endpoints.
          * For illustration purposes, the endpoint list is hardcoded here
          */
         List<String> newEndpointList = new ArrayList<>();
         newEndpointList.add("myauroracluster.cluster-c9bfei4hjlrd.us-east-1-
beta.rds.amazonaws.com:5432");
         newEndpointList.add("myauroracluster.cluster-ro-c9bfei4hjlrd.us-east-1-
beta.rds.amazonaws.com:5432");

        return newEndpointList;
    }

    private static String getFormattedEndpointList(List<String> endpoints) {
        return IntStream.range(0, endpoints.size())
                .mapToObj(i -> endpoints.get(i).toString())
                .collect(Collectors.joining(","));
    }
}
```

Schnelle Wiederherstellung nach Failover mit der Cluster-Cacheverwaltung für Aurora PostgreSQL

Verwenden Sie bei einem Failover zur schnellen Wiederherstellung der Writer-DB-Instance in den Aurora PostgreSQL-Clustern die Cluster-Cacheverwaltung für Amazon Aurora PostgreSQL. Die Cluster-Cacheverwaltung stellt bei einem Failover die Anwendungsleistung sicher.

Bei einem typischen Failover kommt es möglicherweise zu einem temporären, aber erheblichen Leitungsabfall. Dieser Abfall ist darauf zurückzuführen, dass der Puffercache beim Start der Failover-DB-Instance leer ist. Ein leerer Cache wird auch als kalter Cache bezeichnet. Ein kalter Cache beeinträchtigt die Leistung, da die DB-Instance vom langsameren Datenträger lesen muss, statt die im Puffercache gespeicherten Werte nutzen zu können.

Mit der Cluster-Cacheverwaltung legen Sie eine bestimmte Reader-DB-Instance als Failover-Ziel fest. Die Cluster-Cacheverwaltung stellt sicher, dass die Daten im Cache des designierten Readers mit den Cachedaten der Writer-DB-Instance synchronisiert werden. Der vorab gefüllte Cache des designierten Readers wird als warmer Cache bezeichnet. Wenn ein Failover auftritt, verwendet der designierte Reader Werte in seinem warmen Cache, sobald er auf die neue Writer-DB-Instance hochgestuft wird. Dank dieses Ansatzes wird die Wiederherstellungsleistung Ihrer Anwendung deutlich verbessert.

Die Cluster-Cacheverwaltung erfordert, dass die zugeordnete Reader-Instance den gleichen Instance-Klassentyp und dieselbe Größe (zum Beispiel `db.r5.2xlarge` oder `db.r5.xlarge`) hat wie der Writer. Denken Sie daran, wenn Sie Ihre Aurora PostgreSQL-DB-Cluster erstellen, damit Ihr Cluster während eines Failovers wiederhergestellt werden kann. Eine Auflistung der Instance-Klassentypen und -größen finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.

> **Note**
>
> Die Verwaltung des Cluster-Cache wird für Aurora-PostgreSQL-DB-Cluster, die Teil der globalen Aurora-Datenbanken sind, nicht unterstützt. Es wird empfohlen, dass kein Workload auf dem angegebenen Tier-0-Leser ausgeführt wird.

Inhalt

- Aktivieren der Cluster-Cache-Verwaltung
- Festlegen der Prioritätsstufe für das Hochstufen für die Writer-DB-Instance
- Festlegen der Prioritätsstufe für das Hochstufen für eine Reader-DB-Instance
- Überwachung des Puffercaches
- Fehlerbehebung bei der CCM-Konfiguration

Konfigurieren der Cluster-Cache-Verwaltung

Führen Sie die folgenden Prozesse der Reihe nach aus, um die Cluster-Cache-Verwaltung zu konfigurieren.

Themen

- Aktivieren der Cluster-Cache-Verwaltung
- Festlegen der Prioritätsstufe für das Hochstufen für die Writer-DB-Instance
- Festlegen der Prioritätsstufe für das Hochstufen für eine Reader-DB-Instance

> **Note**
>
> Warten Sie nach Abschluss dieser Schritte mindestens 1 Minute ab, damit die Cluster-Cache-Verwaltung voll einsatzbereit ist.

Aktivieren der Cluster-Cache-Verwaltung

Um die Cluster-Cache-Verwaltung zu aktivieren, führen Sie die im Folgenden beschriebenen Schritte aus,.

Konsole

So aktivieren Sie die Cluster-Cacheverwaltung:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie die Parametergruppe für Ihren Aurora PostgreSQL-DB-Cluster in der Liste aus.

Der DB-Cluster muss eine andere als die Standardparametergruppe verwenden, da die Werte in dieser Gruppe nicht geändert werden können.

4. Wählen Sie für Parameter group actions (Parametergruppenaktionen) die Option Bearbeiten.
5. Legen Sie den Wert des Cluster-Parameters `apg_ccm_enabled` auf 1 fest.
6. Wählen Sie Änderungen speichern aus.

AWS CLI

Verwenden Sie zum Aktivieren der Cluster-Cacheverwaltung für einen Aurora-PostgreSQL-DB-Cluster den AWS CLI `modify-db-cluster-parameter-group`-Befehl mit den folgenden erforderlichen Parametern:

- `--db-cluster-parameter-group-name`
- `--parameters`

Example

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name my-db-cluster-parameter-group \
    --parameters "ParameterName=apg_ccm_enabled,ParameterValue=1,ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name my-db-cluster-parameter-group ^
    --parameters "ParameterName=apg_ccm_enabled,ParameterValue=1,ApplyMethod=immediate"
```

Festlegen der Prioritätsstufe für das Hochstufen für die Writer-DB-Instance

Für die Cluster-Cache-Verwaltung muss die Prioritätsstufe für das Hochstufen für die Writer-DB-Instance des Aurora PostgreSQL-DB-Clusters tier-0 sein. Die Prioritätsstufe für das Hochstufen gibt die Reihenfolge an, in der ein Aurora-Reader nach einem Ausfall zur Writer-DB-Instance hochgestuft wird. Gültige Werte sind 0 – 15, wobei 0 die erste und 15 die letzte Prioritätsstufe darstellt. Weitere Informationen zur Hochstufungspriorität finden Sie unter Fehlertoleranz für einen Aurora-DB-Cluster.

Konsole

So legen Sie die Prioritätsstufe für das Hochstufen auf die Writer-DB-Instance auf „tier-0“ fest

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie die Writer-DB-Instance des Aurora PostgreSQL-DB-Clusters aus.
4. Wählen Sie Modify aus. Die Seite Modify DB Instance (DB-Instance ändern) wird angezeigt.
5. Wählen Sie im Bereich Zusätzliche Konfiguration für Failover priority (Failover-Priorität) die Option tier-0 aus.
6. Klicken Sie auf Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.
7. Wählen Sie Apply immediately (Sofort anwenden) aus, um die Änderungen nach dem Speichern sofort zu übernehmen.
8. Klicken Sie auf Modify DB Instance (DB-Instance ändern), um Ihre Änderungen zu speichern.

AWS CLI

Um die Prioritätsstufe für das Hochstufen auf 0 für die Writer-DB-Instance mithilfe der festzulegenAWS CLI, rufen Sie den modify-db-instance Befehl mit den folgenden erforderlichen Parametern auf:

- `--db-instance-identifier`
- `--promotion-tier`
- `--apply-immediately`

Example

Für Linux, macOSoder Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier writer-db-instance \
    --promotion-tier 0 \
    --apply-immediately
```

Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier writer-db-instance ^
    ---promotion-tier 0  ^
    --apply-immediately
```

Festlegen der Prioritätsstufe für das Hochstufen für eine Reader-DB-Instance

Sie müssen nur eine Reader-DB-Instance für die Cluster-Cache-Verwaltung festlegen. Wählen Sie dazu einen Reader aus dem Aurora PostgreSQL-Cluster aus, der dieselbe Instance-Klasse und -Größe hat wie die Writer-DB-Instance. Wenn der Writer beispielsweise `db.r5.xlarge` verwendet, dann wählen Sie einen Reader aus, der denselben Instance-Klassentyp und dieselbe Größe verwendet. Legen Sie dann die Prioritätsstufe für das Hochstufen auf 0 fest.

Die Prioritätsstufe für das Hochstufen gibt die Reihenfolge an, in der ein Aurora-Reader nach einem Ausfall zur Writer-DB-Instance hochgestuft wird. Gültige Werte sind 0 – 15, wobei 0 die erste und 15 die letzte Prioritätsstufe darstellt.

Konsole

So legen Sie die Prioritätsstufe für das Hochstufen auf die Reader-DB-Instance auf „tier-0“ fest

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie eine Reader-DB-Instance aus dem Aurora PostgreSQL-DB-Cluster aus, der der Instance-Klasse der Writer-DB-Instance entspricht.
4. Wählen Sie Modify aus. Die Seite Modify DB Instance (DB-Instance ändern) wird angezeigt.
5. Wählen Sie im Bereich Zusätzliche Konfiguration für Failover priority (Failover-Priorität) die Option tier-0 aus.
6. Klicken Sie auf Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.
7. Wählen Sie Apply immediately (Sofort anwenden) aus, um die Änderungen nach dem Speichern sofort zu übernehmen.
8. Klicken Sie auf Modify DB Instance (DB-Instance ändern), um Ihre Änderungen zu speichern.

AWS CLI

Um die Prioritätsstufe für das Hochstufen auf 0 für die Reader-DB-Instance mithilfe der festzulegenAWS CLI, rufen Sie den modify-db-instance Befehl mit den folgenden erforderlichen Parametern auf:

- `--db-instance-identifier`
- `--promotion-tier`
- `--apply-immediately`

Example

Für Linux, macOSoder Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier reader-db-instance \
    --promotion-tier 0 \
    --apply-immediately
```

Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier reader-db-instance ^
    ---promotion-tier 0  ^
    --apply-immediately
```

Überwachung des Puffercaches

Nach dem Einrichten der Cluster-Cache-Verwaltung können Sie den Synchronisierungsstatus zwischen dem Puffercache der Writer-DB-Instance und dem Warm-Puffercache des jeweiligen Readers überwachen. Um den Inhalt des Puffercache sowohl auf der Writer-DB-Instance als auch auf der angegebenen Reader-DB-Instance zu untersuchen, verwenden Sie das PostgreSQL-Modul `pg_buffercache`. Weitere Informationen finden Sie in der PostgreSQL `pg_buffercache`-Dokumentation.

Verwendung der **`aurora_ccm_status`**-Funktion

Die Cluster-Cacheverwaltung stellt außerdem die Funktion `aurora_ccm_status` zur Verfügung. Verwenden Sie die Funktion `aurora_ccm_status` auf der Writer-DB-Instance, um die folgenden Informationen zum Verlauf des Cache-Warmings auf dem designierten Reader abzurufen.

- `buffers_sent_last_minute` – Die Anzahl der Puffer, die in der letzten Minute an den designierten Reader gesendet wurden.
- `buffers_found_last_minute` – Die Anzahl der Puffer, auf die in der letzten Minute häufig zugegriffen wurde.
- `buffers_sent_last_scan` – Die Anzahl der Puffer, die während des letzten vollständigen Scanvorgangs des Puffercaches an den designierten Reader gesendet wurden.
- `buffers_found_last_scan` – Die Anzahl der Puffer, die häufig aufgerufen wurden und die während des letzten vollständigen Scanvorgangs des Puffercaches gesendet werden mussten. Puffer, die bereits im Cache des designierten Readers abgelegt wurden, werden nicht gesendet.
- `buffers_sent_current_scan` – Die Anzahl der Puffer, die während des aktuellen Scanvorgangs bisher gesendet wurden.
- `buffers_found_current_scan` – Die Anzahl der Puffer, die während des aktuellen Scanvorgangs häufig aufgerufen wurden.
- `current_scan_progress` – Die Anzahl der Puffer, die während des aktuellen Scanvorgangs bisher besucht wurden.

Das folgende Beispiel veranschaulicht, wie ein Teil der Ausgabe mithilfe der Funktion `aurora_ccm_status` in eine aktive Rate und einen aktiven Prozentsatz konvertiert wird.

```
SELECT buffers_sent_last_minute*8/60 AS warm_rate_kbps,
   100*(1.0-buffers_sent_last_scan::float/buffers_found_last_scan) AS warm_percent
   FROM aurora_ccm_status();
```

Fehlerbehebung bei der CCM-Konfiguration

Wenn Sie den `apg_ccm_enabled` Cluster-Parameter aktivieren, wird die Cluster-Cache-Verwaltung automatisch auf Instance-Ebene auf der Writer-DB-Instance und einer Reader-DB-Instance auf dem Aurora-PostgreSQL-DB-Cluster aktiviert. Die Writer- und Reader-Instance sollten denselben Instance-Klassentyp und dieselbe Größe verwenden. Ihre Prioritätsstufe für das Hochstufen ist auf festgelegt`0`. Andere Reader-Instances im DB-Cluster sollten eine Hochstufungsstufe ungleich Null haben und die Cluster-Cache-Verwaltung ist für diese Instances deaktiviert.

Die folgenden Gründe können zu Problemen in der Konfiguration führen und die Cluster-Cache-Verwaltung deaktivieren:

- Wenn keine einzelne Reader-DB-Instance auf Hochstufungsstufe 0 festgelegt ist.
- Wenn die Writer-DB-Instance nicht auf Hochstufungsstufe 0 festgelegt ist.
- Wenn mehr als eine Reader-DB-Instance auf Hochstufungsstufe 0 festgelegt ist.
- Wenn der Writer und eine Reader-DB-Instance mit Hochstufungsstufe 0 nicht dieselbe Instance-Größe haben.

Verwalten von Aurora PostgreSQL Verbindungsabwanderung mit Pooling

Wenn Clientanwendungen so oft eine Verbindung herstellen und trennen, dass sich die Reaktionszeit des Aurora PostgreSQL DB-Clusters verlangsamt, erfährt der Cluster Verbindungsprobleme. Jede neue Verbindung zum Aurora PostgreSQL DB-Cluster-Endpunkt verbraucht Ressourcen und reduziert so die Ressourcen, die zur Verarbeitung der tatsächlichen Workload verwendet werden können. Verbindungsprobleme sollten Sie anhand einiger der unten beschriebenen bewährten Methoden lösen.

Für den Anfang können Sie die Antwortzeiten auf Aurora PostgreSQL DB-Clustern mit hohen Verbindungsproblemvorkommnissen verbessern. Sie können beispielsweise einen Verbindungspooler wie RDS-Proxy verwenden. Ein Verbindungspooler stellt einen Cache mit gebrauchsfertigen Verbindungen für Clients bereit. Fast alle Versionen von Aurora PostgreSQL unterstützen RDS Proxy. Weitere Informationen finden Sie unter Amazon RDS Proxy mit Aurora PostgreSQL.

Wenn Ihre spezielle Version von Aurora PostgreSQL RDS Proxy nicht unterstützt, können Sie einen anderen PostgreSQL-kompatiblen Verbindungspooler wie PGBouncer verwenden. Weitere Informationen hierzu finden Sie auf der PG Bouncer-Website.

Um zu sehen, ob Ihr Aurora-PostgreSQL-DB-Cluster vom Verbindungspooling profitieren kann, können Sie die `postgresql.log`-Datei für Verbindungen und Verbindungstrennungen prüfen. Sie können Performance Insights auch verwenden, um herauszufinden, wie viel Verbindungsprobleme in Ihrem Aurora PostgreSQL DB-Cluster auftreten. Im Folgenden finden Sie Informationen zu beiden Themen.

Verbindungen und Verbindungstrennungen protokollieren

Die PostgreSQL `log_connections`- und `log_disconnections`-Parameter können Verbindungen und Verbindungsabbrüche zur Writer-Instance des Aurora-PostgreSQL-DB-Clusters. Diese Parameter sind standardmäßig deaktiviert. Um diese Parameter zu aktivieren, verwenden Sie eine benutzerdefinierte Parametergruppe, und aktivieren Sie sie, indem Sie den Wert in 1 ändern. Weitere Informationen zu benutzerdefinierten DB-Parametergruppen finden Sie unter Arbeiten mit DB-Cluster-Parametergruppen. Um die Einstellungen zu überprüfen, stellen Sie mithilfe von psql eine Verbindung zu Ihrem DB-Cluster-Endpunkt für Aurora PostgreSQL her und fragen Sie wie folgt ab.

```
labdb=> SELECT setting FROM pg_settings
  WHERE name = 'log_connections';
 setting
---------
on
(1 row)
labdb=> SELECT setting FROM pg_settings
  WHERE name = 'log_disconnections';
setting
---------
on
(1 row)
```

Wenn beide Parameter aktiviert sind, erfasst das Protokoll alle neuen Verbindungen und Verbindungsabbrüche. Sie sehen den Benutzer und die Datenbank für jede neue autorisierte Verbindung. Beim Verbindungstrennungen wird auch die Sitzungsdauer protokolliert, wie im folgenden Beispiel gezeigt.

```
2022-03-07 21:44:53.978 UTC [16641] LOG: connection authorized: user=labtek
 database=labdb application_name=psql
2022-03-07 21:44:55.718 UTC [16641] LOG: disconnection: session time: 0:00:01.740
 user=labtek database=labdb host=[local]
```

Um Ihre Anwendung auf Verbindungsprobleme zu überprüfen, aktivieren Sie diese Parameter, falls sie noch nicht aktiviert sind. Sammeln Sie dann Daten im PostgreSQL-Protokoll zur Analyse, indem Sie Ihre Anwendung mit einer realistischen Workload und einem realistischen Zeitraum ausführen. Sie können die Protokolldatei in der RDS-Konsole anzeigen. Wählen Sie die Writer-Instance Ihres Aurora-PostgreSQL-DB-Clusters aus und klicken Sie dann auf den Tab Logs & Ereignisse. Weitere Informationen finden Sie unter Anzeigen und Auflisten von Datenbank-Protokolldateien.

Sie können auch die Protokolldatei von der Konsole herunterladen und die folgende Befehlssequenz verwenden. Diese Sequenz ermittelt die Gesamtzahl der autorisierten und unterbrochenen Verbindungen pro Minute.

```
grep "connection authorized\|disconnection: session time:"
 postgresql.log.2022-03-21-16|\
awk {'print $1,$2}' |\
sort |\
uniq -c |\
sort -n -k1
```

In der Beispielausgabe sehen Sie einen Anstieg der autorisierten Verbindungen, gefolgt von Verbindungsabbrüchen ab 16:12:10.

```
.....
,.......
.........
5 2022-03-21 16:11:55 connection authorized:
9 2022-03-21 16:11:55 disconnection: session
5 2022-03-21 16:11:56 connection authorized:
5 2022-03-21 16:11:57 connection authorized:
5 2022-03-21 16:11:57 disconnection: session
32 2022-03-21 16:12:10 connection authorized:
30 2022-03-21 16:12:10 disconnection: session
31 2022-03-21 16:12:11 connection authorized:
27 2022-03-21 16:12:11 disconnection: session
27 2022-03-21 16:12:12 connection authorized:
27 2022-03-21 16:12:12 disconnection: session
41 2022-03-21 16:12:13 connection authorized:
47 2022-03-21 16:12:13 disconnection: session
46 2022-03-21 16:12:14 connection authorized:
41 2022-03-21 16:12:14 disconnection: session
24 2022-03-21 16:12:15 connection authorized:
29 2022-03-21 16:12:15 disconnection: session
28 2022-03-21 16:12:16 connection authorized:
24 2022-03-21 16:12:16 disconnection: session
40 2022-03-21 16:12:17 connection authorized:
42 2022-03-21 16:12:17 disconnection: session
40 2022-03-21 16:12:18 connection authorized:
40 2022-03-21 16:12:18 disconnection: session
.....
,.......
.........
```

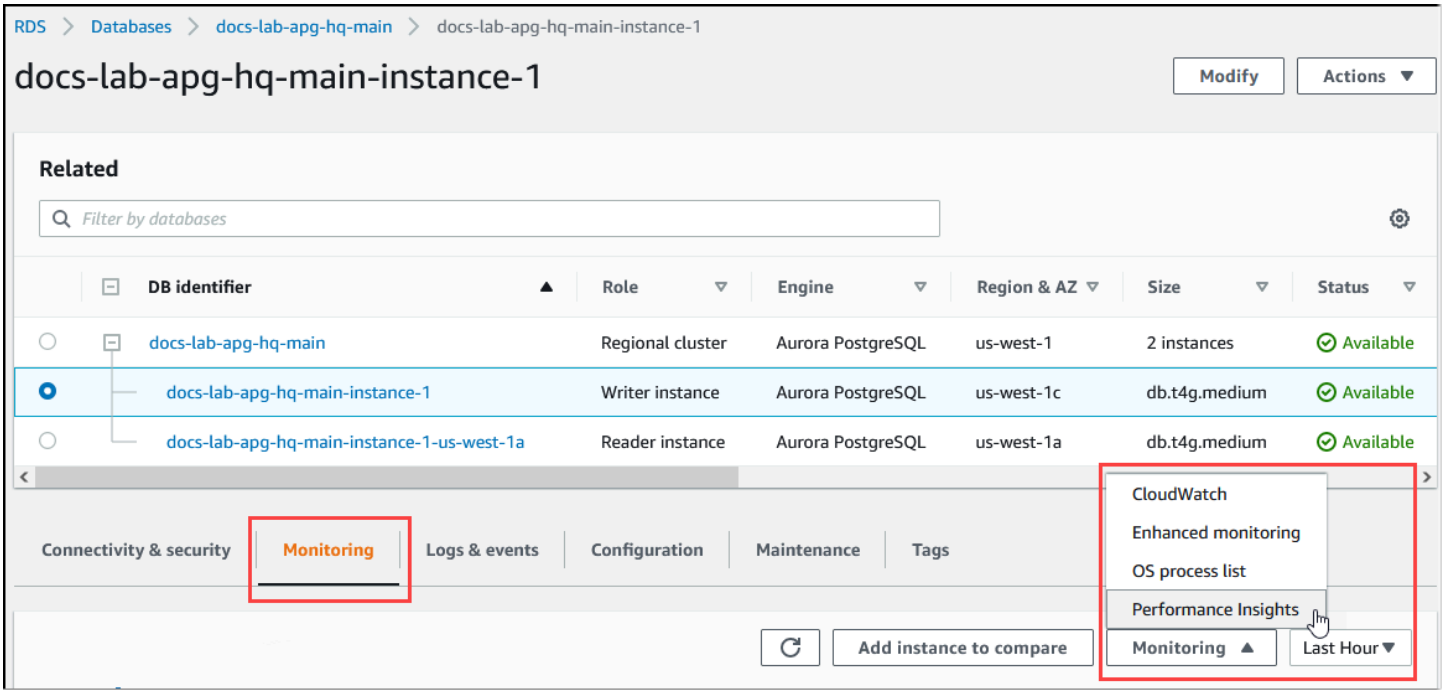
```
1 2022-03-21 16:14:10 connection authorized:
1 2022-03-21 16:14:10 disconnection: session
1 2022-03-21 16:15:00 connection authorized:
1 2022-03-21 16:16:00 connection authorized:
```

Anhand dieser Informationen können Sie entscheiden, ob Ihr Workload von einem Verbindungspooler profitieren kann. Für detailliertere Analysen können Sie Performance Insights verwenden.

Erkennen eines Verbindungsproblems mit Performance Insights

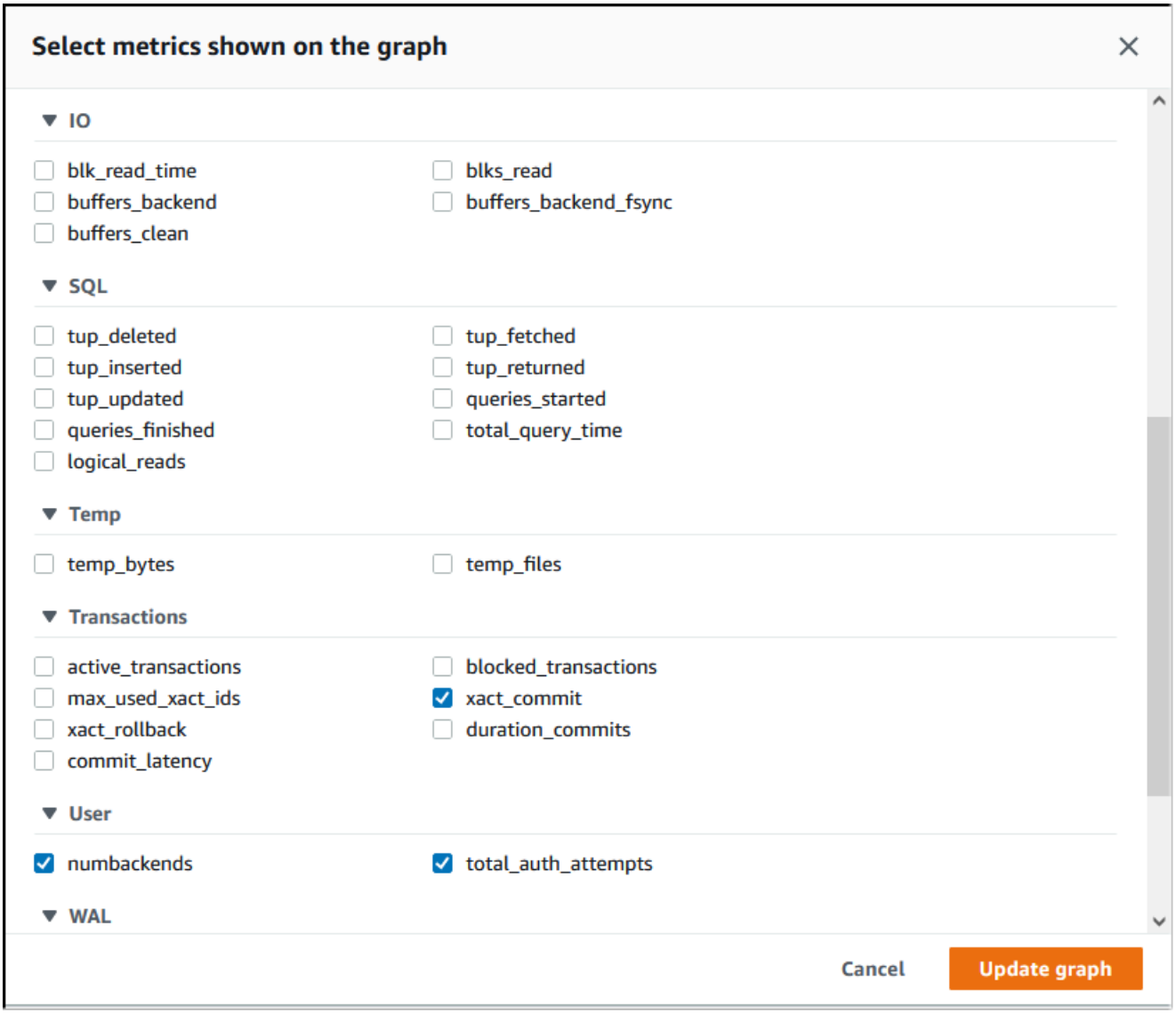
Mit Performance Insights können Sie den Umfang der Verbindungsprobleme auf Ihrem Aurora-PostgreSQL-kompatiblen Edition-DB-Cluster beurteilen. Wenn Sie einen Aurora-PostgreSQL-DB-Cluster erstellen, ist die Einstellung für Performance Insights standardmäßig aktiviert. Wenn Sie diese Auswahl beim Erstellen des DB-Clusters deaktiviert haben, ändern Sie Ihren Cluster, um die Funktion zu aktivieren. Weitere Informationen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Wenn Performance Insights auf Ihrem Aurora PostgreSQL DB-Cluster ausgeführt wird, können Sie die Metriken auswählen, die Sie überwachen möchten. Sie können über den Navigationsbereich der -Konsole auf Performance Insights zugreifen. Sie können auch auf Performance Insights vom Tab Überwachung der Writer-Instance für Ihren Aurora PostgreSQL DB-Cluster, wie in der folgenden Abbildung gezeigt, zugreifen.



Wählen Sie in der Performance Insights-Konsole Metriken verwalten. Wählen Sie die folgenden Metriken aus, um die Verbindungs- und Trennungsaktivitäten Ihres Aurora PostgreSQL DB-Clusters zu analysieren. Dies sind alles Metriken von PostgreSQL.

- `xact_commit` – Die Anzahl von committeter Transaktionen.
- `total_auth_attempts` – Die Anzahl von versuchten authentifizierten Benutzerverbindungen pro Minute.
- `numbackends` – Die Anzahl der Backends, die derzeit mit der Datenbank verbunden sind.

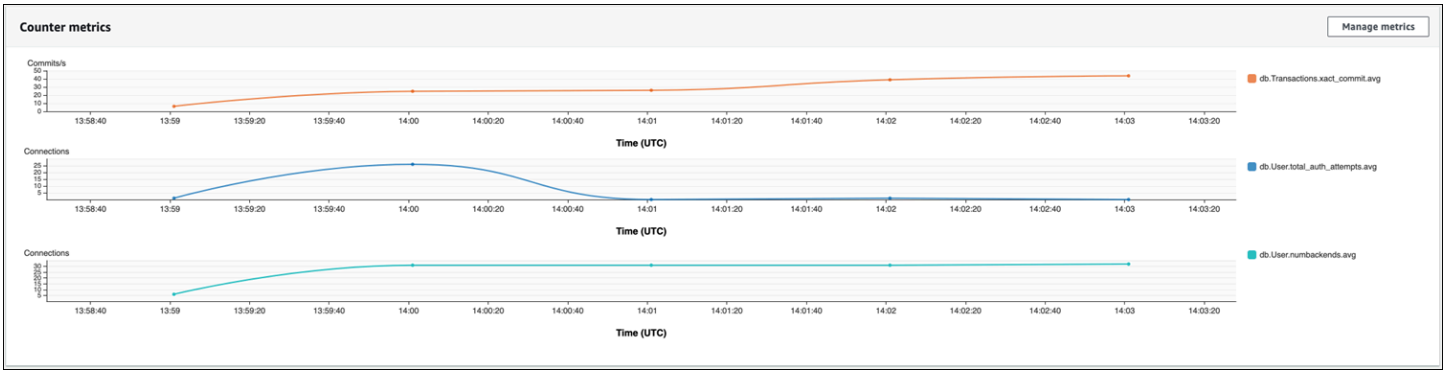


Wählen Sie zum Speichern der Einstellungen und Anzeigen der Verbindungsaktivität Grafik aktualisieren.

In der folgenden Abbildung sehen Sie die Auswirkungen der Ausführung von pgbench mit 100 Benutzern. Die Linie, die Verbindungen zeigt, ist konstant nach oben geneigt. Weitere Informationen zu pgbench finden Sie unter pgbench in der PostgreSQL-Dokumentation.

Das Bild zeigt, dass das Ausführen einer Workload mit nur 100 Benutzern ohne Verbindungspooler zu einem signifikanten Anstieg der Anzahl von `total_auth_attempts` während der gesamten Dauer der Workloadverarbeitung führt.

Beim RDS-Proxy-Verbindungspooling nehmen die Verbindungsversuche zu Beginn der Workload zu. Nach dem Einrichten des Verbindungspools sinkt der Durchschnitt. Die für Transaktionen und Backend-Nutzung verwendeten Ressourcen bleiben während der gesamten Workloadverarbeitung konsistent.



Weitere Informationen über die Verwendung von Performance Insights mit Ihrem Aurora-PostgreSQL-DB-Cluster finden Sie unter Überwachung mit Performance Insights auf . Informationen zum Analysieren der Metriken finden Sie unter Analyse der Metriken mit dem Performance Insights-Dashboard.

Vorführen der Vorteile von Verbindungspooling

Wie bereits erwähnt, können Sie RDS Proxy verwenden, um die Leistung zu verbessern, wenn Sie feststellen, dass Ihr Aurora PostgreSQL DB-Cluster ein Verbindungsproblem aufweist. Im Folgenden

finden Sie ein Beispiel, das die Unterschiede bei der Verarbeitung einer Workload zeigt, wenn Verbindungen gepoolt werden und wenn sie nicht gepoolt sind. Das Beispiel verwendet pgbench, um einen Transaktionsworkload zu modellieren.

Wie psql ist pgbench eine PostgreSQL-Clientanwendung, die Sie von Ihrem lokalen Client-Computer aus installieren und ausführen können. Sie können es auch über die Amazon-EC2-Instance installieren und ausführen, die Sie für die Verwaltung Ihres Aurora-PostgreSQL-DB-Clusters verwenden. Weitere Informationen finden Sie unter pgbench in der PostgreSQL-Dokumentation.

Um dieses Beispiel Schritt für Schritt durchzugehen, erstellen Sie zunächst die pgbench-Umgebung in Ihrer Datenbank. Der folgende Befehl ist die grundlegende Vorlage für die Initialisierung der pgbench-Tabellen in der angegebenen Datenbank. In diesem Beispiel wird das standardmäßige Hauptbenutzerkonto, `postgres`, für die Anmeldung verwendet. Ändern Sie es nach Bedarf für Ihren Aurora-PostgreSQL-DB-Cluster. Sie erstellen die pgbench-Umgebung in einer Datenbank auf der Writer-Instance Ihres Clusters.

> **Note**
>
> Der Initialisierungsprozess von pgbench löscht Tabellen mit den Namen `pgbench_accounts`, `pgbench_branches`, `pgbench_history` und `pgbench_tellers` erstellt sie neu. Stellen Sie sicher, dass die Datenbank, die Sie für *`dbname`* wählen, diese Namen nicht verwendet, wenn Sie pgbench initialisieren.

```
pgbench -U postgres -h db-cluster-instance-1.111122223333.aws-region.rds.amazonaws.com
 -p 5432 -d -i -s 50 dbname
```

Geben Sie folgende Parameter für pgbench an.

-d

Gibt einen Debugging-Bericht aus, während pgbench ausgeführt wird.

-h

Gibt den Endpunkt der Writer-DB-Instance des Aurora-PostgreSQL-DB-Clusters an.

-i

Initialisiert die pgbench-Umgebung in der Datenbank für die Benchmark-Tests.

-p

Identifiziert den Port, der für Datenbankverbindungen verwendet wird. Die Standardeinstellung für Aurora PostgreSQL ist typischerweise 5432 oder 5433.

-s

Gibt den Skalierungsfaktor an, der zum Füllen der Tabellen mit Zeilen verwendet werden soll. Der Standard-Skalierungsfaktor ist 1, wodurch 1 Zeile in der `pgbench_branches`-Tabelle, 10 Zeilen in der `pgbench_tellers`-Tabelle und 100000 Zeilen in der `pgbench_accounts`-Tabelle erzeugt werden.

-U

Gibt das Benutzerkonto für die Writer-Instance des Aurora-PostgreSQL-DB-Clusters an.

Nachdem die pgbench-Umgebung eingerichtet wurde, können Sie Benchmarking-Tests mit und ohne Verbindungspooling ausführen. Der Standardtest besteht aus einer Reihe von fünf SELECT-, UPDATE- und INSERT-Befehlen pro Transaktion, die für die angegebene Zeit wiederholt ausgeführt werden. Sie können Skalierungsfaktor, Anzahl der Clients und andere Details angeben, um Ihre eigenen Anwendungsfälle zu modellieren.

Der folgende Befehl führt beispielsweise den Benchmark 60 Sekunden lang aus (Option -T, für Zeit) mit 20 gleichzeitigen Verbindungen (Option -c). Mit der Option -C wird der Test jedes Mal mit einer neuen Verbindung ausgeführt, anstatt einmal pro Clientsitzung. Diese Einstellung gibt Ihnen einen Hinweis auf den Verbindungsaufwand.

```
pgbench -h docs-lab-apg-133-test-instance-1.c3zr2auzukpa.us-west-1.rds.amazonaws.com -U
 postgres -p 5432 -T 60 -c 20 -C labdb
Password:**********
pgbench (14.3, server 13.3)
  starting vacuum...end.
  transaction type: <builtin: TPC-B (sort of)>
    scaling factor: 50
    query mode: simple
    number of clients: 20
    number of threads: 1
    duration: 60 s
    number of transactions actually processed: 495
    latency average = 2430.798 ms
    average connection time = 120.330 ms
    tps = 8.227750 (including reconnection times)
```

Das Ausführen von pgbench auf der Writer-Instance eines Aurora PostgreSQL DB-Clusters ohne Wiederverwendung von Verbindungen zeigt, dass nur etwa 8 Transaktionen pro Sekunde verarbeitet werden. Dies ergibt insgesamt 495 Transaktionen während des 1-Minutentests.

Wenn Sie Verbindungen wiederverwenden, ist die Antwort des Aurora PostgreSQL DB-Clusters für die Anzahl der Benutzer fast 20-mal schneller. Bei der Wiederverwendung werden insgesamt 9.042 Transaktionen verarbeitet, verglichen mit 495 in derselben Zeit und für dieselbe Anzahl von Benutzerverbindungen. Der Unterschied besteht darin, dass im Folgenden jede Verbindung wiederverwendet wird.

```
pgbench -h docs-lab-apg-133-test-instance-1.c3zr2auzukpa.us-west-1.rds.amazonaws.com -U
 postgres -p 5432 -T 60 -c 20 labdb
Password:*********
pgbench (14.3, server 13.3)
      starting vacuum...end.
      transaction type: <builtin: TPC-B (sort of)>
      scaling factor: 50
      query mode: simple
      number of clients: 20
      number of threads: 1
      duration: 60 s
      number of transactions actually processed: 9042
      latency average = 127.880 ms
      initial connection time = 2311.188 ms
      tps = 156.396765 (without initial connection time)
```

Dieses Beispiel zeigt, dass das Pooling von Verbindungen die Reaktionszeiten erheblich verbessern kann. Informationen über die Einrichtung von RDS Proxy für Ihren Aurora-PostgreSQL-DB-Cluster finden Sie unter Verwenden von Amazon RDS Proxy für Aurora.

Ändern von Speicherparametern für Aurora PostgreSQL

In Amazon Aurora PostgreSQL können Sie mehrere Parameter verwenden, die die Speichermenge steuern, die für verschiedene Verarbeitungsaufgaben verwendet wird. Wenn eine Aufgabe mehr Speicher beansprucht als die für einen bestimmten Parameter festgelegte Menge, verwendet Aurora PostgreSQL andere Ressourcen für die Verarbeitung, z. B. durch Schreiben auf die Festplatte. Dies kann dazu führen, dass Ihr Aurora PostgreSQL DB-Cluster langsamer wird oder möglicherweise angehalten wird, mit einem Fehler bei unzureichendem Arbeitsspeicher.

Die Standardeinstellung für jeden Speicherparameter kann normalerweise die beabsichtigten Verarbeitungsaufgaben verarbeiten. Sie können jedoch auch Ihre speicherbezogenen Parameter von

Aurora PostgreSQL DB-Cluster optimieren. Sie führen diese Optimierung durch, um sicherzustellen, dass genügend Speicher für die Verarbeitung Ihrer spezifischen Workload zugewiesen ist.

Nachstehend finden Sie Informationen über Parameter, die die Speicherverwaltung steuern. Sie können auch lernen, wie Sie die Speicherauslastung bewerten.

Überprüfen und Einstellen von Parameterwerten

Zu den Parametern, die Sie festlegen können, um den Speicher zu verwalten und die Speicherauslastung Ihres Aurora PostgreSQL DB-Clusters zu bewerten, gehören die folgenden:

- `work_mem` – Gibt die Speichermenge an, die der Aurora PostgreSQL DB-Cluster für interne Sortiervorgänge und Hash-Tabellen verwendet, bevor er in temporäre Plattendateien schreibt.
- `log_temp_files` – Protokolliert die Erstellung temporärer Dateien, Dateinamen und -größen. Wenn dieser Parameter aktiviert ist, wird für jede temporäre Datei, die erstellt wird, ein Protokolleintrag gespeichert. Aktivieren Sie diese Option, um zu sehen, wie oft Ihr Aurora PostgreSQL DB-Cluster auf die Festplatte schreiben muss. Schalten Sie es wieder aus, nachdem Sie Informationen über die temporäre Dateigenerierung Ihres Aurora PostgreSQL DB-Clusters gesammelt haben, um eine übermäßige Protokollierung zu vermeiden.
- `logical_decoding_work_mem` – Gibt die Speichermenge (in Megabyte) an, die für die logische Dekodierung verwendet werden soll. Logische Dekodierung ist der Prozess, der verwendet wird, um ein Replikat zu erstellen. Dieser Prozess erfolgt durch Konvertieren von Daten aus der Write-Ahead-Log-Datei (WAL) in die logische Streaming-Ausgabe, die vom Ziel benötigt wird.

  Der Wert dieses Parameters erstellt einen einzelnen Puffer mit der für jede Replikationsverbindung angegebenen Größe. Standardmäßig sind es 65 536 KB. Nachdem dieser Puffer gefüllt ist, wird der Überschuss als Datei auf die Festplatte geschrieben. Um Plattenaktivität zu minimieren, können Sie den Wert dieses Parameters auf einen viel höheren Wert setzen als den von `work_mem`.

Dies sind alles dynamische Parameter, sodass Sie sie für die aktuelle Sitzung ändern können. Stellen Sie dazu eine Verbindung mit dem Aurora PostgreSQL DB-Cluster mit „psql“ und unter Verwendung der `SET`-Anweisung, wie unten angezeigt.

```
SET parameter_name TO parameter_value;
```

Sitzungseinstellungen sind nur für die Dauer der Sitzung gültig. Wenn die Sitzung endet, kehrt der Parameter auf seine Einstellung in der DB-Cluster-Parametergruppe zurück. . Bevor Sie Parameter

ändern, überprüfen Sie zunächst die aktuellen Werte, indem Sie die `pg_settings`-Tabelle wie folgt abfragen.

```
SELECT unit, setting, max_val
   FROM pg_settings WHERE name='parameter_name';
```

Um zum Beispiel den Wert des `work_mem`-Parameters zu finden, stellen Sie eine Verbindung zur Writer-Instance des Aurora PostgreSQL DB-Clusters her und führen Sie die folgende Abfrage aus.

```
SELECT unit, setting, max_val, pg_size_pretty(max_val::numeric)
  FROM pg_settings WHERE name='work_mem';
unit  | setting  | max_val   | pg_size_pretty
------+----------+-----------+---------------
 kB   | 1024     | 2147483647| 2048 MB
(1 row)
```

Um Parametereinstellungen so zu ändern, dass sie bestehen bleiben, müssen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe verwenden. . Nach dem Trainieren Ihrer Aurora PostgreSQL DB-Cluster mit unterschiedlichen Werten für diese Parameter unter Verwendung der `SET`-Anweisung können Sie eine benutzerdefinierte Parametergruppe erstellen und auf Ihre Parametergruppe Aurora PostgreSQL DB-Cluster anwenden. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen.

Den Arbeitsspeicherparameter verstehen

Der Arbeitsspeicherparameter (`work_mem`) gibt die maximale Speichermenge an, die Aurora PostgreSQL zur Verarbeitung komplexer Abfragen verwenden kann. Zu komplexen Abfragen gehören solche, die Sortier- oder Gruppierungsvorgänge beinhalten, also Abfragen, die die folgenden Klauseln verwenden:

- ORDER BY
- DISTINCT
- GROUP BY
- JOIN (MERGE und HASH)

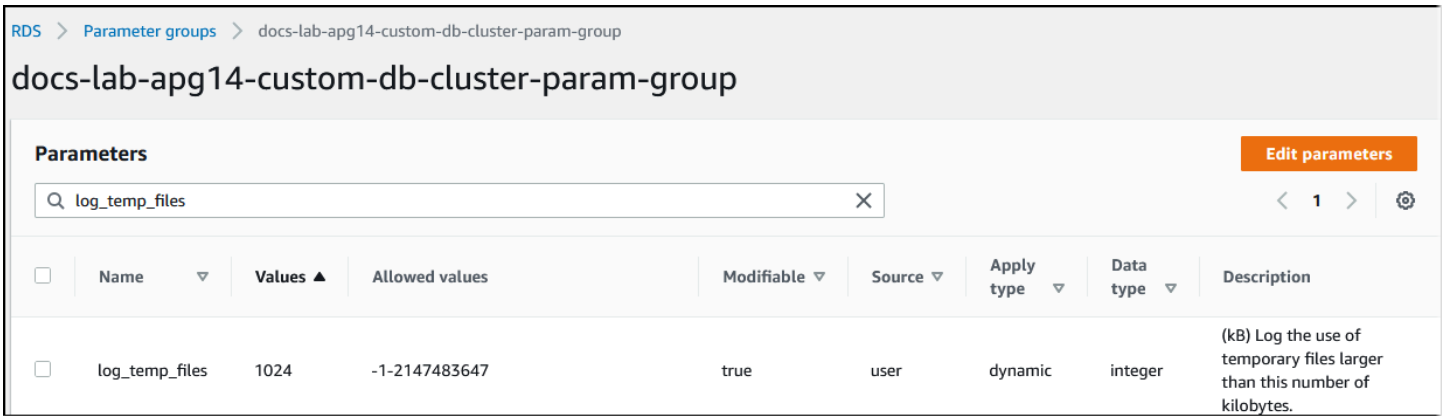
Der Abfrageplaner beeinflusst indirekt, wie Ihr Aurora PostgreSQL DB-Cluster Arbeitsspeicher verwendet. Der Abfrageplaner generiert Ausführungspläne für die Verarbeitung von SQL-Anweisungen. Ein bestimmter Plan kann eine komplexe Abfrage in mehrere Arbeitseinheiten

aufteilen, die parallel ausgeführt werden können. Wenn möglich, verwendet Aurora PostgreSQL die Speichermenge, die im `work_mem`-Parameter für jede Sitzung vor dem Schreiben auf die Festplatte für jeden parallelen Prozess angegeben ist.

Mehrere Datenbankbenutzer, die mehrere Operationen gleichzeitig ausführen und mehrere Arbeitseinheiten parallel generieren, können den zugewiesenen Arbeitsspeicher Ihres Aurora PostgreSQL DB-Clusters erschöpfen. Dies kann zu einer übermäßigen Erstellung temporärer Dateien und Festplatten-I/O führen, oder schlimmer noch, es kann zu einem Speicherausfall führen.

Identifizieren temporärer Dateiverwendung

Immer, wenn der für die Verarbeitung von Abfragen erforderliche Speicher den im `work_mem`-Parameter angegebenen Wert übersteigt, werden die Arbeitsdaten in einer temporären Datei auf die Festplatte ausgelagert. Sie können sehen, wie oft dies geschieht, indem Sie den `log_temp_files`-Parameter aktivieren. Standardmäßig ist dieser Parameter deaktiviert (Einstellung auf -1). Um alle temporären Dateiinformationen zu erfassen, setzen Sie diesen Parameter auf 0. Setzen Sie `log_temp_files` auf eine andere positive Ganzzahl, um temporäre Dateiinformationen für Dateien zu erfassen, die dieser Datenmenge entsprechen oder größer sind (in Kilobyte). In der folgenden Abbildung sehen Sie ein Beispiel von AWS Management Console.



Nachdem Sie die temporäre Dateiprotokollierung konfiguriert haben, können Sie mit Ihrer eigenen Workload testen, ob Ihre Arbeitsspeichereinstellung ausreichend ist. Sie können eine Workload auch mithilfe von pgbench simulieren, einer einfachen Benchmarking-Anwendung aus der PostgreSQL-Community.

Das folgende Beispiel initialisiert (`-i`)`pgbench`, indem es die notwendigen Tabellen und Zeilen für die Ausführung der Tests erstellt. In diesem Beispiel erstellt der Skalierungsfaktor (`-s` 50) 50 Zeilen in der `pgbench_branches`-Tabelle, 500 Zeilen in `pgbench_tellers` und 5.000.000 Zeilen in der `pgbench_accounts`-Tabelle in der `labdb`Datenbank.

```
pgbench -U postgres -h your-cluster-instance-1.111122223333.aws-regionrds.amazonaws.com
 -p 5432 -i -s 50 labdb
Password:
dropping old tables...
NOTICE:  table "pgbench_accounts" does not exist, skipping
NOTICE:  table "pgbench_branches" does not exist, skipping
NOTICE:  table "pgbench_history" does not exist, skipping
NOTICE:  table "pgbench_tellers" does not exist, skipping
creating tables...
generating data (client-side)...
5000000 of 5000000 tuples (100%) done (elapsed 15.46 s, remaining 0.00 s)
vacuuming...
creating primary keys...
done in 61.13 s (drop tables 0.08 s, create tables 0.39 s, client-side generate 54.85
 s, vacuum 2.30 s, primary keys 3.51 s)
```

Nach der Initialisierung der Umgebung können Sie den Benchmark für eine bestimmte Zeit (`-T`) und die Anzahl der Kunden (`-c`) ausführen. In diesem Beispiel wird auch die `-d`-Option zur Ausgabe von Debugging-Informationen verwendet, während die Transaktionen vom Aurora PostgreSQL DB-Cluster verarbeitet werden.

```
pgbench -h -U postgres your-cluster-instance-1.111122223333.aws-regionrds.amazonaws.com
 -p 5432 -d -T 60 -c 10 labdb
Password:*******
pgbench (14.3)
starting vacuum...end.
transaction type: <builtin: TPC-B (sort of)>
scaling factor: 50
query mode: simple
number of clients: 10
number of threads: 1
duration: 60 s
number of transactions actually processed: 1408
latency average = 398.467 ms
initial connection time = 4280.846 ms
tps = 25.096201 (without initial connection time)
```

Weitere Informationen über „pgbench“ finden Sie in pgbench in der PostgreSQL-Dokumentation.

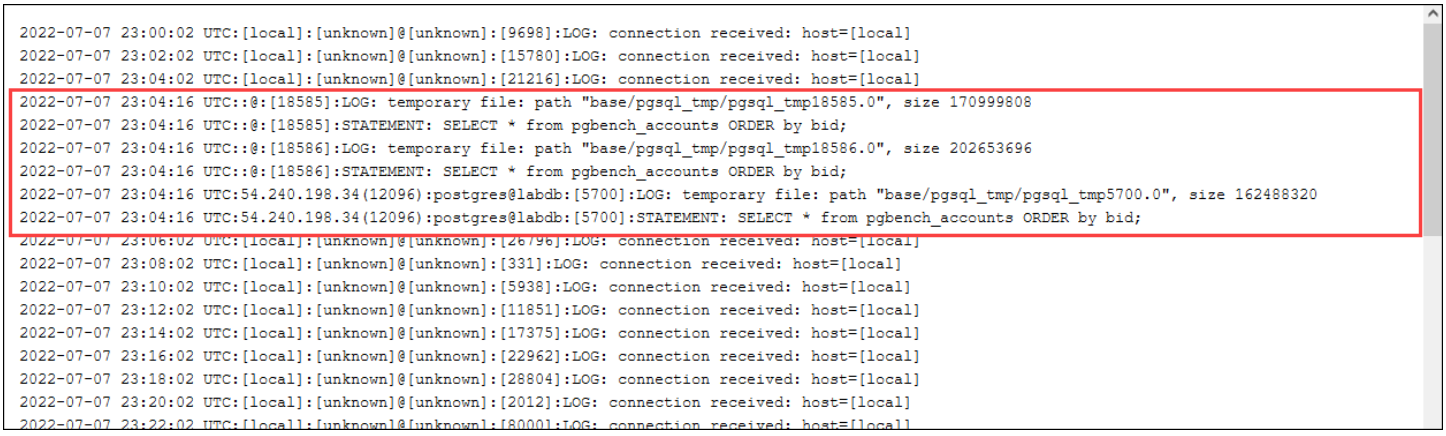
Sie können den Befehl „psql metacommand“ (\d) verwenden, um die von „pgbench“ erstellten Relationen wie Tabellen, Ansichten und Indizes aufzulisten.

```
labdb=>  \d pgbench_accounts
 Table "public.pgbench_accounts"
  Column  |     Type      | Collation | Nullable | Default
----------+---------------+-----------+----------+---------
 aid      | integer       |           | not null |
 bid      | integer       |           |          |
 abalance | integer       |           |          |
 filler   | character(84) |           |          |
Indexes:
    "pgbench_accounts_pkey" PRIMARY KEY, btree (aid)
```

Wie in der Ausgabe gezeigt, wird die `pgbench_accounts`-Tabelle nach der `aid`-Spalte indiziert. Um sicherzustellen, dass diese nächste Abfrage Arbeitsspeicher verwendet, fragen Sie eine beliebige nicht indizierte Spalte ab, z. B. die im folgenden Beispiel gezeigte.

```
postgres=> SELECT * FROM pgbench_accounts ORDER BY bid;
```

Überprüfen Sie das Protokoll auf die temporären Dateien. Öffnen Sie dazu AWS Management Console, wählen Sie die Aurora PostgreSQL DB-Cluster-Instance und dann den Tab Logs & Events (Protokolle und Ereignisse). Zeigen Sie die Protokolle in der Konsole an oder laden Sie sie zur weiteren Analyse herunter. Wie in der folgenden Abbildung dargestellt, zeigt die Größe der temporären Dateien, die für die Verarbeitung der Abfrage benötigt werden, an, dass Sie erwägen sollten, die für die `work_mem`-Parameter angegebene Menge zu erhöhen.



Sie können diesen Parameter für Einzelpersonen und Gruppen unterschiedlich konfigurieren, je nach Ihren betrieblichen Anforderungen. Sie können beispielsweise den `work_mem`-Parameter auf 8 GB für die Rolle mit dem Namen `dev_team` festlegen.

```
postgres=> ALTER ROLE dev_team SET work_mem='8GB';
```

Mit dieser Einstellung für `work_mem` wird jeder Rolle, die ein Mitglied der `dev_team`-Rolle ist, bis zu 8 GB Arbeitsspeicher zugewiesen.

Verwenden von Indizes für schnellere Reaktionszeit

Wenn Ihre Abfragen zu lange dauern, bis Ergebnisse zurückgegeben werden, können Sie überprüfen, ob Ihre Indizes erwartungsgemäß verwendet werden. Aktivieren Sie zuerst `\timing`, das psql-Metakommando, wie folgt.

```
postgres=>  \timing on
```

Verwenden Sie nach dem Aktivieren des Timings eine einfache SELECT-Anweisung.

```
postgres=> SELECT COUNT(*) FROM
  (SELECT * FROM pgbench_accounts
  ORDER BY bid)
  AS accounts;
count
-------
5000000
(1 row)
Time: 3119.049 ms (00:03.119)
```

Wie in der Ausgabe gezeigt, dauerte die Ausführung dieser Abfrage etwas mehr als 3 Sekunden. Um die Reaktionszeit zu verbessern, erstellen Sie einen Index für `pgbench_accounts` wie folgt.

```
postgres=> CREATE INDEX ON pgbench_accounts(bid);
CREATE INDEX
```

Führen Sie die Abfrage erneut aus und beachten Sie die kürzere Antwortzeit. In diesem Beispiel wurde die Abfrage etwa fünfmal schneller abgeschlossen, in etwa einer halben Sekunde.

```
postgres=>  SELECT COUNT(*) FROM (SELECT * FROM pgbench_accounts ORDER BY bid) AS
 accounts;
 count
-------
 5000000
(1 row)
Time: 567.095 ms
```

Arbeitsspeicher für logische Dekodierung anpassen

Logische Replikation war in allen Versionen von Aurora PostgreSQL seit seiner Einführung in PostgreSQL Version 10 verfügbar. Wenn Sie die logische Replikation konfigurieren, können Sie auch die `logical_decoding_work_mem`-Parameter einstellen, um die Speichermenge anzugeben, die der logische Dekodierungsprozess für den Dekodierungs- und Streaming-Prozess verwenden kann.

Bei der logischen Dekodierung werden Write-Ahead-Log-Datensätze (WAL) in SQL-Anweisungen konvertiert, die dann zur logischen Replikation oder einer anderen Aufgabe an ein anderes Ziel gesendet werden. Wenn eine Transaktion in die WAL geschrieben und dann konvertiert wird, muss die gesamte Transaktion in den für `logical_decoding_work_mem` angegebenen Wert passen. Standardmäßig ist dieser Parameter auf 65 536 KB eingestellt. Jeder Überlauf wird auf den Datenträger geschrieben. Dies bedeutet, dass es erneut von der Festplatte gelesen werden muss, bevor es an sein Ziel gesendet werden kann, wodurch der Gesamtprozess verlangsamt wird.

Sie können den Betrag des Transaktionsüberlaufs in Ihre aktuelle Workload zu einem bestimmten Zeitpunkt bewerten, indem Sie die `aurora_stat_file`-Funktion wie im folgenden Beispiel gezeigt, verwenden.

```
SELECT split_part (filename, '/', 2)
   AS slot_name, count(1) AS num_spill_files,
   sum(used_bytes) AS slot_total_bytes,
   pg_size_pretty(sum(used_bytes)) AS slot_total_size
   FROM aurora_stat_file()
   WHERE filename like '%spill%'
   GROUP BY 1;
  slot_name | num_spill_files | slot_total_bytes | slot_total_size
------------+-----------------+------------------+-----------------
 slot_name  |       590       |      411600000   | 393 MB
(1 row)
```

Diese Abfrage gibt die Anzahl und Größe der Spill-Dateien auf Ihrem Aurora PostgreSQL DB-Cluster zurück, wenn die Abfrage aufgerufen wird. Bei länger laufenden Workloads befinden sich möglicherweise noch keine Spill-Dateien auf der Festplatte. Um ein Profil lang andauernder Workloads zu erstellen, empfehlen wir Ihnen, eine Tabelle zu erstellen, in der die Informationen der Spill-Datei während der Ausführung der Workload erfasst werden. Sie können die Tabelle wie folgt erstellen.

```
CREATE TABLE spill_file_tracking AS
    SELECT now() AS spill_time,*
```

```
    FROM aurora_stat_file()
    WHERE filename LIKE '%spill%';
```

Um zu sehen, wie Spill-Dateien während der logischen Replikation verwendet werden, richten Sie einen Publisher und einen Abonnenten ein und starten Sie dann eine einfache Replikation. Weitere Informationen finden Sie unter Einrichten der logischen Replikation für Ihren DB-Cluster von Aurora PostgreSQL. Während der Replikation können Sie einen Auftrag erstellen, der die Ergebnismenge aus der `aurora_stat_file()`-spill-File-Funktion wie folgt erfasst.

```
INSERT INTO spill_file_tracking
  SELECT now(),*
  FROM aurora_stat_file()
  WHERE filename LIKE '%spill%';
```

Verwenden Sie den folgenden psql-Befehl, um den Job einmal pro Sekunde auszuführen.

```
\watch 0.5
```

Stellen Sie während der Ausführung des Auftrags eine Verbindung zur Writer-Instance von einer anderen psql-Sitzung her. Verwenden Sie die folgende Reihe von Anweisungen, um eine Workload auszuführen, die die Speicherkonfiguration überschreitet und Aurora PostgreSQL veranlasst, eine Spill-Datei zu erstellen.

```
labdb=> CREATE TABLE my_table (a int PRIMARY KEY, b int);
CREATE TABLE
labdb=> INSERT INTO my_table SELECT x,x FROM generate_series(0,10000000) x;
INSERT 0 10000001
labdb=> UPDATE my_table SET b=b+1;
UPDATE 10000001
```

Diese Anweisungen dauern einige Minuten. Wenn Sie fertig sind, drücken Sie die Strg-Taste und die C-Taste gleichzeitig, um die Überwachungsfunktion zu beenden. Verwenden Sie dann den folgenden Befehl, um eine Tabelle zu erstellen, in der die Informationen über die Verwendung der Spill-Datei des Aurora PostgreSQL DB-Clusters gespeichert werden.

```
SELECT spill_time, split_part (filename, '/', 2)
    AS slot_name, count(1)
    AS spills, sum(used_bytes)
    AS slot_total_bytes, pg_size_pretty(sum(used_bytes))
    AS slot_total_size FROM spill_file_tracking
```

```
  GROUP BY 1,2 ORDER BY 1;
                  spill_time | slot_name             | spills | slot_total_bytes |
 slot_total_size
-------------------------------+----------------------+--------+-----------------
+-----------------
2022-04-15 13:42:52.528272+00 | replication_slot_name | 1      | 142352280        | 136
 MB
2022-04-15 14:11:33.962216+00 | replication_slot_name | 4      | 467637996        | 446
 MB
2022-04-15 14:12:00.997636+00 | replication_slot_name | 4      | 569409176        | 543
 MB
2022-04-15 14:12:03.030245+00 | replication_slot_name | 4      | 569409176        | 543
 MB
2022-04-15 14:12:05.059761+00 | replication_slot_name | 5      | 618410996        | 590
 MB
2022-04-15 14:12:07.22905+00  | replication_slot_name | 5      | 640585316        | 611
 MB
(6 rows)
```

Die Ausgabe zeigt, dass beim Ausführen des Beispiels fünf Spill-Dateien erstellt wurden, die 611 MB Speicher verbrauchten. Um zu vermeiden, dass auf den Datenträger geschrieben wird, empfehlen wir, den `logical_decoding_work_mem`-Parameter auf die nächsthöhere Speichergröße, 1024, einzustellen.

Verwendung von CloudWatch Amazon-Metriken zur Analyse der Ressourcennutzung für Aurora PostgreSQL

Aurora sendet automatisch Metrikdaten innerhalb von 1 Minute an CloudWatch . Sie können die Ressourcennutzung für Aurora PostgreSQL mithilfe CloudWatch von Metriken analysieren. Mit den Metriken können Sie den Netzwerkdurchsatz und die Netzwerknutzung bewerten.

Bewertung des Netzwerkdurchsatzes mit CloudWatch

Wenn sich Ihre Systemauslastung den Ressourcenlimits für Ihren Instance-Typ nähert, kann sich die Verarbeitung verlangsamen. Sie können CloudWatch Logs Insights verwenden, um die Nutzung Ihrer Speicherressourcen zu überwachen und sicherzustellen, dass ausreichend Ressourcen verfügbar sind. Bei Bedarf können Sie die DB-Instance auf eine größere Instance-Klasse umstellen.

Die Verarbeitung des Aurora-Speichers kann aus folgenden Gründen langsam sein:

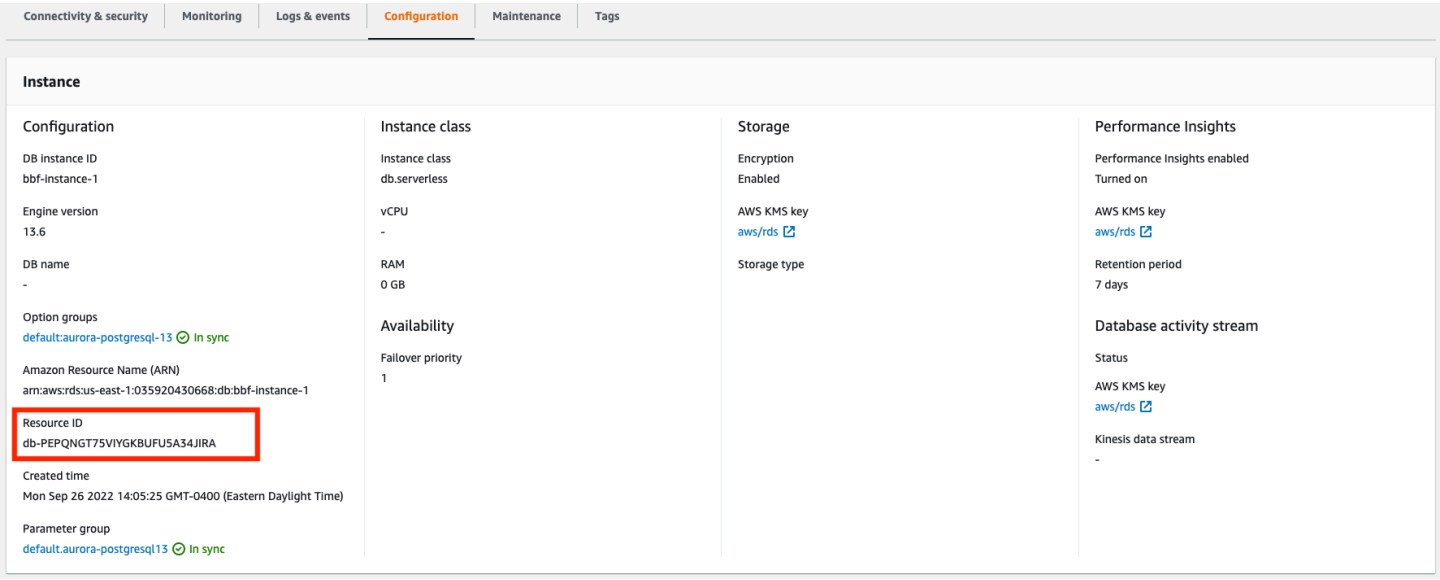
- Unzureichende Netzwerkbandbreite zwischen Client und DB-Instance.

- Unzureichende Netzwerkbandbreite für das Speichersubsystem.
- Eine Workload, die im Hinblick auf Ihren Instance-Typ groß ist.

Sie können CloudWatch Logs Insights abfragen, um ein Diagramm der Aurora-Speicherressourcennutzung zur Überwachung der Ressourcen zu erstellen. Das Diagramm zeigt die CPU-Auslastung und Metriken, anhand derer Sie entscheiden können, ob Sie auf eine größere Instance-Größe hochskalieren sollten. Informationen zur Abfragesyntax für CloudWatch Logs Insights finden Sie unter CloudWatch Logs Insights-Abfragesyntax

Um es zu verwenden CloudWatch, müssen Sie Ihre Aurora PostgreSQL-Protokolldateien nach exportieren. CloudWatch Sie können Ihren vorhandenen Cluster auch ändern, um Logs in diesen zu exportieren. CloudWatch Informationen zum Exportieren von Protokollen nach CloudWatch finden Sie unterAktivieren der Option zum Veröffentlichen von Protokollen in Amazon CloudWatch.

Sie benötigen die Ressourcen-ID Ihrer DB-Instance, um CloudWatch Logs Insights abzufragen. Die Resource ID (Ressourcen-ID) ist auf der Registerkarte Configuration (Konfiguration) in Ihrer Konsole verfügbar:



So fragen Sie Ihre Protokolldateien nach Metriken für den Ressourcenspeicher ab:

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.

   Die CloudWatch Übersichts-Startseite wird angezeigt.

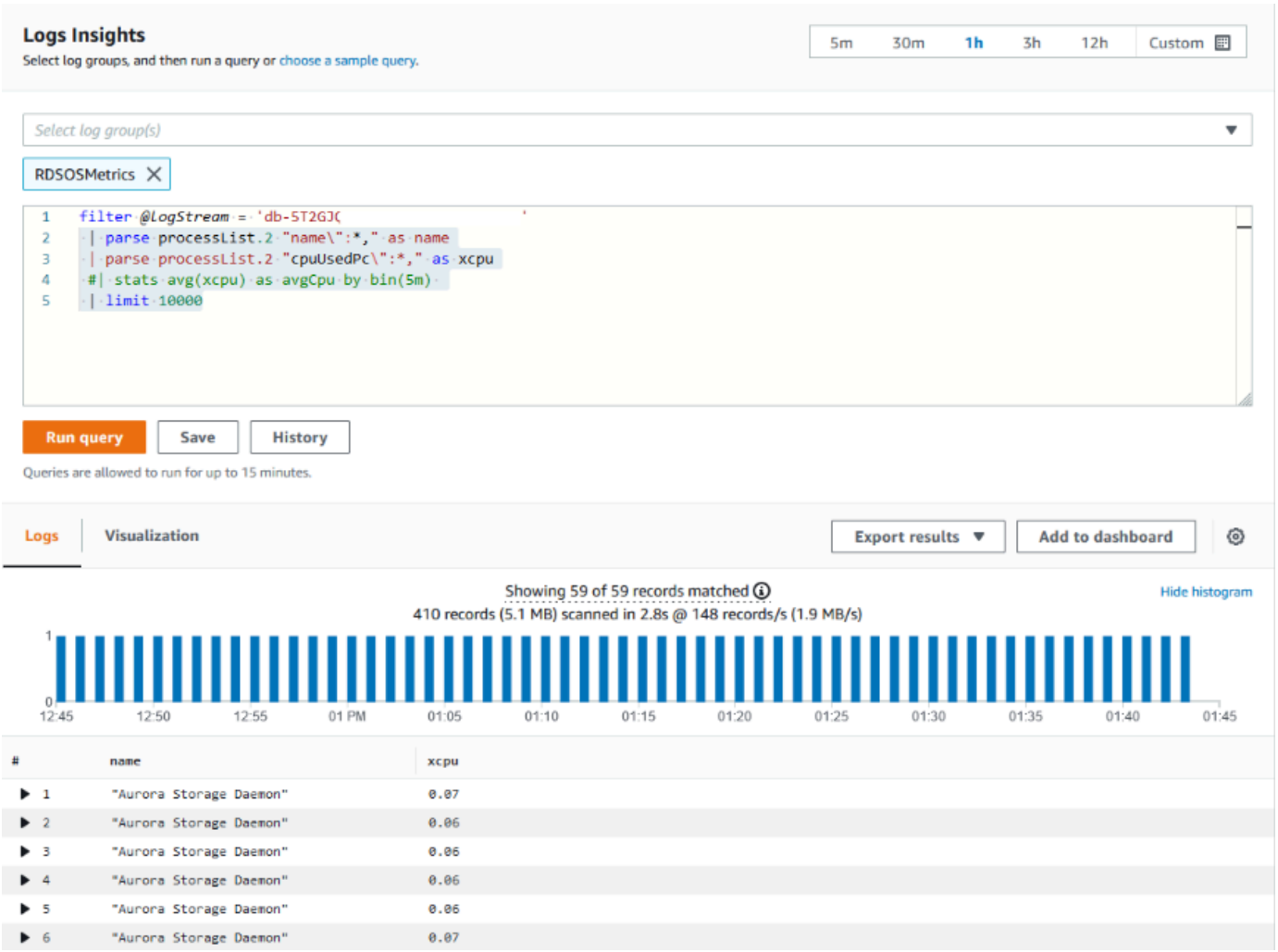
2. Ändern Sie, falls erforderlich, die AWS-Region. Wählen Sie in der Navigationsleiste aus, AWS-Region wo sich Ihre AWS Ressourcen befinden. Weitere Informationen finden Sie unter Regionen und Endpunkte.
3. Wählen Sie im Navigationsbereich Logs (Protokolle) und dann Logs Insights aus.

   Die Seite Logs Insights wird angezeigt.
4. Wählen Sie die Protokolldateien, die Sie analysieren möchten, aus der Dropdown-Liste aus.
5. Geben Sie die folgende Abfrage in das Feld ein und ersetzen Sie `<resource ID>` durch die Ressourcen-ID Ihres DB-Clusters:

   ```
   filter @logStream = <resource ID> | parse @message "\"Aurora Storage
   Daemon\"*memoryUsedPc\":*,\"cpuUsedPc\":*," as a,memoryUsedPc,cpuUsedPc
   | display memoryUsedPc,cpuUsedPc #| stats avg(xcpu) as avgCpu by
   bin(5m) | limit 10000
   ```
6. Klicken Sie auf Run query (Abfrage ausführen).

   Das Diagramm zur Speicherauslastung wird angezeigt.

   Die folgende Abbildung veranschaulicht die Seite Logs Insights und die Diagrammanzeige.



Bewertung der DB-Instance-Nutzung anhand von CloudWatch Metriken

Mithilfe von CloudWatch Metriken können Sie den Durchsatz Ihrer Instance beobachten und herausfinden, ob Ihre Instance-Klasse ausreichend Ressourcen für Ihre Anwendungen bereitstellt. Informationen zu Ihren DB-Instance-Klassenlimits finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora. Suchen Sie die Spezifikationen für Ihre DB-Instance-Klasse, um Ihre Netzwerkleistung zu ermitteln.

Wenn sich Ihre DB-Instance-Nutzung dem Instance-Klassenlimit nähert, kann sich die Leistung verschlechtern. Die CloudWatch Metriken können diese Situation bestätigen, sodass Sie planen können, manuell auf eine größere Instance-Klasse hochzuskalieren.

Kombinieren Sie die folgenden CloudWatch Metrikwerte, um herauszufinden, ob Sie sich dem Instance-Klassenlimit nähern:

- NetworkThroughput— Die Menge des Netzwerkdurchsatzes, der von den Clients für jede Instance im Aurora-DB-Cluster empfangen und übertragen wird. Dieser Durchsatzwert berücksichtigt nicht den Netzwerkdatenverkehr zwischen den Instances im DB-Cluster und dem Cluster-Volume.
- StorageNetworkDurchsatz — Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Aurora-DB-Cluster empfangen und an das Aurora-Speichersubsystem gesendet wird.

Fügen Sie den NetworkThroughputzum StorageNetworkDurchsatz hinzu, um den Netzwerkdurchsatz zu ermitteln, der von jeder Instance in Ihrem Aurora-DB-Cluster vom Aurora-Speichersubsystem empfangen und an dieses gesendet wurde. Das Instance-Klassenlimit für Ihre Instance sollte größer sein als die Summe dieser beiden kombinierten Metriken.

Sie können die folgenden Metriken verwenden, um zusätzliche Details des Netzwerkverkehrs Ihrer Client-Anwendungen beim Senden und Empfangen zu überprüfen:

- NetworkReceiveDurchsatz — Die Menge des Netzwerkdurchsatzes, den jede Instance im Aurora PostgreSQL-DB-Cluster von Clients erhält. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im -DB-Cluster und dem Cluster-Volume.
- NetworkTransmitDurchsatz — Die Menge des Netzwerkdurchsatzes, der von jeder Instance im Aurora-DB-Cluster an Clients gesendet wird. Dieser Durchsatz beinhaltet nicht den Netzwerkdatenverkehr zwischen den Instances im -DB-Cluster und dem Cluster-Volume.
- StorageNetworkReceiveThroughput— Die Menge des Netzwerkdurchsatzes, den jede Instance im DB-Cluster vom Aurora-Speichersubsystem erhält.
- StorageNetworkTransmitThroughput— Die Menge des Netzwerkdurchsatzes, der von jeder Instance im DB-Cluster an das Aurora-Speichersubsystem gesendet wird.

Addieren Sie all diese Metriken, um zu bewerten, wie Ihre Netzwerknutzung im Vergleich zum Instance-Klassenlimit abschneidet. Das Instance-Klassenlimit sollte größer sein als die Summe dieser kombinierten Metriken.

Die Netzwerklimits und die CPU-Auslastung für Speicher bedingen sich gegenseitig. Wenn der Netzwerkdurchsatz steigt, steigt auch die CPU-Auslastung. Die Überwachung der CPU- und Netzwerknutzung gibt Aufschluss darüber, wie und warum die Ressourcen erschöpft werden.

Sie können Folgendes in Betracht ziehen, um die Netzwerknutzung zu minimieren:

- Verwenden einer größeren Instance-Klasse
- Verwenden von `pg_partman`-Partitionierungsstrategien

- Aufteilen der Schreibanforderungen in Batches, um die Gesamttransaktionen zu reduzieren
- Weiterleiten der schreibgeschützten Workload an eine schreibgeschützte Instance
- Löschen aller ungenutzten Indizes
- Suchen nach aufgeblähten Objekten und VACUUM. Verwenden Sie bei stark aufgeblähten Objekten die PostgreSQL-Erweiterung `pg_repack`. Weitere Informationen zu `pg_repack` finden Sie unter Reorganisieren von Tabellen in PostgreSQL-Datenbanken mit minimalen Sperren.

Verwenden der logischen Replikation, um ein Hauptversions-Upgrade für Aurora PostgreSQL durchzuführen

Wenn Sie die logische Replikation und schnelles Aurora-Klonen verwenden, können Sie ein Hauptversions-Upgrade unter Verwendung der aktuellen Version der Aurora-PostgreSQL-Datenbank durchführen, während Sie die sich ändernden Daten schrittweise auf die neue Hauptversionsdatenbank migrieren. Dieser Upgrade-Prozess mit geringen Ausfallzeiten wird als Blau/Grün-Upgrade bezeichnet. Die aktuelle Version der Datenbank wird als „blaue“ Umgebung und die neue Datenbankversion als „grüne“ Umgebung bezeichnet.

Dank des schnellen Klonens von Aurora werden die vorhandenen Daten vollständig geladen, indem ein Snapshot der Quelldatenbank erstellt wird. Das schnelle Klonen verwendet ein copy-on-write Protokoll, das auf der Aurora-Speicherschicht aufbaut, sodass Sie in kurzer Zeit einen Klon der Datenbank erstellen können. Diese Methode ist sehr effektiv beim Upgrade auf eine große Datenbank.

Die logische Replikation in PostgreSQL verfolgt und überträgt Ihre Datenänderungen von der ursprünglichen Instance auf eine neue Instance, die parallel läuft, bis Sie zur neueren Version von PostgreSQL wechseln. Für die logische Replikation wird ein Veröffentlichungs- und Abonnementmodell verwendet. Weitere Informationen über die logische Replikation von Aurora PostgreSQL finden Sie unter Replikation mit Amazon Aurora PostgreSQL.

> **Tip**
>
> Sie können die für ein Hauptversions-Upgrade erforderlichen Ausfallzeiten minimieren, indem Sie die verwaltete Blau/Grün-Bereitstellungsfunktion von Amazon RDS verwenden. Weitere Informationen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

Themen

Voraussetzungen

Sie müssen die folgenden Anforderungen erfüllen, um diesen Upgrade-Prozess mit geringen Ausfallzeiten durchzuführen:

- Sie müssen über rds_superuser-Berechtigungen verfügen.
- Auf dem DB-Cluster von Aurora PostgreSQL, den Sie aktualisieren möchten, muss eine unterstützte Version ausgeführt werden, die mithilfe logischer Replikation Hauptversions-Upgrades durchführen kann. Sie müssen alle Nebenversions-Updates und -Patches auf Ihren DB-Cluster anwenden. Die `aurora_volume_logical_start_lsn`-Funktion, die bei dieser Methode zum Einsatz kommt, wird in den folgenden Versionen von Aurora PostgreSQL unterstützt:
  - 15.2 und höhere 15-Versionen
  - 14.3 und höhere 14-Versionen
  - 13.6 und höhere 13-Versionen
  - 12.10 und höhere 12-Versionen
  - 11.15 und höhere 11-Versionen
  - 10.20 und höhere 10-Versionen

  Weitere Informationen über die `aurora_volume_logical_start_lsn`-Funktion finden Sie unter aurora_volume_logical_start_lsn.
- Alle Ihre Tabellen müssen einen Primärschlüssel haben oder eine PostgreSQL-Identitätsspalte enthalten.
- Konfigurieren Sie die Sicherheitsgruppe für Ihre VPC, um eingehenden und ausgehenden Zugriff zwischen den beiden DB-Clustern von Aurora PostgreSQL (dem alten und dem neuen) zu ermöglichen. Sie können Zugriff auf einen speziellen Classless Inter-Domain Routing (CIDR)-Bereich oder auf eine andere Sicherheitsgruppe in Ihrer VPC oder einer Peer-VPC gewähren. (Eine Peer-VPC erfordert eine VPC-Peering-Verbindung.)

> **Note**
>
> Detaillierte Informationen zu den Berechtigungen, die für die Konfiguration und Verwaltung eines laufenden logischen Replikationsszenarios erforderlich sind, finden Sie in der PostgreSQL-Core-Dokumentation.

Einschränkungen

Wenn Sie ein Upgrade mit niedriger Ausfallzeit für Ihren DB-Cluster von Aurora PostgreSQL durchführen, um ihn auf eine neue Hauptversion zu aktualisieren, verwenden Sie die native logische PostgreSQL-Replikationsfunktion. Sie weist die gleichen Fähigkeiten und Einschränkungen wie die logische PostgreSQL-Replikation auf. Weitere Informationen finden Sie unter Die logische Replikation von PostgreSQL.

- Data Definition Language (DDL)-Befehle werden nicht repliziert.
- Die Replikation unterstützt keine Schemaänderungen in einer Live-Datenbank. Das Schema wird während des Klonvorgangs in seiner ursprünglichen Form neu erstellt. Wenn Sie das Schema nach dem Klonen, aber vor Abschluss des Upgrades ändern, werden die Änderungen nicht in der aktualisierten Instance angezeigt.
- Große Objekte werden nicht repliziert, aber Sie können Daten in normalen Tabellen speichern.
- Die Replikation wird nur von Tabellen unterstützt, einschließlich partitionierter Tabellen. Die Replikation auf andere Relationstypen wie Ansichten, materialisierte Ansichten oder fremde Tabellen wird nicht unterstützt.
- Sequenzdaten werden nicht repliziert und müssen nach dem Failover manuell aktualisiert werden.

> **Note**
>
> Dieses Upgrade unterstützt kein Auto-Scripting. Sie sollten alle Schritte manuell ausführen.

Festlegen und Überprüfen von Parameterwerten

Vor dem Upgrade müssen Sie die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL so konfigurieren, dass sie als Veröffentlichungsserver fungiert. Die Instance sollte eine benutzerdefinierte DB-Cluster-Parametergruppe mit den folgenden Einstellungen verwenden:

- `rds.logical_replication` – Stellen Sie diesen Parameter auf 1 ein. Der `rds.logical_replication`-Parameter dient demselben Zweck wie der Parameter `wal_level` eines eigenständigen PostgreSQL-Servers und andere Parameter, die die Write-Ahead-Protokolldateiverwaltung steuern.
- `max_replication_slots` – Legen Sie diesen Parameter auf die Gesamtzahl der Abonnements fest, die Sie erstellen möchten. Wenn Sie verwenden AWS DMS, legen Sie diesen Parameter auf die Anzahl der AWS DMS Aufgaben fest, die Sie für die Erfassung geänderter Daten aus diesem DB-Cluster verwenden möchten.
- `max_wal_senders` – Legen Sie die Anzahl der gleichzeitigen Verbindungen sowie einige zusätzliche Verbindungen fest, um sie für Verwaltungsaufgaben und neue Sitzungen verfügbar zu machen. Wenn Sie verwenden AWS DMS, sollte die Anzahl der max_wal_senders der Anzahl der gleichzeitigen Sitzungen plus der Anzahl der AWS DMS Aufgaben entsprechen, die zu einem bestimmten Zeitpunkt möglicherweise funktionieren.
- `max_logical_replication_workers` – Legen Sie diesen Parameter auf die Anzahl der Worker für logische Replikation und Tabellensynchronisierung fest, die Sie erwarten. Im Allgemeinen ist es sicher, die Anzahl der Replikations-Worker auf den gleichen Wert festzulegen, der für max_wal_senders verwendet wird. Die Worker stammen aus dem Pool der Hintergrundprozesse (max_worker_processes), die dem Server zugewiesen sind.
- `max_worker_processes` – Legen Sie diesen Parameter auf die Anzahl der Hintergrundprozesse für den Server fest. Diese Anzahl sollte groß genug sein, um Worker für Replikation, Selbstbereinigungsprozesse und andere Wartungsprozesse, die möglicherweise gleichzeitig stattfinden, zur Verfügung zu stellen.

Wenn Sie auf eine neuere Version von Aurora PostgreSQL aktualisieren, müssen Sie alle Parameter duplizieren, die Sie in der früheren Version der Parametergruppe geändert haben. Diese Parameter werden auf die aktualisierte Version angewendet. Sie können die `pg_settings`-Tabelle abfragen, um eine Liste der Parametereinstellungen zu erhalten, sodass Sie sie in Ihrem neuen DB-Cluster von Aurora PostgreSQL neu erstellen können.

Führen Sie beispielsweise die folgende Abfrage aus, um die Einstellungen für Replikationsparameter abzurufen:

```
SELECT name, setting FROM pg_settings WHERE name in
('rds.logical_replication', 'max_replication_slots',
'max_wal_senders', 'max_logical_replication_workers',
'max_worker_processes');
```

Durchführen eines Upgrades von Aurora PostgreSQL auf eine neue Hauptversion

So bereiten Sie den Herausgeber vor (blau)

1. Im folgenden Beispiel ist die Writer-Quell-Instance (blau) ein DB-Cluster von Aurora PostgreSQL, auf dem PostgreSQL Version 11.15 ausgeführt wird. Dies ist der Veröffentlichungsknoten in unserem Replikationsszenario. Für diese Demonstration hostet unsere Writer-Quell-Instance eine Beispieltabelle, die eine Reihe von Werten enthält:

   ```
   CREATE TABLE my_table (a int PRIMARY KEY);
   INSERT INTO my_table VALUES (generate_series(1,100));
   ```

2. Um eine Publikation auf der Quell-Instance zu erstellen, stellen Sie mit psql (die CLI für PostgreSQL) oder mit dem Client Ihrer Wahl eine Verbindung zum Writer-Knoten der Instance her. Geben Sie in jeder Datenbank den folgenden Befehl ein:

   ```
   CREATE PUBLICATION publication_name FOR ALL TABLES;
   ```

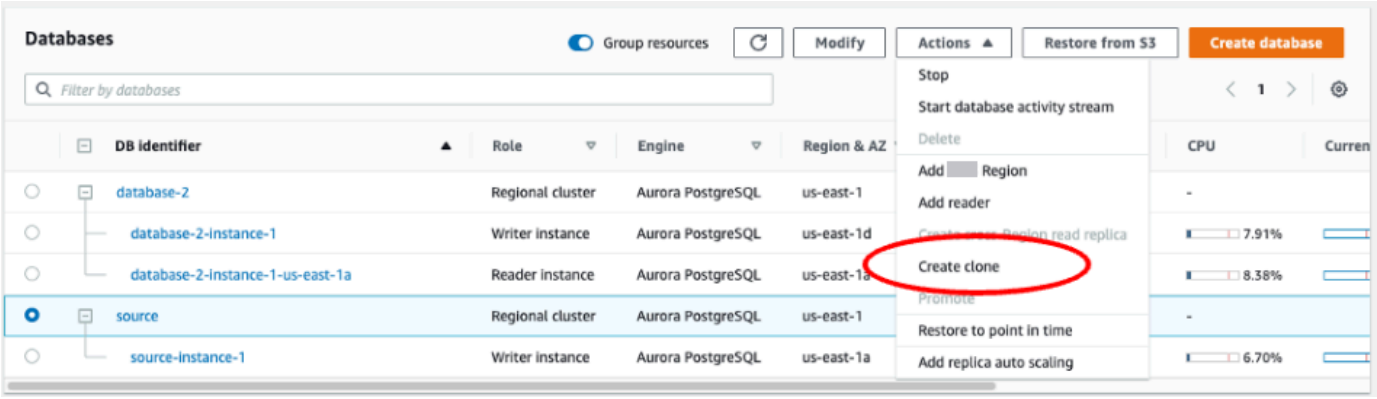
   Der Wert publication_name gibt den Namen der Publikation an.

3. Sie müssen auch einen Replikations-Slot auf der Instance erstellen. Der folgende Befehl erstellt einen Replikations-Slot und lädt das logische Dekodierungs-Plug-in `pgoutput`. Das Plug-in ändert den von Write-Ahead Logging (WAL) in das logische Replikationsprotokoll gelesenen Inhalt und filtert die Daten gemäß der Veröffentlichungsspezifikation.

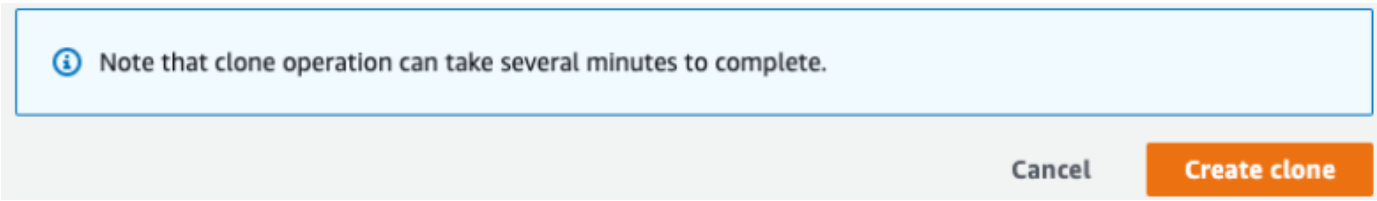
   ```
   SELECT pg_create_logical_replication_slot('replication_slot_name', 'pgoutput');
   ```

So klonen Sie den Herausgeber

1. Verwenden Sie die Amazon-RDS-Konsole, um einen Klon der Quell-Instance zu erstellen. Markieren Sie den Instance-Namen in der Amazon-RDS-Konsole und wählen Sie dann im Menü Actions (Aktionen) die Option Create Clone (Klon erstellen) aus.



2. Geben Sie einen eindeutigen Namen für die Instance ein. Die meisten Einstellungen sind Standardeinstellungen aus der Quell-Instance. Wenn Sie die für die neue Instance erforderlichen Änderungen vorgenommen haben, wählen Sie Create clone (Klon erstellen) aus.



3. Während die Ziel-Instance initiiert wird, wird in der Spalte Status des Writer-Knotens Creating angezeigt. Sobald die Instance bereit ist, ändert sich ihr Status in „Available“.

So bereiten Sie den Klon für ein Upgrade vor

1. Der Klon ist die „grüne“ Instance im Bereitstellungsmodell. Er ist der Host des Replikationsabonnementknotens. Wenn der Knoten verfügbar ist, stellen Sie eine Verbindung mit psql her und fragen Sie den neuen Writer-Knoten ab, um die Log-Sequenznummer (LSN) zu erhalten. Die LSN identifiziert den Anfang eines Datensatzes im WAL-Stream.

```
SELECT aurora_volume_logical_start_lsn();
```

2. Die LSN-Nummer finden Sie in der Antwort auf die Abfrage. Da Sie diese Nummer zu einem späteren Zeitpunkt des Vorgangs benötigen, sollten Sie sich diese notieren.

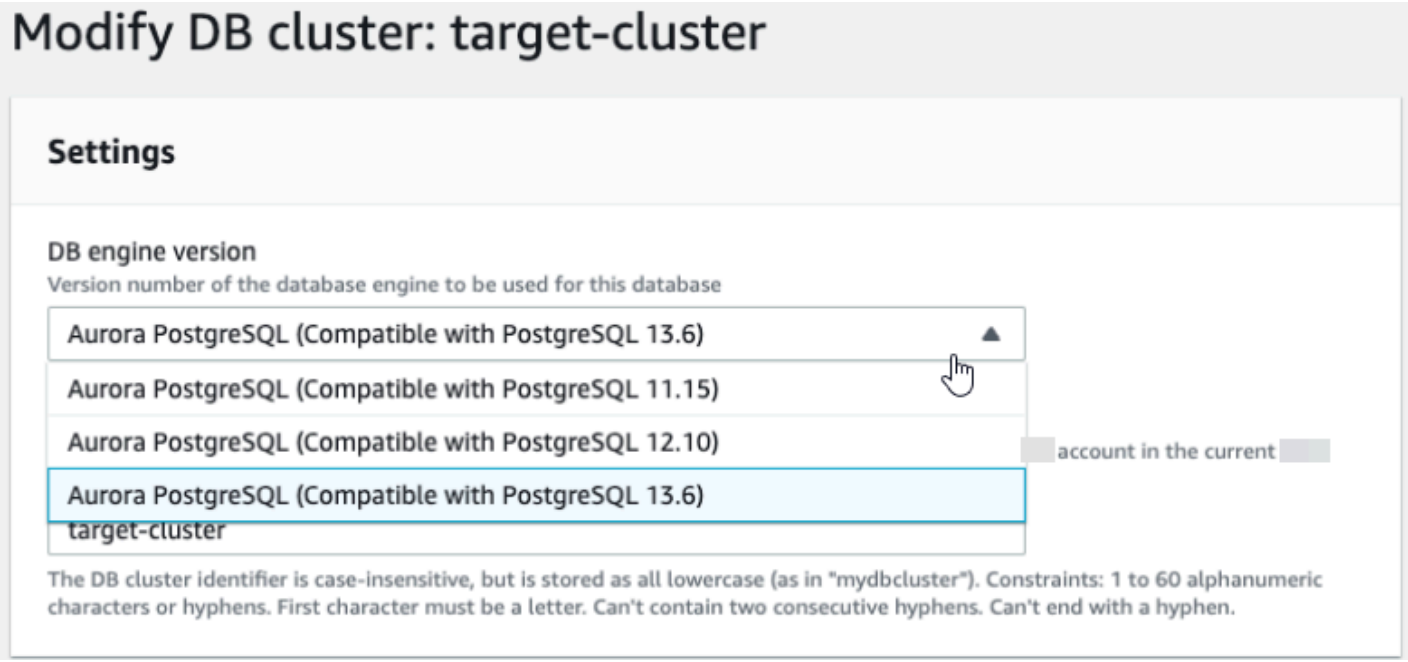
```
postgres=> SELECT aurora_volume_logical_start_lsn();
aurora_volume_logical_start_lsn
---------------
0/402E2F0
(1 row)
```

3. Bevor Sie den Klon aktualisieren, löschen Sie den Replikationsslot des Klons.

```
SELECT pg_drop_replication_slot('replication_slot_name');
```

So aktualisieren Sie einen Cluster auf eine neue Hauptversion

- Verwenden Sie nach dem Klonen des Provider-Knotens die Amazon-RDS-Konsole, um ein Hauptversions-Upgrade auf dem Abonnementknoten zu initiieren. Markieren Sie den Instance-Namen in der RDS-Konsole und klicken Sie auf die Schaltfläche Modify (Ändern). Wählen Sie die aktualisierte Version und Ihre aktualisierten Parametergruppen aus und wenden Sie die Einstellungen sofort an, um die Ziel-Instance zu aktualisieren.



- Sie können auch die CLI verwenden, um ein Upgrade durchzuführen:

```
aws rds modify-db-cluster –db-cluster-identifier $TARGET_Aurora_ID –engine-version
 13.6 –allow-major-version-upgrade –apply-immediately
```

So bereiten Sie den Abonnenten (grün) vor

1. Sobald der Klon nach dem Upgrade verfügbar ist, stellen Sie eine Verbindung mit psql her und definieren Sie das Abonnement. Dazu müssen Sie die folgenden Optionen im `CREATE SUBSCRIPTION`-Befehl angeben:

- `subscription_name` – Der Name des Abonnements.
- `admin_user_name` – Der Name eines Administratorbenutzers mit rds_superuser-Berechtigungen.
- `admin_user_password` – Das Passwort, das dem Administrator zugeordnet ist.
- `source_instance_URL` – Die URL der Veröffentlichungsserver-Instance.
- `database` – Die Datenbank, mit der der Abonnementserver eine Verbindung herstellen wird.
- `publication_name` – Der Name des Veröffentlichungsservers.
- `replication_slot_name` – Der Name der Replikationsgruppe.

```
CREATE SUBSCRIPTION subscription_name
CONNECTION 'postgres://admin_user_name:admin_user_password@source_instance_URL/
database' PUBLICATION publication_name
WITH (copy_data = false, create_slot = false, enabled = false, connect = true,
 slot_name = 'replication_slot_name');
```

2. Nachdem Sie das Abonnement erstellt haben, fragen Sie die Ansicht pg_replication_origin ab, um den Roname-Wert abzurufen. Dieser Wert ist die ID des Replikationsursprungs. Jede Instance hat einen `roname`-Wert:

   ```
   SELECT * FROM pg_replication_origin;
   ```

   Beispielsweise:

   ```
   postgres=>
   SELECT * FROM pg_replication_origin;

   roident | roname
   ---------+----------
   1 | pg_24586
   ```

3. Geben Sie im Befehl die LSN an, die Sie aus der vorherigen Abfrage des Veröffentlichungsknotens gespeichert haben, und den `roname`-Wert, der vom Abonnementknoten [INSTANCE] zurückgegeben wurde. Dieser Befehl verwendet die pg_replication_origin_advance-Funktion, um den Ausgangspunkt in der Protokollsequenz für die Replikation anzugeben.

```
SELECT pg_replication_origin_advance('roname', 'log_sequence_number');
```

`roname` ist die ID, die von der Ansicht pg_replication_origin zurückgegeben wird.

`log_sequence_number` ist der Wert, der von der vorherigen Abfrage der `aurora_volume_logical_start_lsn`-Funktion zurückgegeben wurde.

4. Verwenden Sie dann die `ALTER SUBSCRIPTION... ENABLE`-Klausel, um die logische Replikation zu aktivieren.

```
ALTER SUBSCRIPTION subscription_name ENABLE;
```

5. An dieser Stelle können Sie bestätigen, dass die Replikation funktioniert. Fügen Sie der Veröffentlichungs-Instance einen Wert hinzu und bestätigen Sie dann, dass der Wert auf den Abonnementknoten repliziert wird.

   Verwenden Sie dann den folgenden Befehl, um die Replikationsverzögerung auf dem Veröffentlichungsknoten zu überwachen:

```
SELECT now() AS CURRENT_TIME, slot_name, active, active_pid,
 pg_size_pretty(pg_wal_lsn_diff(pg_current_wal_lsn(),
confirmed_flush_lsn)) AS diff_size, pg_wal_lsn_diff(pg_current_wal_lsn(),
confirmed_flush_lsn) AS diff_bytes FROM pg_replication_slots WHERE slot_type =
 'logical';
```

   Beispielsweise:

```
postgres=> SELECT now() AS CURRENT_TIME, slot_name, active, active_pid,
 pg_size_pretty(pg_wal_lsn_diff(pg_current_wal_lsn(),
confirmed_flush_lsn)) AS diff_size, pg_wal_lsn_diff(pg_current_wal_lsn(),
 confirmed_flush_lsn) AS diff_bytes FROM pg_replication_slots WHERE slot_type =
 'logical';

current_time                   | slot_name             | active | active_pid |
 diff_size | diff_bytes
-------------------------------+-----------------------+--------+------------
+-----------+------------
2022-04-13 15:11:00.243401+00  | replication_slot_name | t      | 21854      | 136
 bytes | 136
(1 row)
```

Sie können die Replikationsverzögerung mit den Werten `diff_size` und`diff_bytes` überwachen. Wenn diese Werte 0 erreichen, hat das Replikat den Stand der Quell-DB-Instance erreicht.

Durchführen von Aufgaben nach dem Upgrade

Wenn das Upgrade abgeschlossen ist, wird der Instance-Status in der Spalte Status des Konsolen-Dashboards als Available angezeigt. Für die neue Instance empfehlen wir Ihnen Folgendes:

- Leiten Sie Ihre Anwendungen so um, dass sie auf den Writer-Knoten verweisen.
- Fügen Sie Reader-Knoten hinzu, um die Fallzahl zu verwalten und eine hohe Verfügbarkeit zu gewährleisten, falls ein Problem mit dem Writer-Knoten auftritt.
- DB-Cluster von Aurora PostgreSQL erfordern gelegentlich Betriebssystem-Updates. Diese Updates können eine neuere Version der Glibc-Bibliothek umfassen. Bei solchen Updates empfehlen wir Ihnen, die unter In Aurora PostgreSQL unterstützte Sortierungen beschriebenen Richtlinien zu befolgen.
- Aktualisieren Sie die Benutzerberechtigungen für die neue Instance, um den Zugriff sicherzustellen.

Nachdem Sie Ihre Anwendung und Daten auf der neuen Instance getestet haben, empfehlen wir Ihnen, ein letztes Backup Ihrer ersten Instance zu erstellen, bevor Sie sie entfernen. Weitere Informationen zur Verwendung der logischen Replikation auf einem Aurora-Host finden Sie unter Einrichten der logischen Replikation für Ihren DB-Cluster von Aurora PostgreSQL.

Fehlerbehebung bei Speicherproblemen

Wenn der von Sortier- oder Indexerstellungsoperationen benötigte Arbeitsspeicher den vom `work_mem`-Parameter zugewiesene Arbeitsspeicher überschreitet, schreibt Aurora PostgreSQL die überschüssigen Daten in temporäre Datenträgerdateien. Dabei verwendet Aurora Postgre SQL den gleichen Speicherort wie für Fehler- und Meldungsprotokolle, d. h. den lokalen Speicher. Für jede Instance in Ihrem DB-Cluster von Aurora PostgreSQL ist eine bestimmte Menge an lokalem Speicher verfügbar. Die Speichermenge basiert auf der entsprechenden DB-Instance-Klasse. Wenn Sie den lokalen Speicherplatz erhöhen möchten, müssen Sie die Instance so ändern, dass sie eine größere DB-Instance-Klasse verwendet. Spezifikationen für DB-Instance-Klassen finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.

Sie können den lokalen Speicherplatz Ihres DB-Clusters von Aurora PostgreSQL überwachen, indem Sie sich die Amazon-CloudWatch-Metrik für `FreeLocalStorage` ansehen. Diese Metrik meldet die Menge des verfügbaren Speicherplatzes jeder DB-Instance im Aurora-DB-Cluster für temporäre Tabellen und Protokolle. Weitere Informationen finden Sie unter Überwachen von Amazon Aurora-Metriken mit Amazon CloudWatch.

Sortier-, Indizierungs- und Gruppierungsoperationen beginnen im Arbeitsspeicher, müssen jedoch häufig in den lokalen Speicher ausgelagert werden. Wenn für Ihren DB-Cluster von Aurora PostgreSQL aufgrund dieser Art von Operationen der lokale Speicherplatz nicht ausreicht, können Sie das Problem lösen, indem Sie eine der folgenden Maßnahmen ergreifen.

- Rüsten Sie den Arbeitsspeicher auf. Dadurch muss weniger lokaler Speicher verwendet werden. Standardmäßig weist PostgreSQL 4 MB für jede Sortier-, Gruppierungs- und Indizierungsoperation zu. Wenn Sie den aktuellen Arbeitsspeicherwert für die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL überprüfen möchten, stellen Sie eine Verbindung mit der Instance über `psql` her und führen Sie den folgenden Befehl aus.

  ```
  postgres=> SHOW work_mem;
  work_mem
  ----------
   4MB
  (1 row)
  ```

  Sie können den Arbeitsspeicher auf Sitzungsebene vor Sortier-, Gruppierungs- und anderen Operationen wie folgt erhöhen.

  ```
  SET work_mem TO '1 GB';
  ```

  Weitere Informationen zum Arbeitsspeicher finden Sie unter Ressourcennutzung in der PostgreSQL-Dokumentation.
- Ändern Sie den Aufbewahrungszeitraum für Protokolle, sodass die Protokolle für kürzere Zeiträume gespeichert werden. Um zu erfahren wie dies geht, vgl. Datenbank-Protokolldateien von Aurora PostgreSQL.

Wenn Ihr DB-Cluster von Aurora PostgreSQL größer als 40 TB ist, verwenden Sie nicht die Instance-Klassen db.t2, db.t3 oder db.t4g. Wir empfehlen, die T-DB-Instance-Klassen nur für Entwicklungs-

und Testserver oder andere Nicht-Produktionsserver zu verwenden. Weitere Informationen finden Sie unter DB-Instance-Klassenarten.

Replikation mit Amazon Aurora PostgreSQL

Im Folgenden finden Sie Informationen zur Replikation mit Amazon Aurora PostgreSQL und wie sie diese überwachen.

Themen

Verwendung von Aurora-Replicas

Eine Aurora Replica ist ein unabhängiger Endpunkt in einem Aurora-DB-Cluster, die die beste Methode für das Skalieren von Leseoperationen und Erhöhen der Verfügbarkeit darstellen. Ein Aurora-DB-Cluster kann bis zu 15 Aurora Replicas enthalten, die sich in den Availability Zones der AWS Region des Aurora-DB-Clusters befinden.

Das DB-Cluster-Volume besteht aus mehreren Kopien der Daten für den DB-Cluster. Die Daten im Cluster-Volume werden jedoch als ein einzelnes logisches Volume der primären Writer-DB-Instance und der Aurora-Replicas im DB-Cluster dargestellt. Weitere Informationen über Aurora-Replicas finden Sie unter Aurora-Replikate.

Aurora Replicas eignen sich für das Skalieren von Lesevorgängen, da sie in Ihrem Cluster-Volume ausschließlich für Lesevorgänge bereitstehen. Schreibvorgänge werden von der Writer-DB-Instance verwaltet. Das Cluster-Volume wird von allen Instance in Ihrem Aurora PostgreSQL-DB-Cluster gemeinsam genutzt. Daher ist keine zusätzliche Arbeit erforderlich, um eine Kopie der Daten für jede Aurora Replica zu replizieren.

Mit Aurora PostgreSQL wird beim Löschen eines Aurora-Replica der Instance-Endpunkt sofort entfernt und das Aurora-Replica vom Leser-Endpunkt entfernt. Wenn Anweisungen vorhanden sind, die auf dem Aurora-Replica ausgeführt werden, das gerade gelöscht wird, besteht eine Übergangsfrist von drei Minuten. Vorhandene Anweisungen können während der Nachfrist geordnet beendet werden. Nach Ablauf der Nachfrist wird das Aurora-Replikat geschlossen und gelöscht.

Aurora PostgreSQL-DB-Cluster unterstützen Aurora Replicas in verschiedenen AWS Regionen unter Verwendung der globalen Aurora-Datenbank. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Global Databases.

> **Note**
>
> Mit der verbesserten Leseverfügbarkeitsfunktion müssen Sie die Aurora Replicas im DB-Cluster ggf. manuell neu starten. Für die DB-Cluster, die vor Einführung dieser Funktion erstellt wurden, werden durch einen Neustart der Writer-DB-Instance automatisch die Aurora Replicas neu gestartet. Durch den automatischen Neustart wird der Einstiegspunkt wiederhergestellt, der die Lese-/Schreibkonsistenz innerhalb des DB-Clusters gewährleistet.

Verbesserung der Leseverfügbarkeit von Aurora Replicas

Aurora PostgreSQL verbessert die Leseverfügbarkeit im DB-Cluster, indem die Leseanforderungen kontinuierlich bearbeitet werden, wenn die Writer-DB-Instance neu gestartet wird oder wenn die Aurora Replica nicht mit dem Schreibverkehr Schritt halten kann.

Die Leseverfügbarkeitsfunktion ist standardmäßig in den folgenden Versionen von Aurora PostgreSQL verfügbar:

- 15.2 und höhere 15-Versionen
- 14.7 und höhere 14-Versionen
- 13.10 und höhere 13-Versionen
- 12.14 und höhere 12-Versionen

Die Leseverfügbarkeitsfunktion wird von der globalen Aurora-Datenbank in den folgenden Versionen unterstützt:

- 15.4 und höhere 15-Versionen
- 14.9 und höhere 14-Versionen
- 13.12 und höhere 13 Versionen
- 12.16 und höhere 12-Versionen

Um die Leseverfügbarkeitsfunktion für einen DB-Cluster zu verwenden, der vor der Einführung der Funktion in einer dieser Versionen erstellt wurde, starten Sie die Writer-Instance des DB-Clusters neu.

Wenn Sie statische Parameter Ihres DB-Clusters von Aurora PostgreSQL ändern, müssen Sie die Writer-Instance neu starten, damit die Parameteränderungen wirksam werden. Sie müssen beispielsweise die Writer-Instance neu starten, wenn Sie den Wert `shared_buffers` festlegen. Dank der verbesserten Verfügbarkeit von Aurora Replicas behält der DB-Cluster die Leseverfügbarkeit während dieser Neustarts bei, wodurch die Auswirkungen von Änderungen auf die Writer-Instance reduziert werden. Die Reader-Instances werden nicht neu gestartet und antworten weiterhin auf die Leseanfragen. Um statische Parameteränderungen anzuwenden, starten Sie jede einzelne Reader-Instance neu.

Eine Aurora Replica eines DB-Clusters von Aurora PostgreSQL kann nach Replikationsfehlern wie Writer-Neustarts, Failover, langsamer Replikation und Netzwerkproblemen wiederhergestellt werden, indem sie nach einer erneuten Verbindung mit dem Writer schnell den In-Memory-Datenbankstatus wiederherstellt. Dieser Ansatz ermöglicht es Aurora-Replica-Instances, die Konsistenz mit den neuesten Speicher-Updates zu erreichen, solange die Client-Datenbank noch verfügbar ist.

Bei laufenden Transaktionen, die mit der Replikationswiederherstellung kollidieren, wird möglicherweise ein Fehler angezeigt, aber der Client kann diese Transaktionen erneut versuchen, sobald die Reader wieder mit dem Writer mithalten.

Überwachen von Aurora Replicas

Sie können die Aurora Replicas bei der Wiederherstellung nach einer Writer-Unterbrechung überwachen. Verwenden Sie die folgenden Metriken, um nach den neuesten Informationen zur Reader-Instance zu suchen und um in Bearbeitung befindliche schreibgeschützte Transaktionen zu verfolgen.

- Die `aurora_replica_status` Funktion wurde aktualisiert, sodass sie die meisten up-to-date Informationen für die Reader-Instanz zurückgibt, wenn diese noch verbunden ist. Der Zeitstempel der letzten Aktualisierung in `aurora_replica_status` ist für die Zeile, die der DB-Instance entspricht, auf der die Abfrage ausgeführt wird, immer leer. Dies bedeutet, dass die Reader-Instance über die neuesten Daten verfügt.
- Wenn das Aurora Replica die Verbindung zur Writer-Instance trennt und wieder eine Verbindung herstellt, wird das folgende Datenbankereignis ausgelöst:

```
Read replica has been disconnected from the writer instance and
reconnected.
```

- Wenn eine schreibgeschützte Abfrage aufgrund eines Wiederherstellungskonflikts abgebrochen wird, werden im Datenbankfehlerprotokoll möglicherweise eine oder mehrere der folgenden Fehlermeldungen angezeigt:

```
Canceling statement due to conflict with recovery.

User query may not have access to page data to replica disconnect.

User query might have tried to access a file that no longer exists.

When the replica reconnects, you will be able to repeat your command.
```

Einschränkungen

Die folgenden Einschränkungen gelten für Aurora Replicas mit verbesserter Verfügbarkeit:

- Aurora Replicas des sekundären DB-Clusters können neu gestartet werden, wenn die Daten während der Replikationswiederherstellung nicht von der Writer-Instance gestreamt werden können.
- Aurora Replicas unterstützen keine Online-Replikationswiederherstellung, wenn eine solche Wiederherstellung bereits läuft und neu gestartet wird.
- Aurora Replicas werden neu gestartet, wenn sich Ihre DB-Instance dem Transaktions-ID-Wraparound nähert. Weitere Informationen zum Transaktions-ID-Wraparound finden Sie unter Verhindern von Transaktions-ID-Wraparound-Fehlern.
- Aurora Replicas können unter bestimmten Umständen neu gestartet werden, wenn der Replikationsprozess blockiert ist.

Überwachung einer Aurora PostgreSQL-Replikation

Skalieren von Lesevorgängen und hohe Verfügbarkeit hängen von der minimalen Verzögerungszeit ab. Sie können überwachen, wie weit eine Aurora Replica der Writer-DB-Instance Ihres Aurora PostgreSQL-DB-Clusters hinterherhinkt, indem Sie die Amazon-Metrik überwachen. CloudWatch `ReplicaLag` Da Aurora Replicas aus demselben Cluster-Volume wie die Writer-DB-Instance lesen, hat die `ReplicaLag`-Metrik für einen Aurora PostgreSQL-DB-Cluster eine andere Bedeutung. Die

`ReplicaLag`-Metrik für eine Aurora Replica ermittelt die Verzögerung für den Seiten-Cache der Aurora Replica im Vergleich zu der der Writer-DB-Instance.

Weitere Informationen zur Überwachung von RDS-Instances und CloudWatch -Metriken finden Sie unter. Überwachung von Metriken in einem Amazon-Aurora-Cluster

Verwenden der logischen Replikation von PostgreSQL mit Aurora

Durch die Verwendung der logischen Replikationsfunktion von PostgreSQL mit Ihrem DB-Cluster von Aurora PostgreSQL können Sie einzelne Tabellen statt der gesamten Datenbank-Instance replizieren und synchronisieren. Für die logische Replikation wird ein Veröffentlichungs- und Abonnementmodell verwendet, um Änderungen aus einer Quelle an einen oder mehrere Empfänger zu replizieren. Dazu werden Änderungsdatensätze aus dem Write-Ahead-Protokoll (WAL) von PostgreSQL verwendet. Die Quelle oder der Herausgeber sendet WAL-Daten für die angegebenen Tabellen an einen oder mehrere Empfänger (Abonnenten). Dadurch werden die Änderungen repliziert und die Tabelle eines Abonnenten wird mit der Tabelle des Herausgebers synchronisiert. Die Änderungen des Herausgebers werden anhand einer Veröffentlichung identifiziert. Abonnenten erhalten die Änderungen, indem sie ein Abonnement erstellen, das die Verbindung mit der Datenbank des Herausgebers und den entsprechenden Veröffentlichungen definiert. Ein Replikationsslot ist der Mechanismus, der in diesem Schema verwendet wird, um den Fortschritt eines Abonnements zu verfolgen.

Bei DB-Clustern von Aurora PostgreSQL werden die WAL-Datensätze im Aurora-Speicher abgelegt. Der DB-Cluster von Aurora PostgreSQL, der in einem logischen Replikationsszenario als Herausgeber fungiert, liest die WAL-Daten aus dem Aurora-Speicher, dekodiert sie und sendet sie an den Abonnenten, sodass die Änderungen auf die Tabelle in dieser Instance angewendet werden können. Der Herausgeber verwendet einen logischen Decoder, um die Daten für die Verwendung durch Abonnenten zu dekodieren. Standardmäßig verwenden DB-Cluster von Aurora PostgreSQL beim Senden von Daten das native `pgoutput`-Plugin von PostgreSQL. Es sind auch andere logische Decoder verfügbar. Zum Beispiel unterstützt Aurora PostgreSQL auch das `wal2json`-Plugin, das WAL-Daten in JSON konvertiert.

Ab Aurora PostgreSQL Version 14.5, 13.8, 12.12 und 11.17 erweitert Aurora PostgreSQL den logischen Replikationsprozess von PostgreSQL um einen Write-Through-Cache, um die Leistung zu verbessern. Die WAL-Transaktionsprotokolle werden lokal in einem Puffer zwischengespeichert, um die Menge an Festplatten-I/O zu reduzieren, d. h. es wird während der logischen Dekodierung aus dem Aurora-Speicher gelesen. Der Write-Through-Cache wird standardmäßig verwendet, wenn Sie die logische Replikation für Ihren DB-Cluster von Aurora PostgreSQL verwenden. Aurora bietet

mehrere Funktionen, mit denen Sie den Cache verwalten können. Weitere Informationen finden Sie unter Verwaltung des Write-Through-Cache für die logische Replikation in Aurora PostgreSQL.

Die logische Replikation wird von allen derzeit verfügbaren Aurora-PostgreSQL-Versionen unterstützt. Weitere Informationen finden Sie unter Aktualisierungen von Amazon Aurora PostgreSQL im Abschnitt Versionshinweise für Aurora PostgreSQL.

> **Note**
>
> Zusätzlich zu der in PostgreSQL 10 eingeführten nativen logischen Replikationsfunktion von PostgreSQL unterstützt Aurora PostgreSQL auch die `pglogical`-Erweiterung. Weitere Informationen finden Sie unter Verwenden von pglogical, um Daten zwischen Instances zu synchronisieren.

Weitere Informationen über die logische Replikation in PostgreSQL finden Sie unter Logical Replication (Logische Replikation) und Logical Decoding Concepts (Logische Dekodierungskonzepte) in der PostgreSQL-Dokumentation.

In den folgenden Themen finden Sie Informationen dazu, wie Sie die logische Replikation auf Ihren DB-Clustern von Aurora PostgreSQL einrichten.

Themen

- Einrichten der logischen Replikation für Ihren DB-Cluster von Aurora PostgreSQL
- Deaktivieren der logischen Replikation
- Verwaltung des Write-Through-Cache für die logische Replikation in Aurora PostgreSQL
- Verwalten logischer Slots für Aurora PostgreSQL
- Beispiel: Verwenden der logischen Replikation mit DB-Clustern von Aurora PostgreSQL
- Beispiel: Die logische Replikation unter Verwendung von Aurora PostgreSQL und AWS Database Migration Service

Einrichten der logischen Replikation für Ihren DB-Cluster von Aurora PostgreSQL

Für das Einrichten der logischen Replikation sind `rds_superuser`-Berechtigungen erforderlich. Ihr DB-Cluster von Aurora PostgreSQL muss für die Verwendung einer benutzerdefinierten DB-Cluster-Parametergruppe konfiguriert sein, damit Sie die erforderlichen Parameter wie im folgenden

Verfahren beschrieben festlegen können. Weitere Informationen finden Sie unter Arbeiten mit DB-Cluster-Parametergruppen.

So richten Sie die logische Replikation von PostgreSQL für einen DB-Cluster von Aurora PostgreSQL ein

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Ihren DB-Cluster von Aurora PostgreSQL im Navigationsbereich aus.
3. Öffnen Sie die Registerkarte Configuration (Konfiguration). Suchen Sie in den Instance-Details den Link Parametergruppe mit der DB-Cluster-Parametergruppe als Typ.
4. Wählen Sie den Link aus, um die benutzerdefinierten Parameter zu öffnen, die Ihrem DB-Cluster von Aurora PostgreSQL zugeordnet sind.
5. Geben Sie in das Suchfeld Parameters (Parameter) `rds` ein, um den `rds.logical_replication`-Parameter zu finden. Der Standardwert für diesen Parameter ist `0`, was bedeutet, dass er standardmäßig deaktiviert ist.
6. Wählen Sie Edit parameters (Parameter bearbeiten) aus, um auf die Eigenschaftswerte zuzugreifen. Wählen Sie dann 1 aus der Auswahl aus, um die Funktion zu aktivieren. Abhängig von Ihrer erwarteten Auslastung müssen Sie möglicherweise auch die Einstellungen für die folgenden Parameter ändern. In vielen Fällen sind die Standardwerte jedoch ausreichend.

   - `max_replication_slots`: Legen Sie diesen Parameter auf einen Wert fest, der mindestens der geplanten Gesamtzahl der Veröffentlichungen und Abonnements der logischen Replikation entspricht. Wenn Sie AWS DMS verwenden, sollte dieser Parameter mindestens den geplanten Aufgaben zur Erfassung von Änderungsdaten aus dem Cluster plus den Veröffentlichungen und Abonnements der logischen Replikation entsprechen.
   - `max_wal_senders` und `max_logical_replication_workers`: Legen Sie diese Parameter auf einen Wert fest, der mindestens der Anzahl der logischen Replikationsslots, die aktiv sein sollen, oder der Anzahl der aktiven AWS DMS-Aufgaben zur Erfassung von Änderungsdaten entspricht. Wenn Sie einen logischen Replikationsslot inaktiv lassen, wird die Bereinigung durch Entfernen überholter Tupel aus Tabellen verhindert. Wir empfehlen daher, Replikationsslots zu überwachen und inaktive Slots nach Bedarf zu entfernen.
   - `max_worker_processes`: Legen Sie diesen Parameter auf einen Wert fest, der mindestens der Summe der Werte `max_logical_replication_workers`, `autovacuum_max_workers` und `max_parallel_workers` entspricht. Bei kleinen DB-Instance-Klassen können sich Hintergrund-Workerprozesse auf Anwendungs-

Workloads auswirken. Überwachen Sie daher die Leistung Ihrer Datenbank, wenn Sie `max_worker_processes` höher als den Standardwert festlegen. (Der Standardwert ist das Ergebnis von `GREATEST(${DBInstanceVCPU*2},8}`, was bedeutet, dass dies standardmäßig entweder 8 oder doppelt so hoch ist wie das CPU-Äquivalent der DB-Instance-Klasse, je nachdem, welcher Wert größer ist).

> **Note**
>
> Sie können die Parameterwerte in einer benutzerdefinierten DB-Parametergruppe ändern. Die Parameterwerte in einer Standard-DB-Parametergruppe können nicht geändert werden.

7. Wählen Sie Änderungen speichern aus.
8. Starten Sie die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL neu, damit Ihre Änderungen wirksam werden. Wählen Sie in der Amazon-RDS-Konsole die primäre DB-Instance des Clusters und dann im Menü Actions (Aktionen) die Option Reboot (Neustart) aus.
9. Wenn die Instance verfügbar ist, können Sie wie folgt überprüfen, ob die logische Replikation aktiviert ist.

   a. Verwenden Sie `psql`, um eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL herzustellen.

   ```
   psql --host=your-db-cluster-instance-1.aws-region.rds.amazonaws.com --port=5432
    --username=postgres --password --dbname=labdb
   ```

   b. Stellen Sie mithilfe des folgenden Befehls sicher, dass die logische Replikation aktiviert wurde.

   ```
   labdb=> SHOW rds.logical_replication;
    rds.logical_replication
   -------------------------
    on
   (1 row)
   ```

   c. Überprüfen Sie, dass `wal_level` auf `logical` festgelegt ist.

   ```
   labdb=> SHOW wal_level;
     wal_level
   ```

```
-----------
 logical
(1 row)
```

Ein Beispiel für die Verwendung der logischen Replikation, um eine Datenbanktabelle mit Änderungen aus einem Quell-DB-Cluster von Aurora PostgreSQL zu synchronisieren, finden Sie unter Beispiel: Verwenden der logischen Replikation mit DB-Clustern von Aurora PostgreSQL.

Deaktivieren der logischen Replikation

Nachdem Sie Ihre Replikationsaufgaben abgeschlossen haben, sollten Sie den Replikationsprozess beenden, Replikationsslots löschen und die logische Replikation deaktivieren. Bevor Sie Slots löschen, vergewissern Sie sich, dass diese nicht mehr benötigt werden. Aktive Replikationsslots können nicht gelöscht werden.

So deaktivieren Sie die logische Replikation

1. Löschen Sie alle Replikations-Slots.

   Wenn Sie alle Replikationsslots löschen möchten, stellen Sie eine Verbindung zum Herausgeber her und führen Sie den folgenden SQL-Befehl aus.

   ```
   SELECT pg_drop_replication_slot(slot_name)
     FROM pg_replication_slots
    WHERE slot_name IN (SELECT slot_name FROM pg_replication_slots);
   ```

   Die Replikationsslots dürfen nicht aktiv sein, wenn Sie diesen Befehl ausführen.

2. Ändern Sie die dem Herausgeber zugeordnete benutzerdefinierte DB-Cluster-Parametergruppe, wie in Einrichten der logischen Replikation für Ihren DB-Cluster von Aurora PostgreSQL beschrieben. Legen Sie den `rds.logical_replication`-Parameter jedoch auf 0 fest.

   Weitere Informationen zu benutzerdefinierten DB-Parametergruppen finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe.

3. Starten Sie den Herausgeber-DB-Cluster von Aurora PostgreSQL neu, damit die Änderung des `rds.logical_replication`-Parameters wirksam wird.

Verwaltung des Write-Through-Cache für die logische Replikation in Aurora PostgreSQL

Standardmäßig verwenden die Aurora-PostgreSQL-Versionen 14.5, 13.8, 12.12 und 11.17 und höher einen Write-Through-Cache, um die Leistung für die logische Replikation zu verbessern. Ohne den Write-Through-Cache verwendet Aurora PostgreSQL die Aurora-Speicherschicht bei der Implementierung des nativen logischen PostgreSQL-Replikationsprozesses. Dazu schreibt es WAL-Daten in den Speicher und liest die Daten dann wieder aus dem Speicher, um sie zu dekodieren und an ihre Ziele (Abonnenten) zu senden (zu replizieren). Dies kann zu Engpässen bei der logischen Replikation für DB-Cluster von Aurora PostgreSQL führen.

Der Write-Through-Cache reduziert die Notwendigkeit, die Aurora-Speicherschicht zu verwenden. Anstatt immer aus der Aurora-Speicherschicht zu schreiben und zu lesen, verwendet Aurora PostgreSQL einen Puffer, um den logischen WAL-Stream zwischenzuspeichern, sodass er während des Replikationsprozesses verwendet werden kann und Daten nicht immer von der Festplatte abgerufen werden müssen. Dieser Puffer ist der native PostgreSQL-Cache, der für die logische Replikation verwendet wird. Er wird in den DB-Clusterparametern von Aurora PostgreSQL als `rds.logical_wal_cache` identifiziert. Standardmäßig verwendet dieser Cache 1/32 der Puffercache-Einstellung (`shared_buffers`) des DB-Clusters von Aurora PostgreSQL, jedoch nicht weniger als 64 kB und nicht mehr als die Größe eines WAL-Segments, in der Regel 16 MB.

Wenn Sie die logische Replikation mit Ihrem DB-Cluster von Aurora PostgreSQL verwenden (für die Versionen, die den Write-Through-Cache unterstützen), können Sie die Cache-Trefferrate überwachen, um festzustellen, wie gut sie für Ihren Anwendungsfall funktioniert. Stellen Sie dazu mit `psql` eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her und verwenden Sie dann die Aurora-Funktion `aurora_stat_logical_wal_cache`, wie im folgenden Beispiel gezeigt.

```
SELECT * FROM aurora_stat_logical_wal_cache();
```

Die Funktion gibt beispielsweise die folgende Ausgabe zurück.

```
name       | active_pid | cache_hit | cache_miss | blks_read | hit_rate |
 last_reset_timestamp
-----------+------------+-----------+------------+-----------+----------+--------------
test_slot1 | 79183      | 24        | 0          | 24        | 100.00%  | 2022-08-05
 17:39...
test_slot2 |            | 1         | 0          |  1        | 100.00%  | 2022-08-05
 17:34...
```

```
(2 rows)
```

Die `last_reset_timestamp`-Werte wurden aus Gründen der Lesbarkeit gekürzt. Weitere Informationen zu dieser Funktion finden Sie unter aurora_stat_logical_wal_cache.

Aurora PostgreSQL bietet die beiden folgenden Funktionen zur Überwachung des Write-Through-Cache.

- Die `aurora_stat_logical_wal_cache`-Funktion – Die Referenzdokumentation finden Sie unter aurora_stat_logical_wal_cache.
- Die `aurora_stat_reset_wal_cache`-Funktion – Die Referenzdokumentation finden Sie unter aurora_stat_reset_wal_cache.

Wenn Sie feststellen, dass die automatisch angepasste WAL-Cache-Größe für Ihre Workloads nicht ausreicht, können Sie den Wert von `rds.logical_wal_cache` manuell ändern, indem Sie den Parameter in Ihrer benutzerdefinierten DB-Cluster-Parametergruppe anpassen. Beachten Sie, dass jeder positive Wert unter 32 kB als 32 kB behandelt wird. Weitere Informationen über `wal_buffers` finden Sie unter Write-Ahead-Protokoll in der PostgreSQL-Dokumentation.

Verwalten logischer Slots für Aurora PostgreSQL

Streaming-Aktivitäten werden in der `pg_replication_origin_status`-Ansicht erfasst. Wenn Sie den Inhalt dieser Ansicht anzeigen möchten, können Sie die `pg_show_replication_origin_status()`-Funktion verwenden, wie im Folgenden gezeigt:

```
SELECT * FROM pg_show_replication_origin_status();
```

Sie können eine Liste Ihrer logischen Slots mit der folgenden SQL-Abfrage abrufen.

```
SELECT * FROM pg_replication_slots;
```

Zum Löschen eines logischen Slots können Sie den `pg_drop_replication_slot` mit dem Namen des Slots verwenden, wie im folgenden Befehl gezeigt.

```
SELECT pg_drop_replication_slot('test_slot');
```

Beispiel: Verwenden der logischen Replikation mit DB-Clustern von Aurora PostgreSQL

Das folgende Verfahren zeigt Ihnen, wie Sie die logische Replikation zwischen zwei DB-Clustern von Aurora PostgreSQL starten. Sowohl der Herausgeber als auch der Abonnent müssen für die logische Replikation konfiguriert sein, wie unter Einrichten der logischen Replikation für Ihren DB-Cluster von Aurora PostgreSQL beschrieben.

Der DB-Cluster von Aurora PostgreSQL, der der designierte Herausgeber ist, muss ebenfalls Zugriff auf den Replikationsslot gewähren. Ändern Sie dazu die Sicherheitsgruppe, die der Virtual Public Cloud (VPC) des DB-Clusters von Aurora PostgreSQL zugeordnet ist, basierend auf dem Amazon-VPC-Service. Erlauben Sie eingehenden Zugriff, indem Sie die Sicherheitsgruppe, die der VPC des Abonnenten zugeordnet ist, zur Sicherheitsgruppe des Herausgebers hinzufügen. Weitere Informationen finden Sie unter Kontrollieren des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen im Benutzerhandbuch von Amazon VPC.

Nachdem diese vorbereitenden Schritte abgeschlossen sind, können Sie die PostgreSQL-Befehle `CREATE PUBLICATION` auf dem Herausgeber und `CREATE SUBSCRIPTION` auf dem Abonnenten verwenden, wie im folgenden Verfahren beschrieben.

So starten Sie den logischen Replikationsprozess zwischen zwei DB-Clustern von Aurora PostgreSQL

Bei diesen Schritten wird davon ausgegangen, dass Ihre DB-Cluster von Aurora PostgreSQL über eine Writer-Instance mit einer Datenbank verfügen, in der die Beispieltabellen erstellt werden können.

1. Auf dem Herausgeber-DB-Cluster von Aurora PostgreSQL

   a. Erstellen Sie mit der folgenden SQL-Anweisung eine Tabelle.

   ```
   CREATE TABLE LogicalReplicationTest (a int PRIMARY KEY);
   ```

   b. Fügen Sie mit der folgenden SQL-Anweisung Daten in die Herausgebertabelle ein.

   ```
   INSERT INTO LogicalReplicationTest VALUES (generate_series(1,10000));
   ```

   c. Stellen Sie sicher, dass Daten in der Tabelle vorhanden sind, indem Sie die folgende SQL-Anweisung verwenden.

   ```
   SELECT count(*) FROM LogicalReplicationTest;
   ```

d. Erstellen Sie eine Veröffentlichung für diese Tabelle, indem Sie die `CREATE PUBLICATION`-Anweisung wie folgt verwenden.

```
CREATE PUBLICATION testpub FOR TABLE LogicalReplicationTest;
```

2. Auf dem Abonnenten-DB-Cluster von Aurora PostgreSQL

a. Erstellen Sie wie folgt dieselbe `LogicalReplicationTest`-Tabelle auf dem Abonnenten, die Sie auf dem Herausgeber erstellt haben.

```
CREATE TABLE LogicalReplicationTest (a int PRIMARY KEY);
```

b. Stellen Sie sicher, dass diese Tabelle leer ist.

```
SELECT count(*) FROM LogicalReplicationTest;
```

c. Erstellen Sie ein Abonnement, um die Änderungen vom Herausgeber zu erhalten. Sie müssen die folgenden Details über den Herausgeber-DB-Cluster von Aurora PostgreSQL verwenden.

- host – Die Writer-DB-Instance des Herausgeber-DB-Clusters von Aurora PostgreSQL.
- port – Der Port, den die Writer-DB-Instance überwacht. Der Standardwert für PostgreSQL lautet 5432.
- dbname – Der Name der Datenbank.

```
CREATE SUBSCRIPTION testsub CONNECTION
   'host=publisher-cluster-writer-endpoint port=5432 dbname=db-name user=user
 password=password'
   PUBLICATION testpub;
```

> **Note**
>
> Geben Sie aus Sicherheitsgründen ein anderes Passwort als hier angegeben an.

Nachdem das Abonnement erstellt wurde, wird für den Herausgeber ein Slot für die logische Replikation erstellt.

d. Um für dieses Beispiel zu überprüfen, dass das Anfangsdatum für den Abonnenten repliziert wird, verwenden Sie die folgende SQL-Anweisung für die Abonnenten-Datenbank.

```
SELECT count(*) FROM LogicalReplicationTest;
```

Alle weiteren Änderungen am Herausgeber werden beim Abonnenten repliziert.

Durch die logische Replikation wird die Leistung beeinträchtigt. Es wird empfohlen, die logische Replikation zu deaktivieren, nachdem Ihre Replikationsaufgaben abgeschlossen sind.

Beispiel: Die logische Replikation unter Verwendung von Aurora PostgreSQL und AWS Database Migration Service

Sie können den AWS Database Migration Service (AWS DMS) verwenden, um eine Datenbank oder einen Teil einer Datenbank zu replizieren. Mit AWS DMS können Sie Ihre Daten aus einer Aurora-PostgreSQL-Datenbank zu einer anderen Open-Source- oder kommerzielle Datenbank migrieren. Weitere Informationen zu AWS DMS finden Sie im AWS Database Migration Service Benutzerhandbuch.

Das folgende Beispiel zeigt, wie die logische Replikation aus einer Aurora-PostgreSQL-Datenbank als Herausgeber eingerichtet und für die Migration dann AWS DMS verwendet wird. In diesem Beispiel werden der gleiche Herausgeber und Abonnent verwendet, die unter erstellt wurde Beispiel: Verwenden der logischen Replikation mit DB-Clustern von Aurora PostgreSQL.

Um die logische Replikation mit AWS DMS einzurichten, benötigen Sie Details zu Ihrem Herausgeber und Abonnenten von Amazon RDS. Insbesondere benötigen Sie Details zur Writer-DB-Instance des Herausgebers und zur DB-Instance des Abonnenten.

Fordern Sie die folgenden Informationen für die Writer-DB-Instance des Herausgebers an:

- Die ID der Virtual Private Cloud (VPC)
- Die Subnetzgruppe
- Die Availability Zone (AZ)
- Die VPC-Sicherheitsgruppe
- Die ID der DB-Instance

Fordern Sie die folgenden Informationen für die DB-Instance des Herausgebers an:

- Die ID der DB-Instance
- Die Quell-Engine

So verwenden Sie AWS DMS für die logische Replikation mit Aurora PostgreSQL

1. Bereiten Sie die Datenbank des Herausgebers auf die Verwendung mit vo AWS DMS.

   Hierzu müssen Sie bei PostgreSQL-Datenbanken der Version 10.x und höher AWS DMS-Wrapper-Funktionen auf die Datenbank des Herausgebers anwenden. Einzelheiten hierzu und weitere Schritte finden Sie in den Anweisungen unter Verwenden von PostgreSQL-Version 10.x und höher als Quelle für AWS DMS im AWS Database Migration Service-Benuterhandbuch.
2. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS DMS-Konsole unter https://console.aws.amazon.com/dms/v2. Wählen Sie rechts oben dieselbe AWS-Region aus, in der sich der Herausgeber und der Abonnent befinden.
3. Erstellen Sie eine AWS DMS-Replikations-Instance.

   Wählen Sie Werte, die mit denen für die Writer-DB-Instance des Herausgebers identisch sind. Dazu gehören die folgenden Einstellungen:

   - Wählen Sie unter VPC dasselbe VPC wie für die Writer-DB-Instance aus.
   - Wählen Sie für Replikations-Subnetzgruppe eine Subnetzgruppe mit denselben Werten wie die Writer-DB-Instance aus. Erstellen Sie bei Bedarf eine Neue.
   - Wählen Sie unter Availability zone (Availability Zone) dieselbe Zone wie für die Writer-DB-Instance aus.
   - Wählen Sie unter VPC Security Group (VPC-Sicherheitsgruppe) dieselbe Gruppe wie für die Writer-DB-Instance aus.
4. Erstellen Sie einen AWS DMS-Endpunkt für die Quelle.

   Geben Sie unter Verwendung der folgenden Einstellungen den Herausgeber als Quellendpunkt an:

   - Wählen Sie unter Endpoint type (Endpunkttyp) die Option Source endpoint (Quellendpunkt) aus.
   - Wählen Sie Select RDS DB Instance (RDS-DB-Instance auswählen).
   - Wählen Sie unter RDS Instance (RDS-Instance) die DB-Kennung der Writer-DB-Instance des Herausgebers aus.

- Wählen Sie unter Source engine (Quellen-Engine) die Option postgres aus.

5. Erstellen Sie einen AWS DMS-Endpunkt für das Ziel.

   Geben Sie den Abonnenten unter Verwendung der folgenden Einstellungen als Zielendpunkt an:

   - Wählen Sie unter Endpoint type (Endpunkttyp) die Option Target endpoint (Zielendpunkt) aus.
   - Wählen Sie Select RDS DB Instance (RDS-DB-Instance auswählen).
   - Wählen Sie unter RDS Instance (RDS-Instance) die DB-Kennung der Abonnenten-DB-Instance aus.
   - Wählen Sie einen Wert für Source engine (Quell-Engine) aus. Beispiel: Wenn der Abonnent eine RDS-PostgreSQL-Datenbank ist, wählen Sie postgres. Wenn der Subscriber eine Aurora PostgreSQL-Datenbank ist, wählen Sie aurora-postgresql aus.

6. Erstellen Sie eine AWS DMS-Datenbankmigrationsaufgabe.

   Sie geben mit der Datenbankmigrationsaufgabe an, welche Datenbanktabelle migriert werden sollen, um Daten mithilfe des Zielschemas zuzuordnen und um neue Tabellen für die Zieldatenbank zu erstellen. Verwenden Sie zumindest die folgenden Einstellungen für Task configuration (Aufgabenkonfiguration):

   - Wählen Sie unter Replication instance (Replikations-Instance) die Replikations-Instance aus, die Sie in einem früheren Schritt erstellt haben.
   - Wählen Sie unter Source database endpoint (Quelldatenbank-Endpunkt) die Herausgeberquelle aus, die Sie in einem früheren Schritt erstellt haben.
   - Wählen Sie unter Target database endpoint (Zieldatenbank-Endpunkt) das Abonnentenziel aus, das Sie in einem früheren Schritt erstellt haben.

   Die übrigen Aufgabendetails sind von Ihrem Migrationsprojekt abhängig. Weitere Informationen zur Angabe aller Details für DMS-Aufgaben finden Sie unter Arbeiten mit AWS DMS-Aufgaben im AWS Database Migration Service-Benutzerhandbuch.

Nachdem AWS DMS die Aufgabe erstellt hat, beginnt sie mit der Migration der Daten vom Publisher zum Subscriber.

Verwendung von Aurora PostgreSQL als Wissensdatenbank für Amazon Bedrock

Ab den Versionen Aurora PostgreSQL 15.4, 14.9, 13.12, 12.16 können Sie den Aurora PostgreSQL-DB-Cluster als Wissensdatenbank für Amazon Bedrock verwenden. Weitere Informationen finden Sie unter Erstellen eines Vektorspeichers in Amazon Aurora. Eine Knowledge Base nimmt automatisch unstrukturierte Textdaten, die in einem Amazon S3 S3-Bucket gespeichert sind, konvertiert sie in Textblöcke und Vektoren und speichert sie in einer PostgreSQL-Datenbank. Mit den generativen KI-Anwendungen können Sie Agents for Amazon Bedrock verwenden, um die in der Knowledge Base gespeicherten Daten abzufragen und die Ergebnisse dieser Abfragen zu verwenden, um die Antworten zu erweitern, die von grundlegenden Modellen bereitgestellt werden. Dieser Workflow wird Retrieval Augmented Generation (RAG) genannt. Weitere Informationen zu RAG finden Sie unter Retrieval Augmented Generation (RAG).

Themen

Voraussetzungen

Machen Sie sich mit den folgenden Voraussetzungen vertraut, um den Aurora PostgreSQL-Cluster als Wissensdatenbank für Amazon Bedrock zu verwenden. Auf hoher Ebene müssen Sie die folgenden Dienste für die Verwendung mit Bedrock konfigurieren:

- Der Amazon Aurora PostgreSQL-DB-Cluster wurde in den folgenden Versionen erstellt:
  - 15.4 und höhere Versionen
  - 14.9 und höhere Versionen
  - 13.12 und höhere Versionen
  - 12.16 und höhere Versionen

> **Note**
>
> Sie müssen die `pgvector` Erweiterung in Ihrer Zieldatenbank aktivieren und Version 0.5.0 oder höher verwenden. Weitere Informationen finden Sie unter pgvector v0.5.0 mit HNSW-Indizierung.

- Daten-API
- Ein Benutzer, der in Secrets Manager verwaltet wird. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager.

Vorbereitung von Aurora PostgreSQL für die Verwendung als Wissensdatenbank für Amazon Bedrock

Sie müssen die folgenden Schritte ausführen, um einen Aurora PostgreSQL-DB-Cluster zu erstellen und zu konfigurieren, um ihn als Wissensdatenbank für Amazon Bedrock zu verwenden.

1. Erstellen Sie einen Aurora PostgreSQL-DB-Cluster. Weitere Informationen finden Sie unter Erstellen eines DB-Clusters von Aurora PostgreSQL und Herstellen einer Verbindung.
2. Aktivieren Sie die Daten-API bei der Erstellung des Aurora PostgreSQL-DB-Clusters. Weitere Informationen zu den unterstützten Versionen finden Sie unter. Verwenden der RDS-Daten-API
3. Notieren Sie sich den Aurora PostgreSQL-DB-Cluster Amazon Resource Names (ARN), um ihn im Amazon Bedrock zu verwenden. Weitere Informationen finden Sie unter Amazon Resource Names (ARNs)
4. Melden Sie sich mit Ihrem Master-Benutzer bei der Datenbank an und richten Sie pgvector ein. Verwenden Sie den folgenden Befehl, wenn die Erweiterung nicht installiert ist:

   ```
   CREATE EXTENSION IF NOT EXISTS vector;
   ```

   Verwenden Sie `pgvector` 0.5.0 und eine höhere Version, die die HNSW-Indizierung unterstützt. Weitere Informationen finden Sie unter pgvector v0.5.0 mit HNSW-Indizierung.

   Verwenden Sie den folgenden Befehl, um die Version der installierten Version zu überprüfen: `pg_vector`

   ```
   postgres=>SELECT extversion FROM pg_extension WHERE extname='vector';
   ```

5. Erstellen Sie ein bestimmtes Schema, mit dem Bedrock die Daten abfragen kann. Verwenden Sie den folgenden Befehl, um ein Schema zu erstellen:

```
CREATE SCHEMA bedrock_integration;
```

6. Erstellen Sie eine neue Rolle, mit der Bedrock die Datenbank abfragen kann. Verwenden Sie den folgenden Befehl, um eine neue Rolle zu erstellen:

```
CREATE ROLE bedrock_user WITH PASSWORD password LOGIN;
```

> **Note**
>
> Notieren Sie sich dieses Passwort so, als würden Sie dasselbe verwenden, um ein Secrets Manager Manager-Passwort zu erstellen.

7. Um ihnen die `bedrock_user` Berechtigung zur Verwaltung des `bedrock_integration` Schemas zu erteilen, damit sie darin Tabellen oder Indizes erstellen können.

```
GRANT ALL ON SCHEMA bedrock_integration to bedrock_user;
```

8. Melden Sie sich als an `bedrock_user` und erstellen Sie eine Tabelle in der`bedrock_integration schema`.

```
CREATE TABLE bedrock_integration.bedrock_kb (id uuid PRIMARY KEY, embedding
 vector(1536), chunks text, metadata json);
```

9. Wir empfehlen Ihnen, einen Index mit dem Kosinusoperator zu erstellen, mit dem das Grundgestein die Daten abfragen kann.

```
CREATE INDEX on bedrock_integration.bedrock_kb USING hnsw (embedding
 vector_cosine_ops);
```

10. Erstellen Sie ein AWS Secrets Manager Datenbankgeheimnis. Weitere Informationen finden Sie unter AWS Secrets Manager Manager-Datenbankgeheimnis.

Eine Wissensdatenbank in der Bedrock-Konsole erstellen

Sammeln Sie bei der Vorbereitung von Aurora PostgreSQL für die Verwendung als Vektorspeicher für eine Knowledge Base die folgenden Informationen, die Sie an die Amazon Bedrock-Konsole übermitteln müssen.

- Amazon Aurora Aurora-DB-Cluster-ARN
- ARN des Secrets
- Datenbankname (z. B. Postgres)
- Tabellenname — Es wird empfohlen, einen schemaqualifizierten Namen anzugeben, d. h. TABELLE ERSTELLEN bedrock_integration.bedrock_kb; wodurch die Tabelle bedrock_kb im Schema bedrock_integration erstellt wird
- Tabellenfelder:

  ID: (ID)

  Textblöcke (Blöcke)

  Vektor-Einbettung (Einbettung)

  Metadaten (Metadaten)

Mit diesen Details können Sie eine Wissensdatenbank in der Bedrock-Konsole erstellen. Weitere Informationen finden Sie unter Erstellen eines Vektorspeichers in Amazon Aurora.

Sobald Aurora als Wissensdatenbank hinzugefügt wurde, nehmen Sie die Datenquellen in die Datenbank auf. Weitere Informationen finden Sie unter Importieren Sie Ihre Datenquellen in die Wissensdatenbank.

Integrieren von Amazon Aurora PostgreSQL in anderen AWS-Services

Amazon Aurora ist auch in anderen AWS-Services integriert, damit Sie Ihren Aurora PostgreSQL-DB-Cluster erweitern können, um zusätzliche Funktionen in der AWS Cloud zu verwenden. Ihr Aurora-PostgreSQL-DB-Cluster kann AWS-Services verwenden, um Folgendes durchzuführen:

- Performance Ihrer Aurora PostgreSQL-DB-Instances mit Amazon RDS-Performance-Insights schnell ermitteln, anzeigen und beurteilen. Performance Insights lässt sich auf vorhandene Amazon

RDS-Überwachungsfunktionen erweitern, damit Sie die Performance Ihrer Datenbank darstellen und mögliche Probleme analysieren können. Mit dem Performance Insights-Dashboard können Sie die Datenbankauslastung visualisieren und die Auslastung nach Wartezeiten, SQL-Anweisungen, Hosts oder Benutzern filtern. Weitere Informationen zu Performance Insights finden Sie unter Überwachung mit Performance Insights auf .

- Konfigurieren Sie Ihren Aurora-PostgreSQL-DB-Cluster so, dass Protokolldaten in Amazon CloudWatch Logs veröffentlicht werden. - CloudWatch Protokolle bieten einen äußerst dauerhaften Speicher für Ihre Protokolldatensätze. Mit - CloudWatch Protokollen können Sie Echtzeitanalysen der Protokolldaten durchführen und verwenden, CloudWatch um Alarme zu erstellen und Metriken anzuzeigen. Weitere Informationen finden Sie unter Veröffentlichen von Aurora-PostgreSQL-Protokollen in Amazon CloudWatch Logs.
- Importieren Sie Daten von einem Amazon S3-Bucket zu einem Aurora PostgreSQL DB-Cluster oder exportieren Sie Daten von einem Aurora PostgreSQL DB-Cluster zu einem Amazon S3-Bucket. Weitere Informationen finden Sie unter Importieren von Amazon S3 in einen Aurora-PostgreSQL-DB-Cluster und Exportieren von Daten aus einem/einer Aurora PostgreSQL-DB-Cluster zu Amazon S3.
- Hinzufügen von auf Machine Learning basierenden Vorhersagen zu Datenbankanwendungen unter Verwendung der SQL-Sprache. Aurora Machine Learning nutzt eine hoch optimierte Integration zwischen der Aurora-Datenbank und den AWS Machine Learning (ML)-Services SageMaker und Amazon Comprehend . Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Machine Learning mit Aurora PostgreSQL.
- Rufen Sie AWS Lambda Funktionen von einem Aurora PostgreSQL DB-Cluster auf. Verwenden Sie dazu die `aws_lambda` PostgreSQL-Erweiterung, die mit Aurora PostgreSQL bereitgestellt wird. Weitere Informationen finden Sie unter Aufrufen einer AWS Lambda Funktion aus einem Aurora PostgreSQL-DB-Cluster (PostgreSQL-DB-Instance).
- Integrieren Sie Abfragen von Amazon Redshift und Aurora PostgreSQL. Weitere Informationen finden Sie im Amazon Redshift Database Developer Guide unter Getting started with using federated queries to PostgreSQL.

Importieren von Amazon S3 in einen Aurora-PostgreSQL-DB-Cluster

Sie können Daten, die mit Amazon Simple Storage Service gespeichert wurden, in eine Tabelle auf einer Aurora PostgreSQL DB-Cluster-Instance importieren. Um dies zu tun, installieren Sie zuerst die `aws_s3`-Erweiterung von Aurora PostgreSQL . Diese Erweiterung stellt die Funktionen bereit, die Sie zum Importieren von einem Amazon S3 Bucket verwenden. Ein Bucket ist ein Amazon S3 Container

für Objekte und Dateien. Die Daten können sich in einer Datei mit kommagetrennten Werten (CSV), einer Textdatei oder einer komprimierten Datei (GZIP) befinden. Im Folgenden erfahren Sie, wie Sie die Erweiterung installieren und Daten aus Amazon S3 in eine Tabelle importieren.

Um von Simple Storage Service (Amazon S3) in zu importieren, muss Ihre Datenbank PostgreSQL Version 10.7 oder höher verwenden. Aurora PostgreSQL

Wenn Sie keine Daten in Amazon S3 gespeichert haben, müssen Sie zunächst einen Bucket erstellen und die Daten speichern. Weitere Informationen finden Sie in den folgenden Themen im Benutzerhandbuch zum Amazon Simple Storage Service.

- Erstellen Sie einen Bucket
- Hinzufügen eines Objekts zu einem Bucket

Das kontoübergreifende Importieren aus Amazon S3 wird unterstützt. Weitere Informationen finden Sie unter Gewähren kontoübergreifender Berechtigungen im Benutzerhandbuch zu Amazon Simple Storage Service.

Sie können den vom Kunden verwalteten Schlüssel für die Verschlüsselung verwenden, wenn Sie Daten aus S3 importieren. Weitere Informationen finden Sie unter In AWS KMS gespeicherte KMS-Schlüssel im Benutzerhandbuch zu Amazon Simple Storage Service.

> **Note**
>
> Das Importieren von Daten aus Amazon S3 wird für Aurora Serverless v1 nicht unterstützt. Es wird für Aurora Serverless v2 unterstützt.

Themen

- Installieren der aws_s3-Erweiterung
- Übersicht über den Import von Daten aus Amazon S3-Daten
- Einrichten des Zugriffs auf einen Amazon S3-Bucket
- Importieren von Daten aus Amazon S3 in Ihren Aurora PostgreSQL DB-Cluster
- Funktionsreferenz

Installieren der aws_s3-Erweiterung

Bevor Sie Amazon S3 mit Ihrem Aurora-PostgreSQL-DB-Cluster verwenden können müssen Sie die `aws_s3`-Erweiterung installieren. Diese Erweiterung bietet Funktionen zum Importieren von Daten aus einem Amazon S3. Sie bietet auch Funktionen zum Exportieren von Daten aus einer Instance eines Aurora-PostgreSQL-DB-Clusters zu einem Amazon-S3-Bucket. Weitere Informationen finden Sie unter Exportieren von Daten aus einem/einer Aurora PostgreSQL-DB-Cluster zu Amazon S3. Die Erweiterung `aws_s3` hängt von einigen Hilfsfunktionen in der Erweiterung `aws_commons` ab, die bei Bedarf automatisch installiert wird.

So installieren Sie die Erweiterung **`aws_s3`**

1. Verwenden Sie psql (oder pgAdmin), um eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL als Benutzer mit `rds_superuser`-Berechtigungen herzustellen. Wenn Sie beim Einrichten den Standardnamen beibehalten haben, stellen Sie eine Verbindung als `postgres` her.

   ```
   psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password
   ```

2. Führen Sie den folgenden Befehl aus, um die Erweiterung zu installieren.

   ```
   postgres=> CREATE EXTENSION aws_s3 CASCADE;
   NOTICE: installing required extension "aws_commons"
   CREATE EXTENSION
   ```

3. Wenn Sie überprüfen möchten, ob die Erweiterung installiert wurde, können Sie psql-Metabefehl `\dx` verwenden.

   ```
   postgres=> \dx
          List of installed extensions
       Name     | Version |   Schema   |                Description
   -------------+---------+------------+-------------------------------------------
    aws_commons | 1.2     | public     | Common data types across AWS services
    aws_s3      | 1.1     | public     | AWS S3 extension for importing data from S3
    plpgsql     | 1.0     | pg_catalog | PL/pgSQL procedural language
   (3 rows)
   ```

Die Funktionen zum Importieren von Daten aus Amazon S3 und exportieren von Daten nach Amazon S3 stehen jetzt zur Verfügung.

Übersicht über den Import von Daten aus Amazon S3-Daten

S3-Daten in Aurora PostgreSQL importieren

Sammeln Sie zunächst die Details, die Sie der Funktion zur Verfügung stellen müssen. Dazu gehören der Name der Tabelle auf der Instance Ihres Aurora PostgreSQL-DB-Clusters, sowie der Bucket-Name, der Dateipfad, der Dateityp und der AWS-Region Speicherort der Amazon S3 S3-Daten. Weitere Informationen finden Sie unter Kopieren von Objekten im Benutzerhandbuch zu Amazon Simple Storage Service.

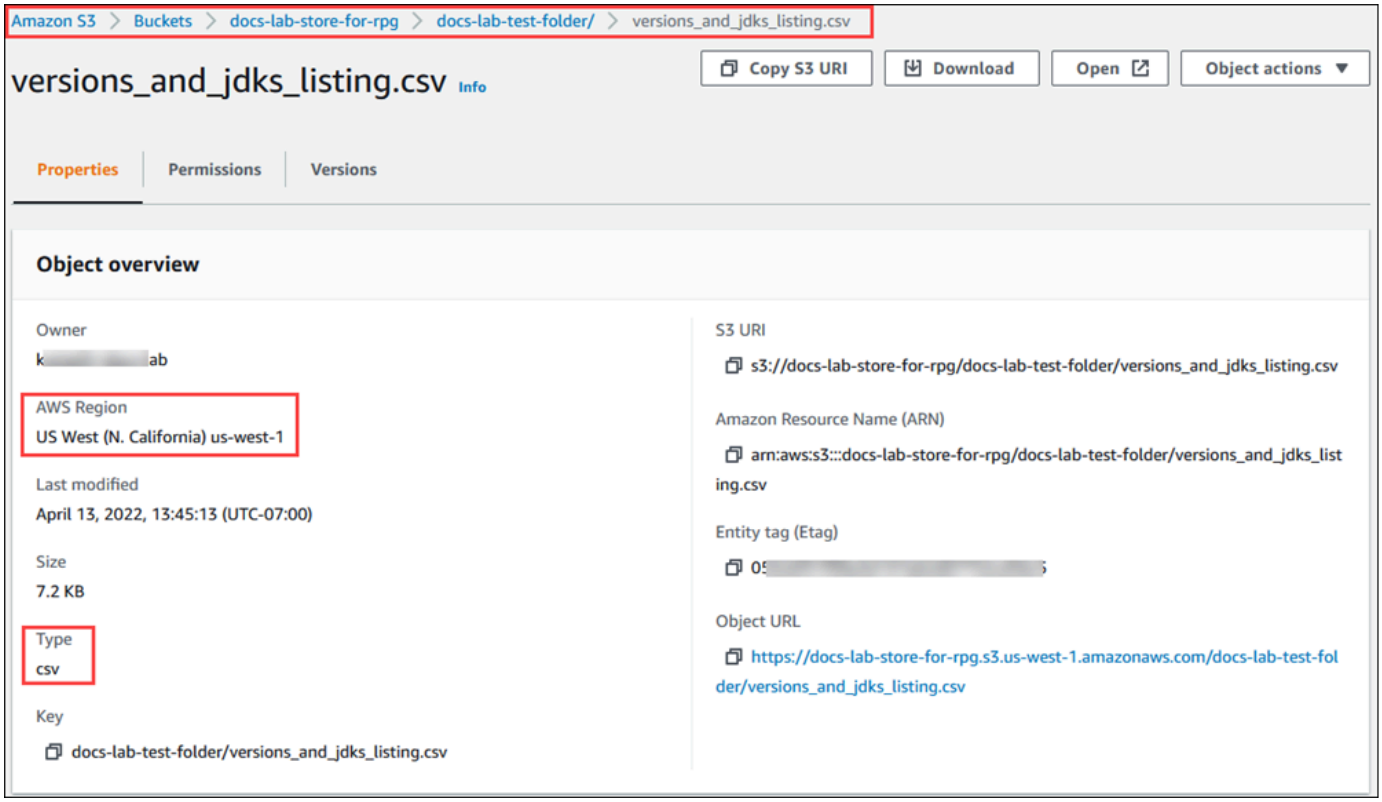
> **Note**
>
> Der mehrteilige Datenimport aus Amazon S3 wird derzeit nicht unterstützt.

1. Ermittelt den Namen der Tabelle, in die die `aws_s3.table_import_from_s3`-Funktion die Daten importieren soll. Mit dem folgenden Befehl wird beispielsweise eine Tabelle `t1` erstellt, die in späteren Schritten verwendet werden kann.

   ```
   postgres=> CREATE TABLE t1
       (col1 varchar(80),
       col2 varchar(80),
       col3 varchar(80));
   ```

2. Rufen Sie die Details zum Amazon-S3-Bucket und die zu importierenden Daten ab. Öffnen Sie dazu die Amazon S3-Konsole unter https://console.aws.amazon.com/s3/ und wählen Sie Buckets. Suchen Sie den Bucket, der Ihre Daten enthält, in der Liste. Wählen Sie den Bucket aus, öffnen Sie die Seite Objektübersicht und wählen Sie dann Properties (Eigenschaften).

   Notieren Sie sich den Namen, den Pfad, den und den Dateityp des AWS-Region Buckets. Sie benötigen den Amazon-Ressourcenname (ARN) später, um den Zugriff auf Amazon S3 über eine IAM-Rolle einzurichten. Weitere Informationen finden Sie unter Einrichten des Zugriffs auf einen Amazon S3-Bucket. In der folgenden Abbildung sehen Sie ein Beispiel.



3. Sie können den Pfad zu den Daten im Amazon S3 S3-Bucket mit dem AWS CLI Befehl überprüfen`aws s3 cp`. Wenn die Informationen korrekt sind, lädt dieser Befehl eine Kopie der Amazon S3-Datei herunter.

```
aws s3 cp s3://DOC-EXAMPLE-BUCKET/sample_file_path ./
```

4. Richten Sie Berechtigungen auf Ihrem Aurora-PostgreSQL-DB-Cluster ein, um den Zugriff auf die Datei im Amazon-S3-Bucket zu gestatten. Dazu verwenden Sie entweder eine AWS Identity and Access Management (IAM-) Rolle oder Sicherheitsanmeldedaten. Weitere Informationen finden Sie unter Einrichten des Zugriffs auf einen Amazon S3-Bucket.

5. Geben Sie den Pfad und andere gesammelte Amazon S3-Objektdetails (siehe Schritt 2) an die `create_s3_uri`-Funktion zum Erstellen eines Amazon S3-URI-Objekts. Weitere Informationen zu dieser Funktion finden Sie unter aws_commons.create_s3_uri. Es folgt ein Beispiel für die Erstellung dieses Objekts während einer psql-Sitzung.

```
postgres=> SELECT aws_commons.create_s3_uri(
   'docs-lab-store-for-rpg',
   'versions_and_jdks_listing.csv',
   'us-west-1'
) AS s3_uri \gset
```

Im nächsten Schritt übergeben Sie dieses Objekt (`aws_commons._s3_uri_1`) an die `aws_s3.table_import_from_s3`-Funktion, um die Daten in die Tabelle zu importieren.

6. Rufen Sie die `aws_s3.table_import_from_s3`-Funktion zum Importieren der Daten aus Amazon S3 in Ihre Tabelle auf. Referenz-Informationen finden Sie unter aws_s3.table_import_from_s3. Beispiele finden Sie unter Importieren von Daten aus Amazon S3 in Ihren Aurora PostgreSQL DB-Cluster.

Einrichten des Zugriffs auf einen Amazon S3-Bucket

Um Daten aus einer Amazon S3-Datei zu importieren, erteilen Sie dem/der Aurora PostgreSQL-DB-Cluster die Berechtigung, auf den Amazon S3-Bucket zuzugreifen, in dem sich die Datei befindet. Sie können den Zugriff auf einen Amazon S3-Bucket auf zwei Arten erlaubt, wie in den folgenden Themen beschrieben.

Themen

- Verwenden einer IAM-Rolle für den Zugriff auf einen Amazon S3-Bucket
- Verwenden von Sicherheitsanmeldeinformationen für den Zugriff auf einen Amazon S3-Bucket
- Fehlerbehebung beim Zugriff auf Amazon S3

Verwenden einer IAM-Rolle für den Zugriff auf einen Amazon S3-Bucket

Bevor Sie Daten aus einer Amazon S3-Datei laden, geben Sie Ihrer Aurora PostgreSQL DB-Cluster die Berechtigung, auf den Amazon S3-Bucket der Datei zuzugreifen. Auf diese Weise müssen Sie keine zusätzlichen Anmeldeinformationen verwalten oder im aws_s3.table_import_from_s3-Funktionsaufruf angeben.

Erstellen Sie dazu eine IAM-Richtlinie, die den Zugriff auf den Amazon S3-Bucket ermöglicht. Erstellen Sie eine IAM-Rolle und hängen Sie die Richtlinie an die Rolle an. Weisen Sie dann die IAM-Rolle Ihrer DB Cluster zu.

> **Note**
>
> Sie können einem Aurora Serverless v1-DB-Cluster keine IAM-Rolle zuordnen, daher gelten die folgenden Schritte nicht.

Einem Aurora-PostgreSQL-DB-Cluster über eine IAM-Rolle Zugriff auf Amazon S3 gewähren

1. Erstellen Sie eine IAM-Richtlinie.

   Diese Richtlinie enthält die Bucket- und Objektberechtigungen, die Ihrer Aurora PostgreSQL DB-Cluster den Zugriff auf Amazon S3 ermöglichen.

   Nehmen Sie die folgenden erforderlichen Aktionen in die Richtlinie auf, um die Übertragung von Dateien von einem Amazon S3-Bucket nach Aurora PostgreSQL zu ermöglichen:

   - `s3:GetObject`
   - `s3:ListBucket`

   Nehmen Sie die folgenden Ressourcen in die Richtlinie auf, um den Amazon S3-Bucket und Objekte im Bucket zu identifizieren. Dies zeigt das Amazon Resource Name (ARN) Format für den Zugriff auf Amazon S3 an.

   - *`arn:aws:s3::: DOC-EXAMPLE-BUCKET`*
   - arn:aws:s3::: *`DOC-EXAMPLE-BUCKET`* /*

   Weitere Informationen zum Erstellen einer IAM-Richtlinie für Aurora PostgreSQL finden Sie unter Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff. Siehe auch Tutorial: Erstellen und Anfügen Ihrer ersten vom Kunden verwalteten Richtlinie im IAM-Benutzerhandbuch.

   Der folgende Befehl erstellt eine IAM-Richtlinie, die mit diesen Optionen benannt AWS CLI ist. `rds-s3-import-policy` Er gewährt Zugriff auf einen Bucket mit dem Namen *`DOC-EXAMPLE-BUCKET`*.

   > **Note**
   >
   > Notieren Sie sich den Amazon-Ressourcennamen (ARN) der Richtlinie, der vom Befehl zurückgegeben wurde. Sie benötigen den ARN in einem nachfolgenden Schritt, in dem Sie die Richtlinie an eine IAM-Rolle anhängen.

Example

Für, oder: Linux macOS Unix

```
aws iam create-policy \
   --policy-name rds-s3-import-policy \
   --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3import",
         "Action": [
           "s3:GetObject",
           "s3:ListBucket"
         ],
         "Effect": "Allow",
         "Resource": [
           "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
           "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ]
       }
     ]
   }'
```

Windows:

```
aws iam create-policy ^
   --policy-name rds-s3-import-policy ^
   --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3import",
         "Action": [
           "s3:GetObject",
           "s3:ListBucket"
         ],
         "Effect": "Allow",
         "Resource": [
           "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
           "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
```

```
        ]
      }
    ]
}'
```

2. Erstellen Sie eine IAM-Rolle.

   Sie tun dies, damit Aurora PostgreSQL in Ihrem Namen diese IAM-Rolle übernehmen kann, um auf Ihre Amazon S3-Buckets zuzugreifen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer im IAM-Benutzerhandbuch.

   Wir empfehlen die Verwendung von `aws:SourceArn` und `aws:SourceAccount` globaler Bedingungskontext-Schlüssel in ressourcenbasierten Richtlinien, um die Berechtigungen des Dienstes auf eine bestimmte Ressource zu beschränken. Dies ist der effektivste Weg, um sich vor dem verwirrtes Stellvertreterproblem zu schützen.

   Wenn Sie sowohl globale Kontextschlüssel nutzen und der `aws:SourceArn`-Wert enthält die Konto-ID, muss der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert die gleiche Konto-ID verwenden, wenn er in der gleichen Richtlinienanweisung verwendet wird.

   - Verwenden von `aws:SourceArn` wenn Sie einen serviceübergreifenden Zugriff für eine einzelne Ressource wünschen.
   - Verwenden von `aws:SourceAccount` wenn Sie zulassen möchten, dass eine Ressource in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft wird.

   Verwenden Sie in der Richtlinie den `aws:SourceArn` globalen Kontextschlüssel mit dem vollständigen ARN der Ressource. Das folgende Beispiel zeigt, wie Sie dazu den AWS CLI Befehl verwenden, um eine Rolle mit dem Namen zu erstellen`rds-s3-import-role`.

   Example

   Für LinuxmacOS, oderUnix:

```
aws iam create-role \
   --role-name rds-s3-import-role \
   --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
```

```
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-
east-1:111122223333:cluster:clustername"
                }
             }
       }
     ]
   }'
```

Windows:

```
aws iam create-role ^
   --role-name rds-s3-import-role ^
   --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-
east-1:111122223333:cluster:clustername"
                }
             }
       }
     ]
   }'
```

3. Fügen Sie die erstellte IAM-Richtlinie der IAM-Rolle an, die Sie erstellt haben.

Mit dem folgenden AWS CLI Befehl wird die im vorherigen Schritt erstellte Richtlinie der Rolle `rds-s3-import-role` Replace *`your-policy-arn`* mit dem Richtlinien-ARN zugeordnet, den Sie in einem früheren Schritt notiert haben.

Example

Für LinuxmacOS, oderUnix:

```
aws iam attach-role-policy \
   --policy-arn your-policy-arn \
   --role-name rds-s3-import-role
```

Windows:

```
aws iam attach-role-policy ^
   --policy-arn your-policy-arn ^
   --role-name rds-s3-import-role
```

4. Fügen Sie die IAM-Rolle der DB Cluster hinzu.

   Sie tun dies, indem Sie das AWS Management Console oder verwenden AWS CLI, wie im Folgenden beschrieben.

Konsole

So fügen Sie eine IAM-Rolle für eine PostgreSQL DB-Cluster- über die Konsole hinzu:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie den Namen der PostgreSQL DB-Cluster- aus, um ihre Details anzuzeigen.
3. Wählen Sie auf der Registerkarte Connectivity & Security im Bereich Manage IAM roles (IAM-Rollen verwalten) die Rolle aus, die unter Add IAM roles (IAM-Rollen hinzufügen) zu diesen Cluster- hinzugefügt werden soll.
4. Wählen Sie unter Feature (Funktion) die Option s3Import aus.
5. Wählen Sie Rolle hinzufügen.

AWS CLI

So fügen Sie eine IAM-Rolle für einen PostgreSQL-DB-Cluster mithilfe der CLI hinzu:

- Verwenden Sie den folgenden Befehl, um die Rolle mit dem Namen `my-db-cluster` zum PostgreSQL DB-Cluster hinzuzufügen. Ersetzen Sie *`your-role-arn`* durch den Rollen-ARN, den Sie im vorherigen Schritt notiert haben. Verwenden Sie `s3Import` für den Wert der `--feature-name`-Option.

  Example

  Für LinuxmacOS, oderUnix:

  ```
  aws rds add-role-to-db-cluster \
     --db-cluster-identifier my-db-cluster \
     --feature-name s3Import \
     --role-arn your-role-arn   \
     --region your-region
  ```

  Windows:

  ```
  aws rds add-role-to-db-cluster ^
     --db-cluster-identifier my-db-cluster ^
     --feature-name s3Import ^
     --role-arn your-role-arn ^
     --region your-region
  ```

RDS-API

Verwenden von Sicherheitsanmeldeinformationen für den Zugriff auf einen Amazon S3-Bucket

Wenn Sie es vorziehen, können Sie Sicherheitsanmeldeinformationen verwenden, um den Zugriff auf einen Amazon S3-Bucket zu ermöglichen, anstatt den Zugriff mit einer IAM-Rolle zu ermöglichen. Dazu geben Sie die `credentials`-Parameter im aws_s3.table_import_from_s3-Funktionsaufruf an.

Der `credentials` Parameter ist eine Struktur vom Typ, die Anmeldeinformationen enthält. `aws_commons._aws_credentials_1` AWS Verwenden Sie die Funktion aws_commons.create_aws_credentials, um den Zugriffs- und den Geheimschlüssel in einer `aws_commons._aws_credentials_1`-Struktur festzulegen, wie nachfolgend dargestellt.

```
postgres=> SELECT aws_commons.create_aws_credentials(
   'sample_access_key', 'sample_secret_key', '')
AS creds \gset
```

Nachdem Sie die `aws_commons._aws_credentials_1` -Struktur erstellt haben, verwenden Sie die Funktion aws_s3.table_import_from_s3 mit dem Parameter `credentials`, um die Daten zu importieren, wie nachfolgend gezeigt.

```
postgres=> SELECT aws_s3.table_import_from_s3(
   't', '', '(format csv)',
   :'s3_uri',
   :'creds'
);
```

Sie können auch den Funktionsaufruf aws_commons.create_aws_credentials in den Funktionsaufruf `aws_s3.table_import_from_s3` einbinden.

```
postgres=> SELECT aws_s3.table_import_from_s3(
   't', '', '(format csv)',
   :'s3_uri',
   aws_commons.create_aws_credentials('sample_access_key', 'sample_secret_key', '')
);
```

Fehlerbehebung beim Zugriff auf Amazon S3

Wenn Sie beim Versuch, Daten aus Amazon S3 zu importieren, auf Verbindungsprobleme stoßen, finden Sie im Folgenden Empfehlungen:

- Fehlerbehebung für Amazon Aurora-Identität und -Zugriff
- Fehlerbehebung bei Amazon S3 im Entwicklerhandbuch für Amazon Simple Storage Service
- Fehlerbehebung bei Amazon S3 und IAM im IAM-Benutzerhandbuch

Importieren von Daten aus Amazon S3 in Ihren Aurora PostgreSQL DB-Cluster

Sie importieren Daten aus Ihrem Amazon-S3-Bucket mithilfe der `table_import_from_s3`-Funktion der aws_s3-Erweiterung. Referenz-Informationen finden Sie unter aws_s3.table_import_from_s3.

> **Note**
>
> Die folgenden Beispiele verwenden die IAM-Rollen-Methode, um den Zugriff auf den Amazon-S3-Bucket zu ermöglichen. Daher enthalten die `aws_s3.table_import_from_s3`-Funktionsaufrufe keine Berechtigungsnachweisparameter.

Nachfolgend ist ein typisches Beispiel aufgeführt.

```
postgres=> SELECT aws_s3.table_import_from_s3(
   't1',
   '',
   '(format csv)',
   :'s3_uri'
);
```

Es werden folgende Parameter verwendet:

- `t1` – Der Name für die Tabelle in der PostgreSQL DB Cluster, in die die Daten kopiert werden.
- `''` – Eine optionale Liste mit Spalten in der Datenbanktabelle. Mithilfe dieses Parameters können Sie angeben, welche Spalten der S3-Daten in die Tabellenspalten übernommen werden sollen. Wenn keine Spalten angegeben sind, werden alle Spalten in die Tabelle kopiert. Ein Beispiel zum Verwenden einer Spaltenliste finden Sie unter Importieren einer Amazon S3-Datei, die ein benutzerdefiniertes Trennzeichen verwendet.
- `(format csv)` – PostgreSQL COPY-Argumente. Der Kopiervorgang verwendet die Argumente und das Format des PostgreSQL-Befehls COPY, um die Daten zu importieren. Zu den Optionen für das Format gehören kommagetrennte Werte (CSV), Text und Binärwerte. Der Standard ist Text.
- `s3_uri` – Eine Struktur mit den Informationen zum Identifizieren der Amazon S3-Datei. Ein Beispiel für die Verwendung der Funktion aws_commons.create_s3_uri zum Erstellen einer `s3_uri`-Struktur finden Sie unter Übersicht über den Import von Daten aus Amazon S3-Daten.

Weitere Informationen zu dieser Funktion finden Sie unter aws_s3.table_import_from_s3.

Die Funktion gibt `aws_s3.table_import_from_s3` zurück. Weitere Informationen zum Angeben von anderen Dateien für den Import aus einem Amazon S3-Bucket finden Sie in einem der folgenden Beispiele.

> **Note**
>
> Beim Importieren einer Datei mit 0 Byte tritt ein Fehler auf.

Themen

- Importieren einer Amazon S3-Datei, die ein benutzerdefiniertes Trennzeichen verwendet
- Importieren einer Amazon S3-komprimierten Datei (gzip)
- Importieren einer kodierten Amazon S3-Datei

Importieren einer Amazon S3-Datei, die ein benutzerdefiniertes Trennzeichen verwendet

Das folgende Beispiel zeigt, wie man eine Datei importiert, die ein benutzerdefiniertes Trennzeichen verwendet. Außerdem wird veranschaulicht, wie mit dem `column_list`-Parameter der Funktion aws_s3.table_import_from_s3 kontrolliert wird, wo die Daten in der Datenbanktabelle platziert werden.

Für dieses Beispiel wird angenommen, dass die folgenden Informationen in durch Pipe-Zeichen getrennte Spalten in der Amazon S3-Datei angeordnet sind.

```
1|foo1|bar1|elephant1
2|foo2|bar2|elephant2
3|foo3|bar3|elephant3
4|foo4|bar4|elephant4
...
```

So importieren Sie eine Datei, die ein benutzerdefiniertes Trennzeichen verwendet:

1. Erstellen Sie eine Tabelle in der Datenbank für die importierten Daten.

   ```
   postgres=> CREATE TABLE test (a text, b text, c text, d text, e text);
   ```

2. Verwenden Sie die folgende Form der Funktion aws_s3.table_import_from_s3, um Daten aus der Amazon S3-Datei zu importieren.

   Zur Angabe der Datei können Sie auch den Funktionsaufruf aws_commons.create_s3_uri in den Funktionsaufruf `aws_s3.table_import_from_s3` einbinden.

   ```
   postgres=> SELECT aws_s3.table_import_from_s3(
      'test',
   ```

```
   'a,b,d,e',
   'DELIMITER ''|''',
   aws_commons.create_s3_uri('DOC-EXAMPLE-BUCKET', 'pipeDelimitedSampleFile', 'us-
east-2')
);
```

Die Daten befinden sich nun in den folgenden Spalten der Tabelle.

```
postgres=> SELECT * FROM test;
a | b | c | d | e
---+------+---+---+------+-----------
1 | foo1 | | bar1 | elephant1
2 | foo2 | | bar2 | elephant2
3 | foo3 | | bar3 | elephant3
4 | foo4 | | bar4 | elephant4
```

Importieren einer Amazon S3-komprimierten Datei (gzip)

Das folgende Beispiel zeigt, wie eine mit gzip komprimierte Datei aus Amazon S3 importiert wird. Die Datei, die Sie importieren, muss die folgenden Amazon-S3-Metadaten aufweisen:

- Schlüssel: `Content-Encoding`
- Wert: `gzip`

Wenn Sie die Datei mit dem hochladen AWS Management Console, werden die Metadaten in der Regel vom System übernommen. Informationen zum Hochladen von Dateien auf Amazon S3 mithilfe der AWS Management Console AWS CLI, der oder der API finden Sie unter Hochladen von Objekten im Amazon Simple Storage Service-Benutzerhandbuch.

Weitere Informationen zu Amazon-S3-Metadaten und zu vom System bereitgestellten Metadaten finden Sie unter Bearbeiten von Objektmetadaten in der Amazon-S3-Konsole im Benutzerhandbuch für Amazon Simple Storage Service.

Importieren Sie die gzip-Datei folgendermaßen in Ihrer Aurora PostgreSQL DB-Cluster-.

```
postgres=> CREATE TABLE test_gzip(id int, a text, b text, c text, d text);
postgres=> SELECT aws_s3.table_import_from_s3(
 'test_gzip', '', '(format csv)',
 'DOC-EXAMPLE-BUCKET', 'test-data.gz', 'us-east-2'
```

```
);
```

Importieren einer kodierten Amazon S3-Datei

Das folgende Beispiel zeigt, wie eine Datei aus Amazon S3 mit Windows-1252-Kodierung importiert wird.

```
postgres=> SELECT aws_s3.table_import_from_s3(
 'test_table', '', 'encoding ''WIN1252''',
 aws_commons.create_s3_uri('DOC-EXAMPLE-BUCKET', 'SampleFile', 'us-east-2')
);
```

Funktionsreferenz

Funktionen

- aws_s3.table_import_from_s3
- aws_commons.create_s3_uri
- aws_commons.create_aws_credentials

aws_s3.table_import_from_s3

Importiert Amazon S3-Daten in eine Aurora PostgreSQL-Tabelle. Die Erweiterung `aws_s3` stellt die Funktion `aws_s3.table_import_from_s3` bereit. Der Rückgabewert ist Text.

Syntax

Die erforderlichen Parameter sind `table_name`, `column_list` und `options`. Diese Parameter identifizieren die Datenbanktabelle und geben an, wie die Daten in die Tabelle kopiert werden.

Sie können auch die folgenden Parameter verwenden:

- Die zu importierende Amazon S3-Datei wird mit dem Parameter `s3_info` übergeben. Wenn Sie diesen Parameter verwenden, wird der Zugriff auf Amazon S3 von einer IAM-Rolle für die PostgreSQL DB-Cluster- bereitgestellt.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   s3_info aws_commons._s3_uri_1
```

```
)
```

- Die Anmeldeinformationen für den Zugriff auf Amazon S3 werden mit dem Parameter `credentials` übergeben. Mit diesem Parameter verwenden Sie keine IAM-Rolle.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   s3_info aws_commons._s3_uri_1,
   credentials aws_commons._aws_credentials_1
)
```

Parameter

table_name

Eine erforderliche Textzeichenfolge mit dem Namen der PostgreSQL-Datenbanktabelle, in die die Daten importiert werden sollen.

column_list

Eine erforderliche Textzeichenfolge mit einer optionalen Liste der Tabellenspalten der PostgreSQL-Datenbank, in die die Daten kopiert werden sollen. Wenn die Zeichenfolge leer ist, werden alle Spalten der Tabelle verwendet. Ein Beispiel finden Sie unter Importieren einer Amazon S3-Datei, die ein benutzerdefiniertes Trennzeichen verwendet.

options

Eine erforderliche Textzeichenfolge mit Argumenten für den PostgreSQL `COPY`-Befehl. Diese Parameter legen fest, wie die Daten in die PostgreSQL-Tabelle kopiert werden. Weitere Informationen finden Sie in der PostgreSQL COPY-Dokumentation.

s3_info

Ein zusammengesetzter `aws_commons._s3_uri_1`-Typ mit den folgenden Informationen zum S3-Objekt:

- `bucket` – Der Name des Amazon S3-Buckets, der die Datei enthält.
- `file_path` – Der Amazon S3-Dateiname einschließlich des Pfads der Datei.
- `region`— Die AWS Region, in der sich die Datei befindet. Eine Liste der AWS Regionsnamen und der zugehörigen Werte finden Sie unterRegionen und Availability Zones.

Anmeldedaten

Ein zusammengesetzter `aws_commons._aws_credentials_1`-Typ mit den folgenden Anmeldeinformationen, die für den Importvorgang verwendet werden sollen:

- Zugriffsschlüssel
- Geheimschlüssel
- Sitzungs-Token

Hinweise zum Erstellen einer zusammengesetzten `aws_commons._aws_credentials_1`-Struktur finden Sie unter aws_commons.create_aws_credentials.

Alternative Syntax

Zum Testen können Sie statt der Parameter `s3_info` und `credentials` eine erweiterte Gruppe von Parametern verwenden. Nachfolgend sind weitere Syntaxvariationen für die Funktion `aws_s3.table_import_from_s3` aufgeführt:

- Statt den Parameter `s3_info` zum Identifizieren einer Amazon S3-Datei zu verwenden, nutzen Sie die Kombination aus den Parametern `bucket`, `file_path` und `region`. Mit dieser Form der Funktion wird der Zugriff auf Amazon S3 mit einer IAM-Rolle für die PostgreSQL-DB-Instance bereitgestellt.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   bucket text,
   file_path text,
   region text
)
```

- Statt den Parameter `credentials` zum Angeben einer Amazon S3-Datei zu verwenden, nutzen Sie die Kombination aus den Parametern `access_key`, `session_key` und `session_token`.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   bucket text,
   file_path text,
```

```
   region text,
   access_key text,
   secret_key text,
   session_token text
)
```

Alternative Parameter

bucket

Eine Textzeichenfolge mit den Namen des Amazon S3-Buckets, der die Datei enthält.

file_path

Eine Textzeichenfolge, die den Amazon S3-Dateinamen einschließlich des Pfades der Datei enthält.

Region

Eine Textzeichenfolge, die den AWS-Region Speicherort der Datei angibt. Eine Liste der AWS-Region Namen und der zugehörigen Werte finden Sie unterRegionen und Availability Zones.

access_key

Eine Textzeichenfolge mit dem Zugriffsschlüssel, der für den Importvorgang verwendet werden soll. Der Standardwert ist „NULL“.

secret_key

Eine Textzeichenfolge mit dem Geheimschlüssel, der für den Importvorgang verwendet werden soll. Der Standardwert ist „NULL“.

session_token

(Optional) Eine Textzeichenfolge mit dem Sitzungsschlüssel, der für den Importvorgang verwendet werden soll. Der Standardwert ist „NULL“.

aws_commons.create_s3_uri

Erstellt eine `aws_commons._s3_uri_1`-Struktur für die Amazon S3-Dateiinformationen. Die Ergebnisse der Funktion `aws_commons.create_s3_uri` werden im Parameter `s3_info` der Funktion aws_s3.table_import_from_s3 verwendet.

Syntax

```
aws_commons.create_s3_uri(
   bucket text,
   file_path text,
   region text
)
```

Parameter

bucket

Eine erforderliche Textzeichenfolge mit dem Namen des Amazon S3-Buckets für die Datei.

file_path

Eine erforderliche Textzeichenfolge, die den Amazon S3-Dateinamen einschließlich des Pfads der Datei enthält.

Region

Eine erforderliche Textzeichenfolge AWS-Region , die den Inhalt der Datei enthält. Eine Liste der AWS-Region Namen und der zugehörigen Werte finden Sie unterRegionen und Availability Zones.

aws_commons.create_aws_credentials

Legt einen Zugriffs- und einen Geheimschlüssel in einer `aws_commons._aws_credentials_1`-Struktur fest. Die Ergebnisse der Funktion `aws_commons.create_aws_credentials` werden im Parameter `credentials` der Funktion aws_s3.table_import_from_s3 verwendet.

Syntax

```
aws_commons.create_aws_credentials(
   access_key text,
   secret_key text,
   session_token text
)
```

Parameter

access_key

Eine erforderliche Textzeichenfolge mit dem Zugriffsschlüssel, der zum Importieren einer Amazon S3-Datei verwendet werden soll. Der Standardwert ist „NULL“.

secret_key

Eine erforderliche Textzeichenfolge mit dem Geheimschlüssel, der zum Importieren einer Amazon S3-Datei verwendet werden soll. Der Standardwert ist „NULL“.

session_token

Eine erforderliche Textzeichenfolge mit dem Sitzungs-Token, der zum Importieren einer Amazon S3-Datei verwendet werden soll. Der Standardwert ist „NULL“. Wenn Sie ein optionales `session_token` angeben, können Sie temporäre Anmeldeinformationen verwenden.

Exportieren von Daten aus einem/einer Aurora PostgreSQL-DB-Cluster zu Amazon S3

Sie können Daten aus einem Aurora-PostgreSQL-DB-Cluster abfragen und direkt in Dateien exportieren, die in einem Amazon-S3-Bucket gespeichert sind. Dazu installieren Sie zuerst die Erweiterung von Aurora PostgreSQL `aws_s3`. Diese Erweiterung stellt die Funktionen bereit, die Sie zum Exportieren von Abfrageergebnissen nach Amazon S3 verwenden. Im Folgenden erfahren Sie, wie Sie die Erweiterung installieren und Daten nach Amazon S3 exportieren.

Sie können nur von einer bereitgestellten oder einer DB-Instance von Aurora Serverless v2 aus exportieren. Diese Schritte werden für Aurora Serverless v1 nicht unterstützt.

> **Note**
>
> Kontoübergreifender Export nach Amazon S3 wird nicht unterstützt.

Alle derzeit verfügbaren Aurora-PostgreSQL-Versionen unterstützen den Export von Daten nach Amazon Simple Storage Service. Ausführliche Versionsinformationen finden Sie unter Aktualisierungen von Amazon Aurora PostgreSQL im Abschnitt Versionshinweise für Aurora PostgreSQL.

Wenn Sie keinen Bucket für Ihren Export eingerichtet haben, lesen Sie die folgenden Themen im Benutzerhandbuch von Amazon Simple Storage Service.

- Einrichten von Amazon S3
- Erstellen Sie einen Bucket

Standardmäßig verwenden die von Aurora PostgreSQL nach Amazon S3 exportierten Daten serverseitige Verschlüsselung mit. Von AWS verwalteter Schlüssel Sie können alternativ den vom Kunden verwalteten Schlüssel verwenden, den Sie bereits erstellt haben. Wenn Sie die Bucket-Verschlüsselung verwenden, muss der Amazon S3 S3-Bucket mit dem AWS Key Management Service (AWS KMS) -Schlüssel (SSE-KMS) verschlüsselt werden. Derzeit werden Buckets, die mit verwalteten Amazon S3 S3-Schlüsseln (SSE-S3) verschlüsselt sind, nicht unterstützt.

> **Note**
>
> Sie können DB- und DB-Cluster-Snapshot-Daten mit der AWS Management Console AWS CLI, oder Amazon RDS-API in Amazon S3 speichern. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Snapshot-Daten nach Amazon S3.

Themen

- Installieren der Erweiterung aws_s3
- Übersicht über das Exportieren von Daten zu Amazon S3
- Angeben des Amazon S3-Dateipfads für den Export
- Einrichten des Zugriffs auf einen Amazon S3-Bucket
- Exportieren von Abfragedaten mithilfe der Funktion aws_s3.query_export_to_s3
- Fehlerbehebung beim Zugriff auf Amazon S3
- Funktionsreferenz

Installieren der Erweiterung aws_s3

Bevor Sie Amazon Simple Storage Service mit Ihrem DB-Cluster voon Aurora PostgreSQL verwenden können, müssen Sie die Erweiterung `aws_s3` installieren. Diese Erweiterung bietet Funktionen zum Exportieren von Daten aus der Writer-Instance eines DB-Clusters von Aurora PostgreSQL in einen Amazon-S3-Bucket Sie stellt außerdem Funktionen zum Importieren von Daten

aus Amazon S3 bereit. Weitere Informationen finden Sie unter Importieren von Amazon S3 in einen Aurora-PostgreSQL-DB-Cluster. Die Erweiterung `aws_s3` hängt von einigen Hilfsfunktionen in der Erweiterung `aws_commons` ab, die bei Bedarf automatisch installiert wird.

So installieren Sie die Erweiterung **`aws_s3`**

1. Verwenden Sie psql (oder pgAdmin), um eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL als Benutzer mit `rds_superuser`-Berechtigungen herzustellen. Wenn Sie beim Einrichten den Standardnamen beibehalten haben, stellen Sie eine Verbindung als `postgres` her.

   ```
   psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password
   ```

2. Führen Sie den folgenden Befehl aus, um die Erweiterung zu installieren.

   ```
   postgres=> CREATE EXTENSION aws_s3 CASCADE;
   NOTICE: installing required extension "aws_commons"
   CREATE EXTENSION
   ```

3. Wenn Sie überprüfen möchten, ob die Erweiterung installiert wurde, können Sie psql-Metabefehl `\dx` verwenden.

   ```
   postgres=> \dx
          List of installed extensions
       Name     | Version |   Schema   |                 Description
   -------------+---------+------------+---------------------------------------------
    aws_commons | 1.2     | public     | Common data types across AWS services
    aws_s3      | 1.1     | public     | AWS S3 extension for importing data from S3
    plpgsql     | 1.0     | pg_catalog | PL/pgSQL procedural language
   (3 rows)
   ```

Die Funktionen zum Importieren von Daten aus Amazon S3 und Exportieren von Daten nach Amazon S3 sind jetzt verfügbar.

Überprüfen, ob Ihre Version von Aurora PostgreSQL Exporte nach Amazon S3 unterstützt

Sie können überprüfen, ob Ihre Version von Aurora PostgreSQL den Export nach Amazon S3 unterstützt, indem Sie den Befehl `describe-db-engine-versions` verwenden. Im folgenden Beispiel wird überprüft, ob Version 10.14 nach Amazon S3 exportieren kann.

```
aws rds describe-db-engine-versions --region us-east-1 \
--engine aurora-postgresql --engine-version 10.14 | grep s3Export
```

Wenn die Ausgabe die Zeichenfolge `"s3Export"` enthält, unterstützt die Engine Amazon S3-Exporte. Ansonsten unterstützt die Engine sie nicht.

Übersicht über das Exportieren von Daten zu Amazon S3

Verwenden Sie das folgende Verfahren, um in einer Aurora PostgreSQL Datenbank gespeicherte Daten in einen Amazon S3 Bucket zu exportieren.

So exportieren Sie Aurora PostgreSQL Daten nach S3

1. Identifizieren Sie einen Amazon S3-Dateipfad, der zum Exportieren von Daten verwendet werden soll. Weitere Informationen zu diesem Prozess finden Sie unter Angeben des Amazon S3-Dateipfads für den Export.
2. Erteilen Sie die Berechtigung für den Zugriff auf den Amazon S3-Bucket.

   Um Daten in eine Amazon S3-Datei zu exportieren, erteilen Sie dem/der Aurora PostgreSQL-DB-Cluster die Berechtigung, auf den Amazon S3-Bucket zuzugreifen, den der Export für die Speicherung verwendet. Dazu gehören die folgenden Schritte:

   1. Erstellen Sie eine IAM-Richtlinie, die Zugriff auf einen Amazon S3-Bucket bietet, in den Sie exportieren möchten.
   2. Erstellen Sie eine IAM-Rolle.
   3. Fügen Sie die erstellte Richtlinie an die erstellte Rolle an.
   4. Fügen Sie diese IAM-Rolle zu Ihrem DB-Cluster Ihrer hinzu.

   Weitere Informationen zu diesem Prozess finden Sie unter Einrichten des Zugriffs auf einen Amazon S3-Bucket.
3. Identifizieren Sie eine Datenbankabfrage, um die Daten abzurufen. Exportieren Sie die Abfragedaten, indem Sie die Funktion `aws_s3.query_export_to_s3` aufrufen.

   Nachdem Sie die vorangegangenen Vorbereitungsaufgaben abgeschlossen haben, verwenden Sie die aws_s3.query_export_to_s3-Funktion, um Abfrageergebnisse in Amazon S3 zu exportieren. Weitere Informationen zu diesem Prozess finden Sie unter Exportieren von Abfragedaten mithilfe der Funktion aws_s3.query_export_to_s3.

Angeben des Amazon S3-Dateipfads für den Export

Geben Sie die folgenden Informationen an, um den Speicherort in Amazon S3 zu identifizieren, in den Sie Daten exportieren möchten:

- Bucket-Name – Ein Bucket ist ein Container für Amazon S3-Objekte oder -Dateien.

  Weitere Informationen zum Speichern von Daten mit Amazon S3 finden Sie unter Erstellen eines Buckets und Anzeigen eines Objekts im Amazon Simple Storage Service Benutzerhandbuch.
- Dateipfad – Der Dateipfad gibt an, wo der Export im Amazon S3-Bucket gespeichert wird. Der Dateipfad besteht aus Folgendem:
  - Ein optionales Pfadpräfix, das einen Pfad für virtuelle Ordner identifiziert.
  - Ein Dateipräfix, das eine oder mehrere Dateien identifiziert, die gespeichert werden sollen. Größere Exporte werden in mehreren Dateien gespeichert, jeweils mit einer maximalen Größe von ca. 6 GB. Die zusätzlichen Dateinamen haben das gleiche Dateipräfix, aber mit `_part`*XX* angefügt. *XX* stellt 2, dann 3 usw. dar.

  Beispielsweise ist ein Dateipfad mit einem `exports`-Ordner und einem `query-1-export`-Dateipräfix `/exports/query-1-export`.
- AWS Region (optional) — Die AWS Region, in der sich der Amazon S3 S3-Bucket befindet. Wenn Sie keinen AWS Regionswert angeben, speichert Aurora Ihre Dateien in Amazon S3 in derselben AWS Region wie die exportierende .

  > **Note**
  >
  > Derzeit muss die AWS Region mit der Region der exportierenden identisch sein.

  Eine Liste der AWS Regionsnamen und der zugehörigen Werte finden Sie unterRegionen und Availability Zones.

Um die Amazon S3-Dateiinformationen darüber zu speichern, wo der Export gespeichert werden soll, können Sie die aws_commons.create_s3_uri-Funktion verwenden, um eine zusammengesetzte `aws_commons._s3_uri_1`-Struktur wie folgt zu erstellen.

```
psql=> SELECT aws_commons.create_s3_uri(
   'DOC-EXAMPLE-BUCKET',
   'sample-filepath',
```

```
   'us-west-2'
) AS s3_uri_1 \gset
```

Sie geben diesen `s3_uri_1`-Wert später als Parameter im Aufruf der aws_s3.query_export_to_s3-Funktion an. Beispiele finden Sie unter Exportieren von Abfragedaten mithilfe der Funktion aws_s3.query_export_to_s3.

Einrichten des Zugriffs auf einen Amazon S3-Bucket

Um Daten zu Amazon S3 zu exportieren, erteilen Sie Ihrem PostgreSQL-DB-Cluster die Berechtigung, auf den Amazon S3-Bucket zuzugreifen, in den die Dateien aufgenommen werden sollen.

Führen Sie dazu die folgenden Schritte aus.

So erteilen Sie einem PostgreSQL-DB-Cluster Zugriff auf Amazon S3 über eine IAM-Rolle

1. Erstellen Sie eine IAM-Richtlinie.

   Diese Richtlinie enthält die Bucket- und Objektberechtigungen, die IhremPostgreSQL-DB-Cluster den Zugriff auf Amazon S3 ermöglichen.

   Führen Sie beim Erstellen dieser Richtlinie die folgenden Schritte aus:

   a. Nehmen Sie die folgenden erforderlichen Aktionen in die Richtlinie auf, um die Übertragung von Dateien aus Ihrem PostgreSQL-DB-Cluster in einen Amazon S3-Bucket zu gestatten:

      - `s3:PutObject`
      - `s3:AbortMultipartUpload`

   b. Geben Sie den Amazon-Ressourcennamen (ARN) ein, der den Amazon S3-Bucket und die Objekte im Bucket identifiziert. Das ARN-Format für den Zugriff auf Amazon S3 lautet: `arn:aws:s3:::DOC-EXAMPLE-BUCKET/*`

   Weitere Informationen zum Erstellen einer IAM-Richtlinie für Aurora PostgreSQL finden Sie unter Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff. Siehe auch Tutorial: Erstellen und Anfügen Ihrer ersten vom Kunden verwalteten Richtlinie im IAM-Benutzerhandbuch.

Mit dem folgenden AWS CLI Befehl wird eine IAM-Richtlinie `rds-s3-export-policy` mit diesen Optionen erstellt. Er gewährt Zugriff auf einen Bucket mit dem Namen *DOC-EXAMPLE-BUCKET*.

> **Warning**
>
> Es wird empfohlen, die Datenbank innerhalb einer privaten VPC einzurichten, deren Endpunktrichtlinien für den Zugriff auf bestimmte Buckets konfiguriert sind. Weitere Informationen finden Sie unter Verwenden von Endpunktrichtlinien für Amazon S3 im Amazon VPC Benutzerhandbuch.
> Es wird dringend empfohlen, keine Richtlinie mit Zugriff auf alle Ressourcen zu erstellen. Dieser Zugriff kann eine Bedrohung für die Datensicherheit darstellen. Wenn Sie eine Richtlinie erstellen, die `S3:PutObject` Zugriff auf alle Ressourcen mit `"Resource":"*"` gewährt, kann ein Benutzer mit Exportberechtigungen Daten in alle Buckets in Ihrem Konto exportieren. Darüber hinaus kann der Benutzer Daten in jeden öffentlich beschreibbaren Bucket in Ihrer AWS -Region exportieren.

Notieren Sie nach dem Erstellen der Richtlinie den Amazon-Ressourcennamen (ARN) der Richtlinie. Sie benötigen den ARN für einen nachfolgenden Schritt, in dem Sie die Richtlinie an eine IAM-Rolle anhängen.

```
aws iam create-policy  --policy-name rds-s3-export-policy  --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3export",
         "Action": [
           "s3:PutObject*",
           "s3:ListBucket",
           "s3:GetObject*",
           "s3:DeleteObject*",
           "s3:GetBucketLocation",
           "s3:AbortMultipartUpload"
         ],
         "Effect": "Allow",
         "Resource": [
           "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ]
```

```
      }
    ]
  }'
```

2. Erstellen Sie eine IAM-Rolle.

   Sie tun dies, damit Aurora PostgreSQL in Ihrem Namen diese IAM-Rolle übernehmen kann, um auf Ihre Amazon S3-Buckets zuzugreifen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer im IAM-Benutzerhandbuch.

   Wir empfehlen die Verwendung von `aws:SourceArn` und `aws:SourceAccount` globaler Bedingungskontext-Schlüssel in ressourcenbasierten Richtlinien, um die Berechtigungen des Dienstes auf eine bestimmte Ressource zu beschränken. Dies ist der effektivste Weg, um sich vor dem verwirrtes Stellvertreterproblem zu schützen.

   Wenn Sie sowohl globale Kontextschlüssel nutzen und der `aws:SourceArn`-Wert enthält die Konto-ID, muss der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert die gleiche Konto-ID verwenden, wenn er in der gleichen Richtlinienanweisung verwendet wird.

   - Verwenden von `aws:SourceArn` wenn Sie einen serviceübergreifenden Zugriff für eine einzelne Ressource wünschen.
   - Verwenden von `aws:SourceAccount` wenn Sie zulassen möchten, dass eine Ressource in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft wird.

   Verwenden Sie in der Richtlinie den `aws:SourceArn` globalen Kontextschlüssel mit dem vollständigen ARN der Ressource. Das folgende Beispiel zeigt, wie Sie dazu den AWS CLI Befehl verwenden, um eine Rolle mit dem Namen zu erstellen. `rds-s3-export-role`

   Example

   Für LinuxmacOS, oderUnix:

```
aws iam create-role  \
    --role-name rds-s3-export-role  \
    --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
```

```
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
             }
       }
     ]
   }'
```

Windows:

```
aws iam create-role  ^
    --role-name rds-s3-export-role  ^
    --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
             }
       }
     ]
   }'
```

3. Fügen Sie die erstellte IAM-Richtlinie der IAM-Rolle an, die Sie erstellt haben.

   Mit dem folgenden AWS CLI Befehl wird die zuvor erstellte Richtlinie an die Rolle `rds-s3-export-role`. Replace *`your-policy-arn`* mit dem Richtlinien-ARN angehängt, den Sie in einem früheren Schritt notiert haben.

```
aws iam attach-role-policy  --policy-arn your-policy-arn  --role-name rds-s3-
export-role
```

4. Fügen Sie die IAM-Rolle der DB Cluster hinzu. Sie tun dies, indem Sie das AWS Management Console oder verwenden AWS CLI, wie im Folgenden beschrieben.

Konsole

So fügen Sie eine IAM-Rolle für eine PostgreSQL DB-Cluster- über die Konsole hinzu:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie den Namen der PostgreSQL DB-Cluster- aus, um ihre Details anzuzeigen.
3. Wählen Sie auf der Registerkarte Connectivity & security (Konnektivität und Sicherheit) im Bereich Manage IAM roles (IAM-Rollen verwalten) die Rolle aus, die unter Add IAM roles to this instance (IAM-Rollen zu dieser Instance hinzufügen) hinzugefügt werden soll.
4. Wählen Sie unter Funktion die Option s3Export aus.
5. Wählen Sie Rolle hinzufügen.

AWS CLI

So fügen Sie eine IAM-Rolle für einen PostgreSQL-DB-Cluster mithilfe der CLI hinzu:

- Verwenden Sie den folgenden Befehl, um die Rolle mit dem Namen `my-db-cluster` zum PostgreSQL DB-Cluster hinzuzufügen. Ersetzen Sie *`your-role-arn`* durch den Rollen-ARN, den Sie im vorherigen Schritt notiert haben. Verwenden Sie `s3Export` für den Wert der `--feature-name`-Option.

  Example

  Für LinuxmacOS, oderUnix:

```
aws rds add-role-to-db-cluster \
   --db-cluster-identifier my-db-cluster \
   --feature-name s3Export \
   --role-arn your-role-arn   \
   --region your-region
```

Windows:

```
aws rds add-role-to-db-cluster ^
   --db-cluster-identifier my-db-cluster ^
   --feature-name s3Export ^
   --role-arn your-role-arn ^
   --region your-region
```

Exportieren von Abfragedaten mithilfe der Funktion aws_s3.query_export_to_s3

Exportieren Sie Ihre PostgreSQL-Daten nach Amazon S3, indem Sie die aws_s3.query_export_to_s3-Funktion aufrufen.

Themen

- Voraussetzungen
- Aufruf von aws_s3.query_export_to_s3
- Exportieren in eine CSV-Datei, die ein benutzerdefiniertes Trennzeichen verwendet
- Exportieren in eine Binärdatei mit Codierung

Voraussetzungen

Bevor Sie die `aws_s3.query_export_to_s3`-Funktion verwenden, müssen Sie die folgenden Voraussetzungen erfüllen:

- Installieren Sie die erforderlichen PostgreSQL-Erweiterungen, wie unter beschriebe Übersicht über das Exportieren von Daten zu Amazon S3.
- Legen Sie fest, wohin die Daten nach Amazon S3 exportiert werden sollen, wie unter beschriebe Angeben des Amazon S3-Dateipfads für den Export.
- Stellen Sie sicher, dass die Exportzugriff auf Amazon S3 hat (wie unter Einrichten des Zugriffs auf einen Amazon S3-Bucket beschrieben).

In den folgenden Beispielen wird eine Datenbanktabelle namens verwende `sample_table`. In diesen Beispielen werden die Daten in einen Bucket namens *DOC-EXAMPLE-BUCKET* exportiert. Die Beispieltabelle und die Daten werden mit den folgenden SQL-Anweisungen in psql erstellt.

```
psql=> CREATE TABLE sample_table (bid bigint PRIMARY KEY, name varchar(80));
```

```
psql=> INSERT INTO sample_table (bid,name) VALUES (1, 'Monday'), (2,'Tuesday'), (3,
 'Wednesday');
```

Aufruf von aws_s3.query_export_to_s3

Im Folgenden werden die grundlegenden Möglichkeiten zum Aufrufen der aws_s3.query_export_to_s3-Funktion dargestellt.

In diesen Beispielen wird die Variable `s3_uri_1` zum Identifizieren einer Struktur verwendet, die die Informationen zur Identifizierung der Amazon S3-Datei enthält. Verwenden Sie die Funktion aws_commons.create_s3_uri, um die Struktur zu erstellen.

```
psql=> SELECT aws_commons.create_s3_uri(
   'DOC-EXAMPLE-BUCKET',
   'sample-filepath',
   'us-west-2'
) AS s3_uri_1 \gset
```

Obwohl die Parameter für die folgenden zwei `aws_s3.query_export_to_s3`-Funktionsaufrufe unterschiedlich sind, sind die Ergebnisse für diese Beispiele identisch. *Alle Zeilen der sample_table Tabelle werden in einen Bucket namens DOC-EXAMPLE-BUCKET exportiert.*

```
psql=> SELECT * FROM aws_s3.query_export_to_s3('SELECT * FROM
 sample_table', :'s3_uri_1');

psql=> SELECT * FROM aws_s3.query_export_to_s3('SELECT * FROM
 sample_table', :'s3_uri_1', options :='format text');
```

Die Parameter werden wie folgt beschrieben:

- `'SELECT * FROM sample_table'` – Der erste Parameter ist eine erforderliche Textzeichenfolge, die eine SQL-Abfrage enthält. Die PostgreSQL-Engine führt diese Abfrage aus. Die Ergebnisse der Abfrage werden in den S3-Bucket kopiert, der in anderen Parametern identifiziert wurde.
- `:'s3_uri_1'` – Dieser Parameter ist eine Struktur, die die Datei Amazon S3 identifiziert. In diesem Beispiel wird die zuvor erstellte Struktur anhand einer Variablen identifiziert. Sie können die Struktur stattdessen erstellen, indem Sie den Funktionsaufruf `aws_commons.create_s3_uri` wie folgt inline in den Funktionsaufruf `aws_s3.query_export_to_s3` einschließen.

```
SELECT * from aws_s3.query_export_to_s3('select * from sample_table',
   aws_commons.create_s3_uri('DOC-EXAMPLE-BUCKET', 'sample-filepath', 'us-west-2')
);
```

- `options :='format text'` – Der `options`-Parameter ist eine optionale Textzeichenfolge, die `COPY`-PostgreSQL-Argumente enthält. Beim Kopiervorgang werden die Argumente und das Format des PostgreSQL COPY-Befehls verwendet.

Wenn die angegebene Datei nicht im Amazon S3-Bucket vorhanden ist, wird sie erstellt. Wenn die Datei bereits vorhanden ist, wird sie überschrieben. Die Syntax für den Zugriff auf die exportierten Daten in Amazon S3 ist die folgende.

```
s3-region://bucket-name[/path-prefix]/file-prefix
```

Größere Exporte werden in mehreren Dateien gespeichert, jeweils mit einer maximalen Größe von ca. 6 GB. Die zusätzlichen Dateinamen haben das gleiche Dateipräfix, aber mit `_part`*XX* angefügt. *XX* stellt 2, dann 3 usw. dar. Angenommen, Sie geben den Pfad, in dem Sie Datendateien speichern, wie folgt an.

```
s3-us-west-2://DOC-EXAMPLE-BUCKET/my-prefix
```

Wenn der Export drei Datendateien anlegen muss, enthält der Amazon S3-Bucket die folgenden Datendateien.

```
s3-us-west-2://DOC-EXAMPLE-BUCKET/my-prefix
s3-us-west-2://DOC-EXAMPLE-BUCKET/my-prefix_part2
s3-us-west-2://DOC-EXAMPLE-BUCKET/my-prefix_part3
```

Die vollständige Referenz für diese Funktion und weitere Aufrufmöglichkeiten finden Sie unter aws_s3.query_export_to_s3. Weitere Informationen zum Zugriff auf Dateien in Amazon S3 finden Sie unter View an object im Amazon Simple Storage Service User Guide.

Exportieren in eine CSV-Datei, die ein benutzerdefiniertes Trennzeichen verwendet

Das folgende Beispiel zeigt, wie die aws_s3.query_export_to_s3-Funktion zum Exportieren von Daten in eine Datei aufgerufen wird, die ein benutzerdefiniertes Trennzeichen verwendet. Im Beispiel werden Argumente des Befehls PostgreSQL COPY verwendet, um das CSV-Dateiformat (durch Kommas getrennte Werte) und ein Doppelpunkt (:)-Trennzeichen anzugeben.

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
 options :='format csv, delimiter $$:$$');
```

Exportieren in eine Binärdatei mit Codierung

Das folgende Beispiel zeigt, wie die aws_s3.query_export_to_s3-Funktion zum Exportieren von Daten in eine Binärdatei mit Windows-1253-Codierung aufgerufen wird.

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
 options :='format binary, encoding WIN1253');
```

Fehlerbehebung beim Zugriff auf Amazon S3

Wenn beim Versuch, Daten nach Amazon S3 zu exportieren, Verbindungsprobleme auftreten, bestätigen Sie zunächst, dass die Regeln für den ausgehenden Zugriff für die mit Ihrer DB-Instance verknüpfte VPC-Sicherheitsgruppe Netzwerkkonnektivität zulassen. Insbesondere muss die Sicherheitsgruppe über eine Regel verfügen, die es der DB-Instance erlaubt, TCP-Datenverkehr über Port 443 und an eine beliebige IPv4-Adresse (0.0.0.0/0) zu senden. Weitere Informationen finden Sie unter Ermöglichen des Zugriffs auf den DB-Cluster in der VPC durch Erstellen einer Sicherheitsgruppe.

Empfehlungen finden Sie im Folgenden:

- Fehlerbehebung für Amazon Aurora-Identität und -Zugriff
- Fehlerbehebung bei Amazon S3 im Entwicklerhandbuch für Amazon Simple Storage Service
- Fehlerbehebung bei Amazon S3 und IAM im IAM-Benutzerhandbuch

Funktionsreferenz

Funktionen

- aws_s3.query_export_to_s3
- aws_commons.create_s3_uri

aws_s3.query_export_to_s3

Exportiert ein PostgreSQL-Abfrageergebnis in einen Amazon S3-Bucket. Die Erweiterung `aws_s3` stellt die Funktion `aws_s3.query_export_to_s3` bereit.

Die zwei erforderlichen Parameter sind `query` und `s3_info`. Diese definieren die zu exportierende Abfrage und identifizieren den Amazon S3-Bucket, in den exportiert werden soll. Ein optionaler Parameter namens `options` ermöglicht die Definition verschiedener Exportparameter. Beispiele für die Verwendung der `aws_s3.query_export_to_s3`-Funktion finden Sie unter Exportieren von Abfragedaten mithilfe der Funktion aws_s3.query_export_to_s3.

Syntax

```
aws_s3.query_export_to_s3(
    query text,
    s3_info aws_commons._s3_uri_1,
    options text,
    kms_key text
)
```

Eingabeparameter

query

Eine erforderliche Textzeichenfolge, die eine SQL-Abfrage enthält, die von der PostgreSQL-Engine ausgeführt wird. Die Ergebnisse dieser Abfrage werden in einen S3-Bucket kopiert, der im `s3_info`-Parameter identifiziert wurde.

s3_info

Ein zusammengesetzter `aws_commons._s3_uri_1`-Typ mit den folgenden Informationen zum S3-Objekt:

- `bucket` – Der Name des Amazon S3-Buckets, der die Datei enthalten soll.
- `file_path` – Der Amazon S3-Dateiname und der -Pfad.
- `region`— Die AWS Region, in der sich der Bucket befindet. Eine Liste der AWS Regionsnamen und der zugehörigen Werte finden Sie unterRegionen und Availability Zones.

  Derzeit muss dieser Wert dieselbe AWS Region wie die der exportierenden sein. Die Standardeinstellung ist die AWS Region der exportierenden .

Informationen zum Erstellen einer zusammengesetzten `aws_commons._s3_uri_1`-Struktur finden Sie in der aws_commons.create_s3_uri-Funktion.

options

Eine optionale Textzeichenfolge mit Argumenten für den PostgreSQL `COPY`-Befehl. Diese Argumente geben an, wie die Daten beim Exportieren kopiert werden sollen. Weitere Informationen finden Sie in der PostgreSQL COPY-Dokumentation.

kms_key-Text

Eine optionale Textzeichenfolge, die den vom Kunden verwalteten KMS-Schlüssel des S3-Buckets enthält, in den die Daten exportiert werden sollen.

Alternative Eingabeparameter

Zum Testen können Sie statt des Parameters `s3_info` eine erweiterte Gruppe von Parametern verwenden. Nachfolgend sind weitere Syntaxvariationen für die Funktion `aws_s3.query_export_to_s3` aufgeführt.

Statt den Parameter `s3_info` zum Identifizieren einer Amazon S3-Datei zu verwenden, nutzen Sie die Kombination aus den Parametern `bucket`, `file_path` und `region`.

```
aws_s3.query_export_to_s3(
    query text,
    bucket text,
    file_path text,
    region text,
    options text,
    kms_key text
)
```

query

Eine erforderliche Textzeichenfolge, die eine SQL-Abfrage enthält, die von der PostgreSQL-Engine ausgeführt wird. Die Ergebnisse dieser Abfrage werden in einen S3-Bucket kopiert, der im `s3_info`-Parameter identifiziert wurde.

bucket

Eine erforderliche Textzeichenfolge mit dem Namen des Amazon S3-Buckets, der die Datei enthält.

file_path

Eine erforderliche Textzeichenfolge, die den Amazon S3-Dateinamen einschließlich des Pfads der Datei enthält.

Region

Eine optionale Textzeichenfolge, die die AWS Region enthält, in der sich der Bucket befindet. Eine Liste der AWS Regionsnamen und der zugehörigen Werte finden Sie unterRegionen und Availability Zones.

Derzeit muss dieser Wert dieselbe AWS Region wie die der exportierenden sein. Die Standardeinstellung ist die AWS Region der exportierenden .

options

Eine optionale Textzeichenfolge mit Argumenten für den PostgreSQL `COPY`-Befehl. Diese Argumente geben an, wie die Daten beim Exportieren kopiert werden sollen. Weitere Informationen finden Sie in der PostgreSQL COPY-Dokumentation.

kms_key-Text

Eine optionale Textzeichenfolge, die den vom Kunden verwalteten KMS-Schlüssel des S3-Buckets enthält, in den die Daten exportiert werden sollen.

Ausgabeparameter

```
aws_s3.query_export_to_s3(
    OUT rows_uploaded bigint,
    OUT files_uploaded bigint,
    OUT bytes_uploaded bigint
)
```

rows_uploaded

Die Anzahl der Tabellenzeilen, die für die angegebene Abfrage erfolgreich in Amazon S3 hochgeladen wurden.

files_uploaded

Die Anzahl der in Amazon S3 hochgeladenen Dateien. Dateien werden in Größen von ca. 6 GB erstellt. Jeder weiteren erstellten Datei wird `_part`*XX* an den Namen angehängt. *XX* stellt 2, dann 3 usw. nach Bedarf dar.

bytes_uploaded

Die Gesamtanzahl der in Amazon S3 hochgeladenen Bytes.

Beispiele

```
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'DOC-
EXAMPLE-BUCKET', 'sample-filepath');
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'DOC-
EXAMPLE-BUCKET', 'sample-filepath','us-west-2');
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'DOC-
EXAMPLE-BUCKET', 'sample-filepath','us-west-2','format text');
```

aws_commons.create_s3_uri

Erstellt eine `aws_commons._s3_uri_1`-Struktur für die Amazon S3-Dateiinformationen. Die Ergebnisse der Funktion `aws_commons.create_s3_uri` werden im Parameter `s3_info` der Funktion aws_s3.query_export_to_s3 verwendet. Ein Beispiel für die Verwendung der `aws_commons.create_s3_uri`-Funktion finden Sie unter Angeben des Amazon S3-Dateipfads für den Export.

Syntax

```
aws_commons.create_s3_uri(
   bucket text,
   file_path text,
   region text
)
```

Eingabeparameter

bucket

Eine erforderliche Textzeichenfolge mit dem Namen des Amazon S3-Buckets für die Datei.

file_path

Eine erforderliche Textzeichenfolge, die den Amazon S3-Dateinamen einschließlich des Pfads der Datei enthält.

Region

Eine erforderliche Textzeichenfolge, die die AWS Region enthält, in der sich die Datei befindet. Eine Liste der AWS Regionsnamen und der zugehörigen Werte finden Sie unterRegionen und Availability Zones.

Aufrufen einer AWS Lambda Funktion aus einem Aurora PostgreSQL-DB-Cluster (PostgreSQL-DB-Instance)

AWS Lambda ist ein ereignisgesteuerter Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. Es ist für die Verwendung mit vielen AWS Diensten verfügbar, einschließlich Aurora PostgreSQL PostgreSQL. Sie können beispielsweise Lambda-Funktionen verwenden, um Ereignisbenachrichtigungen aus einer Datenbank zu verarbeiten oder Daten aus Dateien zu laden, wann immer eine neue Datei in Amazon S3 hochgeladen wird. Weitere Informationen zu Lambda finden Sie unter Was ist AWS Lambda? im AWS Lambda Entwicklerhandbuch.

> **Note**
>
> Das Aufrufen von AWS Lambda Funktionen wird in Aurora PostgreSQL 11.9 und höher (einschließlich) unterstützt. Aurora Serverless v2

Im Folgenden finden Sie Zusammenfassungen der notwendigen Schritte.

Weitere Informationen über Lambda-Funktionen finden Sie unter Erste Schritte mit Lambda und Grundlagen von AWS Lambda im AWS Lambda -Entwicklerhandbuch.

Themen

- Schritt 1: Konfigurieren Sie Ihren Aurora PostgreSQL DB-Cluster für ausgehende Verbindungen zu AWS Lambda
- Schritt 2: Konfigurieren Sie IAM für Ihren Aurora PostgreSQL-DB-Cluster, und AWS Lambda
- Schritt 3: Installieren der aws_lambda-Erweiterung für einen Aurora-PostgreSQL-DB-Cluster
- Schritt 4: Verwenden von Lambda-Hilfsfunktionen mit Ihrem Aurora-PostgreSQL-DB-Cluster (optional)
- Schritt 5: Aufrufen einer Lambda-Funktion von Ihrem Aurora-PostgreSQL-DB-Cluster

- Schritt 6: Erteilen der Berechtigung, Lambda-Funktionen aufzurufen, für andere Benutzer
- Beispiele: Aufrufen von Lambda-Funktionen von Ihrem Aurora-PostgreSQL-DB-Cluster
- Fehlermeldungen von Lambda-Funktionen
- AWS Lambda Funktions- und Parameterreferenz

Schritt 1: Konfigurieren Sie Ihren Aurora PostgreSQL DB-Cluster für ausgehende Verbindungen zu AWS Lambda

Lambda-Funktionen werden immer in einer Amazon-VPC ausgeführt, die dem AWS Lambda Service gehört. Lambda wendet Netzwerkzugriffs- und Sicherheitsregeln auf diese VPC an und pflegt und überwacht die VPC automatisch. Ihr DB-Cluster von Aurora-PostgreSQL muss Netzwerkdatenverkehr an die VPC des Lambda-Services senden. Wie Sie dies konfigurieren, hängt davon ab, ob die primäre DB-Instance Ihres Aurora-DB-Clusters öffentlich oder privat ist.

- Öffentlicher Aurora PostgreSQL-DB-Cluster — Die primäre eines DB-Clusters ist öffentlich, wenn sie sich in einem öffentlichen Subnetz auf Ihrer VPC befindet und wenn die Eigenschaft "" der Instance lautet. PubliclyAccessible `true` Um den Wert dieser Eigenschaft zu ermitteln, können Sie den Befehl describe-db-instances verwenden. AWS CLI Alternativ können Sie über die AWS Management Console die Registerkarte Connectivity & security (Konnektivität und Sicherheit) öffnen und prüfen, ob Publicly accessible (Öffentlich zugänglich) auf Yes (Ja) eingestellt ist. Wenn Sie überprüfen möchten, ob sich die Instance im öffentlichen Subnetz Ihrer VPC befindet, können Sie die AWS Management Console oder die AWS CLI verwenden.

  Um den Zugriff auf Lambda einzurichten, verwenden Sie AWS Management Console oder, AWS CLI um eine ausgehende Regel für die Sicherheitsgruppe Ihrer VPC zu erstellen. Die Regel für ausgehenden Datenverkehr legt fest, dass TCP Port 443 verwenden kann, um Pakete an eine beliebige IPv4-Adresse (0.0.0.0/0) zu senden.
- Private Aurora PostgreSQL DB-Cluster — In diesem Fall befindet sich die Eigenschaft "PubliclyAccessible" der Instance in einem privaten Subnetz `false` oder sie befindet sich in einem privaten Subnetz. Damit die Instance mit Lambda arbeiten kann, können Sie ein Network Address Translation (NAT)-Gateway verwenden. Weitere Informationen finden Sie unter NAT-Gateways. Sie können Ihre VPC auch mit einem VPC-Endpunkt für Lambda konfigurieren. Weitere Informationen finden Sie unter VPC-Endpunkte im Amazon-VPC-Benutzerhandbuch. Der Endpunkt gibt Antworten auf Aufrufe Ihrer Lambda-Funktionen von Ihrem DB-Cluster von Aurora PostgreSQL zurück.

Ihre VPC kann jetzt auf Netzwerkebene mit der AWS Lambda VPC interagieren. Als Nächstes konfigurieren Sie die Berechtigungen mithilfe von IAM.

Schritt 2: Konfigurieren Sie IAM für Ihren Aurora PostgreSQL-DB-Cluster, und AWS Lambda

Das Aufrufen von Lambda-Funktionen von Ihrem Aurora-PostgreSQL-DB-Cluster erfordert bestimmte Berechtigungen. Um die erforderlichen Berechtigungen zu konfigurieren, empfehlen wir Ihnen, eine IAM-Richtlinie zu erstellen, die es ermöglicht, Lambda-Funktionen aufzurufen, diese Richtlinie einer Rolle zuzuweisen und die Rolle dann auf Ihren DB-Cluster anzuwenden. Dieser Ansatz gewährt dem DB-Cluster Berechtigungen zum Aufrufen der angegebenen Lambda-Funktion in Ihrem Namen. Nachfolgend wird beschrieben, wie Sie dazu die AWS CLI verwenden können.

IAM-Berechtigungen für die Verwendung Ihrer Cluster mit Lambda konfigurieren

1. Verwenden Sie den AWS CLI Befehl create-policy, um eine IAM-Richtlinie zu erstellen, die es Ihrer Aurora ermöglicht, die angegebene Lambda-Funktion aufzurufen. (Die Anweisungs-ID (Sid) ist eine optionale Beschreibung für Ihre Richtlinienanweisung und hat keine Auswirkungen auf die Verwendung.) Diese Richtlinie gewährt Ihrem Aurora-DB-Cluster die Mindestberechtigungen zum Aufrufen der angegebenen Lambda-Funktion.

   ```
   aws iam create-policy  --policy-name rds-lambda-policy --policy-document '{
       "Version": "2012-10-17",
       "Statement": [
           {
           "Sid": "AllowAccessToExampleFunction",
           "Effect": "Allow",
           "Action": "lambda:InvokeFunction",
           "Resource": "arn:aws:lambda:aws-region:444455556666:function:my-function"
           }
       ]
   }'
   ```

   Alternativ können Sie die vordefinierte `AWSLambdaRole`-Richtlinie verwenden, mit der Sie alle Ihre Lambda-Funktionen aufrufen können. Weitere Informationen finden Sie unter Identitätsbasierte IAM-Richtlinien für Lambda.

2. Verwenden Sie den AWS CLI Befehl create-role, um eine IAM-Rolle zu erstellen, die die Richtlinie zur Laufzeit annehmen kann.

```
aws iam create-role  --role-name rds-lambda-role --assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal": {
            "Service": "rds.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
        }
    ]
}'
```

3. Wenden Sie die Richtlinie mithilfe des Befehls attach-role-policy auf die Rolle an. AWS CLI

```
aws iam attach-role-policy \
    --policy-arn arn:aws:iam::444455556666:policy/rds-lambda-policy \
    --role-name rds-lambda-role --region aws-region
```

4. https://awscli.amazonaws.com/v2/documentation/api/latest/reference/rds/add-role-to-db-cluster.html AWS CLI Dieser letzte Schritt erlaubt den Datenbankbenutzern Ihres DB-Clusters, Lambda-Funktionen aufzurufen.

```
aws rds add-role-to-db-cluster \
       --db-cluster-identifier my-cluster-name \
       --feature-name Lambda \
       --role-arn  arn:aws:iam::444455556666:role/rds-lambda-role   \
       --region aws-region
```

Wenn die VPC- und die IAM-Konfigurationen abgeschlossen sind, können Sie jetzt die `aws_lambda`-Erweiterung installieren. (Beachten Sie, dass Sie die Erweiterung jederzeit installieren können, bis Sie jedoch die richtige VPC-Unterstützung und IAM-Berechtigungen eingerichtet haben, hat die `aws_lambda`-Erweiterung keinerlei Auswirkungen auf die Funktionen Ihrer Aurora-PostgreSQL-DB-Cluster.)

Schritt 3: Installieren der **aws_lambda**-Erweiterung für einen Aurora-PostgreSQL-DB-Cluster

Diese Erweiterung bietet Ihrem Aurora-PostgreSQL-DB-Cluster die Möglichkeit, Lambda-Funktionen von PostgreSQL aus aufzurufen.

aws_lambda-Erweiterung in einem Aurora-PostgreSQL-DB-Cluster installieren

Verwenden Sie die PostgreSQL-`psql`-Befehlszeile oder das pgAdmin-Tool, um Ihren Aurora-PostgreSQL-DB-Cluster zu verbinden.

1. Verbinden Sie Ihren Aurora-PostgreSQL-DB-Cluster als Benutzer mit `rds_superuser`-Berechtigungen. Im Beispiel wird der `postgres`-Standardbenutzer dargestellt.

   ```
   psql -h cluster-instance.444455556666.aws-region.rds.amazonaws.com -U postgres -p
    5432
   ```

2. Installieren Sie die `aws_lambda`-Erweiterung. Die `aws_commons`-Erweiterung ist auch erforderlich. Sie bietet Hilfsfunktionen für `aws_lambda` und viele andere Aurora-Erweiterungen für PostgreSQL. Wenn Sie noch nicht auf Ihrem Aurora-PostgreSQL-DB-Cluster installiert ist, wird sie mit `aws_lambda` wie folgt installiert.

   ```
   CREATE EXTENSION IF NOT EXISTS aws_lambda CASCADE;
   NOTICE:  installing required extension "aws_commons"
   CREATE EXTENSION
   ```

Die `aws_lambda`-Erweiterung wird in Ihrer primären, auf Ihrem Aurora-PostgreSQL-DB-Cluster befindlichen DB-Instance installiert. Sie können jetzt praktische Strukturen für den Aufruf Ihrer Lambda-Funktionen erstellen.

Schritt 4: Verwenden von Lambda-Hilfsfunktionen mit Ihrem Aurora-PostgreSQL-DB-Cluster (optional)

Sie können die Hilfsfunktionen in der `aws_commons`-Erweiterung verwenden, um Entitäten vorzubereiten, die sich einfacher über PostgreSQL aufrufen lassen. Hierzu sind die folgenden Informationen zu Ihren Lambda-Funktionen erforderlich:

- Funktionsname – Der Name, der Amazon-Ressourcenname (ARN), die Version oder der Alias der Lambda-Funktion. Die in Schritt 2: Konfigurieren von IAM für Ihren Cluster und Lambda

erstellte IAM-Richtlinie benötigt den ARN, daher empfehlen wir Ihnen, den ARN Ihrer Funktion zu verwenden.

- AWS Region — (Optional) Die AWS Region, in der sich die Lambda-Funktion befindet, wenn sie sich nicht in derselben Region wie Ihre Aurora befindet.

Um die Daten zum Lambda-Funktionsnamen zu speichern, verwenden Sie die aws_commons.create_lambda_function_arn-Funktion. Diese Hilfsfunktion erstellt eine zusammengesetzte `aws_commons._lambda_function_arn_1`-Struktur mit den Details, die von der Aufruffunktion benötigt werden. Im Folgenden finden Sie drei alternative Ansätze zum Einrichten dieser zusammengesetzten Struktur.

```
SELECT aws_commons.create_lambda_function_arn(
   'my-function',
   'aws-region'
) AS aws_lambda_arn_1 \gset
```

```
SELECT aws_commons.create_lambda_function_arn(
   '111122223333:function:my-function',
   'aws-region'
) AS lambda_partial_arn_1 \gset
```

```
SELECT aws_commons.create_lambda_function_arn(
   'arn:aws:lambda:aws-region:111122223333:function:my-function'
) AS lambda_arn_1 \gset
```

Jeder dieser Werte kann in Aufrufen der aws_lambda.invoke-Funktion verwendet werden. Beispiele finden Sie unter Schritt 5: Aufrufen einer Lambda-Funktion von Ihrem Aurora-PostgreSQL-DB-Cluster.

Schritt 5: Aufrufen einer Lambda-Funktion von Ihrem Aurora-PostgreSQL-DB-Cluster

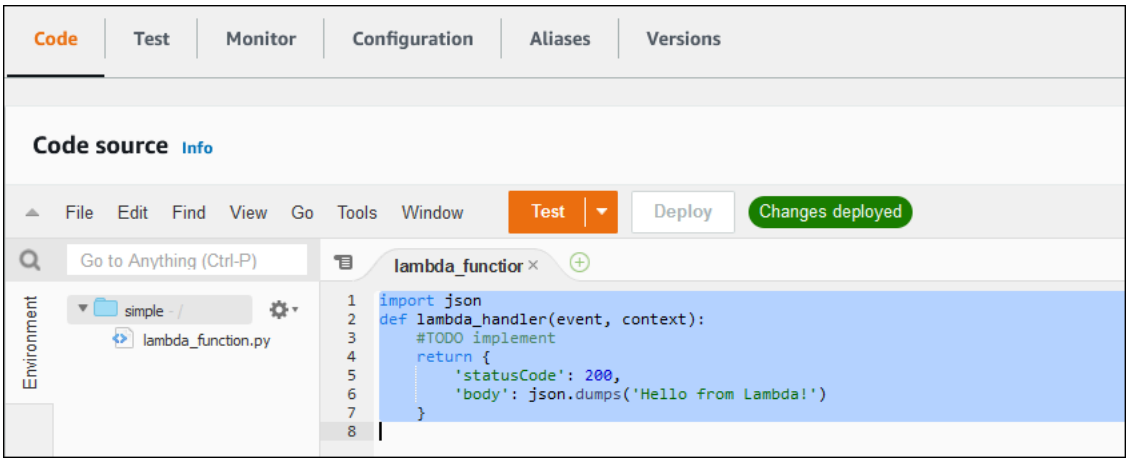
Die `aws_lambda.invoke`-Funktion verhält sich synchron oder asynchron, je nach `invocation_type`. Die beiden Alternativen für diesen Parameter sind `RequestResponse` (der Standardwert) und `Event`, wie folgt.

- **`RequestResponse`** – Dieser Aufrufstyp ist synchron. Dies ist das Standardverhalten, wenn der Aufruf erfolgt, ohne einen Aufruftyp anzugeben. Die Antwort-Nutzlast beinhaltet die Ergebnisse der

`aws_lambda.invoke`-Funktion. Verwenden Sie diesen Aufruftyp, wenn Ihr Workflow Ergebnisse von der Lambda-Funktion erhalten muss, bevor er fortfährt.

- **`Event`** – Dieser Aufrufstyp ist asynchron. Die Antwort umfasst keine Nutzlast, die Ergebnisse enthält. Verwenden Sie diesen Aufruftyp, wenn Ihr Workflow kein Ergebnis der Lambda-Funktion benötigt, um die Verarbeitung fortzusetzen.

Als einfacher Test Ihres Setups können Sie mittels `psql` eine Verbindung mit Ihrer DB-Instance herstellen und eine Beispielfunktion über die Befehlszeile aufrufen. Angenommen, Sie haben eine der Grundfunktionen Ihres Lambda-Services eingerichtet, z. B. die einfache Python-Funktion, die im folgenden Screenshot gezeigt wird.



Beispielfunktion aufrufen

1. Stellen Sie per `psql` oder pgAdmin eine Verbindung zu Ihrer primären DB-Instance her.

   ```
   psql -h cluster.444455556666.aws-region.rds.amazonaws.com -U postgres -p 5432
   ```

2. Rufen Sie die Funktion mit ihrem ARN auf.

   ```
   SELECT * from
    aws_lambda.invoke(aws_commons.create_lambda_function_arn('arn:aws:lambda:aws-
   region:444455556666:function:simple', 'us-west-1'), '{"body": "Hello from
    Postgres!"}'::json );
   ```

   Die Antwort sieht wie folgt aus.

   ```
   status_code |                          payload                          |
    executed_version | log_result
   ```

```
-------------+------------------------------------------------------------
+------------------+------------
         200 | {"statusCode": 200, "body": "\"Hello from Lambda!\""} | $LATEST
     |
(1 row)
```

Schlägt der Aufruf fehl, siehe Fehlermeldungen von Lambda-Funktionen .

Schritt 6: Erteilen der Berechtigung, Lambda-Funktionen aufzurufen, für andere Benutzer

An dieser Stelle in den Prozeduren können nur Sie als `rds_superuser` Ihre Lambda-Funktionen aufrufen. Damit andere Benutzer alle von Ihnen erstellten Funktionen aufrufen können, müssen Sie ihnen die entsprechende Berechtigung erteilen.

Gewähren der Berechtigung zum Aufrufen von Lambda-Funktionen

1. Stellen Sie per `psql` oder pgAdmin eine Verbindung zu Ihrer primären DB-Instance her.

   ```
   psql -h cluster.444455556666.aws-region.rds.amazonaws.com -U postgres -p 5432
   ```

2. Führen Sie die folgenden SQL-Befehle aus:

   ```
   postgres=>  GRANT USAGE ON SCHEMA aws_lambda TO db_username;
   GRANT EXECUTE ON ALL FUNCTIONS IN SCHEMA aws_lambda TO db_username;
   ```

Beispiele: Aufrufen von Lambda-Funktionen von Ihrem Aurora-PostgreSQL-DB-Cluster

Nachfolgend finden Sie einige Beispiele für den Aufruf der aws_lambda.invoke-Funktion. In den meisten Beispielen wird die Verbundstruktur verwendet`aws_lambda_arn_1`, die Sie erstellen, Schritt 4: Verwenden von Lambda-Hilfsfunktionen mit Ihrem Aurora-PostgreSQL-DB-Cluster (optional) um die Übergabe der Funktionsdetails zu vereinfachen. Ein Beispiel für einen asynchronen Aufruf finden Sie unter Beispiel: Asynchroner Ereignisaufruf (Event) von Lambda-Funktionen. Alle anderen aufgelisteten Beispiele verwenden einen synchronen Aufruf.

Weitere Informationen zu Lambda-Aufruftypen finden Sie unter Aufrufen von Lambda-Funktionen im AWS Lambda -Entwicklerhandbuch. Mehr über `aws_lambda_arn_1` erfahren Sie unter aws_commons.create_lambda_function_arn.

Liste mit Beispielen

- Beispiel: Synchroner (RequestResponse) -Aufruf von Lambda-Funktionen
- Beispiel: Asynchroner Ereignisaufruf (Event) von Lambda-Funktionen
- Beispiel: Erfassen des Lambda-Ausführungsprotokolls in einer Funktionsantwort
- Beispiel: Einschließen von Client-Kontext in einer Lambda-Funktion
- Beispiel: Aufrufen einer bestimmten Version einer Lambda-Funktion

Beispiel: Synchroner (RequestResponse) -Aufruf von Lambda-Funktionen

Es folgen zwei Beispiele für einen synchronen Lambda-Funktionsaufruf. Die Ergebnisse dieser `aws_lambda.invoke`-Funktionen sind identisch.

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json);
```

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json, 'RequestResponse');
```

Die Parameter werden wie folgt beschrieben:

- `:'aws_lambda_arn_1'` – Dieser Parameter identifiziert die zusammengesetzte Struktur, die in Schritt 4: Verwenden von Lambda-Hilfsfunktionen mit Ihrem Aurora-PostgreSQL-DB-Cluster (optional) erstellt wurde, mit der `aws_commons.create_lambda_function_arn`-Hilfsfunktion. Sie können diese Struktur wie folgt auch in Ihren `aws_lambda.invoke`-Aufruf einbinden.

  ```
  SELECT * FROM aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-function',
   'aws-region'),
  '{"body": "Hello from Postgres!"}'::json
  );
  ```

- `'{"body": "Hello from PostgreSQL!"}'::json` – Die JSON-Nutzlast, die an die Lambda-Funktion übergeben werden soll.
- `'RequestResponse'` – Der Lambda Aufruftyp.

Beispiel: Asynchroner Ereignisaufruf (Event) von Lambda-Funktionen

Es folgt ein Beispiel für einen asynchronen Lambda-Funktionsaufruf. Der `Event`-Aufruftyp plant den Lambda-Funktionsaufruf mit der angegebenen Eingabe-Nutzlast und sofort Rückgabe. Verwenden Sie den `Event`-Aufruftyp in bestimmten Workflows, die nicht von den Ergebnissen der Lambda-Funktion abhängen.

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json, 'Event');
```

Beispiel: Erfassen des Lambda-Ausführungsprotokolls in einer Funktionsantwort

Sie können die letzten 4 KB des Ausführungsprotokolls in die Funktionsantwort aufnehmen, indem Sie den Parameter `log_type` in Ihrem `aws_lambda.invoke`-Funktionsaufruf verwenden. Standardmäßig ist dieser Parameter auf `None` festgelegt, aber Sie können `Tail` angeben, um die Ergebnisse des Lambda-Ausführungsprotokolls in der Antwort zu erfassen, wie nachfolgend gezeigt.

```
SELECT *, select convert_from(decode(log_result, 'base64'), 'utf-8') as log FROM
 aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}'::json,
 'RequestResponse', 'Tail');
```

Legen Sie den Parameter aws_lambda.invoke der `log_type`-Funktion auf `Tail`, um das Ausführungsprotokoll in die Antwort aufzunehmen. Der Standardwert für diesen `log_type`-Parameter ist `None`.

Das `log_result`, was zurückgegeben wird, ist eine `base64` codierte Zeichenfolge. Sie können den Inhalt mit einer Kombination der PostgreSQL-Funktionen `decode` und `convert_from` dekodieren.

Mehr über `log_type` erfahren Sie unter aws_lambda.invoke.

Beispiel: Einschließen von Client-Kontext in einer Lambda-Funktion

Die `aws_lambda.invoke`-Funktion hat einen `context`-Parameter, den Sie verwenden können, um Informationen getrennt von der Nutzlast zu übergeben, wie nachfolgend gezeigt.

```
SELECT *, convert_from(decode(log_result, 'base64'), 'utf-8') as log FROM
 aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}'::json,
 'RequestResponse', 'Tail');
```

Um den Clientkontext einzuschließen, verwenden Sie ein JSON-Objekt für den Parameter aws_lambda.invoke der `context`-Funktion.

Weitere Informationen zum `context`-Parameter finden Sie in der aws_lambda.invoke-Referenz.

Beispiel: Aufrufen einer bestimmten Version einer Lambda-Funktion

Sie können eine bestimmte Version einer Lambda-Funktion angeben, indem Sie den `qualifier`-Parameter mit dem `aws_lambda.invoke`-Aufruf einschließen. Im Folgenden finden Sie ein Beispiel, das diese Funktion mit '*custom_version*' als Alias für die Version erfüllt.

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json, 'RequestResponse', 'None', NULL, 'custom_version');
```

Sie können auch einen Lambda-Funktionsqualifizierer wie folgt mit den Daten zum Funktionsnamen angeben.

```
SELECT * FROM aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-
function:custom_version', 'us-west-2'),
'{"body": "Hello from Postgres!"}'::json);
```

Weitere Informationen zu `qualifier` und anderen Parametern finden Sie in der aws_lambda.invoke-Referenz.

Fehlermeldungen von Lambda-Funktionen

In der folgenden Liste finden Sie Informationen zu Fehlermeldungen sowie mögliche Ursachen und Lösungen.

- VPC-Konfigurationsprobleme

  Probleme mit der VPC-Konfiguration können beim Versuch, eine Verbindung herzustellen, die folgenden Fehlermeldungen auslösen:

  ```
  ERROR:  invoke API failed
  DETAIL: AWS Lambda client returned 'Unable to connect to endpoint'.
  CONTEXT:  SQL function "invoke" statement 1
  ```

  Eine häufige Ursache für diesen Fehler ist eine falsch konfigurierte VPC-Sicherheitsgruppe. Stellen Sie sicher, dass eine Regel Port 443 Ihrer VPC-Sicherheitsgruppe für ausgehenden TCP-Datenverkehr öffnet, damit Ihre VPC eine Verbindung zur Lambda-VPC herstellen kann.
- Fehlende Berechtigungen, die zum Aufrufen von Lambda-Funktionen erforderlich sind

Wenn eine der folgenden Fehlermeldungen angezeigt wird, verfügt der Benutzer (Rolle), der die Funktion aufruft, nicht über die entsprechenden Berechtigungen.

```
ERROR:  permission denied for schema aws_lambda
```

```
ERROR:  permission denied for function invoke
```

Ein Benutzer (Rolle) muss bestimmte Berechtigungen erhalten, um Lambda-Funktionen aufrufen zu können. Weitere Informationen finden Sie unter Schritt 6: Erteilen der Berechtigung, Lambda-Funktionen aufzurufen, für andere Benutzer.

- Unsachgemäße Handhabung von Fehlern in Ihren Lambda-Funktionen

  Wenn eine Lambda-Funktion während der Anforderungsverarbeitung eine Ausnahme auslöst, `aws_lambda.invoke` schlägt dies mit einem PostgreSQL-Fehler wie folgt fehl.

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json);
ERROR:  lambda invocation failed
DETAIL:  "arn:aws:lambda:us-west-2:555555555555:function:my-function" returned error
 "Unhandled", details: "<Error details string>".
```

  Kümmern Sie sich unbedingt um Fehler in Ihren Lambda-Funktionen oder in Ihrer PostgreSQL-Anwendung.

AWS Lambda Funktions- und Parameterreferenz

Im Folgenden finden Sie die Referenz für die Funktionen und Parameter, die zum Aufrufen von Lambda mit Aurora PostgreSQL .

Funktionen und Parameter

- aws_lambda.invoke
- aws_commons.create_lambda_function_arn
- aws_lambda-Parameter

aws_lambda.invoke

Führt eine Lambda-Funktion für eine Aurora PostgreSQL DB-Cluster-RDS aus.

Weitere Informationen zum Aufrufen von Lambda-Funktionen finden Sie unter Invoke (Aufrufen) auch im AWS Lambda-Entwicklerhandbuch.

Syntax

JSON

```
aws_lambda.invoke(
IN function_name TEXT,
IN payload JSON,
IN region TEXT DEFAULT NULL,
IN invocation_type TEXT DEFAULT 'RequestResponse',
IN log_type TEXT DEFAULT 'None',
IN context JSON DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
OUT status_code INT,
OUT payload JSON,
OUT executed_version TEXT,
OUT log_result TEXT)
```

```
aws_lambda.invoke(
IN function_name aws_commons._lambda_function_arn_1,
IN payload JSON,
IN invocation_type TEXT DEFAULT 'RequestResponse',
IN log_type TEXT DEFAULT 'None',
IN context JSON DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
OUT status_code INT,
OUT payload JSON,
OUT executed_version TEXT,
OUT log_result TEXT)
```

JSONB

```
aws_lambda.invoke(
IN function_name TEXT,
IN payload JSONB,
IN region TEXT DEFAULT NULL,
```

```
IN invocation_type TEXT DEFAULT 'RequestResponse',
IN log_type TEXT DEFAULT 'None',
IN context JSONB DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
OUT status_code INT,
OUT payload JSONB,
OUT executed_version TEXT,
OUT log_result TEXT)
```

```
aws_lambda.invoke(
IN function_name aws_commons._lambda_function_arn_1,
IN payload JSONB,
IN invocation_type TEXT DEFAULT 'RequestResponse',
IN log_type TEXT DEFAULT 'None',
IN context JSONB DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
OUT status_code INT,
OUT payload JSONB,
OUT executed_version TEXT,
OUT log_result TEXT
)
```

Eingabeparameter

function_name

Der spezifizierte Name der Lambda-Funktion. Der Wert kann der Funktionsname, ein ARN oder ein partieller ARN sein. Eine Auflistung möglicher Formate finden Sie unter Lambda Funktionsnamenformate im AWS Lambda-Entwicklerhandbuch.

Nutzlast

Die Eingabe für die Funktion Lambda. Das Format kann JSON oder JSONB sein. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation zu JSON Types.

region

(Optional) Die Lambda-Region für die Funktion. Standardmäßig verwendet Aurora die AWS-Region aus dem vollständigen ARN in der `function_name` oder die Aurora PostgreSQL -DB-Instance-Region. Wenn dieser Region-Wert mit dem im `function_name` ARN angegebenen Wert in Konflikt steht, wird ein Fehler ausgelöst.

invocation_type

Die Aufruftyp der Lambda-Funktion. Bei -Wert ist die Groß- und Kleinschreibung zu beachten. Die folgenden Werte sind möglich:

- `RequestResponse` – Der Standardwert. Diese Art des Aufrufens für eine Lambda-Funktion ist synchron und gibt eine Antwortnutzlast im Ergebnis zurück. Verwenden Sie den `RequestResponse` Aufruftyp, wenn Ihr Workflow vom sofortigen Erhalt des Lambda-Funktionsergebnisses abhängt.
- `Event` – Diese Art des Aufrufs für eine Lambda-Funktion ist asynchron und wird sofort ohne Rückgabe einer Nutzlast zurückgegeben. Verwenden Sie den `Event`-Aufruftyp, wenn Sie keine Ergebnisse der Lambda-Funktion benötigen, bevor Ihr Workflow weitergeht.
- `DryRun` – Diese Art des Aufrufs testet den Zugriff, ohne die Lambda-Funktion auszuführen.

log_typ

Der Typ des Lambda-Protokolls, das im Ausgabeparameter `log_result` ausgegeben werden soll. Bei -Wert ist die Groß- und Kleinschreibung zu beachten. Die folgenden Werte sind möglich:

- Tail – Der zurückgegebene Ausgabeparameter `log_result` enthält die letzten 4 KB des Ausführungsprotokolls.
- Keiner – Es werden keine Lambda-Protokollinformationen zurückgegeben.

context

Client-Kontext im JSON- oder JSONB-Format. Zu verwendende Felder sind dann `custom` und `env`.

Qualifier

Ein Qualifier, der die aufzurufende Version einer Lambda-Funktion spezifiziert. Wenn dieser Wert mit einem im `function_name` ARN angegebenen Wert in Konflikt steht, wird ein Fehler ausgelöst.

Ausgabeparameter

status_code

Ein HTTP-Status-Antwortcode. Weitere Informationen finden Sie unter Lambda Antwortelemente aufrufen im AWS Lambda-Entwicklerhandbuch.

Nutzlast

Die von der ausgeführten Lambda-Funktion zurückgegebenen Daten. Das Format ist in JSON oder JSONB.

executed_version

Die Version der Lambda-Funktion, die ausgeführt wurde.

log_resultat

Die Ausführungsprotokollinformationen werden zurückgegeben, wenn der Wert `log_type` beim Aufruf der Lambda-Funktion `Tail` beträgt. Das Ergebnis enthält die letzten 4 KB des in Base64 codierten Ausführungsprotokolls.

aws_commons.create_lambda_function_arn

Erstellt eine `aws_commons._lambda_function_arn_1`-Struktur für Daten zum Lambda Funktionsnamen. Sie können die Ergebnisse der `aws_commons.create_lambda_function_arn`-Funktion im Parameter `function_name` der aws_lambda.invoke-Funktion aws_lambda.invoke verwenden.

Syntax

```
aws_commons.create_lambda_function_arn(
    function_name TEXT,
    region TEXT DEFAULT NULL
    )
    RETURNS aws_commons._lambda_function_arn_1
```

Eingabeparameter

function_name

Eine erforderliche Textzeichenfolge mit dem Lambda-Funktionsnamen. Der Wert kann ein Funktionsname, ein partieller ARN oder ein vollständiger ARN sein.

region

Eine optionale Textzeichenfolge mit der AWS-Region, in der sich die Lambda-Funktion befindet. Eine Liste der -Regionsnamen und der zugehörigen Werte finden Sie unter Regionen und Availability Zones.

aws_lambda-Parameter

In dieser Tabelle finden Sie Parameter, die der `aws_lambda` Funktion zugeordnet sind.

Parameter	Beschreibung
`aws_lambda.connect_timeout_ms`	Dies ist ein dynamischer Parameter, der die maximale Wartezeit beim Herstellen einer Verbindung mit AWS Lambda festlegt. Die Standardwerte sind `1000`. Zulässige Werte für diesen Parameter sind 1 bis 90 000.
`aws_lambda.request_timeout_ms`	Dies ist ein dynamischer Parameter und er legt die maximale Wartezeit fest, während er auf die Antwort von AWS Lambda wartet. Die Standardwerte sind `3000`. Zulässige Werte für diesen Parameter sind 1 bis 90 000.
`aws_lambda.endpoint_override`	Gibt den Endpunkt an, der für die Verbindung mit AWS Lambda verwendet werden kann. Eine leere Zeichenfolge wählt den StandardAWS-Lambda-Endpunkt für die Region aus. Sie müssen die Datenbank neu starten, damit diese statische Parameteränderung wirksam wird.

Veröffentlichen von Aurora-PostgreSQL-Protokollen in Amazon CloudWatch Logs

Sie können Ihren DB-Cluster von Aurora PostgreSQL so konfigurieren, dass Protokolldaten regelmäßig nach Amazon CloudWatch Logs exportiert werden. Wenn Sie dies tun, werden Ereignisse aus dem PostgreSQL-Protokoll Ihres Aurora-PostgreSQL-DB-Clusters automatisch als Amazon CloudWatch Logs CloudWatchin Amazon veröffentlicht. In finden Sie die CloudWatchexportierten Protokolldaten in einer Protokollgruppe für Ihren DB-Cluster von Aurora PostgreSQL. Die Protokollgruppe enthält einen oder mehrere Protokollstreams, die die Ereignisse aus dem PostgreSQL-Protokoll von jeder Instance im Cluster enthalten.

Durch die Veröffentlichung der Protokolle in CloudWatch Logs können Sie die PostgreSQL-Protokolldatensätze Ihres Clusters in einem Speicher mit hoher Beständigkeit aufbewahren. Mit den in - CloudWatch Protokollen verfügbaren Protokolldaten können Sie den Betrieb Ihres Clusters bewerten und verbessern. Sie können auch verwenden CloudWatch , um Alarme zu

erstellen und Metriken anzuzeigen. Weitere Informationen hierzu finden Sie unter Überwachen von Protokollereignissen in Amazon CloudWatch.

> **Note**
>
> Das Veröffentlichen Ihrer PostgreSQL-Protokolle in CloudWatch Logs verbraucht Speicher und es fallen Gebühren für diesen Speicher an. Löschen Sie alle CloudWatch Protokolle, die Sie nicht mehr benötigen.

Das Deaktivieren der Exportprotokolloption für einen vorhandenen DB-Cluster von Aurora PostgreSQL wirkt sich nicht auf Daten aus, die bereits in - CloudWatch Protokollen gespeichert sind. Vorhandene Protokolle bleiben basierend auf Ihren Einstellungen für die Aufbewahrung von Protokollen in CloudWatch -Protokollen verfügbar. Weitere Informationen zu - CloudWatch Protokollen finden Sie unter Was ist Amazon CloudWatch Logs?

Aurora PostgreSQL unterstützt das Veröffentlichen von Protokollen in CloudWatch Logs für die folgenden Versionen.

- 14.3 und höhere 14-Versionen
- 13.3 und höhere 13 Versionen
- 12.8 und höhere 12 Versionen
- 11.12 und höher 11 Versionen

Aktivieren der Option zum Veröffentlichen von Protokollen in Amazon CloudWatch

Um das PostgreSQL-Protokoll Ihres DB-Clusters von Aurora PostgreSQL in CloudWatch Logs zu veröffentlichen, wählen Sie die Option Protokollexport für den Cluster aus. Sie können die Log-Export-Einstellung beim Erstellen Ihres Aurora-PostgreSQL-DB-Clusters auswählen. Sie können den Cluster auch später ändern. Wenn Sie einen vorhandenen Cluster ändern, werden seine PostgreSQL-Protokolle von jeder Instance ab diesem Zeitpunkt im CloudWatch Cluster veröffentlicht. Für Aurora PostgreSQL ist das PostgreSQL-Protokoll (`postgresql.log`) das einzige Protokoll, das in Amazon veröffentlicht wird CloudWatch.

Sie können das AWS Management Console, das AWS CLI oder die RDS-API verwenden, um die Protokollexportfunktion für Ihren Aurora PostgreSQL DB-Cluster zu aktivieren.

Konsole

Sie wählen die Option Protokollexporte, um mit der Veröffentlichung der PostgreSQL-Protokolle aus Ihrem Aurora-PostgreSQL-DB-Cluster in CloudWatch Logs zu beginnen.

So aktivieren Sie die Funktion zum Exportieren von Protokollen über die Konsole

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den Aurora-PostgreSQL-DB-Cluster aus, dessen Protokolldaten Sie in CloudWatch Logs veröffentlichen möchten.
4. Wählen Sie Ändern aus.
5. Wählen Sie im Abschnitt Log exports (Protokollexporte) die Option PostgreSQL log aus.
6. Wählen Sie Continue (Weiter) und dann auf der Übersichtsseite Modify cluster (Cluster ändern).

AWS CLI

Sie können die Option zum Exportieren von Protokollen aktivieren, um mit der Veröffentlichung von Aurora-PostgreSQL-Protokollen in Amazon CloudWatch Logs zu beginnenAWS CLI. Führen Sie dazu den modify-db-cluster AWS CLI Befehl mit den folgenden Optionen aus:

- `--db-cluster-identifier` – Die DB-Cluster-Kennung.
- `--cloudwatch-logs-export-configuration`– Die Konfigurationseinstellung für die Protokolltypen, die für den Export in CloudWatch Protokolle für den DB-Cluster festgelegt werden sollen.

Sie können Aurora-PostgreSQL-Protokolle auch veröffentlichen, indem Sie einen der folgenden AWS CLI-Befehle ausführen:

- create-db-cluster
- restore-db-cluster-from-s3
- restore-db-cluster-from-Snapshot
- restore-db-cluster-to-point-in-time

Führen Sie einen dieser AWS CLI-Befehle mit den folgenden Optionen aus:

- `--db-cluster-identifier` – Die DB-Cluster-Kennung.
- `--engine`— Die Datenbank-Engine.
- `--enable-cloudwatch-logs-exports`– Die Konfigurationseinstellung für die Protokolltypen, die für den Export in CloudWatch Protokolle für den DB-Cluster aktiviert werden sollen.

Je nach ausgeführtem AWS CLI-Befehl müssen möglicherweise noch weitere Optionen angegeben werden.

Example

Der folgende Befehl erstellt einen Aurora PostgreSQL-DB-Cluster zum Veröffentlichen von Protokolldateien in - CloudWatch Protokollen.

Für Linux, macOSoder Unix:

```
aws rds create-db-cluster \
    --db-cluster-identifier my-db-cluster \
    --engine aurora-postgresql \
    --enable-cloudwatch-logs-exports postgresql
```

Windows:

```
aws rds create-db-cluster ^
    --db-cluster-identifier my-db-cluster ^
    --engine aurora-postgresql ^
    --enable-cloudwatch-logs-exports postgresql
```

Example

Mit dem folgenden Befehl wird ein vorhandener DB-Cluster von Aurora PostgreSQL so konfiguriert, dass Protokolldateien in - CloudWatch Protokollen veröffentlicht werden. Der `--cloudwatch-logs-export-configuration`-Wert ist ein JSON-Objekt. Der Schlüssel für dieses Objekt ist „`EnableLogTypes`“ und sein Wert lautet „`postgresql`“.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier my-db-cluster \
```

```
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":["postgresql"]}'
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier my-db-cluster ^
    --cloudwatch-logs-export-configuration '{\"EnableLogTypes\":[\"postgresql\"]}'
```

> **Note**
>
> Wenn Sie die Windows-Befehlszeile verwenden, stellen Sie sicher, dass Sie doppelte Anführungszeichen (") im JSON-Code maskieren, indem Sie ihnen einen umgekehrten Schrägstrich (\) voranstellen.

Example

Im folgenden Beispiel wird ein vorhandener DB-Cluster von Aurora PostgreSQL so konfiguriert, dass die Veröffentlichung von Protokolldateien in - CloudWatch Protokollen deaktiviert wird. Der `--cloudwatch-logs-export-configuration`-Wert ist ein JSON-Objekt. Der Schlüssel für dieses Objekt ist „`DisableLogTypes`“ und sein Wert lautet „`postgresql`“.

Für Linux, macOSoder Unix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"DisableLogTypes":["postgresql"]}'
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration "{\"DisableLogTypes\":[\"postgresql\"]}"
```

> **Note**
>
> Bei Verwendung der Windows-Befehlszeile müssen doppelte Anführungszeichen (") im JSON-Code mit einem umgekehrten Schrägstrich (\) als Escape-Zeichen versehen werden.

RDS-API

Sie können die Log-Export-Option aktivieren, um die Veröffentlichung von Aurora-PostgreSQL-Protokollen mit der RDS-API zu starten. Hierzu führen Sie den Vorgang ModifyDBCluster mit den folgenden Optionen aus:

- `DBClusterIdentifier` – Die DB-Cluster-ID.
- `CloudwatchLogsExportConfiguration` – Die Konfigurationseinstellung für die Protokolltypen, die für den Export in CloudWatch Protokolle für den DB-Cluster aktiviert werden sollen.

Sie können Aurora PostgreSQL-Protokolle auch mit der RDS-API veröffentlichen, indem Sie eine der folgenden RDS-API-Operationen ausführen:

- CreateDBCluster
- RestoreDBClusterFromS3
- RestoreDBClusterFromSnapshot
- RestoreDBClusterToPointInTime

Führen Sie die RDS-API-Operation mit den folgenden Parametern aus:

- `DBClusterIdentifier` – Die DB-Cluster-Kennung.
- `Engine`— Die Datenbank-Engine.
- `EnableCloudwatchLogsExports`– Die Konfigurationseinstellung für die Protokolltypen, die für den Export in CloudWatch Protokolle für den DB-Cluster aktiviert werden sollen.

Je nach ausgeführtem AWS CLI-Befehl müssen möglicherweise noch weitere Parameter angegeben werden.

Überwachen von Protokollereignissen in Amazon CloudWatch

Wenn Aurora-PostgreSQL-Protokollereignisse veröffentlicht und als Amazon CloudWatch Logs verfügbar sind, können Sie Ereignisse mit Amazon anzeigen und überwachen CloudWatch. Weitere Informationen zur Überwachung finden Sie unter Anzeigen von Protokolldaten, die an - CloudWatch Protokolle gesendet wurden.

Wenn Sie Log exports (Protokollexporte) aktivieren, wird mit dem Präfix `/aws/rds/cluster/` automatisch eine neue Protokollgruppe mit dem Namen Ihrer Aurora PostgreSQL und dem Protokolltyp, wie im folgenden Muster erstellt.

```
/aws/rds/cluster/your-cluster-name/postgresql
```

Angenommen, ein Aurora-PostgreSQL-DB-Cluster mit dem Namen `docs-lab-apg-small` exportiert sein Protokoll nach Amazon CloudWatch Logs. Der Name der Protokollgruppe in Amazon CloudWatch wird im Folgenden angezeigt.

```
/aws/rds/cluster/docs-lab-apg-small/postgresql
```

Wenn bereits eine Protokollgruppe mit dem angegebenen Namen existiert, verwendet Aurora diese Protokollgruppe, um Protokolldaten für den Aurora-DB-Cluster zu exportieren. Jede DB-Instance im Aurora PostgreSQL DB-Cluster lädt ihr PostgreSQL-Protokoll als eigenständigen Protokollstream in die Protokollgruppe hoch. Sie können die Protokollgruppe und ihre Protokollstreams mit den verschiedenen grafischen und analytischen Tools untersuchen, die in Amazon verfügbar sind CloudWatch.

Sie können beispielsweise nach Informationen innerhalb der Protokollereignisse aus Ihrem Aurora-PostgreSQL-DB-Cluster suchen und Ereignisse mithilfe der CloudWatch Logs-KonsoleAWS CLI, der oder der CloudWatch Logs-API filtern. Weitere Informationen finden Sie unter Suchen und Filtern von Protokolldaten im Amazon- CloudWatch Logs-Benutzerhandbuch.

Standardmäßig werden neue Protokollgruppen mit Läuft niemals ab für ihre Aufbewahrungszeit erstellt. Sie können die CloudWatch Logs-Konsole, die oder die CloudWatch Logs-API verwendenAWS CLI, um den Aufbewahrungszeitraum für Protokolle zu ändern. Weitere Informationen finden Sie unter Ändern der Aufbewahrung von Protokolldaten in - CloudWatch Protokollen im Amazon- CloudWatch Logs-Benutzerhandbuch.

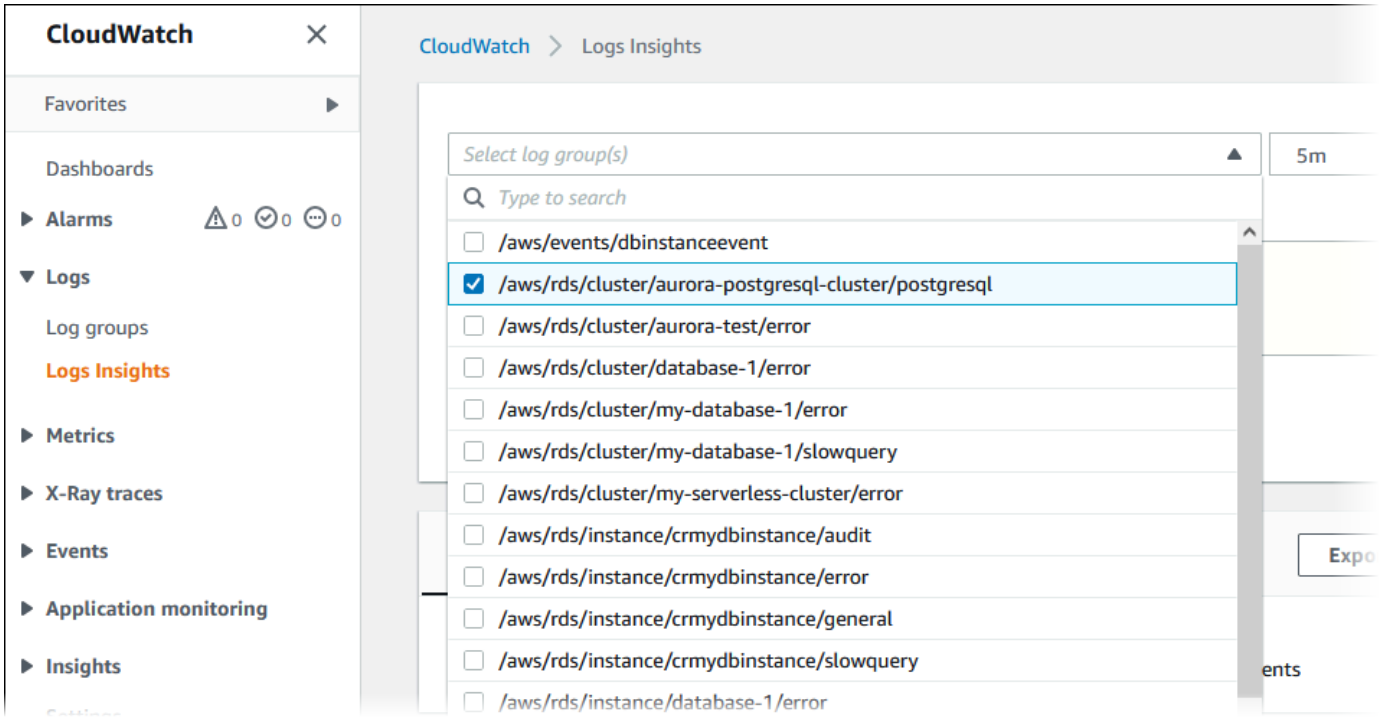
> **Tip**
>
> Sie können die automatisierte Konfiguration, wie z. B. AWS CloudFormation, verwenden, um Protokollgruppen mit vordefinierten Protokollaufbewahrungszeiten, Metrikfiltern und Zugriffsberechtigung zu erstellen.

Analysieren von PostgreSQL-Protokollen mit CloudWatch Logs Insights

Wenn die PostgreSQL-Protokolle aus Ihrem Aurora-PostgreSQL-DB-Cluster als CloudWatch Protokolle veröffentlicht wurden, können Sie CloudWatch Logs Insights verwenden, um interaktiv Ihre Protokolldaten in Amazon CloudWatch Logs zu durchsuchen und zu analysieren. CloudWatch Logs Insights enthält eine Abfragesprache, Beispielabfragen und andere Tools zur Analyse Ihrer Protokolldaten, sodass Sie potenzielle Probleme identifizieren und Korrekturen überprüfen können. Weitere Informationen finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im Amazon- CloudWatch Logs-Benutzerhandbuch. Amazon CloudWatch -Protokolle

So analysieren Sie PostgreSQL-Protokolle mit CloudWatch Logs Insights

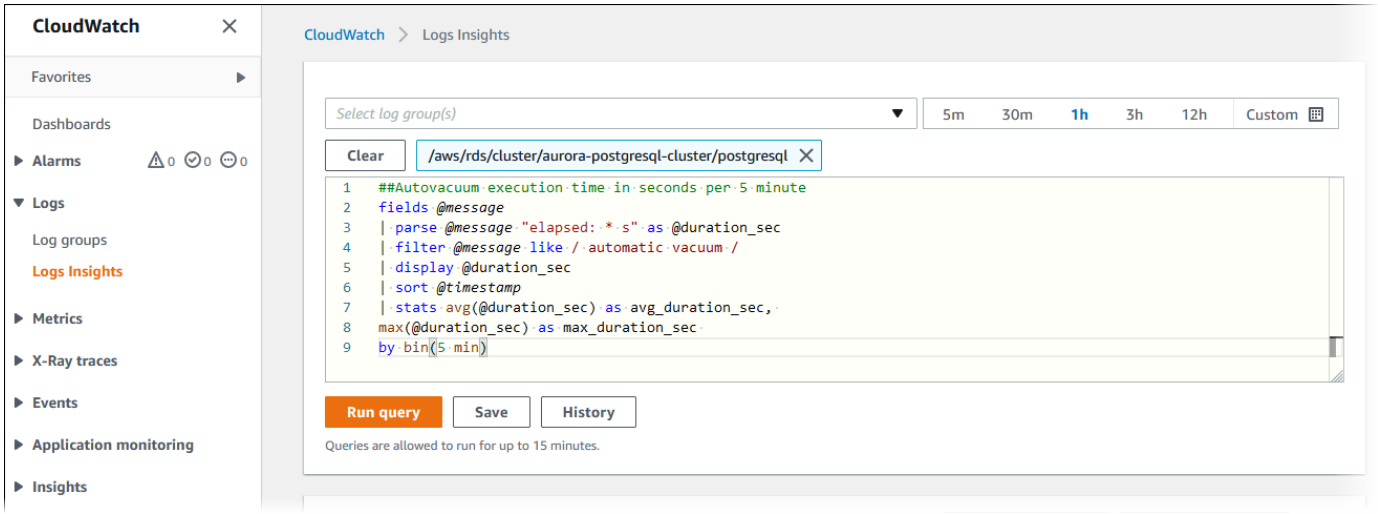
1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Öffnen Sie im Navigationsbereich Logs (Protokolle) und wählen Sie Log insights (Protokoll-Erkenntnisse) aus.
3. Wählen Sie unter Select log group(s) (Protokollgruppe(n) auswählen) die Protokollgruppe für Ihren Aurora-PostgreSQL-DB-Cluster aus.



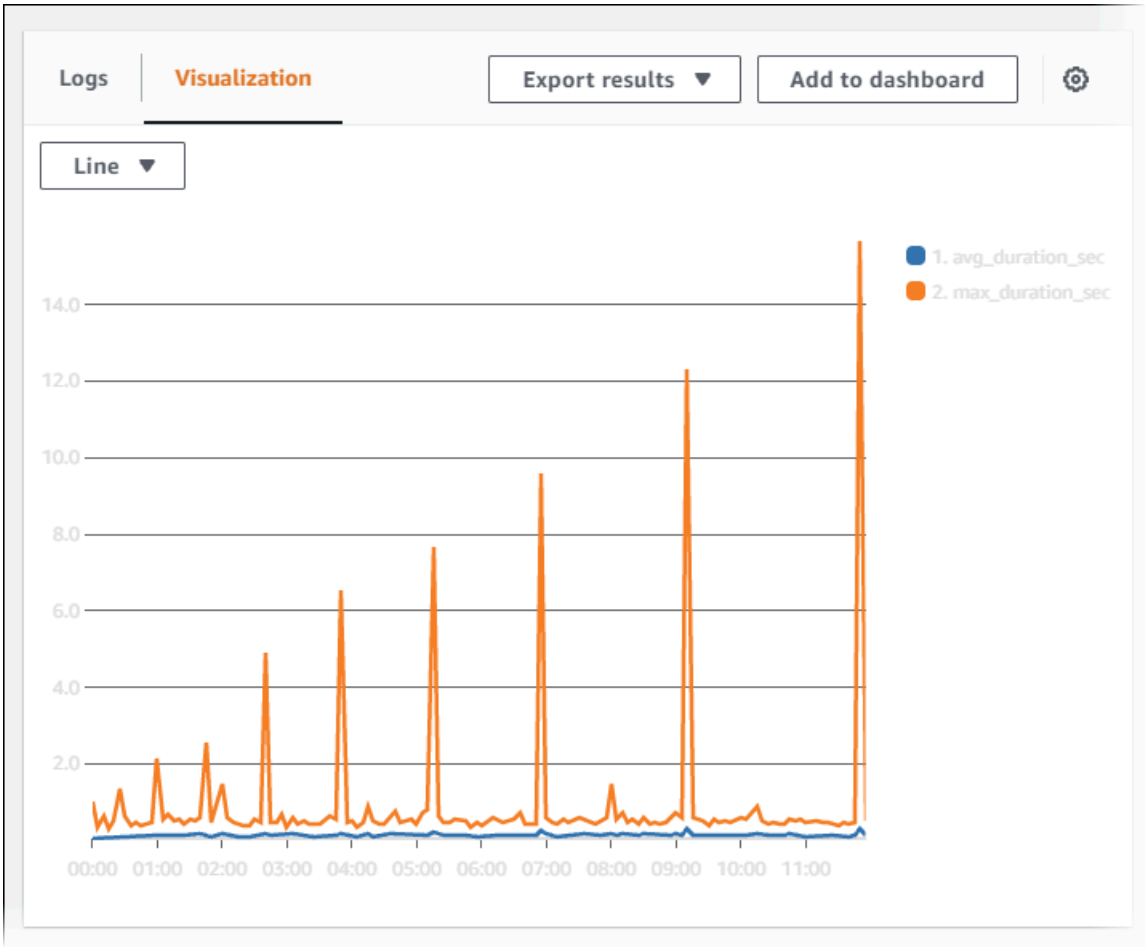
4. Löschen Sie im Abfrage-Editor die aktuell angezeigte Abfrage und geben Sie Folgendes ein. Wählen Sie anschließend Run query (Abfrage ausführen) aus.

```
##Autovacuum execution time in seconds per 5 minute
fields @message
```

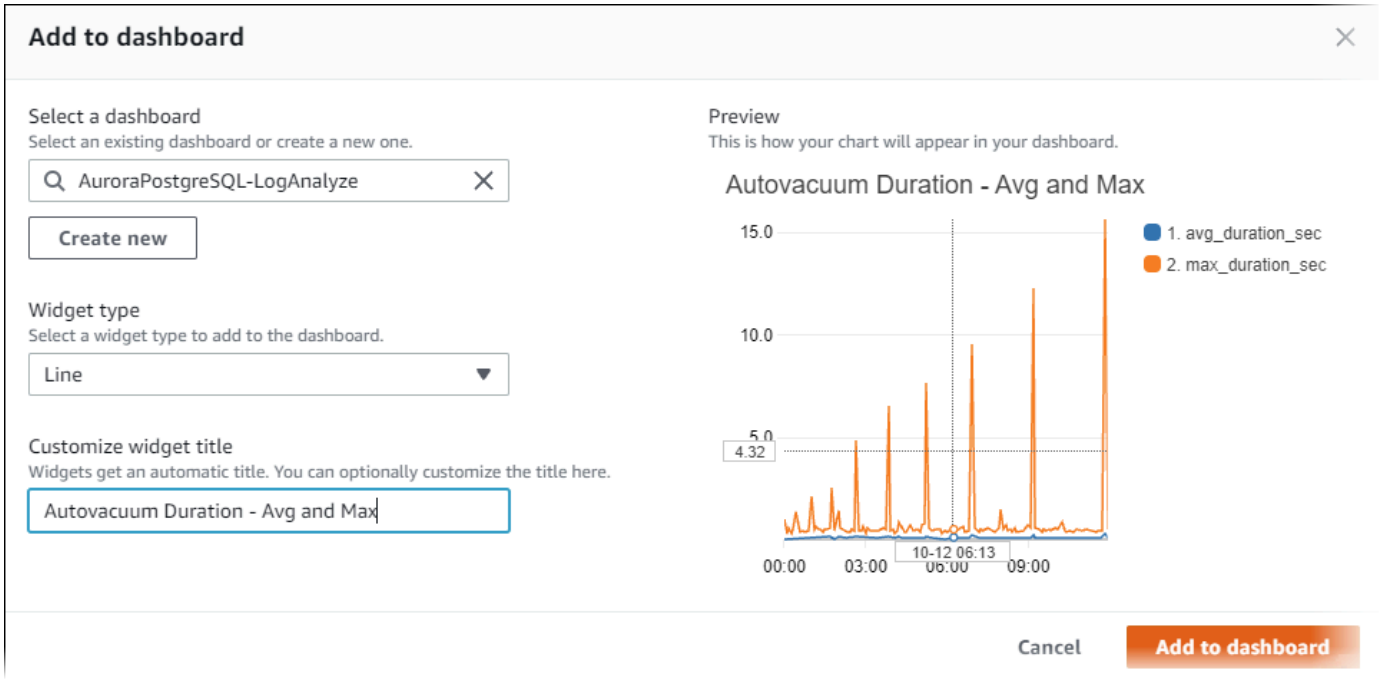
```
| parse @message "elapsed: * s" as @duration_sec
| filter @message like / automatic vacuum /
| display @duration_sec
| sort @timestamp
| stats avg(@duration_sec) as avg_duration_sec,
max(@duration_sec) as max_duration_sec
by bin(5 min)
```



5. Wählen Sie die Registerkarte Visualization (Visualisierung) aus.



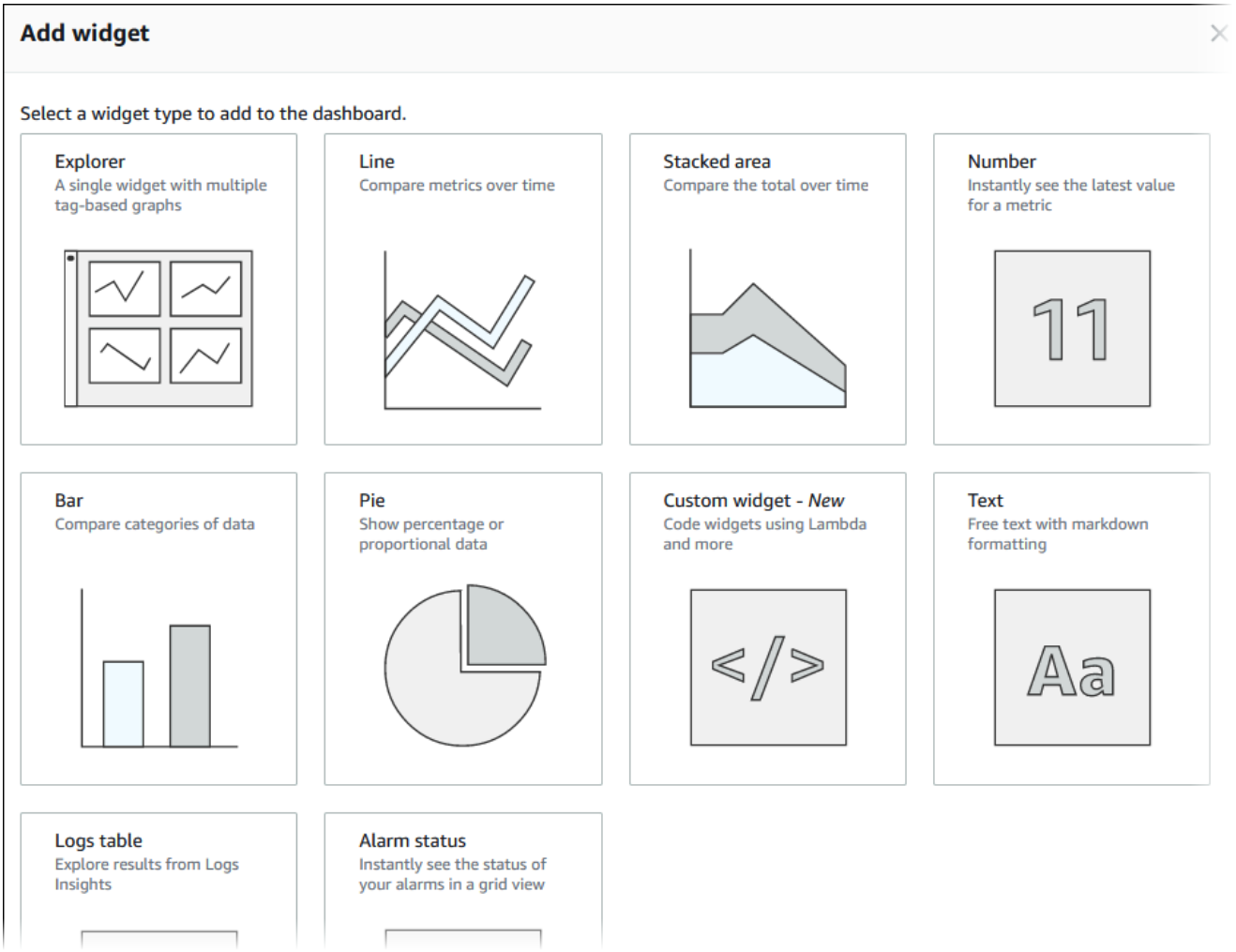
6. Wählen Sie Add to dashboard (Zu Dashboard hinzufügen) aus.
7. Wählen Sie unter Dashboard auswählen entweder ein Dashboard aus oder geben Sie einen Namen ein, um ein neues Dashboard zu erstellen.
8. Wählen Sie unter Widget-Typ einen Widget-Typ für Ihre Visualisierung aus.



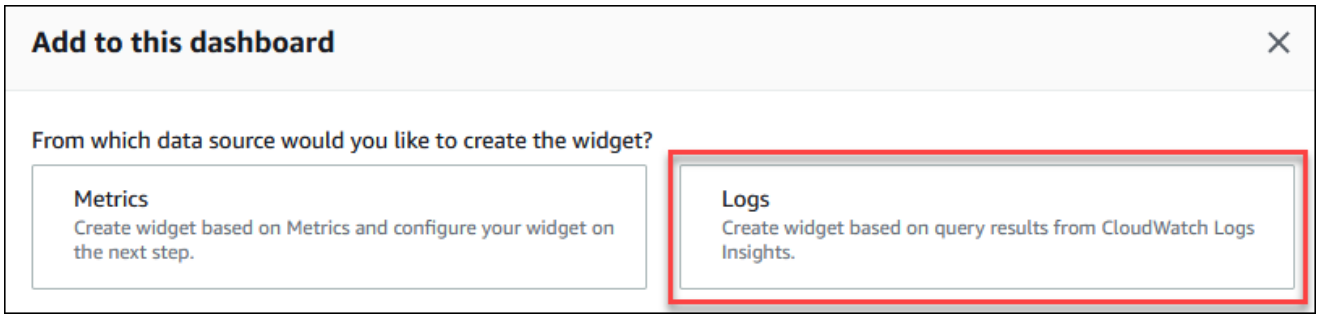
9. (Optional) Fügen Sie basierend auf Ihren Protokollabfrage-Ergebnissen weitere Widgets hinzu.

   a. Wählen Sie Add widget aus.

   b. Wählen Sie einen Widget-Typ aus, z. B. Linie.



c. Wählen Sie im Fenster Zu diesem Dashboard hinzufügen die Option Protokolle aus.

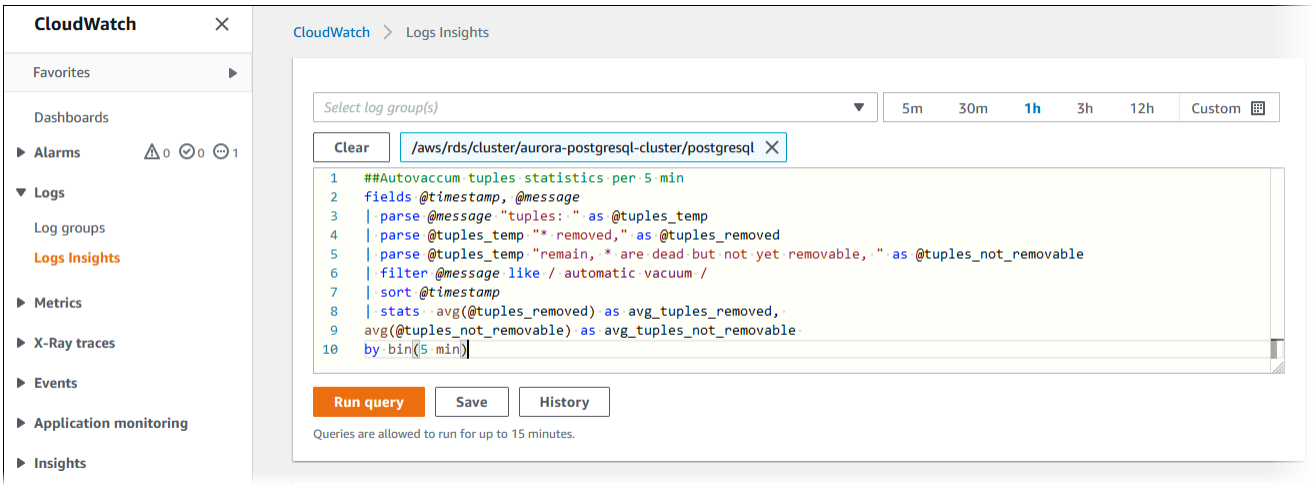


d. Wählen Sie unter Select log group(s) die Protokollgruppe für Ihren DB-Cluster aus.

e. Löschen Sie im Abfrage-Editor die aktuell angezeigte Abfrage und geben Sie Folgendes ein. Wählen Sie anschließend Run query aus.

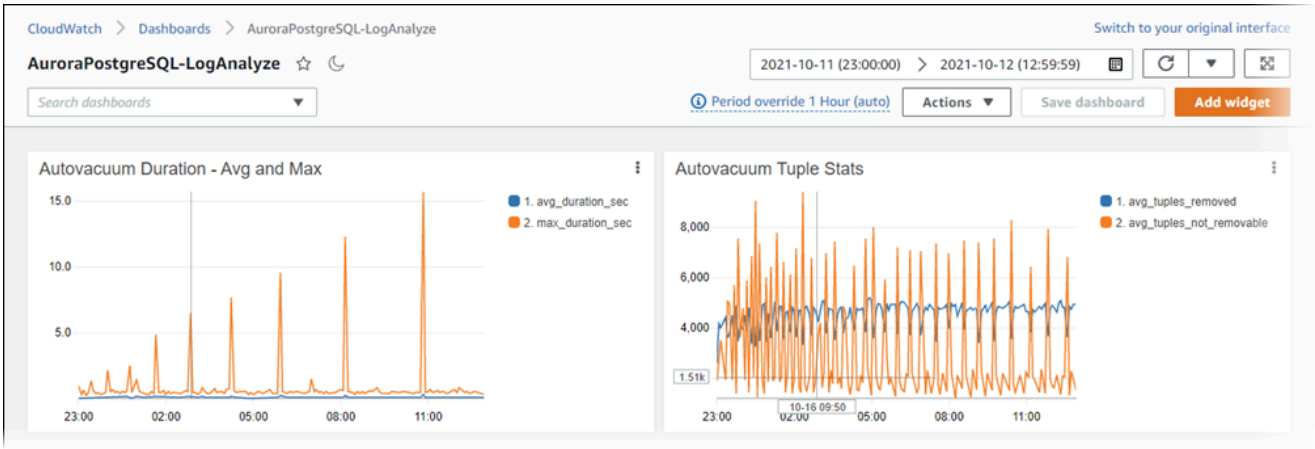
```
##Autovacuum tuples statistics per 5 min
fields @timestamp, @message
| parse @message "tuples: " as @tuples_temp
```

```
| parse @tuples_temp "* removed," as @tuples_removed
| parse @tuples_temp "remain, * are dead but not yet removable, " as
 @tuples_not_removable
| filter @message like / automatic vacuum /
| sort @timestamp
| stats  avg(@tuples_removed) as avg_tuples_removed,
avg(@tuples_not_removable) as avg_tuples_not_removable
by bin(5 min)
```



f. Wählen Sie Create widget aus.

Ihr Dashboard sollte folgender Abbildung ähnlich sein.



Überwachen von Abfrageausführungsplänen für Aurora PostgreSQL

Sie können Abfrageausführungspläne in Ihrer DB-Instance von Aurora PostgreSQL überwachen, um die Ausführungspläne zu erkennen, die zur aktuellen Datenbanklast beitragen, und Leistungsstatistiken von Ausführungsplänen im Laufe der Zeit mithilfe des `aurora_compute_plan_id` Parameters zu verfolgen. Bei jeder Ausführung einer Abfrage wird dem von der Abfrage verwendeten Ausführungsplan eine Kennung zugewiesen und dieselbe Kennung wird von nachfolgenden Ausführungen desselben Plans verwendet.

Die `aurora_compute_plan_id` ist standardmäßig in der DB-Parametergruppe von Aurora PostgreSQL Version 14.10, 15.5 und höheren Versionen aktiviert. Die Zuweisung einer Plan-ID ist ein Standardverhalten und kann deaktiviert werden, indem in der Parametergruppe `aurora_compute_plan_id` auf OFF gesetzt wird.

Diese Plankennung wird in mehreren Dienstprogrammen verwendet, die einen anderen Zweck erfüllen.

Themen

Zugreifen auf Abfrageausführungspläne mithilfe von Aurora-Funktionen

Mit können `aurora_compute_plan_id`Sie mit den folgenden Funktionen auf die Ausführungspläne zugreifen:

- aurora_stat_activity
- aurora_stat_plans

Weitere Informationen zu diesen Funktionen finden Sie unter Aurora-PostgreSQL-Funktionsreferenz.

Parameterreferenz für Aurora-PostgreSQL-Abfrageausführungspläne

Sie können die Abfrageausführungspläne mit den folgenden Parametern in einer DB-Parametergruppe überwachen.

Parameter

- aurora_compute_plan_id
- aurora_stat_plans.minutes_until_recapture
- aurora_stat_plans.calls_until_recapture
- aurora_stat_plans.with_costs
- aurora_stat_plans.with_analyze
- aurora_stat_plans.with_timing
- aurora_stat_plans.with_buffers
- aurora_stat_plans.with_wal
- aurora_stat_plans.with_triggers

> **Note**
>
> Die Konfiguration für `aurora_stat_plans.with_*` Parameter wird nur für neu erfasste Pläne wirksam.

aurora_compute_plan_id

Setzen Sie auf `off`, um zu verhindern, dass eine Plan-ID zugewiesen wird.

Standard	Zulässige Werte	Beschreibung
on	0 (aus)	Setzen Sie auf `off`, um zu verhindern, dass eine Plan-ID zugewiesen wird.
	1 (ein)	Legen Sie den Wert auf feston, um eine Plan-ID zuzuweisen.

aurora_stat_plans.minutes_until_recapture

Die Anzahl der Minuten, die vergehen sollen, bevor ein Plan erneut erfasst wird. Der Standardwert ist 0, wodurch die erneute Erfassung eines Plans deaktiviert wird. Wenn der `aurora_stat_plans.calls_until_recapture` Schwellenwert überschritten wird, wird der Plan erneut erfasst.

Standard	Zulässige Werte	Beschreibung
0	0-1073741823	Legen Sie die Anzahl der Minuten fest, die vergehen sollen, bevor ein Plan erneut erfasst wird.

aurora_stat_plans.calls_until_recapture

Die Anzahl der Aufrufe an einen Plan, bevor er erneut erfasst wird. Der Standardwert ist 0, wodurch die erneute Erfassung eines Plans nach einer Reihe von Aufrufen deaktiviert wird. Wenn der `aurora_stat_plans.minutes_until_recapture` Schwellenwert überschritten wird, wird der Plan erneut erfasst.

Standard	Zulässige Werte	Beschreibung
0	0-1073741823	Legen Sie die Anzahl der Aufrufe fest, bevor ein Plan erneut erfasst wird.

aurora_stat_plans.with_costs

Erfasst einen EXPLAIN-Plan mit geschätzten Kosten. Die zulässigen Werte sind on und `off`. Der Standardwert ist on.

Standard	Zulässige Werte	Beschreibung
on	0 (aus)	Zeigt nicht die geschätzten Kosten und Zeilen für jeden Planknoten an.
	1 (ein)	Zeigt die geschätzten Kosten und Zeilen für jeden Planknoten an.

aurora_stat_plans.with_analyze

Steuert den EXPLAIN-Plan mit ANALYZE. Dieser Modus wird nur verwendet, wenn ein Plan zum ersten Mal erfasst wird. Die zulässigen Werte sind on und `off`. Der Standardwert ist `off`.

Standard	Zulässige Werte	Beschreibung
aus	0 (aus)	Enthält keine tatsächlichen Laufzeitstatistiken für den Plan.
	1 (ein)	Enthält tatsächliche Laufzeitstatistiken für den Plan.

aurora_stat_plans.with_timing

Das Plan-Timing wird in der Erläuterung erfasst, wann ANALYZE verwendet wird. Der Standardwert ist on.

Standard	Zulässige Werte	Beschreibung
on	0 (aus)	Enthält nicht die tatsächliche Startzeit und die aufgewendete Zeit in jedem Planknoten.
	1 (ein)	Enthält die tatsächliche Startzeit und die auf jeden Planknoten aufgewendete Zeit.

aurora_stat_plans.with_buffers

Nutzungsstatistiken für den Planpuffer werden in der Erläuterung erfasst, wann ANALYZE verwendet wird. Der Standardwert ist `off`.

Standard	Zulässige Werte	Beschreibung
aus	0 (aus)	Enthält keine Informationen zur Puffernutzung.
	1 (ein)	Enthält Informationen zur Puffernutzung.

aurora_stat_plans.with_wal

Statistiken zur Plannutzung werden in der Erläuterung erfasst, wann ANALYZE verwendet wird. Der Standardwert ist `off`.

Standard	Zulässige Werte	Beschreibung
aus	0 (aus)	Enthält keine Informationen zur Generierung von WAL-Daten sätzen.
	1 (ein)	Enthält Informationen zur Generierung von WAL-Datensätzen.

aurora_stat_plans.with_triggers

Die Ausführungsstatistiken für den Planauslöser werden in der Erläuterung erfasst, wann verwendet `ANALYZE` wird. Der Standardwert ist `off`.

Standard	Zulässige Werte	Beschreibung
aus	0 (aus)	Enthält keine Ausführungsstatistiken für Auslöser.
	1 (ein)	Enthält Ausführungsstatistiken für Auslöser.

Verwalten von Abfrageausführungsplänen für Aurora PostgreSQL

Die Abfrageplanverwaltung in Aurora PostgreSQL ist eine optionale Funktion, die Sie mit Ihrem DB-Cluster der mit Amazon Aurora PostgreSQL kompatiblen Edition verwenden können. Diese Funktion ist als `apg_plan_mgmt`-Erweiterung verpackt, die Sie in Ihrem DB-Cluster von Aurora PostgreSQL installieren können. Die Abfrageplanverwaltung ermöglicht Ihnen, die Abfrageausführungspläne zu verwalten, die vom Optimierer für Ihre SQL-Anwendungen generiert wurden. Die AWS-Erweiterung `apg_plan_mgmt` baut auf der nativen Abfrageverarbeitungsfunktionalität der PostgreSQL-Datenbank-Engine auf.

Im Folgenden finden Sie Informationen zu den Funktionen der Abfrageplanverwaltung in Aurora PostgreSQL sowie deren Einrichtung und Verwendung mit Ihrem DB-Cluster von Aurora PostgreSQL. Bevor Sie beginnen, sollten Sie alle Versionshinweise für die spezifische Version der `apg_plan_mgmt`-Erweiterung zu lesen, die für Ihre Aurora-PostgreSQL-Version verfügbar ist. Weitere Informationen finden Sie unter Versionen der apg_plan_mgmt-Erweiterung von Aurora PostgreSQL in den Versionshinweisen für Aurora PostgreSQL.

Themen

Übersicht über die Abfrageplanverwaltung in Aurora PostgreSQL

Die Aurora-PostgreSQL-Abfrageplanverwaltung wurde entwickelt, um die Planstabilität unabhängig von Änderungen an der Datenbank zu gewährleisten, die eine Regression des Abfrageplans verursachen könnten. Eine Regression des Abfrageplans tritt auf, wenn der Optimierer nach System- oder Datenbankänderungen einen suboptimalen Plan für eine bestimmte SQL-Anweisung auswählt. Änderungen von Statistiken, Einschränkungen, Umgebungseinstellungen, Abfrageparameter-

Bindungen und Upgrades der PostgreSQL-Datenbank-Engine können eine Planregression verursachen.

Mit der Abfrageplanverwaltung in Aurora PostgreSQL steuern Sie, wie und wann sich Abfrageausführungspläne ändern. Zu den Vorteilen der Abfrageplanverwaltung in Aurora PostgreSQL gehören die nachfolgend aufgeführten.

- Verbesserung der Planstabilität, indem der Optimierer zur Auswahl aus einer kleinen Anzahl bekannter, bewährter Pläne gezwungen wird.
- Zentrale Optimierung von Plänen, gefolgt von einer globalen Verteilung der besten Pläne.
- Ermittlung von nicht verwendeten Indizes und Bewertung der Auswirkungen einer Indexerstellung oder -löschung.
- Automatische Erkennung eines vom Optimierer ermittelten Minimalkostenplans.
- Test neuer Optimierer-Funktionen mit geringerem Risiko, da Sie nur die Planänderungen genehmigen können, die zu Performance-Steigerungen führen.

Sie können die von der Abfrageplanverwaltung bereitgestellten Tools proaktiv verwenden, um den besten Plan für bestimmte Abfragen festzulegen. Sie können die Abfrageplanverwaltung auch verwenden, um auf sich ändernde Umstände zu reagieren und Planregressionen zu vermeiden. Weitere Informationen finden Sie unter Bewährte Methoden für die Aurora-PostgreSQL-Abfrageplanverwaltung.

Themen

Unterstützte SQL-Anweisungen

Die Abfrageplanverwaltung unterstützt die folgenden Typen von SQL-Anweisungen.

- SELECT-, INSERT-, UPDATE- oder DELETE-Anweisungen, unabhängig von ihrer Komplexität.
- Vorbereitete Anweisungen. Weitere Informationen finden Sie unter PREPARE in der PostgreSQL-Dokumentation.
- Dynamische Anweisungen, einschließlich solcher, die im Sofortmodus ausgeführt werden. Weitere Informationen finden Sie unter Dynamisches SQL und EXECUTE IMMEDIATE in der PostgreSQL-Dokumentation.
- Eingebettete SQL-Befehle und -Anweisungen. Weitere Informationen finden Sie unter Eingebettete SQL-Befehle in der PostgreSQL-Dokumentation.
- Anweisungen innerhalb benannter Funktionen. Weitere Informationen finden Sie im Abschnitt CREATE FUNCTION der PostgreSQL-Dokumentation.
- Anweisungen, die temporäre Tabellen enthalten.
- Anweisungen innerhalb von Prozeduren und DO-Blöcken.

Sie können die Abfrageplanverwaltung mit `EXPLAIN` im manuellen Modus verwenden, um einen Plan zu erfassen, ohne ihn tatsächlich auszuführen. Weitere Informationen finden Sie unter Analysieren des vom Optimierer ausgewählten Plans. Weitere Informationen zu den Modi der Abfrageplanverwaltung (manuell, automatisch) finden Sie unter Erfassung von Aurora PostgreSQL-Ausführungsplänen.

Die Abfrageplanverwaltung in Aurora PostgreSQL unterstützt sämtliche PostgreSQL-Sprachfunktionen, darunter partitionierte Tabellen, Vererbung, Sicherheit auf Zeilenebene und rekursive allgemeine Tabellenausdrücke (CTEs). Weitere Informationen zu diesen PostgreSQL-Sprachfunktionen finden Sie unter Table Partitioning (Tabellenpartitionierung), Row Security Policies (Zeilensicherheitsrichtlinien) und WITH Queries (Common Table Expressions) (WITH-Abfragen (allgemeine Tabellenausdrücke)) und anderen Themen in der PostgreSQL-Dokumentation.

Informationen zu den verschiedenen Versionen der Abfrageplanverwaltung von Aurora PostgreSQL finden Sie unter Versionen der apg_plan_mgmt-Erweiterung in den Versionshinweisen für Aurora PostgreSQL.

Einschränkungen der Abfrageplanverwaltung

Die aktuelle Version der Abfrageplanverwaltung von Aurora PostgreSQL unterliegt folgenden Einschränkungen.

- Pläne werden nicht für Anweisungen erfasst, die auf Systembeziehungen verweisen – Anweisungen, die auf Systembeziehungen verweisen, wie z. B. `pg_class`, werden nicht erfasst.

Dies ist beabsichtigt, um zu verhindern, dass eine große Anzahl von systemgenerierten Plänen, die intern verwendet werden, erfasst werden. Dies gilt auch für Systemtabellen innerhalb von Ansichten.

- Für Ihren DB-Cluster von Aurora PostgreSQL ist möglicherweise eine größere DB-Instance-Klasse erforderlich – Je nach Workload erfordert die Abfrageplanverwaltung möglicherweise eine DB-Instance-Klasse mit mehr als 2 vCPUs. Die Anzahl von `max_worker_processes` ist durch die Größe der DB-Instance-Klasse begrenzt. Die Anzahl von `max_worker_processes`, die von einer 2-vCPU-DB-Instance-Klasse (z. B. db.t3.medium) bereitgestellt wird, ist möglicherweise für eine bestimmte Workload nicht ausreichend. Wir empfehlen Ihnen, bei Verwendung der Abfrageplanverwaltung eine DB-Instance-Klasse mit mehr als 2 vCPUs für Ihren DB-Cluster von Aurora PostgreSQL auszuwählen.

  Wenn die DB-Instance-Klasse Ihre Workload nicht unterstützen kann, gibt die Abfrageplanverwaltung eine Fehlermeldung wie die folgende aus.

  ```
  WARNING: could not register plan insert background process
  HINT: You may need to increase max_worker_processes.
  ```

  In diesem Fall sollten Sie Ihren DB-Cluster von Aurora PostgreSQL auf eine DB-Instance-Klassengröße mit mehr Speicher hochskalieren. Weitere Informationen finden Sie unter Unterstützte DB-Engines für DB-Instance-Klassen.
- Pläne, die bereits in Sitzungen gespeichert sind, sind nicht betroffen. – Die Abfrageplanverwaltung bietet eine Möglichkeit, Abfragepläne zu beeinflussen, ohne den Anwendungscode ändern zu müssen. Wenn jedoch ein generischer Plan bereits in einer vorhandenen Sitzung gespeichert ist und Sie den Abfrageplan ändern möchten, müssen Sie zunächst `plan_cache_mode` in der DB-Cluster-Parametergruppe auf `force_custom_plan` setzen.
- `queryid` in `apg_plan_mgmt.dba_plans` und `pg_stat_statements` kann in folgenden Fällen abweichen:
  - Objekte werden nach dem Speichern in apg_plan_mgmt.dba_plans gelöscht und neu erstellt.
  - Die Tabelle `apg_plan_mgmt.plans` wird aus einem anderen Cluster importiert.

Informationen zu den verschiedenen Versionen der Abfrageplanverwaltung von Aurora PostgreSQL finden Sie unter Versionen der apg_plan_mgmt-Erweiterung in den Versionshinweisen für Aurora PostgreSQL.

Terminologie der Abfrageplanverwaltung

Die folgenden Begriffe werden in diesem Thema verwendet.

verwaltete Anweisung

Eine SQL-Anweisung, die vom Optimierer im Rahmen der Abfrageplanverwaltung erfasst wurde. Eine verwaltete Anweisung verfügt über einen oder mehrere Abfrageausführungspläne, die in der `apg_plan_mgmt.dba_plans`-Ansicht gespeichert sind.

Plan-Baseline

Die Menge der genehmigten Pläne für eine bestimmte verwaltete Anweisung. Das heißt, alle Pläne für die verwaltete Anweisung, für die in der `status`-Spalte der `dba_plan`-Ansicht „Approved“ angegeben ist.

Planverlauf

Die Menge der erfassten Pläne für eine bestimmte verwaltete Anweisung. Der Planverlauf enthält alle Pläne, die für die Anweisung erfasst wurden, unabhängig vom Status.

Abfrageplanregression

Tritt auf, wenn der Optimierer einen weniger optimalen Plan als vor einer bestimmten Änderung an der Datenbankumgebung auswählt, z. B. eine neue PostgreSQL-Version oder Änderungen an Statistiken.

Die Abfrageplanverwaltung in Aurora-PostgreSQL-Versionen

Die Abfrageplanverwaltung wird von allen derzeit verfügbaren Aurora-PostgreSQL-Versionen unterstützt. Weitere Informationen finden Sie unter Aktualisierungen von Amazon Aurora PostgreSQL im Abschnitt Versionshinweise für Aurora PostgreSQL.

Die Funktion für die Abfrageplanverwaltung wird Ihrem DB-Cluster von Aurora PostgreSQL hinzugefügt, wenn Sie die `apg_plan_mgmt`-Erweiterung installieren. Verschiedene Versionen von Aurora PostgreSQL unterstützen unterschiedliche Versionen der `apg_plan_mgmt`-Erweiterung. Wir empfehlen Ihnen, die Erweiterung für die Abfrageplanverwaltung auf die neueste Version für Ihre Version von Aurora PostgreSQL zu aktualisieren.

> **Note**
>
> Versionshinweise für die Versionen jeder `apg_plan_mgmt`-Erweiterung finden Sie unter Aurora PostgreSQL apg_plan_mgmt extension versions (Versionen der apg_plan_mgmgmt-Erweiterung von Aurora PostgreSQL) in den Release Notes for Aurora PostgreSQL (Versionshinweisen für Aurora PostgreSQL).

Sie können die auf Ihrem Cluster ausgeführte Version identifizieren, indem Sie mit `psql` eine Verbindung mit einer Instance herstellen und den Metabefehl \dx verwenden, um Erweiterungen aufzulisten, wie nachfolgend gezeigt.

```
labdb=> \dx
                       List of installed extensions
     Name      | Version |    Schema     |                            Description
---------------+---------+---------------
+-------------------------------------------------------------------
 apg_plan_mgmt | 1.0     | apg_plan_mgmt | Amazon Aurora with PostgreSQL compatibility
 Query Plan Management
 plpgsql       | 1.0     | pg_catalog    | PL/pgSQL procedural language
(2 rows)
```

Die Ausgabe zeigt, dass dieser Cluster die Version 1.0 der Erweiterung verwendet. Für eine bestimmte Aurora-PostgreSQL-Version sind nur bestimmte `apg_plan_mgmt`-Versionen verfügbar. In einigen Fällen müssen Sie möglicherweise den DB-Cluster von Aurora PostgreSQL auf eine neue Nebenversion aktualisieren oder einen Patch anwenden, damit Sie ein Upgrade auf die neueste Version der Abfrageplanverwaltung durchführen können. Die in der Ausgabe angezeigte `apg_plan_mgmt`-Version 1.0 stammt von einem DB-Cluster von Aurora-PostgreSQL-Version 10.17, für den keine neuere `apg_plan_mgmt`-Version verfügbar ist. In diesem Fall sollte der DB-Cluster von Aurora PostgreSQL auf eine neuere Version von PostgreSQL aktualisiert werden.

Weitere Informationen über die Aktualisierung Ihres DB-Clusters von Aurora PostgreSQL auf eine neue PostgreSQL-Version finden Sie unter Amazon Aurora PostgreSQL-Aktualisierungen.

Informationen zum Upgrade der `apg_plan_mgmt`-Erweiterung finden Sie unter Aktualisieren der Abfrageplanverwaltung in Aurora PostgreSQL.

Aktivieren der Abfrageplanverwaltung in Aurora PostgreSQL

Das Einrichten der Abfrageplanverwaltung für Ihren DB-Cluster von Aurora PostgreSQL umfasst die Installation einer Erweiterung und das Ändern mehrerer DB-Cluster-Parametereinstellungen. Sie benötigen `rds_superuser`-Berechtigungen, um die `apg_plan_mgmt`-Erweiterung zu installieren und die Funktion für den DB-Cluster von Aurora PostgreSQL zu aktivieren.

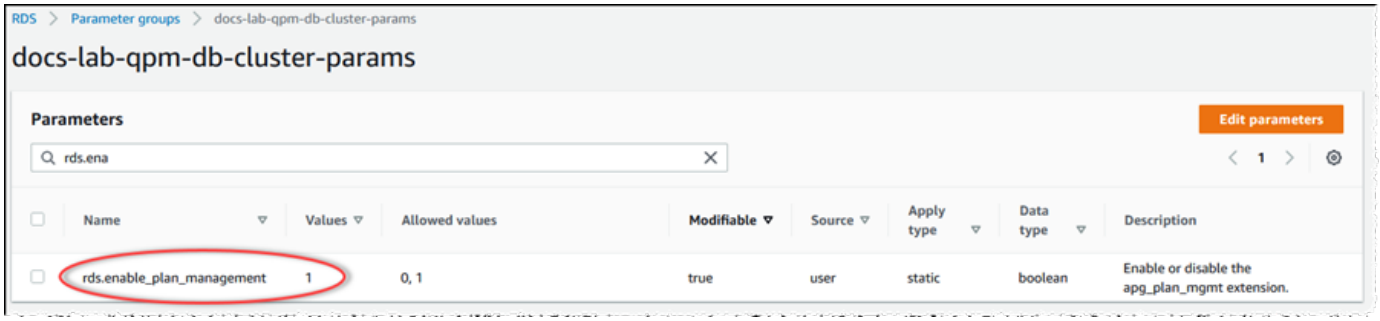
Durch die Installation der Erweiterung wird eine neue Rolle, `apg_plan_mgmt`, erstellt. Diese Rolle ermöglicht Datenbankbenutzern, Abfragepläne anzuzeigen, zu verwalten und zu pflegen. Als Administrator mit `rds_superuser`-Berechtigungen müssen Sie die `apg_plan_mgmt`-Rolle Datenbankbenutzern nach Bedarf zuweisen.

Nur Benutzer mit der `rds_superuser`-Rolle können den folgenden Vorgang ausführen. `rds_superuser` ist erforderlich, um die Erweiterung `apg_plan_mgmt` und die zugehörige Rolle `apg_plan_mgmt` zu erstellen. Benutzer benötigen die Rolle `apg_plan_mgmt` zur Verwaltung der Erweiterung `apg_plan_mgmt`.

So aktivieren Sie die Abfrageplanverwaltung für Ihren DB-Cluster von Aurora PostgreSQL

Mit den folgenden Schritten wird die Abfrageplanverwaltung für alle SQL-Anweisungen aktiviert, die an den DB-Cluster von Aurora PostgreSQL übermittelt werden. Dies wird als automatischer Modus bezeichnet. Weitere Informationen zum Unterschied zwischen den Modi finden Sie unter Erfassung von Aurora PostgreSQL-Ausführungsplänen.

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Erstellen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe für Ihren DB-Cluster von Aurora PostgreSQL. Sie müssen bestimmte Parameter ändern, um die Abfrageplanverwaltung zu aktivieren und ihr Verhalten festzulegen. Weitere Informationen finden Sie unter Erstellen einer DB-Parametergruppe.
3. Öffnen Sie die benutzerdefinierte DB-Cluster-Parametergruppe und legen Sie den `rds.enable_plan_management`-Parameter auf 1 fest, wie in der folgenden Abbildung gezeigt.



Weitere Informationen finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe.

4. Erstellen Sie eine benutzerdefinierte DB-Parametergruppe, mit der Sie Abfrageplanparameter auf Instance-Ebene festlegen können. Weitere Informationen finden Sie unter Erstellen einer DB-Cluster-Parametergruppe.
5. Ändern Sie die Writer-Instance des DB-Clusters von Aurora PostgreSQL, um die benutzerdefinierte DB-Parametergruppe zu verwenden. Weitere Informationen finden Sie unter Ändern einer DB-Instance in einem DB-Cluster.
6. Ändern Sie den DB-Cluster von Aurora PostgreSQL, um die benutzerdefinierte DB-Parametergruppe zu verwenden. Weitere Informationen finden Sie unter Ändern des DB-Clusters über die Konsole, die CLI und die API.
7. Starten Sie Ihre DB-Instance neu, um die Einstellungen der benutzerdefinierten Parametergruppe zu aktivieren.
8. Stellen Sie eine Verbindung mit dem DB-Instance-Endpunkt Ihres DB-Clusters von Aurora PostgreSQL mit `psql` oder `pgAdmin` her. Im folgenden Beispiel wird das `postgres`-Standardkonto für die `rds_superuser`-Rolle verwendet.

```
psql --host=cluster-instance-1.111122223333.aws-region.rds.amazonaws.com --
port=5432 --username=postgres --password --dbname=my-db
```

9. Erstellen Sie die `apg_plan_mgmt`-Erweiterung für Ihre DB-Instance, wie nachfolgend gezeigt.

```
labdb=> CREATE EXTENSION apg_plan_mgmt;
CREATE EXTENSION
```

> **Tip**
>
> Installieren Sie die `apg_plan_mgmt`-Erweiterung in der Vorlagendatenbank für Ihre Anwendung. Der Name der Standard-Vorlagendatenbank lautet `template1`. Weitere

Informationen finden Sie unter Template Databases (Vorlagendatenbanken) in der PostgreSQL-Dokumentation.

10. Ändern Sie den Parameter `apg_plan_mgmt.capture_plan_baselines` in `automatic`. Diese Einstellung veranlasst den Optimierer, Pläne für jede SQL-Anweisung zu generieren, die entweder geplant oder mindestens zweimal ausgeführt wird.

> **Note**
>
> Die Abfrageplanverwaltung verfügt auch über einen manuellen Modus, den Sie für bestimmte SQL-Anweisungen verwenden können. Weitere Informationen hierzu finden Sie unter Erfassung von Aurora PostgreSQL-Ausführungsplänen.

11. Ändern Sie den Wert des `apg_plan_mgmt.use_plan_baselines`-Parameters in „on“. Dieser Parameter veranlasst den Optimierer, einen Plan für die Anweisung aus der Plan-Baseline auszuwählen. Weitere Informationen hierzu finden Sie unter Verwenden von Aurora PostgreSQL-Plänen.

> **Note**
>
> Sie können den Wert eines dieser dynamischen Parameter für die Sitzung ändern, ohne die Instance neu starten zu müssen.

Wenn die Einrichtung der Abfrageplanverwaltung abgeschlossen ist, müssen Sie die `apg_plan_mgmt`-Rolle allen Datenbankbenutzern zuweisen, die Abfragepläne anzeigen, verwalten oder pflegen müssen.

Aktualisieren der Abfrageplanverwaltung in Aurora PostgreSQL

Wir empfehlen Ihnen, die Erweiterung für die Abfrageplanverwaltung auf die neueste Version für Ihre Version von Aurora PostgreSQL zu aktualisieren.

1. Stellen Sie eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL als Benutzer mit `rds_superuser`-Berechtigungen her. Wenn Sie beim Einrichten Ihrer Instance den Standardnamen beibehalten haben, stellen Sie eine Verbindung als `postgres` her. In diesem Beispiel wird die Verwendung von `psql` gezeigt, Sie können jedoch auch pgAdmin verwenden, wenn Sie möchten.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password
```

2. Führen Sie die folgende Abfrage aus, um die Erweiterung zu aktualisieren.

```
ALTER EXTENSION apg_plan_mgmt UPDATE TO '2.1';
```

3. Verwenden Sie die Funktion apg_plan_mgmt.validate_plans, um die Hashes aller Pläne zu aktualisieren. Der Optimierer validiert alle genehmigten, nicht genehmigten und abgelehnten Pläne, um sicherzustellen, dass es sich weiterhin um durchführbare Pläne für die neue Version der Erweiterung handelt.

```
SELECT apg_plan_mgmt.validate_plans('update_plan_hash');
```

   Weitere Informationen zu dieser Funktion finden Sie unter Validieren von Plänen.

4. Verwenden Sie die Funktion apg_plan_mgmt.reload, um alle Pläne im gemeinsam genutzten Arbeitsspeicher mit den validierten Plänen aus der dba_plans-Ansicht zu aktualisieren.

```
SELECT apg_plan_mgmt.reload();
```

Weitere Informationen zu allen Funktionen, die für die Abfrageplanverwaltung verfügbar sind, finden Sie unter Funktionsreferenz für die Aurora-PostgreSQL-Abfrageplanverwaltung.

Deaktivieren der Abfrageplanverwaltung in Aurora PostgreSQL

Sie können die Abfrageplanverwaltung jederzeit deaktivieren, indem Sie die `apg_plan_mgmt.use_plan_baselines` und `apg_plan_mgmt.capture_plan_baselines` deaktivieren.

```
labdb=> SET apg_plan_mgmt.use_plan_baselines = off;

labdb=> SET apg_plan_mgmt.capture_plan_baselines = off;
```

Bewährte Methoden für die Aurora-PostgreSQL-Abfrageplanverwaltung

Mit der Abfrageplanverwaltung steuern Sie, wie und wann sich Abfrageverwaltungspläne ändern. Als DBA gehören zu Ihren Hauptzielen bei der Verwendung von QPM, Regressionen bei Änderungen

an Ihrer Datenbank zu verhindern und zu kontrollieren, ob der Optimierer einen neuen Plan verwenden darf. Im Folgenden finden Sie einige empfohlene bewährte Methoden zur Verwendung der Abfrageplanverwaltung. Proaktive und reaktive Planverwaltungsansätze unterscheiden sich hinsichtlich der Frage, wie und wann neue Pläne zur Verwendung genehmigt werden.

Inhalt

Proaktive Planverwaltung zur Vermeidung von Performancerückgängen

Um Regressionen bei der Planleistung zu verhindern, entwickeln Sie den Basisplan weiter. Dazu führen Sie ein Verfahren aus, das die Leistung neu entdeckter Pläne mit der Leistung des vorhandenen Basisplans der genehmigten Pläne vergleicht und dann automatisch die schnellsten Pläne als neuen Basisplan genehmigt. Auf diese Weise verbessert sich die Ausgangsbasis der Pläne im Laufe der Zeit, da schnellere Pläne entdeckt werden.

1. Bestimmen Sie in einer Entwicklungsumgebung die SQL-Anweisungen, die die größten Auswirkungen auf die Performance oder den Durchsatz des Systems haben. Erfassen Sie dann die Pläne für diese Anweisungen anhand der unter Manuelles Erfassen von Plänen für bestimmte SQL-Anweisungen und Automatisches Erfassen von Plänen beschriebenen Vorgehensweise.
2. Exportieren Sie die erfassten Pläne aus der Entwicklungsumgebung und importieren Sie sie in die Produktionsumgebung. Weitere Informationen finden Sie unter Exportieren und Importieren von Plänen.
3. Führen Sie in der Produktion Ihre Anwendung aus und erzwingen Sie die Verwendung genehmigter verwalteter Pläne. Weitere Informationen finden Sie unter Verwenden von Aurora PostgreSQL-Plänen. Fügen Sie bei laufender Anwendung auch neue Pläne hinzu, sobald diese vom Optimierer erkannt werden. Weitere Informationen finden Sie unter Automatisches Erfassen von Plänen.
4. Analysieren Sie die nicht genehmigten Pläne und genehmigen Sie jene, die ordnungsgemäß funktionieren. Weitere Informationen finden Sie unter Auswerten der Performance von Plänen.
5. Während Ihre Anwendung ausgeführt wird, verwendet der Optimierer die neuen Pläne bei Bedarf.

Sicherstellen der Planstabilität nach einem größeren Versions-Upgrade

Jede Hauptversion von PostgreSQL enthält Verbesserungen und Änderungen am Abfrageoptimierer, die auf eine Leistungssteigerung ausgelegt sind. Pläne zur Abfrageausführung, die in früheren Versionen vom Optimierer generiert wurden, können jedoch in neueren, aktualisierten Versionen zu Leistungseinbußen führen. Sie können das Abfrageplan-Management verwenden, um diese Leistungsprobleme zu beheben und die Planstabilität nach einem größeren Versions-Upgrade sicherzustellen.

Der Optimierer verwendet immer den kostengünstigsten genehmigten Plan, auch wenn mehr als ein genehmigter Plan für die gleiche Anweisung vorhanden ist. Nach einem Upgrade ermittelt der Optimierer möglicherweise neue Pläne, diese werden jedoch als nicht genehmigte Pläne gespeichert. Diese Pläne werden nur ausgeführt, wenn sie im reaktiven Planverwaltungsstil mit dem Parameter unapproved_plan_execution_threshold genehmigt wurden. Sie können die Planstabilität maximieren, indem Sie den proaktiven Planverwaltungsstil mit dem Parameter evolve_plan_baselines verwenden. Dadurch werden die Leistung der neuen Pläne mit den alten Plänen verglichen und Pläne genehmigt oder abgelehnt, die mindestens 10 % schneller sind als der nächstbeste Plan.

Nach dem Upgrade können Sie die Funktion `evolve_plan_baselines` verwenden, um die Planleistung vor und nach dem Upgrade mit Ihren Abfrageparameter-Bindungen zu vergleichen. Die folgenden Schritte gehen davon aus, dass Sie genehmigte verwaltete Pläne in Ihrer Produktionsumgebung verwendet haben, wie in Verwenden von Aurora PostgreSQL-Plänen ausgeführt.

1. Führen Sie Ihre Anwendung vor dem Upgrade mit dem laufenden Abfrageplan-Manager aus. Fügen Sie bei laufender Anwendung neue Pläne hinzu, sobald diese vom Optimierer erkannt werden. Weitere Informationen finden Sie unter Automatisches Erfassen von Plänen.
2. Bewerten Sie die Leistung jedes Plans. Weitere Informationen finden Sie unter Auswerten der Performance von Plänen.
3. Analysieren Sie nach dem Upgrade Ihre genehmigten Pläne erneut mit der Funktion `evolve_plan_baselines`. Vergleichen Sie die Leistung vor und nach der Verwendung Ihrer Abfrageparameter-Bindungen. Wenn der neue Plan schnell ist, können Sie ihn zu Ihren genehmigten Plänen hinzufügen. Wenn er für dieselben Parameter-Bindungen schneller als ein anderer Plan ist, können Sie den langsameren Plan als „Rejected“ (Abgelehnt) markieren.

   Weitere Informationen finden Sie unter Genehmigen besserer Pläne. Referenzinformationen zu dieser Funktion finden Sie unter apg_plan_mgmt.evolve_plan_baselines.

Weitere Informationen finden Sie unter Sicherstellen einer konsistenten Leistung nach größeren Versions-Upgrades mit der Abfrageplanverwaltung der PostgreSQL-kompatiblen Edition von Amazon Aurora.

> **Note**
>
> Wenn Sie ein Upgrade der Hauptversion mithilfe der logischen Replikation oder mit AWS DMS durchführen, stellen Sie sicher, dass Sie das Schema `apg_plan_mgmt` replizieren, damit die vorhandenen Pläne auf die aktualisierte Instance kopiert werden. Weitere Informationen zur logischen Replikation finden Sie unter Verwenden der logischen Replikation, um ein Hauptversions-Upgrade für Aurora PostgreSQL durchzuführen.

Reaktive Planverwaltung zur Erkennung und Behebung von Performancerückgängen

Durch Überwachen Ihrer laufende Anwendung können Sie Pläne erkennen, die zu Performancerückgängen führen. Werden Rückgänge erkannt, können Sie die nicht funktionierenden Pläne manuell ablehnen oder reparieren. Führen Sie dazu die folgenden Schritte aus:

1. Erzwingen Sie bei laufender Anwendung die Verwendung verwalteter Pläne und fügen Sie automatisch neu entdeckte Pläne als nicht genehmigte Pläne hinzu. Weitere Informationen erhalten Sie unter Verwenden von Aurora PostgreSQL-Plänen und Automatisches Erfassen von Plänen.
2. Überwachen Sie die laufende Anwendung auf Performance-Regressionen.
3. Setzen Sie den Status des Plans auf , wenn Sie eine Planregression feststelle `rejected`. Wenn der Optimierer die SQL-Anweisung das nächste Mal ausführt, wird der abgelehnte Plan automatisch ignoriert und stattdessen ein anderer genehmigter Plan verwendet. Weitere Informationen finden Sie unter Ablehnen oder Deaktivieren langsamerer Pläne.

   In einigen Fällen ist es möglicherweise sinnvoll, einen nicht funktionierenden Plan zu reparieren, anstatt ihn abzulehnen, zu deaktivieren oder zu löschen. Verwenden Sie die Erweiterung `pg_hint_plan`, um das Verbessern eines Plans zu testen. Mit `pg_hint_plan` nutzen Sie besondere Kommentare, um die üblicherweise vom Optimierer angewendete Planerstellungsmethode zu überschreiben. Weitere Informationen finden Sie unter Reparieren von Plänen mit pg_hint_plan.

Grundlagen zur Abfrageplanverwaltung in Aurora PostgreSQL

Wenn die Abfrageplanverwaltung für Ihren DB-Cluster von Aurora PostgreSQL aktiviert ist, generiert und speichert der Optimierer Abfrageausführungspläne für jede SQL-Anweisung, die er mehr als einmal verarbeitet. Der Status des zuerst generierten Plans einer verwalteten Anweisung wird vom Optimierer immer auf`Approved` festgelegt und in der `dba_plans`-Ansicht gespeichert.

Der Satz an genehmigten Plänen, der für eine verwaltete Anweisung gespeichert wird, wird als Plan-Baseline bezeichnet. Während der Ausführung Ihrer Anwendung generiert der Optimierer möglicherweise zusätzliche Pläne für verwaltete Anweisungen. Der Status zusätzlich erfasster Pläne wird vom Optimierer auf `Unapproved` festgelegt.

Später können Sie entscheiden, ob die `Unapproved`-Pläne ordnungsgemäß funktionieren und ihren Status bei Bedarf in `Approved`, `Rejected` oder `Preferred` ändern. Dazu verwenden Sie die Funktion `apg_plan_mgmt.evolve_plan_baselines` oder `apg_plan_mgmt.set_plan_status`.

Wenn der Optimierer einen Plan für eine SQL-Anweisung generiert, speichert die Abfrageplanverwaltung den Plan in der `apg_plan_mgmt.plans`-Tabelle. Datenbankbenutzer, denen die `apg_plan_mgmt`-Rolle zugewiesen wurde, können die Plandetails anzeigen, indem sie die `apg_plan_mgmt.dba_plans`-Ansicht abfragen. Die folgende Abfrage listet beispielsweise Details zu Plänen auf, die sich derzeit in der Ansicht für einen DB-Cluster von Aurora PostgreSQL außerhalb der Produktion befinden.

- `sql_hash`: Ein Bezeichner für die SQL-Anweisung, der der Hashwert für den normalisierten Text der SQL-Anweisung ist.
- `plan_hash`: Ein eindeutiger Bezeichner für den Plan, der eine Kombination aus dem `sql_hash` und einem Hash des Plans ist.
- `status`: der Status des Plans Der Optimierer kann einen genehmigten Plan ausführen.
- `enabled`: Gibt an, ob der Plan einsatzbereit ist (true) oder nicht (false).
- `plan_outline`: Eine Darstellung des Plans, mit der der tatsächliche Ausführungsplan neu erstellt wird. Operatoren in der Baumstruktur werden Operatoren in der EXPLAIN-Ausgabe zugeordnet.

Die `apg_plan_mgmt.dba_plans`-Ansicht hat viele weitere Spalten, die alle Details des Plans enthalten, z. B. wann der Plan zuletzt verwendet wurde. Vollständige Details finden Sie unter Referenz für die apg_plan_mgmt.dba_plans-Ansicht.

Normalisierung und der SQL-Hash

In der `apg_plan_mgmt.dba_plans`-Ansicht können Sie eine verwaltete Anweisung anhand ihres SQL-Hash-Werts erkennen. Der SQL-Hash wird auf Basis einer normalisierten Darstellung der SQL-Anweisung berechnet, bei der einige Unterschiede (z. B. Literalwerte) nicht berücksichtigt sind.

Beim Normalisierungsprozess für jede SQL-Anweisung werden Leerzeichen und Groß- und Kleinschreibung beibehalten, sodass Sie das Wesentliche der SQL-Anweisung weiterhin lesen und verstehen können. Durch die Normalisierung werden die folgenden Elemente entfernt oder ersetzt.

- Führende Blockkommentare
- Das Schlüsselwort EXPLAIN und EXPLAIN-Optionen sowie EXPLAIN ANALYZE
- Leerzeichen am Zeilenende
- Alle Literale

Sehen Sie sich die folgende Anweisung als Beispiel an.

```
/*Leading comment*/ EXPLAIN SELECT /* Query 1 */ * FROM t WHERE x > 7 AND y = 1;
```

Der Optimierer normalisiert diese Anweisung wie im Folgenden gezeigt.

```
SELECT /* Query 1 */ * FROM t WHERE x > CONST AND y = CONST;
```

Durch die Normalisierung kann derselbe SQL-Hash für ähnliche SQL-Anweisungen verwendet werden, die sich ggf. ausschließlich in ihren Literal- oder Parameterwerten unterscheiden. Mit anderen Worten, es können mehrere Pläne für denselben SQL-Hash existieren, wobei ein anderer Plan unter anderen Bedingungen optimal ist.

> **Note**
>
> Eine einzelne SQL-Anweisung, die mit verschiedenen Schemas verwendet wird, hat unterschiedliche Pläne, da sie an das spezifische Schema zur Laufzeit gebunden ist. Der Planer verwendet die Statistiken für die Schemabindung, um den optimalen Plan auszuwählen.

Weitere Informationen dazu, wie der Optimierer den Plan auswählt, finden Sie unter Verwenden von Aurora PostgreSQL-Plänen. In diesem Abschnitt erfahren Sie, wie Sie einen Plan mit `EXPLAIN`

und `EXPLAIN ANALYZE` in der Vorschau anzeigen, bevor er tatsächlich verwendet wird. Details hierzu finden Sie unter Analysieren des vom Optimierer ausgewählten Plans. Ein Abbildung, die den Prozess zur Auswahl eines Plans beschreibt, finden Sie unter Erfahren Sie, wie der Optimierer bestimmt, welche Pläne ausgeführt werden..

Erfassung von Aurora PostgreSQL-Ausführungsplänen

Die Aurora-PostgreSQL-Abfrageplanverwaltung bietet zwei verschiedene Modi zum Erfassen von Abfrageausführungsplänen: automatisch oder manuell. Sie wählen den Modus aus, indem Sie den Wert `apg_plan_mgmt.capture_plans_baselines` auf `automatic` oder `manual` festlegen. Sie können Ausführungspläne für bestimmte SQL-Anweisungen mit der manuellen Planerfassung erfassen. Alternativ können Sie mit der automatischen Planerfassung alle (oder nur die langsamsten) Pläne erfassen, die bei laufender Anwendung mindestens zwei Mal ausgeführt werden.

Bei der Planerfassung wird der Status des zuerst erfassten Plans einer verwalteten Anweisung vom Optimierer auf gesetz `approved`. Der Status zusätzlich hinzugefügter Pläne, die für eine verwaltete Anweisung erfasst wurden, wird vom Optimierer auf festgeleg `unapproved`. Gelegentlich wird jedoch mehr als ein Plan möglicherweise mit dem Status `approved` gespeichert. Dies kann passieren, wenn für eine Anweisung mehrere Pläne gleichzeitig erstellt werden und der erste Plan für die Anweisung noch nicht übermittelt wurde.

Legen Sie den Parameter `dba_plans` in der Parametergruppe der DB-Instance-Ebene fest, um die maximale Anzahl an Plänen zu bestimmen, die in der `apg_plan_mgmt.max_plans`-Ansicht erfasst und gespeichert werden können. Damit der Parameter `apg_plan_mgmt.max_plans` geändert werden und ein neuer Wert übernommen werden kann, muss die DB-Instance neu gestartet werden. Informieren Sie sich über den Parameter apg_plan_mgmt.max_plans, um weitere Informationen hierzu zu erhalten.

Manuelles Erfassen von Plänen für bestimmte SQL-Anweisungen

Wenn Sie einen bekannten Satz an SQL-Anweisungen verwalten, verschieben Sie die Anweisungen in eine SQL-Skriptdatei und erfassen Sie anschließend Pläne manuell. Im folgenden psql-Beispiel wird gezeigt, wie Abfragepläne für einen Satz an SQL-Anweisungen manuell erfasst werden.

```
psql> SET apg_plan_mgmt.capture_plan_baselines = manual;
psql> \i my-statements.sql
psql> SET apg_plan_mgmt.capture_plan_baselines = off;
```

Nachdem für jede SQL-Anweisung ein Plan erfasst wurde, fügt der Optimierer der `apg_plan_mgmt.dba_plans`-Ansicht eine neue Zeile hinzu.

Wir empfehlen, dass Sie in der SQL-Skriptdatei entweder EXPLAN- oder EXPLAIN EXECUTE-Anweisungen verwenden. Stellen Sie sicher, dass eine ausreichende Auswahl an Parameterwerten einzukalkulieren, damit alle relevanten Pläne erfasst werden.

Falls Sie einen besseren Plan als den Minimalkostenplan des Optimierers nutzen möchten, können Sie den Optimierer zur Verwendung dieses bevorzugten Plans zwingen, indem Sie einen oder mehrere Optimierungshinweise angeben. Geben Sie hierzu mindestens einen Optimierungshinweis an. Weitere Informationen finden Sie unter Reparieren von Plänen mit pg_hint_plan. Unter `unapproved` erfahren Sie, wie Sie die Performance der `approved`- und Auswerten der Performance von Plänen-Pläne vergleichen und diese genehmigen, ablehnen oder löschen.

Automatisches Erfassen von Plänen

Verwenden Sie die automatische Planerfassung u. a. in den folgenden Fällen:

- Sie wissen nicht, welche spezifischen SQL-Anweisungen Sie verwalten möchten.
- Sie müssen hunderte oder tausende von SQL-Anweisungen verwalten.
- Ihre Anwendung verwendet eine Client-API. Beispielsweise verwendet JDBC unbenannte vorbereitete Anweisungen oder Anweisungen in großen Mengen, die in psql nicht wiedergegeben werden können.

So erfassen Sie Pläne automatisch:

1. Aktivieren Sie die automatische Planerfassung, indem Sie in der Parametergruppe der DB-Instance-Ebene `apg_plan_mgmt.capture_plan_baselines` auf `automatic` setzen. Weitere Informationen finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.
2. Starten Sie Ihre DB-Instance neu.
3. Während der Ausführung der Anwendung erfasst der Optimierer Pläne für alle SQL-Anweisungen, die mindestens zwei Mal ausgeführt werden.

   Wenn die Anwendung mit den standardmäßigen Parametereinstellungen für die Abfrageplanverwaltung ausgeführt wird, erfasst der Optimierer Pläne für alle SQL-Anweisungen, die mindestens zwei Mal ausgeführt werden. Das Erfassen aller Pläne mit den Standardeinstellungen ist mit einem sehr geringen Laufzeitaufwand verbunden und kann in der Produktivumgebung erfolgen.

So deaktivieren Sie die automatische Planerfassung:

- Setzen Sie in der Parametergruppe der DB-Instance-Ebene den Parameter `apg_plan_mgmt.capture_plan_baselines` auf `off`.

Erfahren Sie unter , wie Sie die Performance der nicht genehmigten Pläne messen und diese Pläne genehmigen, ablehnen oder lösche Auswerten der Performance von Plänen.

Verwenden von Aurora PostgreSQL-Plänen

Setzen Sie den Parameter `apg_plan_mgmt.use_plan_baselines` auf `true`, damit der Optimierer erfasste Pläne für Ihre verwalteten Anweisungen verwendet. Im Folgenden wird ein Beispiel mit einer lokalen Instance gezeigt:

```
SET apg_plan_mgmt.use_plan_baselines = true;
```

Diese Einstellung führt bei laufender Anwendung dazu, dass der Optimierer für jede verwaltete Anweisung jenen kostengünstigsten, bevorzugten oder genehmigten Plan verwendet, der gültig und aktiviert ist.

Analysieren des vom Optimierer ausgewählten Plans

Wenn der Parameter `apg_plan_mgmt.use_plan_baselines` auf `true` gesetzt ist, können Sie mit SQL-Anweisungen vom Typ EXPLAIN ANALYZE erfahren, welchen Plan der Optimierer zum Ausführen der Anweisung auswählen würde. Im Folgenden wird ein Beispiel gezeigt.

```
EXPLAIN ANALYZE EXECUTE rangeQuery (1,10000);
```

```
                                                        QUERY PLAN
-----------------------------------------------------------------------------
 Aggregate  (cost=393.29..393.30 rows=1 width=8) (actual time=7.251..7.251 rows=1
 loops=1)
   ->  Index Only Scan using t1_pkey on t1 t  (cost=0.29..368.29 rows=10000 width=0)
 (actual time=0.061..4.859 rows=10000 loops=1)
Index Cond: ((id >= 1) AND (id <= 10000))
         Heap Fetches: 10000
 Planning time: 1.408 ms
 Execution time: 7.291 ms
 Note: An Approved plan was used instead of the minimum cost plan.
 SQL Hash: 1984047223, Plan Hash: 512153379
```

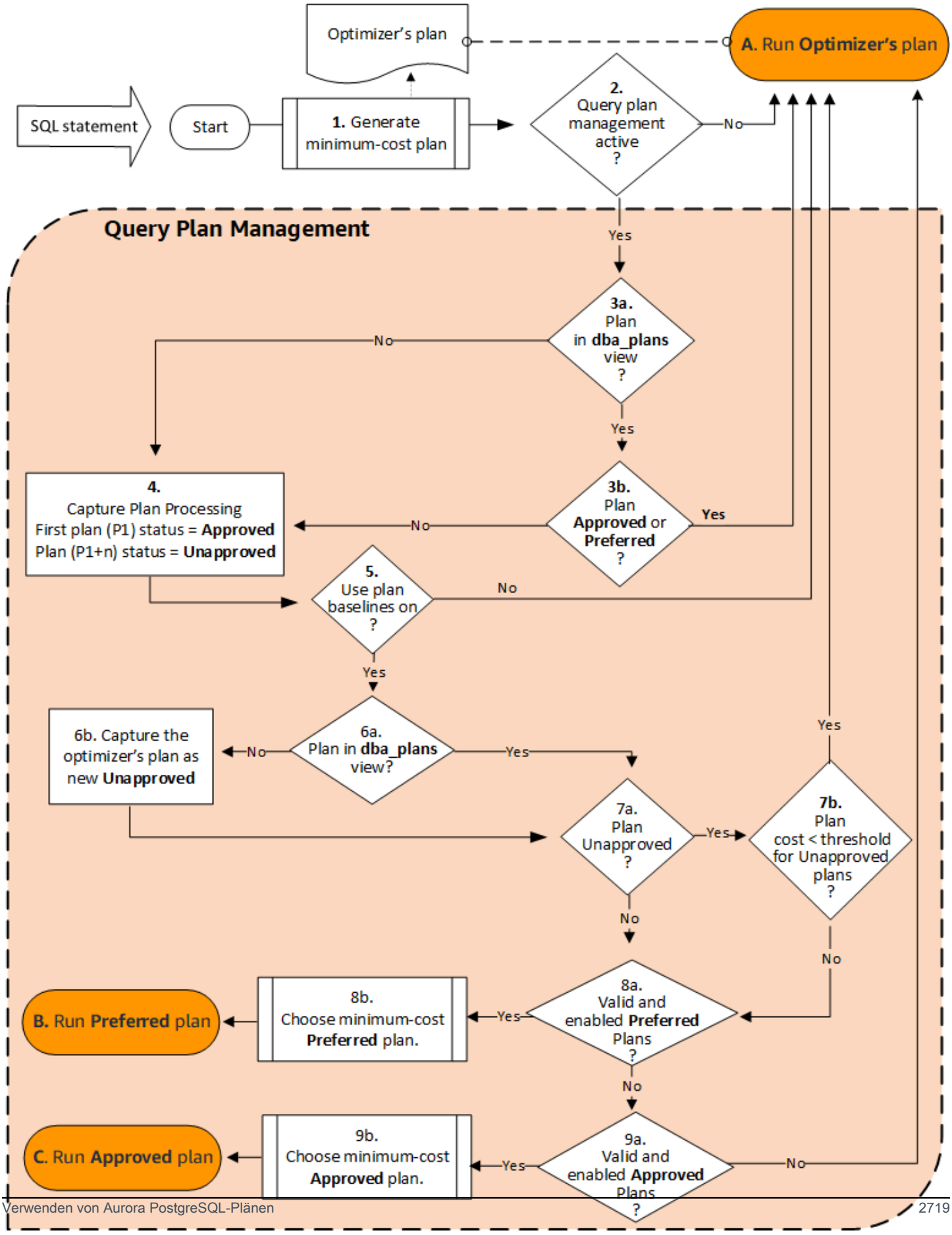
Die Ausgabe zeigt den genehmigten Plan aus der Baseline, der ausgeführt werden würde. Die Ergebnisse zeigen jedoch auch, dass ein kostengünstigerer Plan gefunden wurde. In diesem Fall erfassen Sie diesen neuen Minimalkostenplan, indem Sie die unter beschriebene automatische Planerfassung aktiviere Automatisches Erfassen von Plänen.

Neue Pläne werden vom Optimierer immer als `Unapproved` erfasst. Mit der Funktion `apg_plan_mgmt.evolve_plan_baselines` vergleichen Sie Pläne und können deren Status zu „Genehmigt“, „Abgelehnt“ oder „Deaktiviert“ ändern. Weitere Informationen finden Sie unter Auswerten der Performance von Plänen.

Erfahren Sie, wie der Optimierer bestimmt, welche Pläne ausgeführt werden.

Die Kosten für einen Ausführungsplan stellen eine Schätzung dar, die der Optimierer zum Vergleichen verschiedener Pläne durchführt. Bei der Berechnung der Kosten eines Plans berücksichtigt der Optimierer Faktoren wie CPU- und I/O-Vorgänge, die für diesen Plan erforderlich sind. Um mehr über Kostenschätzungen des PostgreSQL-Abfrageplaners zu erfahren, lesen Sie bitte Query Planning (Abfrageplanung) in der PostgreSQL-Dokumentation.

Die folgende Abbildung zeigt, wie ein Plan für eine bestimmte SQL-Anweisung ausgewählt wird, wenn die Abfrageplanverwaltung aktiv und nicht aktiv ist.


Optimizer's plan
A. Run Optimizer's plan
SQL statement
Start
1. Generate minimum-cost plan
2. Query plan management active ?
No
Query Plan Management
Yes
3a. Plan in dba_plans view ?
No
Yes
4. Capture Plan Processing
First plan (P1) status = Approved
Plan (P1+n) status = Unapproved
3b. Plan Approved or Preferred ?
No
Yes
5. Use plan baselines on ?
No
Yes
6a. Plan in dba_plans view?
No
Yes
6b. Capture the optimizer's plan as new Unapproved
7a. Plan Unapproved ?
Yes
7b. Plan cost < threshold for Unapproved plans ?
Yes
No
No
8a. Valid and enabled Preferred Plans ?
Yes
8b. Choose minimum-cost Preferred plan.
B. Run Preferred plan
No
9a. Valid and enabled Approved Plans ?
Yes
9b. Choose minimum-cost Approved plan.
C. Run Approved plan
No

Der Ablauf ist wie folgt:

1. Der Optimierer erstellt einen Minimalkostenplan für die SQL-Anweisung.
2. Wenn die Abfrageplanverwaltung nicht aktiv ist, wird der Plan des Optimierers sofort ausgeführt (A. Optimizer-Plan ausführen). Die Abfrageplanverwaltung ist inaktiv, wenn die `apg_plan_mgmt.capture_plan_baselines` und `apg_plan_mgmt.use_plan_baselines`-Parameter beide ihre Standardeinstellungen haben („off“ bzw. „false“).

   Andernfalls ist die Abfrageplanverwaltung aktiv. In diesem Fall werden die SQL-Anweisung und der Plan des Optimierers dafür weiter bewertet, bevor ein Plan ausgewählt wird.

   > **Tip**
   >
   > Datenbankbenutzer mit der `apg_plan_mgmt`-Rolle können proaktiv Pläne vergleichen, den Status von Plänen ändern und die Verwendung bestimmter Pläne nach Bedarf erzwingen. Weitere Informationen finden Sie unter Pflege der Aurora-PostgreSQL-Ausführungspläne.

3. Die SQL-Anweisung enthält möglicherweise bereits Pläne, die in der Vergangenheit von der Abfrageplanverwaltung gespeichert wurden. Pläne werden in der `apg_plan_mgmt.dba_plans` aufbewahrt, zusammen mit Informationen über die SQL-Anweisungen, mit denen sie erstellt wurden. Informationen zu einem Plan beinhalten seinen Status. Der Status eines Plans kann wie folgt bestimmen, ob er verwendet wird oder nicht.
   a. Wenn der Plan nicht zu den gespeicherten Plänen für die SQL-Anweisung gehört, bedeutet dies, dass dieser spezielle Plan zum ersten Mal vom Optimierer für die angegebene SQL-Anweisung generiert wurde. Der Plan wird an die Erfassungsplanverarbeitung gesendet (4).
   b. Wenn der Plan zu den gespeicherten Plänen gehört und sein Status Genehmigt oder Bevorzugt ist, wird der Plan ausgeführt (A. Optimizer-Plan ausführen).

      Wenn der Plan zu den gespeicherten Plänen gehört, aber weder Genehmigt noch Bevorzugt ist, wird der Plan an die Erfassungsplanverarbeitung gesendet (4).
4. Wenn ein Plan zum ersten Mal für eine bestimmte SQL-Anweisung erfasst wird, wird der Status des Plans immer auf Genehmigt (P1) gesetzt. Wenn der Optimierer anschließend denselben Plan für dieselbe SQL-Anweisung generiert, wird der Status dieses Plans in Nicht genehmigt (P1+n) geändert.

Nachdem der Plan erfasst und sein Status aktualisiert wurde, wird die Bewertung im nächsten Schritt fortgesetzt (5).

5. Die Baseline eines Plans besteht aus der Historie der SQL-Anweisung und ihrer Pläne in verschiedenen Stadien. Die Abfrageplanverwaltung kann den Basisplan bei der Auswahl eines Plans berücksichtigen, je nachdem, ob die Option Plan-Baselines verwenden aktiviert ist oder nicht, wie folgt.
   - Plan-Baselines ist „Aus“ verwenden, wenn der `apg_plan_mgmt.use_plan_baselines`-Parameter auf den Standardwert (`false`) gesetzt ist. Der Plan wird nicht mit der Baseline verglichen, bevor er ausgeführt wird (A. Optimizer-Plan ausführen).
   - Plan-Baselines ist „Ein“ verwenden, wenn der `apg_plan_mgmt.use_plan_baselines`-Parameter auf den Standardwert (`true`) gesetzt ist. Der Plan wird anhand der Basislinie weiter bewertet (6).
6. Der Plan wird mit anderen Plänen für den Kontoauszug in der Basislinie verglichen.
   a. Wenn der Plan des Optimierers zu den Plänen in der Baseline gehört, wird sein Status überprüft (7a).
   b. Befindet sich der Plan des Optimierers nicht unter den Plänen in der Baseline, wird der Plan als neuer `Unapproved`-Plan zu den Plänen für die Anweisung hinzugefügt.
7. Der Status des Plans wird überprüft, um nur festzustellen, ob er nicht genehmigt ist.
   a. Wenn der Status des Plans Nicht genehmigt lautet, werden die geschätzten Kosten des Plans mit der Kostenschätzung verglichen, die für den Schwellenwert für den nicht genehmigten Ausführungsplan angegeben wurde.
      - Wenn die geschätzten Kosten des Plans unter dem Schwellenwert liegen, verwendet der Optimierer ihn, obwohl es sich um einen nicht genehmigten Plan handelt (A. Optimizer-Plan ausführen). Im Allgemeinen führt der Optimierer keinen nicht genehmigten Plan aus. Wenn der `apg_plan_mgmt.unapproved_plan_execution_threshold`-Parameter jedoch einen Kostenschwellenwert angibt, vergleicht der Optimierer die Kosten des nicht genehmigten Plans mit dem Schwellenwert. Falls die geschätzten Kosten niedriger als der Schwellenwert sind, führt der Optimierer den Plan aus. Weitere Informationen finden Sie unter apg_plan_mgmt.unapproved_plan_execution_threshold.
      - Wenn die geschätzten Kosten des Plans nicht unter dem Schwellenwert liegen, werden die anderen Attribute des Plans überprüft (8a).
   b. Wenn der Status des Plans etwas anderes als Nicht genehmigt ist, werden seine anderen Attribute überprüft (8a).

8. Der Optimierer wird keinen Plan verwenden, der deaktiviert ist. Das heißt, der Plan, dessen `enable`-Attribut auf ‚f' (false) gesetzt ist. Der Optimierer verwendet auch keinen Plan mit dem Status Abgelehnt.

   Der Optimierer kann keine Pläne verwenden, die nicht gültig sind. Pläne können mit der Zeit ungültig werden, wenn die Objekte, von denen sie abhängen, wie Indizes und Tabellenpartitionen, entfernt oder gelöscht werden.

   a. Falls die Anweisung über aktivierte und gültige bevorzugte Pläne verfügt, wählt der Optimierer den kostengünstigsten Plan aus den für diese SQL-Anweisung gespeicherten bevorzugten Plan aus. Der Optimierer führt dann den kostengünstigsten bevorzugten Plan aus.

   b. Wenn die Abrechnung keine aktivierten und gültigen Preferred-Pläne enthält, wird sie im nächsten Schritt bewertet (9).

9. Falls die Anweisung über aktivierte und gültige Genehmigte Pläne verfügt, wählt der Optimierer den kostengünstigsten Plan aus den für diese SQL-Anweisung gespeicherten Genehmigten Plan aus. Der Optimierer führt dann den kostengünstigsten genehmigten Plan aus.

   Wenn die Abrechnung keine gültigen und aktivierten Genehmigten Pläne enthält, verwendet der Optimierer den Mindestkostenplan (A. Optimierer-Plan ausführen).

Untersuchen von Aurora PostgreSQL-Abfrageplänen in der dba_plans-Ansicht

Datenbankbenutzer und Administratoren, denen die `apg_plan_mgmt`-Rolle zugewiesen wurde, können die in `apg_plan_mgmt.dba_plans` gespeicherten Pläne anzeigen und verwalten. Der Administrator eines DB-Clusters von Aurora PostgreSQL (ein Benutzer mit `rds_superuser`-Berechtigungen) muss diese Rolle explizit den Datenbankbenutzern zuweisen, die mit der Abfrageplanverwaltung arbeiten müssen.

Die `apg_plan_mgmt`-Ansicht enthält den Planverlauf für alle verwalteten SQL-Anweisungen für jede Datenbank auf der Writer-Instance des DB-Clusters von Aurora PostgreSQL. In dieser Ansicht können Sie Pläne, ihren Status, wann sie zuletzt verwendet wurden und alle anderen relevanten Details untersuchen.

Wie in Normalisierung und der SQL-Hash erörtert, wird jeder verwaltete Plan anhand der Kombination aus einem SQL- und einem Plan-Hash-Wert identifiziert. Mit diesen IDs können Sie Tools wie Amazon RDS-Performance-Insights nutzen, um die Performance einzelner Pläne

nachzuverfolgen. Weitere Informationen über Performance-Insights finden Sie unter Verwenden von Amazon RDS-Performance-Insights.

Auflisten von verwalteten Plänen.

Mit der SELECT-Anweisung in der Ansicht `apg_plan_mgmt.dba_plans` listen Sie die verwalteten Pläne auf. Im folgenden Beispiel werden einige Spalten in der `dba_plans`-Ansicht aufgeführt, so z. B. die Spalte `status`, in der Sie sehen können, ob ein Plan genehmigt oder nicht genehmigt wurde.

```
SELECT sql_hash, plan_hash, status, enabled, stmt_name
FROM apg_plan_mgmt.dba_plans;

 sql_hash   | plan_hash |   status   | enabled | stmt_name
------------+-----------+------------+---------+------------
 1984047223 | 512153379 | Approved   | t       | rangequery
 1984047223 | 512284451 | Unapproved | t       | rangequery
 (2 rows)
```

Zur besseren Lesbarkeit listen die Abfrage und die angezeigte Ausgabe nur einige Spalten aus der `dba_plans`-Ansicht auf. Ausführliche Informationen finden Sie unter Referenz für die apg_plan_mgmt.dba_plans-Ansicht.

Pflege der Aurora-PostgreSQL-Ausführungspläne

Die Abfrageplanverwaltung stellt Techniken und Funktionen zum Hinzufügen, Pflegen und Verbessern von Ausführungsplänen bereit.

Auswerten der Performance von Plänen

Nachdem der Optimierer Pläne als „Nicht genehmigt“ erfasst hat, können Sie mit der Funktion `apg_plan_mgmt.evolve_plan_baselines` Pläne hinsichtlich ihrer tatsächlichen Performance miteinander vergleichen. Je nach Ergebnis dieses Performance-Vergleichs können Sie den Status eines Plans von „Nicht genehmigt“ zu „Genehmigt“ oder „Abgelehnt“ ändern. Alternativ besteht die Möglichkeit, mit der Funktion `apg_plan_mgmt.evolve_plan_baselines` einen Plan auf bestimmte Zeit zu deaktivieren, falls er Ihre Anforderungen nicht erfüllt.

Genehmigen besserer Pläne

Im folgenden Beispiel wird beschrieben, wie der Status verwalteter Pläne mit der Funktion `apg_plan_mgmt.evolve_plan_baselines` auf „Genehmigt“ geändert werden kann.

```
SELECT apg_plan_mgmt.evolve_plan_baselines (
   sql_hash,
   plan_hash,
   min_speedup_factor := 1.0,
   action := 'approve'
)
FROM apg_plan_mgmt.dba_plans WHERE status = 'Unapproved';
```

```
NOTICE:     rangequery (1,10000)
NOTICE:     Baseline   [ Planning time 0.761 ms, Execution time 13.261 ms]
NOTICE:     Baseline+1 [ Planning time 0.204 ms, Execution time 8.956 ms]
NOTICE:     Total time benefit: 4.862 ms, Execution time benefit: 4.305 ms
NOTICE:     Unapproved -> Approved
evolve_plan_baselines
----------------------
0
(1 row)
```

In der Ausgabe wird ein Performance-Bericht für die`rangequery`-Anweisung mit Parameterbindungen von 1 und 10 000 angezeigt. Der neue nicht genehmigte Plan (`Baseline+1`) ist besser als der beste zuvor genehmigte Plan (`Baseline`). Rufen Sie die `Approved`-Ansicht auf, um zu sehen, ob der neue Plan nun den Status „`apg_plan_mgmt.dba_plans`“ aufweist.

```
SELECT sql_hash, plan_hash, status, enabled, stmt_name
FROM apg_plan_mgmt.dba_plans;
```

```
sql_hash  | plan_hash |  status  | enabled | stmt_name
------------+-----------+----------+---------+------------
1984047223 | 512153379 | Approved | t       | rangequery
1984047223 | 512284451 | Approved | t       | rangequery
(2 rows)
```

Der verwaltete Plan enthält jetzt zwei genehmigte Pläne, die zusammen die Plan-Baseline der Anweisung bilden. Sie können auch die Funktion „`apg_plan_mgmt.set_plan_status`“ aufrufen, um das Statusfeld eines Plans direkt auf `'Approved'`, `'Rejected'`, `'Unapproved'` oder `'Preferred'` festzulegen.

Ablehnen oder Deaktivieren langsamerer Pläne

Leiten Sie `'reject'` oder `'disable'` als Aktionsparameter an die Funktion `apg_plan_mgmt.evolve_plan_baselines` weiter, um Pläne abzulehnen oder zu deaktivieren. In diesem Beispiel wird jeder erfasste Plan mit dem Status „`Unapproved`“ deaktiviert, der um mindestens 10 Prozent langsamer als der beste Plan mit dem Status „`Approved`“ der Anweisung ist.

```
SELECT apg_plan_mgmt.evolve_plan_baselines(
sql_hash,  -- The managed statement ID
plan_hash, -- The plan ID
1.1,       -- number of times faster the plan must be
'disable'  -- The action to take. This sets the enabled field to false.
)
FROM apg_plan_mgmt.dba_plans
WHERE status = 'Unapproved' AND   -- plan is Unapproved
origin = 'Automatic';       -- plan was auto-captured
```

Sie können den Status eines Plans auch direkt auf „Abgelehnt“ oder „Deaktiviert“ setzen. Rufen Sie die Funktion `true` auf, um das aktivierte Feld eines Plans direkt auf `false` oder `apg_plan_mgmt.set_plan_enabled` festzulegen. Mit der Funktion „`'Approved'`“ legen Sie das Statusfeld eines Plans direkt auf `'Rejected'`, `'Unapproved'`, `'Preferred'` oder `apg_plan_mgmt.set_plan_status` fest.

Validieren von Plänen

Verwenden Sie die Funktion `apg_plan_mgmt.validate_plans`, um ungültige Pläne zu löschen oder zu deaktivieren.

Pläne können ungültig oder veraltet werden, wenn Objekte entfernt werden, von denen sie abhängig sind (z. B. ein Index oder eine Tabelle). Wenn das entfernte Objekt jedoch erneut erstellt wird, kann ein Plan auch nur für eine bestimmte Zeit ungültig sein. Falls ein ungültiger Plan zu einem späteren Zeitpunkt gültig werden kann, ist es möglicherweise sinnvoller, diesen nicht zu löschen, sondern zu deaktivieren oder einfach nichts zu unternehmen.

Über die Funktion `apg_plan_mgmt.validate_plans` suchen und löschen Sie alle ungültigen und während der vergangenen Woche nicht verwendeten Pläne. Gehen Sie hierzu folgendermaßen vor:

```
SELECT apg_plan_mgmt.validate_plans(sql_hash, plan_hash, 'delete')
```

```
FROM apg_plan_mgmt.dba_plans
WHERE last_used < (current_date - interval '7 days');
```

Verwenden Sie die Funktion `apg_plan_mgmt.set_plan_enabled` zum direkten Aktivieren oder Deaktivieren eines Plans.

Reparieren von Plänen mit pg_hint_plan

Mit dem Abfrageoptimierer kann für jede Anweisung der bestmögliche Plan gefunden werden. In den meisten Fällen findet der Abfrageoptimierer in der Tat einen guten Plan. Manchmal gibt es jedoch einen weitaus besseren als den vom Optimierer erstellten Plan. Um zu gewährleisten, dass der Optimierer einen passenden Plan erstellt, wird zum einen die Verwendung der Erweiterung `pg_hint_plan`, zum anderen die Festlegung der Grand Unified Configuration (GUC)-Variablen in PostgreSQL empfohlen:

- `pg_hint_plan`-Erweiterung – Geben Sie mithilfe der `pg_hint_plan`-Erweiterung von PostgreSQL einen „Hinweis“, um die Arbeitsweise des Planers zu ändern. Informationen zur Installation und Verwendung der `pg_hint_plan`-Erweiterung finden Sie in der pg_hint_plan-Dokumentation.
- GUC-Variablen: Überschreiben Sie einen oder mehrere Kostenmodellparameter oder Parameter des Optimierers, wie z. B. `from_collapse_limit` oder `GEQO_threshold`.

Wenn Sie den Abfrageoptimierer mit einer dieser Methoden zur Verwendung eines Plans zwingen, können Sie auch die Abfrageplanverwaltung nutzen, um den neuen Plan zu erfassen und dessen Anwendung durchzusetzen.

Mit der Erweiterung `pg_hint_plan` können Sie die Join-Reihenfolge, die Join-Methoden oder die Zugriffspfade für eine SQL-Anweisung ändern. Sie nutzen einen SQL-Kommentar mit einer besonderen `pg_hint_plan`-Syntax, um die üblicherweise vom Optimierer angewendete Planerstellungsmethode zu ändern. Angenommen, die entsprechende SQL-Anweisung verfügt über eine Zwei-Wege-Verknüpfung.

```
SELECT *
FROM t1, t2
WHERE t1.id = t2.id;
```

Der Optimierer wählt nun die Join-Reihenfolge (t1, t2) aus. Wir wissen jedoch, dass die Reihenfolge (t2, t1) schneller ist. Der folgende Hinweis zwingt den Optimierer dazu, die schnellere Join-

Reihenfolge (t2, t1) zu wählen. Schließen Sie EXPLAIN ein, damit der Optimierer einen Plan für die SQL-Anweisung generiert, ohne jedoch die Anweisung auszuführen. (Ausgabe wird nicht angezeigt.)

```
/*+ Leading ((t2 t1)) */ EXPLAIN SELECT *
FROM t1, t2
WHERE t1.id = t2.id;
```

Im Folgenden wird beschrieben, wie Sie verwende `pg_hint_plan`.

So ändern und erfassen Sie mit pg_hint_plan den vom Optimierer erstellten Plan:

1. Aktivieren Sie den manuellen Erfassungsmodus.

   ```
   SET apg_plan_mgmt.capture_plan_baselines = manual;
   ```

2. Geben Sie für die entsprechende SQL-Anweisung einen Hinweis an.

   ```
   /*+ Leading ((t2 t1)) */ EXPLAIN SELECT *
   FROM t1, t2
   WHERE t1.id = t2.id;
   ```

   Nach der Ausführung erfasst der Optimierer den Plan in der `apg_plan_mgmt.dba_plans`-Ansicht. Der erfasste Plan berücksichtigt nicht die Syntax des besonderen Kommentars `pg_hint_plan`, weil die Abfrageplanverwaltung die Anweisung durch das Entfernen führender Kommentare normalisiert.

3. Sie können die verwalteten Pläne über die `apg_plan_mgmt.dba_plans`-Ansicht anzeigen.

   ```
   SELECT sql_hash, plan_hash, status, sql_text, plan_outline
   FROM apg_plan_mgmt.dba_plans;
   ```

4. Legen Sie den Status des Plans auf fes `Preferred`. Dadurch wird sichergestellt, dass der Optimierer den Plan ausführt, anstatt ihn aus dem Satz an genehmigten Plänen auszuwählen, wenn der Minimalkostenplan nicht bereits `Approved` oder `Preferred` ist.

   ```
   SELECT apg_plan_mgmt.set_plan_status(sql-hash, plan-hash, 'preferred' );
   ```

5. Deaktivieren Sie die manuelle Planerfassung und erzwingen Sie die Verwendung verwalteter Pläne.

   ```
   SET apg_plan_mgmt.capture_plan_baselines = false;
   ```

```
SET apg_plan_mgmt.use_plan_baselines = true;
```

Während der Ausführung der ursprünglichen SQL-Anweisung wählt der Optimierer einen Plan aus, der entweder `Approved` oder `Preferred` ist. Wenn der Minimalkostenplan weder den Status „`Approved`“ noch „`Preferred`“ aufweist, wählt der Optimierer den Plan mit Status „`Preferred`“ aus.

Löschen von Plänen

Pläne werden automatisch gelöscht, wenn sie seit über einem Monat, genauer gesagt 32 Tagen, nicht mehr verwendet wurden. Dies ist die Standardeinstellung des Parameters `apg_plan_mgmt.plan_retention_period`. Sie können den Aufbewahrungszeitraum des Plans zu einem längeren oder kürzeren Zeitraum ändern, beginnend mit dem Wert 1. Die Bestimmung der Anzahl von Tagen, seit ein Plan zuletzt verwendet wurde, wird berechnet, indem das `last_used`-Datum vom aktuellen Datum abgezogen wird. Das `last_used`-Datum ist das letzte Datum, an dem der Optimierer den Plan als Minimalkostenplan ausgewählt hat oder der Plan ausgeführt wurde. Das Datum wird in der `apg_plan_mgmt.dba_plans`-Ansicht für den Plan gespeichert.

Wir empfehlen Ihnen, Pläne zu löschen, die lange nicht mehr verwendet wurden oder nicht nützlich sind. Jeder Plan verfügt über ein `last_used`-Datum, das vom Optimierer aktualisiert wird, wenn er einen Plan ausführt oder den Plan als Minimalkostenplan für eine Anweisung auswählt. Überprüfen Sie die letzten `last_used`-Daten, um die Pläne zu identifizieren, die Sie ohne Bedenken löschen können.

Die folgende Abfrage gibt eine dreispaltige Tabelle mit der Gesamtanzahl der Pläne, der Anzahl der Pläne, die nicht gelöscht wurden, und der Anzahl der Pläne, die erfolgreich gelöscht wurden, zurück. Sie enthält eine verschachtelte Abfrage, die ein Beispiel dafür ist, wie Sie die `apg_plan_mgmt.delete_plan`-Funktion verwenden, um alle Pläne zu löschen, die in den letzten 31 Tagen nicht als Minimalkostenplan ausgewählt wurden und deren Status nicht `Rejected` lautet.

```
SELECT (SELECT COUNT(*) from apg_plan_mgmt.dba_plans) total_plans,
       COUNT(*) FILTER (WHERE result = -1) failed_to_delete,
       COUNT(*) FILTER (WHERE result = 0) successfully_deleted
       FROM (
            SELECT apg_plan_mgmt.delete_plan(sql_hash, plan_hash) as result
            FROM apg_plan_mgmt.dba_plans
            WHERE last_used < (current_date - interval '31 days')
            AND status <> 'Rejected'
```

```
            ) as dba_plans ;
```

```
 total_plans | failed_to_delete | successfully_deleted
-------------+------------------+----------------------
           3 |                0 |                    2
```

Weitere Informationen finden Sie unter apg_plan_mgmt.delete_plan.

Verwenden Sie die `apg_plan_mgmt.validate_plans`-Funktion, um Pläne zu löschen, die nicht gültig sind und voraussichtlich ungültig bleiben werden. Mit dieser Funktion können Sie ungültige Pläne löschen oder deaktivieren. Weitere Informationen finden Sie unter Validieren von Plänen.

> **Important**
>
> Wenn Sie Ihre irrelevanten Pläne nicht löschen, verfügen Sie möglicherweise über keinen gemeinsam genutzten Speicher mehr, der für die Abfrageplanverwaltung reserviert wird. Mit dem Parameter `apg_plan_mgmt.max_plans` legen Sie fest, wie viel Speicher für verwaltete Pläne zur Verfügung steht. Legen Sie diesen Parameter in der benutzerdefinierten Parametergruppe fest und starten Sie Ihre DB-Instance neu, damit die Änderungen wirksam werden. Informieren Sie sich über den Parameter apg_plan_mgmt.max_plans, um weitere Informationen hierzu zu erhalten.

Exportieren und Importieren von Plänen

Sie können Ihre verwalteten Pläne exportieren und in eine andere DB-Instance importieren.

So exportieren Sie verwaltete Pläne:

Autorisierte Benutzer können ein beliebiges Subset der `apg_plan_mgmt.plans`-Tabelle in eine andere Tabelle kopieren und dann mit dem Befehl `pg_dump` speichern. Im Folgenden wird ein Beispiel gezeigt.

```
CREATE TABLE plans_copy AS SELECT *
FROM apg_plan_mgmt.plans [ WHERE predicates ] ;
```

```
% pg_dump --table apg_plan_mgmt.plans_copy -Ft mysourcedatabase > plans_copy.tar
```

```
DROP TABLE apg_plan_mgmt.plans_copy;
```

So importieren Sie verwaltete Pläne:

1. Kopieren Sie die .tar-Datei der exportierten verwalteten Pläne in das System, in dem die Pläne wiederhergestellt werden sollen.
2. Verwenden Sie den Befehl `pg_restore`, um die .tar-Datei in eine neue Tabelle zu kopieren.

   ```
   % pg_restore --dbname mytargetdatabase -Ft plans_copy.tar
   ```

3. Führen Sie die Tabellen `plans_copy` und `apg_plan_mgmt.plans` entsprechend dem folgenden Beispiel zusammen.

   > **Note**
   >
   > In einigen Fällen verwenden Sie möglicherweise für die Sicherung eine bestimmte Version der Erweiterung `apg_plan_mgmt` und für die Wiederherstellung eine andere Version der Erweiterung. In diesem Fällen fallen die Spalten in der Plantabelle möglicherweise unterschiedlich aus. Geben Sie den Spalten in diesem Fall einen bestimmten Namen, anstatt SELECT* zu verwenden.

   ```
   INSERT INTO apg_plan_mgmt.plans SELECT * FROM plans_copy
    ON CONFLICT ON CONSTRAINT plans_pkey
    DO UPDATE SET
    status = EXCLUDED.status,
    enabled = EXCLUDED.enabled,
    -- Save the most recent last_used date
    --
    last_used = CASE WHEN EXCLUDED.last_used > plans.last_used
    THEN EXCLUDED.last_used ELSE plans.last_used END,
    -- Save statistics gathered by evolve_plan_baselines, if it ran:
    --
    estimated_startup_cost = EXCLUDED.estimated_startup_cost,
    estimated_total_cost = EXCLUDED.estimated_total_cost,
    planning_time_ms = EXCLUDED.planning_time_ms,
    execution_time_ms = EXCLUDED.execution_time_ms,
    total_time_benefit_ms = EXCLUDED.total_time_benefit_ms,
    execution_time_benefit_ms = EXCLUDED.execution_time_benefit_ms;
   ```

4. Laden Sie die verwalteten Pläne erneut in den gemeinsam genutzten Speicher und entfernen Sie die Tabelle für die temporären Pläne.

```
SELECT apg_plan_mgmt.reload(); -- refresh shared memory
DROP TABLE plans_copy;
```

Referenz für die Abfrageplanverwaltung in Aurora PostgreSQL

Im Folgenden finden Sie Referenzinformationen für verschiedene Einstellungen und Funktionen der Abfrageplanverwaltung in Aurora PostgreSQL.

Themen

- Parameterreferenz für Aurora-PostgreSQL-Abfrageplanverwaltung
- Funktionsreferenz für die Aurora-PostgreSQL-Abfrageplanverwaltung
- Referenz für die apg_plan_mgmt.dba_plans-Ansicht

Parameterreferenz für Aurora-PostgreSQL-Abfrageplanverwaltung

Sie können Ihre Einstellungen für die `apg_plan_mgmt`-Erweiterung unter Verwendung der in diesem Abschnitt aufgeführten Parameter vornehmen. Diese sind im benutzerdefinierten DB-Cluster-Parameter und in der DB-Parametergruppe verfügbar, die Ihrem Aurora PostgreSQL DB-Cluster zugeordnet ist. Diese Parameter steuern das Verhalten der Abfrageplanverwaltungsfunktion und deren Auswirkungen auf den Optimierer. Weitere Informationen zum Einrichten einer Abfrageverwaltung finden Sie unter Aktivieren der Abfrageplanverwaltung in Aurora PostgreSQL. Das Ändern der folgenden Parameter hat keine Auswirkung, wenn die `apg_plan_mgmt`-Erweiterung nicht wie in diesem Abschnitt beschrieben eingerichtet ist. Weitere Informationen zum Ändern von Parametern finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe und Arbeiten mit DB-Parametergruppen in einer DB-Instance.

Parameter

- apg_plan_mgmt.capture_plan_baselines
- apg_plan_mgmt.plan_capture_threshold
- apg_plan_mgmt.explain_hashes
- apg_plan_mgmt.log_plan_enforcement_result
- apg_plan_mgmt.max_databases

- apg_plan_mgmt.max_plans
- apg_plan_mgmt.plan_hash_version
- apg_plan_mgmt.plan_retention_period
- apg_plan_mgmt.unapproved_plan_execution_threshold
- apg_plan_mgmt.use_plan_baselines
- auto_explain.hashes

apg_plan_mgmt.capture_plan_baselines

Erfasst Abfrageausführungspläne, die vom Optimierer für jede SQL-Anweisung generiert wurden, und speichert sie im der `dba_plans`-Ansicht. Standardmäßig beträgt die maximale Anzahl von Plänen, die gespeichert werden können, 10.000, wie im `apg_plan_mgmt.max_plans`-Parameter angegeben. Referenzinformationen finden Sie unter apg_plan_mgmt.max_plans.

Sie können diesen Parameter in der benutzerdefinierten DB-Cluster-Parametergruppe oder in der benutzerdefinierten DB-Parametergruppe festlegen. Um den Wert dieses Parameters zu ändern, ist kein Neustart erforderlich.

Standard	Zulässige Werte	Beschreibung
aus	Automatisch	Aktiviert die Planerfassung für alle Datenbanken auf der DB-Instance. Sammelt einen Plan für jede SQL-Anweisung, die mindestens zwei Mal ausgeführt wird. Verwenden Sie diese Einstellung für große oder sich entwickelnde Workloads, um Planstabilität zu gewährleisten.
	Manuell	Aktiviert die Planerfassung nur für nachfolgende Anweisungen, bis Sie sie wieder deaktivieren. Mit dieser Einstellung können Sie Abfrageausführungspläne nur für bestimmte kritische SQL-Anweisungen oder für bekannte problematische Abfragen erfassen.
	aus	Deaktiviert die Planerfassung.

Weitere Informationen finden Sie unter Erfassung von Aurora PostgreSQL-Ausführungsplänen.

apg_plan_mgmt.plan_capture_threshold

Gibt einen Schwellenwert an, sodass der Plan nicht in der Ansicht `apg_plan_mgmt.dba_plans` erfasst wird, wenn die Gesamtkosten des Abfrageausführungsplans unter dem Schwellenwert liegen.

Um den Wert dieses Parameters zu ändern, ist kein Neustart erforderlich.

Standard	Zulässige Werte	Beschreibung
0	0 – 1.79769e+308	Legt den Schwellenwert der Gesamtausführungskosten des Abfrageplans `apg_plan_mgmt` für die Erfassung von Plänen fest.

Weitere Informationen finden Sie unter Untersuchen von Aurora PostgreSQL-Abfrageplänen in der dba_plans-Ansicht.

apg_plan_mgmt.explain_hashes

Gibt an, ob der `EXPLAIN [ANALYZE]` am Ende seiner Ausgabe `sql_hash` und `plan_hash` anzeigt. Um den Wert dieses Parameters zu ändern, ist kein Neustart erforderlich.

Standard	Zulässige Werte	Beschreibung
0	0 (aus)	EXPLAIN zeigt sql_hash und plan_hash ohne die Option true für die Hashes nicht an.
	1 (ein)	EXPLAIN zeigt sql_hash und plan_hash ohne die Option true für die Hashes an.

apg_plan_mgmt.log_plan_enforcement_result

Gibt an, ob die Ergebnisse aufgezeichnet werden müssen, um zu überprüfen, ob die von QPM verwalteten Pläne ordnungsgemäß verwendet werden. Wenn ein gespeicherter generischer Plan verwendet wird, werden keine Datensätze in die Protokolldateien geschrieben. Um den Wert dieses Parameters zu ändern, ist kein Neustart erforderlich.

Standard	Zulässige Werte	Beschreibung
none	none	Zeigt in den Protokolldateien kein Ergebnis der Plandurch setzung an.
	on_error	Zeigt nur das Ergebnis der Plandurchsetzung in Protokolldateien an, wenn QPM keine verwalteten Pläne verwendet.
	all	Zeigt alle Ergebnisse der Plandurchsetzung in Protokolldateien an, einschließlich Erfolgen und Fehlern.

apg_plan_mgmt.max_databases

Gibt die maximale Anzahl an Datenbanken in der Writer-Instance Ihres Aurora-PostgreSQL-Datenbank-Clusters an, die die Abfrageplanverwaltung nutzen können. Standardmäßig können bis zu 10 Datenbanken die Abfrageplanverwaltung verwenden. Wenn die Instance über mehr als 10 Datenbanken verfügt, können Sie den Wert dieser Einstellung ändern. Um herauszufinden, wie viele Datenbanken sich in einer bestimmten Instanz befinden, stellen Sie eine Verbindung mit der Instance über `psql` her. Verwenden Sie dann den psql-Meta-Befehl, `\l`, um die Datenbanken aufzulisten.

Wenn Sie den Wert dieses Parameters ändern, müssen Sie die Instance neu starten, damit die Einstellung wirksam wird.

Standard	Zulässige Werte	Beschreibung
10	10-2147483647	Maximale Anzahl von Datenbanken, die die Abfrageplanverwalt ung auf der Instance verwenden können.

Sie können diesen Parameter in der benutzerdefinierten DB-Cluster-Parametergruppe oder in der benutzerdefinierten DB-Parametergruppe festlegen.

apg_plan_mgmt.max_plans

Legt die maximale Anzahl von SQL-Anweisungen fest, die die Abfrageplanverwaltung in der Ansicht `apg_plan_mgmt.dba_plans` anzeigen kann. Wir empfehlen, diesen Parameter für alle Aurora-PostgreSQL-Versionen auf `10000` oder höher zu setzen.

Sie können diesen Parameter in der benutzerdefinierten DB-Cluster-Parametergruppe oder in der benutzerdefinierten DB-Parametergruppe festlegen. Wenn Sie den Wert dieses Parameters ändern, müssen Sie die Instance neu starten, damit die Einstellung wirksam wird.

Standard	Zulässige Werte	Beschreibung
10000	10-2147483647	Maximale Anzahl von Plänen, die in der `apg_plan_mgmt.dba_plans` -Ansicht gespeichert werden können. Die Standardeinstellung für Aurora-PostgreSQL-Version 10 und älter ist 1000.

Weitere Informationen finden Sie unter Untersuchen von Aurora PostgreSQL-Abfrageplänen in der dba_plans-Ansicht.

apg_plan_mgmt.plan_hash_version

Gibt die Anwendungsfälle an, für die die plan_hash-Berechnung konzipiert ist. Eine höhere Version von `apg_plan_mgmt.plan_hash_version` deckt den gesamten Funktionsumfang der niedrigeren Version ab. Version 3 deckt beispielsweise die von Version 2 unterstützten Anwendungsfälle ab.

Auf die Änderung des Werts dieses Parameters muss ein Aufruf von `apg_plan_mgmt.validate_plans('update_plan_hash')` folgen. Dadurch werden die plan_hash-Werte in jeder Datenbank, in der apg_plan_mgmt installiert ist, und Einträge in der Plantabelle aktualisiert. Weitere Informationen finden Sie unter Validieren von Plänen.

Standard	Zulässige Werte	Beschreibung
1	1	Standardberechnung von plan_hash.
	2	plan_hash-Berechnung für die Unterstützung mehrerer Schemas geändert.
	3	plan_hash-Berechnung für die Unterstützung mehrerer Schemas und Unterstützung partitionierter Tabellen geändert.
	4	plan_hash-Berechnung für parallele Operatoren und zur Unterstützung von Materialisierungsknoten geändert.

apg_plan_mgmt.plan_retention_period

Gibt an, wie viele Tage lang Pläne in der `apg_plan_mgmt.dba_plans`-Ansicht aufbewahrt werden, danach werden sie automatisch gelöscht. Standardmäßig wird ein Plan gelöscht, wenn 32 Tage seit der letzten Verwendung des Plans vergangen sind (Die `last_used`-Spalte in der `apg_plan_mgmt.dba_plans`-Ansicht). Sie können diese Einstellung auf eine beliebige Zahl ändern (1 und höher).

Wenn Sie den Wert dieses Parameters ändern, müssen Sie die Instance neu starten, damit die Einstellung wirksam wird.

Standard	Zulässige Werte	Beschreibung
32	1-2147483647	Maximale Anzahl von Tagen seit der letzten Nutzung eines Plans, bevor er gelöscht wird.

Weitere Informationen finden Sie unter Untersuchen von Aurora PostgreSQL-Abfrageplänen in der dba_plans-Ansicht.

apg_plan_mgmt.unapproved_plan_execution_threshold

Gibt einen Kostenschwellenwert an, unterhalb dessen ein nicht genehmigter Plan vom Optimierer verwendet werden kann. Der Schwellenwert lautet standardmäßig 0, nicht genehmigte Pläne werden vom Optimierer also nicht ausgeführt. Wenn dieser Parameter auf einen belanglos niedrigen Kostenschwellenwert wie 100 gesetzt wird, wird der Overhead für die Plandurchsetzung bei trivialen Plänen vermieden. Sie können diesen Parameter auch unter Verwendung des reaktiven Planverwaltungstils auf einen extrem hohen Wert wie 10000000 festlegen. Auf diese Weise kann der Optimierer alle ausgewählten Pläne ohne Overhead für die Plandurchsetzung verwenden. Wenn jedoch ein fehlerhafter Plan gefunden wird, können Sie diesen manuell als „abgelehnt“ markieren, sodass er beim nächsten Mal nicht verwendet wird.

Der Wert dieses Parameters stellt eine Kostenschätzung für die Ausführung eines bestimmten Plans dar. Wenn ein nicht genehmigter Plan unter diesen geschätzten Kosten liegt, verwendet der Optimierer ihn für die SQL-Anweisung. Sie können erfasste Pläne und ihren Status (Genehmigt, Nicht genehmigt) in der `dba_plans`-Ansicht anzeigen. Weitere Informationen hierzu finden Sie unter Untersuchen von Aurora PostgreSQL-Abfrageplänen in der dba_plans-Ansicht.

Um den Wert dieses Parameters zu ändern, ist kein Neustart erforderlich.

Standard	Zulässige Werte	Beschreibung
0	0-2147483647	Geschätzte Plankosten, unter denen ein nicht genehmigter Plan verwendet wird.

Weitere Informationen finden Sie unter Verwenden von Aurora PostgreSQL-Plänen.

apg_plan_mgmt.use_plan_baselines

Gibt an, dass der Optimierer einen der genehmigten Pläne verwenden soll, der in der `apg_plan_mgmt.dba_plans`-Ansicht erfasst und gespeichert ist. Standardmäßig ist dieser Parameter deaktiviert (false), was dazu führt, dass der Optimierer den von ihm generierten Mindestkostenplan ohne weitere Bewertung verwendet. Wenn Sie diesen Parameter aktivieren (ihn auf true setzen), muss der Optimierer einen Abfrageausführungsplan für die Anweisung aus seiner Plan-Baseline auswählen. Weitere Informationen finden Sie unter Verwenden von Aurora PostgreSQL-Plänen. Ein Bild, das diesen Prozess detailliert beschreibt, finden Sie unter Erfahren Sie, wie der Optimierer bestimmt, welche Pläne ausgeführt werden..

Sie können diesen Parameter in der benutzerdefinierten DB-Cluster-Parametergruppe oder in der benutzerdefinierten DB-Parametergruppe festlegen. Um den Wert dieses Parameters zu ändern, ist kein Neustart erforderlich.

Standard	Zulässige Werte	Beschreibung
false	true	Verwenden Sie einen genehmigten, bevorzugten oder nicht genehmigten Plan aus dem `apg_plan_mgmt.dba_plans` . Wenn keiner von ihnen alle Bewertungskriterien für den Optimierer erfüllt, kann er seinen eigenen generierten Mindestkostenplan verwenden. Weitere Informationen finden Sie unter Erfahren Sie, wie der Optimierer bestimmt, welche Pläne ausgeführt werden..
	false	Verwenden Sie den vom Optimierer generierten Minimalkostenplan.

Sie können die Reaktionszeiten verschiedener erfasster Pläne auswerten und den Planstatus nach Bedarf ändern. Weitere Informationen finden Sie unter Pflege der Aurora-PostgreSQL-Ausführungspläne.

auto_explain.hashes

Gibt an, ob die auto_explain-Ausgabe sql_hash und plan_hash anzeigt. Um den Wert dieses Parameters zu ändern, ist kein Neustart erforderlich.

Standard	Zulässige Werte	Beschreibung
0 (aus)	0 (aus)	Das Ergebnis von `auto_explain` zeigt `sql_hash` und `plan_hash` nicht an.
	1 (ein)	Das Ergebnis von `auto_explain` zeigt `sql_hash` und `plan_hash` an.

Funktionsreferenz für die Aurora-PostgreSQL-Abfrageplanverwaltung

Die Erweiterung `apg_plan_mgmt` stellt die folgenden Funktionen bereit:

Funktionen

- apg_plan_mgmt.copy_outline
- apg_plan_mgmt.delete_plan
- apg_plan_mgmt.evolve_plan_baselines
- apg_plan_mgmt.get_explain_plan
- apg_plan_mgmt.plan_last_used
- apg_plan_mgmt.reload
- apg_plan_mgmt.set_plan_enabled
- apg_plan_mgmt.set_plan_status
- apg_plan_mgmt.update_plans_last_used
- apg_plan_mgmt.validate_plans

apg_plan_mgmt.copy_outline

Kopiert einen bestimmten SQL-Plan-Hash und eine Plangliederung in einen Ziel-SQL-Plan-Hash und eine Gliederung, wodurch der Plan-Hash und die Gliederung des Ziels überschrieben werden. Diese Funktion ist in `apg_plan_mgmt` 2.3 und höheren Versionen verfügbar.

Syntax

```
apg_plan_mgmt.copy_outline(
    source_sql_hash,
    source_plan_hash,
    target_sql_hash,
    target_plan_hash,
    force_update_target_plan_hash
)
```

Rückgabewert

Gibt 0 zurück, wenn das Kopieren erfolgreich ist. Löst Ausnahmen bei ungültigen Eingaben aus.

Parameter

Parameter	Beschreibung
`source_sql_hash`	Die `sql_hash`-ID, die mit `plan_hash` verknüpft ist, um sie in die Zielabfrage zu kopieren.
`source_plan_hash`	Die `plan_hash` -ID, die in die Zielabfrage kopiert werden soll.
`target_sql_hash`	Die `sql_hash`-ID der Abfrage, die mit dem Hash und der Gliederung des Quellplans aktualisiert werden soll.
`target_plan_hash`	Die `plan_hash` -ID der Abfrage, die mit dem Hash und der Gliederung des Quellplans aktualisiert werden soll.
`force_update_target_plan_hash`	(Optional) Die `target_plan_hash` ID der Abfrage wird auch dann aktualisiert, wenn

Parameter	Beschreibung
	der Quellplan für die nicht reproduzierbar ist`target_sql_hash` . Wenn auf „true“ gesetzt, kann die Funktion verwendet werden, um Pläne über Schemata hinweg zu kopieren, in denen Beziehungsnamen und Spalten konsistent sind.

Nutzungshinweise

Mit dieser Funktion können Sie einen Plan-Hash und eine Plangliederung kopieren, die Hinweise auf andere, ähnliche Anweisungen verwendet, und Ihnen so die Verwendung von Inline-Hinweisanweisungen bei jedem Vorkommen in den Zielanweisungen erspart. Wenn die aktualisierte Zielabfrage zu einem ungültigen Plan führt, löst diese Funktion einen Fehler aus und macht den Aktualisierungsversuch rückgängig.

apg_plan_mgmt.delete_plan

Löschen Sie einen verwalteten Plan.

Syntax

```
apg_plan_mgmt.delete_plan(
    sql_hash,
    plan_hash
)
```

Rückgabewert

Gibt bei erfolgreichen Löschvorgängen „0“, bei gescheiterten Löschvorgängen „-1“ zurück.

Parameter

Parameter	Beschreibung
`sql_hash`	Die `sql_hash`-ID der verwalteten SQL-Anweisung des Plans.
`plan_hash`	Die `plan_hash` -ID des verwalteten Plans.

apg_plan_mgmt.evolve_plan_baselines

Dieser Parameter überprüft, ob ein bereits genehmigter Plan oder ein vom Optimierer erkannter Minimalkostenplan schneller ist.

Syntax

```
apg_plan_mgmt.evolve_plan_baselines(
    sql_hash,
    plan_hash,
    min_speedup_factor,
    action
)
```

Rückgabewert

Die Anzahl der Pläne, die nicht schneller als der beste genehmigte Plan waren.

Parameter

Parameter	Beschreibung
`sql_hash`	Die `sql_hash`-ID der verwalteten SQL-Anweisung des Plans.
`plan_hash`	Die `plan_hash` -ID des verwalteten Plans. Verwenden Sie NULL, um alle Pläne mit demselben `sql_hash`-ID-Wert anzugeben.
`min_speed up_factor`	Der Mindestbeschleunigungsfaktor kann angeben, um wie viel schneller ein Plan im Vergleich zum besten der bereits genehmigten Pläne sein muss, um genehmigt zu werden. Alternativ kann dieser Faktor auch angeben, um wie viel langsamer ein Plan sein muss, um abgelehnt oder deaktiviert zu werden. Dieser Wert ist ein positiver Gleitkommawert.
`action`	Bezeichnet die Aktion, die von der Funktion ausgeführt wird. Im Folgenden sind Beispiele für gültige Werte aufgeführt. Die Groß-/Kle inschreibung muss nicht beachtet werden. • `'disable'` – Deaktiviert alle übereinstimmenden Pläne, die die Kriterien des Mindestbeschleunigungsfaktors nicht erfüllen.

Parameter	Beschreibung
	• `'approve'` – Aktiviert alle übereinstimmenden Pläne, die die Kriterien des Mindestbeschleunigungsfaktors erfüllen, und setzt ihren Status auf `approved`. • `'reject'` – Setzt den Status aller übereinstimmenden Pläne, die die Kriterien des Mindestbeschleunigungsfaktors nicht erfüllen, auf `rejected`. • NULL – Die Funktion gibt die Anzahl der Pläne zurück, die zu keiner Performance-Verbesserung führen, weil sie die Kriterien des Mindestbeschleunigungsfaktors nicht erfüllen.

Nutzungshinweise

Je nachdem, ob die kombinierte Planungs- und Ausführungszeit eines Plans kürzer ist als beim schnellsten genehmigten Plan, können Sie anhand eines von Ihnen festlegbaren Faktors den Status bestimmter Pläne auf „Genehmigt“, „Abgelehnt“ oder „Deaktiviert“ setzen. Der Aktionsparameter kann auf `'approve'` oder `'reject'` gesetzt werden, um einen Plan automatisch zu genehmigen oder abzulehnen, wenn er die Performance-Kriterien erfüllt. Alternativ kann auch die Einstellung '' (leere Zeichenfolge) gewählt werden, um den Performance-Vergleich durchzuführen und einen Bericht zu erstellen, wobei in diesem Fall keine Aktion ausgeführt wird.

Sie können vermeiden, dass die Funktion `apg_plan_mgmt.evolve_plan_baselines` bei einem Plan unnötigerweise erneut ausgeführt wird. Dazu schränken Sie die Auswahl der Pläne auf die kürzlich erstellten, nicht genehmigten Pläne ein. Das Ausführen der Funktion `apg_plan_mgmt.evolve_plan_baselines` kann auch vermieden werden, wenn ein genehmigter Plan über einen aktuellen `last_verified`-Zeitstempel verfügt.

Führen Sie einen Performance-Vergleich durch, um die kombinierte Planungs- und Ausführungszeit aller Baseline-Pläne miteinander zu vergleichen. In einigen Fällen gibt es für eine Anweisung nur einen Plan, der dann auch genehmigt wird. Vergleichen Sie in einem solchen Fall die kombinierte Planungs- und Ausführungszeit des Plans mit der kombinierten Planungs- und Ausführungszeit, die sich ergibt, wenn kein Plan verwendet wird.

Der inkrementelle Vorteil (oder Nachteil) aller Pläne wird in der `apg_plan_mgmt.dba_plans`-Ansicht in der Spalte `total_time_benefit_ms` aufgezeichnet. Ist dieser Wert positiv, führt die Aufnahme dieses Plans in die Baseline zu einem messbaren Performance-Vorteil.

Zusätzlich zur Planungs- und Ausführungszeit aller ausgewählten Pläne wird in der Spalte `last_verified` der `apg_plan_mgmt.dba_plans`-Ansicht auch der aktuelle `current_timestamp` angezeigt. Durch den Zeitstempel `last_verified` kann das erneute Ausführen dieser Funktion bei einem Plan vermieden werden, dessen Performance erst kürzlich verifiziert wurde.

apg_plan_mgmt.get_explain_plan

Erzeugt den Text einer `EXPLAIN`-Anweisung für die angegebene SQL-Anweisung.

Syntax

```
apg_plan_mgmt.get_explain_plan(
    sql_hash,
    plan_hash,
    [explainOptionList]
)
```

Rückgabewert

Gibt Laufzeitstatistiken für die angegebenen SQL-Anweisungen zurück. Verwenden ohne `explainOptionList`, um einen einfachen `EXPLAIN`-Plan zurückzugeben.

Parameter

Parameter	Beschreibung
`sql_hash`	Die `sql_hash`-ID der verwalteten SQL-Anweisung des Plans.
`plan_hash`	Die `plan_hash` -ID des verwalteten Plans.
`explainOptionList`	Eine durch Kommas getrennte Liste von Explain-Optionen. Gültige Werte sind `'analyze'` , `'verbose'` , `'buffers'` , `'hashes'` und `'format json'`. Wenn `explainOptionList` NULL ist oder eine leere Zeichenfolge („), generiert diese Funktion eine `EXPLAIN`-Anweisung, ohne irgendwelche Statistiken.

Nutzungshinweise

Für `explainOptionList` können Sie eine der gleichen Optionen verwenden, die Sie mit einer `EXPLAIN`-Anweisung verwenden würden. Der Aurora-PostgreSQL-Optimizer verkettet die Liste der Optionen, die Sie für die `EXPLAIN`-Anweisung bereitstellen.

apg_plan_mgmt.plan_last_used

Gibt das `last_used`-Datum des angegebenen Plans aus dem gemeinsam genutzten Speicher zurück.

> **Note**
>
> Der Wert im gemeinsam genutzten Speicher ist auf der primären DB-Instance im DB-Cluster immer aktuell. Der Wert wird nur periodisch in die `last_used`-Spalte der `apg_plan_mgmt.dba_plans`-Ansicht gespült.

Syntax

```
apg_plan_mgmt.plan_last_used(
    sql_hash,
    plan_hash
)
```

Rückgabewert

Gibt das Datum des Typs `last_used` zurück.

Parameter

Parameter	Beschreibung
`sql_hash`	Die `sql_hash`-ID der verwalteten SQL-Anweisung des Plans.
`plan_hash`	Die `plan_hash` -ID des verwalteten Plans.

apg_plan_mgmt.reload

Laden Sie Pläne in der `apg_plan_mgmt.dba_plans`-Ansicht erneut in den gemeinsam genutzten Speicher.

Syntax

```
apg_plan_mgmt.reload()
```

Rückgabewert

Keine.

Parameter

Keine.

Nutzungshinweise

Rufen Sie `reload` in den folgenden Fällen auf:

- Verwenden Sie diesen Parameter, um den gemeinsam genutzten Speicher eines schreibgeschützten Replica sofort zu aktualisieren. So müssen Sie nicht warten, bis neue Pläne an das Replica übermittelt werden.
- Verwenden Sie diesen Parameter auch nach dem Import verwalteter Pläne.

apg_plan_mgmt.set_plan_enabled

Aktivieren oder deaktivieren Sie einen verwalteten Plan.

Syntax

```
apg_plan_mgmt.set_plan_enabled(
    sql_hash,
    plan_hash,
    [true | false]
)
```

Rückgabewert

Gibt bei erfolgreicher Einstellung „0“ und „-1“ zurück, wenn die Einstellung nicht übernommen wurde.

Parameter

Parameter	Beschreibung
`sql_hash`	Die `sql_hash`-ID der verwalteten SQL-Anweisung des Plans.
`plan_hash`	Die `plan_hash` -ID des verwalteten Plans.
`enabled`	Boolescher Wert („true“ oder „false“) • Durch einen Wert des Typs `true` wird der Plan aktiviert. • Durch einen Wert des Typs `false` wird der Plan deaktiviert.

apg_plan_mgmt.set_plan_status

Legen Sie den Status eines verwalteten Plans auf `Approved`, `Unapproved`, `Rejected` oder `Preferred` fest.

Syntax

```
apg_plan_mgmt.set_plan_status(
    sql_hash,
    plan_hash,
    status
)
```

Rückgabewert

Gibt bei erfolgreicher Einstellung „0“ und „-1“ zurück, wenn die Einstellung nicht übernommen wurde.

Parameter

Parameter	Beschreibung
`sql_hash`	Die `sql_hash`-ID der verwalteten SQL-Anweisung des Plans.

Parameter	Beschreibung
`plan_hash`	Die `plan_hash` -ID des verwalteten Plans.
`status`	Eine Zeichenfolge mit einem der folgenden Werte: • `'Approved'` • `'Unapproved'` • `'Rejected'` • `'Preferred'` Der von Ihnen verwendete Fall spielt keine Rolle, aber der Statuswert wird in der `apg_plan_mgmt.dba_plans` -Ansicht auf anfängliche Großbuchstaben gesetzt. Weitere Informationen zu diesen Werten finden Sie unter `status`. Referenz für die apg_plan_mgmt.dba_plans-Ansicht

apg_plan_mgmt.update_plans_last_used

Aktualisiert die Plantabelle sofort mit dem `last_used`-Datum, das im freigegebenen Speicher gespeichert ist.

Syntax

```
apg_plan_mgmt.update_plans_last_used()
```

Rückgabewert

Keine.

Parameter

Keine.

Nutzungshinweise

Rufen Sie `update_plans_last_used` auf, um sicherzustellen, dass Abfragen für die Spalte `dba_plans.last_used` die neusten Informationen verwenden. Wenn das `last_used`-Datum nicht

sofort aktualisiert wird, aktualisiert ein Hintergrundprozess die Plantabelle einmal stündlich mit dem `last_used`-Datum (standardmäßig).

Wenn beispielsweise eine Anweisung mit einem bestimmten `sql_hash` langsam ausgeführt wird, können Sie feststellen, welche Pläne für diese Anweisung seit Beginn der Leistungsregression ausgeführt wurden. Leeren Sie dazu zuerst die Daten im freigegebenen Speicher auf die Festplatte, damit die `last_used`-Daten aktuell sind, und fragen Sie dann alle Pläne des `sql_hash` der Anweisung mit der Leistungsregression ab. Stellen Sie in der Abfrage sicher, dass das Datum `last_used` größer oder gleich dem Datum ist, an dem die Leistungsregression begann. Die Abfrage identifiziert den Plan oder die Gruppe von Plänen, die für die Leistungsregression verantwortlich sein könnten. Sie können `apg_plan_mgmt.get_explain_plan` verwenden, wenn `explainOptionList` auf `verbose, hashes` gesetzt ist. Sie können `apg_plan_mgmt.evolve_plan_baselines` auch verwenden, um den Plan und alle alternativen Pläne zu analysieren, die möglicherweise eine bessere Leistung erbringen.

Die `update_plans_last_used`-Funktion wirkt sich nur auf die primäre DB-Instance des DB-Clusters aus.

apg_plan_mgmt.validate_plans

Überprüfen Sie, ob der Optimierer immer noch eine Neuerstellung von Plänen durchführen kann. Der Optimierer überprüft die Pläne `Approved`, `Unapproved` und `Preferred` dahingehend, ob der Plan aktiviert oder deaktiviert ist. `Rejected`-Pläne werden nicht validiert. Alternativ können Sie auch die Funktion `apg_plan_mgmt.validate_plans` verwenden, um ungültige Pläne zu löschen oder zu deaktivieren.

Syntax

```
apg_plan_mgmt.validate_plans(
    sql_hash,
    plan_hash,
    action)

apg_plan_mgmt.validate_plans(
    action)
```

Rückgabewert

Die Anzahl ungültiger Pläne

Parameter

Parameter	Beschreibung
`sql_hash`	Die `sql_hash`-ID der verwalteten SQL-Anweisung des Plans.
`plan_hash`	Die `plan_hash` -ID des verwalteten Plans. Verwenden Sie NULL, um alle Pläne für denselben `sql_hash`-ID-Wert anzugeben.
`action`	Die Aktion, die die Funktion für ungültige Pläne ausführen wird. Gültige Zeichenfolgenwerte sind unter anderem die folgenden: Die Groß-/Kleinschreibung muss nicht beachtet werden. • `'disable'` – Alle ungültigen Pläne werden deaktiviert. • `'delete'` – Alle ungültigen Pläne werden gelöscht. • `'update_plan_hash'` – Aktualisiert die `plan_hash` -ID für Pläne, die nicht genau reproduziert werden können. Damit können Sie auch einen Plan korrigieren, indem Sie die SQL-Anweisung neu schreiben. Anschließend können Sie den korrigierten Plan als `Approved`-Plan für die ursprüngliche SQL-Anweisung registrieren. • NULL – Diese Funktion gibt die Anzahl der ungültigen Pläne zurück. Keine weitere Aktion wird ausgeführt. • '' – Durch eine leere Zeichenfolge wird eine Nachricht mit der Anzahl gültiger und ungültiger Pläne erstellt. Alle anderen Werte werden wie die leere Zeichenfolge behandelt.

Nutzungshinweise

Mit dem Formular `validate_plans(action)` validieren Sie alle verwalteten Pläne für alle verwalteten Anweisungen in der gesamten `apg_plan_mgmt.dba_plans`-Ansicht.

Nutzen Sie das Formular `validate_plans(sql_hash, plan_hash, action)`, um einen mit `plan_hash` angegebenen verwalteten Plan für eine mit `sql_hash` spezifizierte verwaltete Anweisung zu validieren.

Mit dem Formular `validate_plans(sql_hash, NULL, action)` können Sie alle verwalteten Pläne für die verwaltete Anweisung validieren, die über den Parameter `sql_hash` spezifiziert wird.

Referenz für die apg_plan_mgmt.dba_plans-Ansicht

Die `apg_plan_mgmt.dba_plans`-Ansicht enthält die folgenden Spalten mit Planinformationen:

dba_plans-Spalte	Beschreibung
`cardinality_error`	Hierbei handelt es sich um ein Maß zur Angabe des Fehlers zwischen der geschätzten und der tatsächlichen Kardinalität. Bei der Kardinalität handelt es sich um die Anzahl der Tabellenzeilen, die der Plan verarbeiten soll. Bei einem schwerwiegenden Kardinalitätsfehler besteht eine erhöhte Wahrscheinlichkeit dafür, dass ein Plan nicht optimal funktioniert. Diese Spalte ist durch die Funktion apg_plan_mgmt.evolve_plan_baselines ausgefüllt.
`compatibility_level`	Diese Spalte informiert über die Funktionsebene des Aurora PostgreSQL-Optimierers.
`created_by`	Hier sehen Sie den authentifizierten Benutzer (`session_user`), der den Plan erstellt hat.
`enabled`	Gibt an, ob der Plan aktiviert oder deaktiviert ist. Alle Pläne sind standardmäßig aktiviert. Sie können Pläne deaktivieren, damit sie nicht vom Optimierer verwendet werden können. Verwenden Sie die Funktion apg_plan_mgmt.set_plan_enabled, um diesen Wert zu ändern.
`environment_variables`	Gibt Aufschluss über die Parameter und Werte der PostgreSQL Grand Unified Configuration (GUC), die vom Optimierer zum Zeitpunkt der Planerfassung überschrieben wurden.
`estimated_startup_cost`	Diese Spalte bezieht sich auf die geschätzten Einrichtungskosten für den Optimierer, bevor dieser Tabellenzeilen übermittelt.
`estimated_total_cost`	Diese Spalte informiert über die geschätzten Optimiererkosten für das Übermitteln der letzten Tabellenzeile.

dba_plans-Spalte	Beschreibung
`execution_time_benefit_ms`	Die Ausführungszeitersparnis (in Millisekunden), die beim Aktivieren des Plans erzielt wird Diese Spalte ist durch die Funktion apg_plan_mgmt.evolve_plan_baselines ausgefüllt.
`execution_time_ms`	Diese Spalte informiert über die geschätzte Laufzeit des Plans (in Millisekunden). Diese Spalte ist durch die Funktion apg_plan_mgmt.evolve_plan_baselines ausgefüllt.
`has_side_effects`	Dieser Wert gibt an, dass die SQL-Anweisung eine Data Manipulation Language (DML)- oder eine SELECT-Anweisung ist, die eine Funktion des Typs TEMPORÄR enthält.
`last_used`	Dieser Wert wird auf das aktuelle Datum aktualisiert, wenn der Plan ausgeführt wird oder als Minimalkostenplan des Abfrageoptimierers fungiert. Dieser Wert wird im gemeinsam genutzten Speicher gespeichert und regelmäßig an den Datenträger übertragen. Um den neuesten Wert zu erhalten, rufen Sie durch das Ausführen der Funktion `apg_plan_mgmt.plan_last_used(sql_hash, plan_hash)` das Datum aus dem gemeinsam genutzten Speicher ab, anstatt den Wert `last_used` zu nutzen. Weitere Informationen erhalten Sie, indem Sie sich über den apg_plan_mgmt.plan_retention_period-Parameter informieren.
`last_validated`	Informiert über den letzten Zeitpunkt, an dem verifiziert wurde, dass der Plan entweder über die Funktion apg_plan_mgmt.validate_plans oder die Funktion apg_plan_mgmt.evolve_plan_baselines neu erstellt werden könnte.
`last_verified`	Informiert über den letzten Zeitpunkt, an dem ein Plan über die Funktion apg_plan_mgmt.evolve_plan_baselines als bester Plan für die angegebenen Parameter ermittelt wurde.

dba_plans-Spalte	Beschreibung
`origin`	Gibt an, wie der Plan mithilfe des Parameters apg_plan_mgmt.capture_plan_baselines erfasst wurde. Gültige Werte sind unter anderem: `M`: Der Plan wurde mit manueller Planerfassung erfasst. `A`: Der Plan wurde mit automatischer Planerfassung erfasst.
`param_list`	Die Parameterwerte, die an die Anweisung gesendet wurden, falls es sich um eine vorbereitete Anweisung handelt.
`plan_created`	Datum und Uhrzeit der Planerstellung
`plan_hash`	Die ID des Plans. Durch die Kombination von `plan_hash` und `sql_hash` wird ein bestimmter Plan eindeutig identifiziert.
`plan_outline`	Eine datenbankunabhängige Darstellung des Plans, mit der der tatsächliche Ausführungsplan neu erstellt wird. Die Operatoren in der Strukturansicht entsprechen den Operatoren in der EXPLAIN-Ausgabe.
`planning_time_ms`	Die tatsächliche Zeit (in Millisekunden), die zum Ausführen des Planers benötigt wird. Diese Spalte ist durch die Funktion apg_plan_mgmt.evolve_plan_baselines ausgefüllt.
`queryId`	Ein von der Erweiterung `pg_stat_statements` berechneter Anweisungs-Hash. Hierbei handelt es sich nicht um eine stabile oder datenbankunabhängige ID, weil dieser Hash von Objekt-IDs (OIDs) abhängig ist. Der Wert wird `0` sein, wenn `compute_query_id` bei der Erfassung des Abfrageplans auf `off` gesetzt ist.
`sql_hash`	Ein Hash-Wert des SQL-Anweisungstexts, normalisiert und ohne Literale
`sql_text`	Der vollständige Text der SQL-Anweisung.

dba_plans-Spalte	Beschreibung
`status`	Informiert über den Status eines Plans. Der Status bestimmt, wie ein Plan vom Optimierer verwendet wird. Im Folgenden sind Beispiele für gültige Werte aufgeführt. • `Approved` – ein nutzbarer Plan, der vom Optimierer ausgeführt werden kann. Der Optimierer wählt aus dem Satz genehmigter Pläne (Baseline) einer verwalteten Anweisung den kostengünstigsten Plan zur Ausführung aus. Verwenden Sie die Funktion apg_plan_mgmt.evolve_plan_baselines, um einen Plan auf „Genehmigt“ zurückzusetzen. • `Unapproved` – ein erfasster Plan, der nicht zur Verwendung verifiziert wurde. Weitere Informationen finden Sie unter Auswerten der Performance von Plänen. • `Rejected` – ein Plan, der nicht vom Optimierer verwendet wird. Weitere Informationen finden Sie unter Ablehnen oder Deaktivieren langsamerer Pläne. • `Preferred` – ein Plan, der von Ihnen für eine verwaltete Anweisung als bevorzugter Plan bestimmt wurde. Wenn der Minimalkostenplan des Optimierers kein genehmigter oder bevorzugter Plan ist, können Sie den Overhead der Plandurchführung reduzieren. Dazu können Sie einer Teilmenge der genehmigten Pläne den Status „“ zuweise `Preferred` . Wenn der Minimalkostenplan des Optimierers kein `Approved`-Plan ist, erhält ein `Preferred` -Plan den Vorzug vor einem `Approved`-Plan. Verwenden Sie die Funktion „`Preferred` “, um einen Plan auf „apg_plan_mgmt.set_plan_status“ zurückzusetzen.
`stmt_name`	Der Name der SQL-Anweisung innerhalb einer PREPARE-Anweisung. Dieser Wert ist eine leere Zeichenfolge für eine namenlose vorbereitete Anweisung. Dieser Wert beträgt bei nicht vorbereiteten Anweisungen NULL.

dba_plans-Spalte	Beschreibung
`total_time_benefit_ms`	Die gesamte Zeitersparnis (in Millisekunden), die beim Aktivieren dieses Plans erzielt wird. Dieser Wert berücksichtigt sowohl die Planungs- als auch die Ausführungszeit. Ist dieser Wert negativ, sind mit dem Aktivieren dieses Plans Nachteile verbunden. Diese Spalte ist durch die Funktion apg_plan_mgmt.evolve_plan_baselines ausgefüllt.

Erweiterte Funktionen der Abfrageplanverwaltung

Im Folgenden finden Sie Informationen zu den erweiterten Funktionen der Abfrageplanverwaltung (Query Plan Management, QPM) in Aurora PostgreSQL:

Themen

- Erfassung von Aurora-PostgreSQL-Ausführungsplänen
- Unterstützung der Tabellenpartition

Erfassung von Aurora-PostgreSQL-Ausführungsplänen

QPM (Query Plan Management) ermöglicht es Ihnen, die von Aurora Replicas generierten Abfragepläne zu erfassen und sie in der primären DB-Instance des Aurora-DB-Clusters zu speichern. Sie können die Abfragepläne von allen Aurora Replicas sammeln und eine Reihe optimaler Pläne in einer zentralen persistenten Tabelle auf der primären Instance verwalten. Sie können diese Pläne dann bei Bedarf auf andere Replicas anwenden. Dies hilft Ihnen, die Stabilität der Ausführungspläne aufrechtzuerhalten und die Leistung der Abfragen in den DB-Clustern und Engine-Versionen zu verbessern.

Themen

- Voraussetzungen
- Verwaltung der Planerfassung für Aurora Replicas
- Fehlerbehebung

Voraussetzungen

Aktivieren Sie **`capture_plan_baselines parameter`** in Aurora Replica – Setzen Sie den `capture_plan_baselines`-Parameter auf automatisch oder manuell, um Pläne in Aurora Replicas zu erfassen. Weitere Informationen finden Sie unter apg_plan_mgmt.capture_plan_baselines.

Installieren Sie die postgres_fdw-Erweiterung – Sie müssen die `postgres_fdw`-Foreign-Data-Wrapper-Erweiterung installieren, um Pläne in Aurora Replicas zu erfassen. Führen Sie den folgenden Befehl in jeder Datenbank aus, um die Erweiterung zu installieren.

```
postgres=> CREATE EXTENSION IF NOT EXISTS postgres_fdw;
```

Verwaltung der Planerfassung für Aurora Replicas

Aktivierung der Planerfassung für Aurora Replicas

Sie müssen über `rds_superuser`-Berechtigungen verfügen, um die Planerfassung in Aurora Replicas zu erstellen oder zu entfernen. Weitere Informationen zu Benutzerrollen und Berechtigungen finden Sie unter PostgreSQL-Rollen und -Berechtigungen verstehen.

Um Pläne zu erfassen, rufen Sie die Funktion apg_plan_mgmt.create_replica_plan_capture in der Writer-DB-Instance auf, wie im Folgenden dargestellt:

```
postgres=> CALL
 apg_plan_mgmt.create_replica_plan_capture('cluster_endpoint', 'password');
```

- cluster_endpoint - cluster_endpoint (Writer-Endpunkt) bietet Failover-Unterstützung für Plan Capture in Aurora Replicas.
- password – Wir empfehlen, bei der Erstellung des Passworts die folgenden Richtlinien zu beachten, um die Sicherheit zu erhöhen:
  - Es muss mindestens 8 Zeichen enthalten.
  - Es muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer enthalten.
  - Es muss mindestens ein Sonderzeichen (?, !, #, <, >, * usw.) enthalten.

> **Note**
>
> Wenn Sie den Cluster-Endpunkt, das Passwort oder die Portnummer ändern, müssen Sie `apg_plan_mgmt.create_replica_plan_capture()` erneut mit dem Cluster-Endpunkt

und dem Passwort ausführen, um die Planerfassung erneut zu initialisieren. Andernfalls schlägt die Erfassung von Plänen von Aurora Replicas fehl.

Deaktivieren der Planerfassung für Aurora Replicas

Sie können den `capture_plan_baselines`-Parameter in Aurora Replica deaktivieren, indem Sie seinen Wert in der Gruppe Parameter auf `off` setzen.

Entfernen der Planerfassung für Aurora Replicas

Sie können die Planerfassung in Aurora Replicas vollständig entfernen, stellen vorher jedoch Folgendes sicher: Rufen Sie `apg_plan_mgmt.remove_replica_plan_capture` wie folgt auf, um Plan Capture zu entfernen:

```
postgres=> CALL apg_plan_mgmt.remove_replica_plan_capture();
```

Sie müssen apg_plan_mgmt.create_replica_plan_capture () erneut aufrufen, um die Planerfassung in Aurora Replicas mit dem Cluster-Endpunkt und dem Passwort zu aktivieren.

Fehlerbehebung

Im Folgenden finden Sie Tipps zur Fehlerbehebung und Workarounds für den Fall, dass der Plan nicht wie erwartet in Aurora Replicas erfasst wird.

- Parametereinstellungen – Prüfen Sie, ob der `capture_plan_baselines`-Parameter auf den richtigen Wert gesetzt ist, um die Planerfassung zu aktivieren.
- Die **`postgres_fdw`**-Erweiterung ist installiert – Verwenden Sie die folgende Abfrage, um zu überprüfen, ob `postgres_fdw` installiert ist.

  ```
  postgres=> SELECT * FROM pg_extension WHERE extname = 'postgres_fdw'
  ```

- create_replica_plan_capture() wird aufgerufen – Verwenden Sie den folgenden Befehl, um zu überprüfen, ob die Benutzerzuordnung vorhanden ist. Rufen Sie andernfalls `create_replica_plan_capture()` auf, um das Feature zu initialisieren.

  ```
  postgres=> SELECT * FROM pg_foreign_server WHERE srvname =
   'apg_plan_mgmt_writer_foreign_server';
  ```

- Cluster-Endpunkt und Portnummer – Überprüfen Sie, ob der Cluster-Endpunkt und die Portnummer korrekt sind. Wenn diese Werte inkorrekt sind, wird keine Fehlermeldung angezeigt.

  Verwenden Sie den folgenden Befehl, um zu überprüfen, ob der Endpunkt in create () verwendet wurde und in welcher Datenbank er sich befindet:

  ```
  postgres=> SELECT srvoptions FROM pg_foreign_server WHERE srvname =
   'apg_plan_mgmt_writer_foreign_server';
  ```

- reload() – Sie müssen apg_plan_mgmt.reload() aufrufen, nachdem Sie apg_plan_mgmt.delete_plan() in Aurora Replicas aufgerufen haben, damit die Löschfunktion wirksam wird. Dadurch wird sichergestellt, dass die Änderung erfolgreich implementiert wurde.
- Passwort – Sie müssen das Passwort in create_replica_plan_capture() gemäß den genannten Richtlinien eingeben. Andernfalls wird eine Fehlermeldung angezeigt. Weitere Informationen finden Sie unter Verwaltung der Planerfassung für Aurora Replicas. Verwenden Sie ein anderes Passwort, das den Anforderungen entspricht.
- Regionsübergreifende Verbindung – Die Planerfassung in Aurora Replicas wird auch in der globalen Aurora-Datenbank unterstützt, wo sich Writer-Instance und Aurora Replicas in verschiedenen Regionen befinden können. Die Writer-Instance und das regionsübergreifende Replikat müssen in der Lage sein, mithilfe von VPC-Peering zu kommunizieren. Weitere Informationen finden Sie unter VPC-Peering. Wenn ein regionsübergreifendes Failover auftritt, müssen Sie den Endpunkt auf einen neuen primären DB-Cluster-Endpunkt umkonfigurieren.

Unterstützung der Tabellenpartition

Aurora PostgreSQL Query Plan Management (QPM) unterstützt die deklarative Tabellenpartitionierung in den folgenden Versionen:

- 15.3 und höhere 15-Versionen
- 14.8 und höhere 14-Versionen
- 13.11 und höhere 13-Versionen

Weitere Informationen finden Sie unter Table Partitioning.

Themen

- Einrichten der Tabellenpartition
- Erfassen von Plänen für die Tabellenpartition

- Erzwingen eines Tabellenpartitionsplans
- Namenskonvention

Einrichten der Tabellenpartition

Gehen Sie wie folgt vor, um die Tabellenpartition in Aurora PostgreSQL QPM einzurichten:

1. Setzen Sie `apg_plan_mgmt.plan_hash_version` in der DB-Cluster-Parametergruppe auf 3 oder mehr.
2. Navigieren Sie zu einer Datenbank, die Query Plan Management verwendet und Einträge in der Ansicht `apg_plan_mgmt.dba_plans` aufweist.
3. Rufen Sie `apg_plan_mgmt.validate_plans('update_plan_hash')` auf, um den `plan_hash`-Wert in der Plantabelle zu aktualisieren.
4. Wiederholen Sie die Schritte 2 bis 3 für alle Datenbanken, für die Query Plan Management aktiviert ist und die Einträge in `apg_plan_mgmt.dba_plans` aufweisen.

Weitere Informationen zu diesen Parametern finden Sie unter Parameterreferenz für Aurora-PostgreSQL-Abfrageplanverwaltung.

Erfassen von Plänen für die Tabellenpartition

In QPM werden verschiedene Pläne durch ihren `plan_hash`-Wert unterschieden. Um die Änderungen am `plan_hash` zu verstehen, müssen Sie zunächst ähnliche Pläne verstehen.

Die Kombination von Zugriffsmethoden, Indexnamen ohne Ziffern und Partitionsnamen ohne Ziffern, die auf der Ebene des Append-Knotens gespeichert sind, muss konstant sein, damit die Pläne als identisch gelten. Die spezifischen Partitionen, auf die in den Plänen zugegriffen wird, sind nicht wichtig. Im folgenden Beispiel wird eine Tabelle `tbl_a` mit 4 Partitionen erstellt.

```
postgres=>create table tbl_a(i int, j int, k int, l int, m int) partition by range(i);
CREATE TABLE
postgres=>create table tbl_a1 partition of tbl_a for values from (0) to (1000);
CREATE TABLE
postgres=>create table tbl_a2 partition of tbl_a for values from (1001) to (2000);
CREATE TABLE
postgres=>create table tbl_a3 partition of tbl_a for values from (2001) to (3000);
CREATE TABLE
postgres=>create table tbl_a4 partition of tbl_a for values from (3001) to (4000);
```

```
CREATE TABLE
postgres=>create index t_i on tbl_a using btree (i);
CREATE INDEX
postgres=>create index t_j on tbl_a using btree (j);
CREATE INDEX
postgres=>create index t_k on tbl_a using btree (k);
CREATE INDEX
```

Die folgenden Pläne gelten als identisch, da unabhängig von der Anzahl der Partitionen, nach denen die Abfrage sucht, eine einzige Scanmethode zum Scannen von `tbl_a` verwendet wird.

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 999 and j < 9910 and k > 50;

                        QUERY PLAN
-----------------------------------------------------------------------
Seq Scan on tbl_a1 tbl_a
    Filter: ((i >= 990) AND (i <= 999) AND (j < 9910) AND (k > 50))
SQL Hash: 1553185667, Plan Hash: -694232056
(3 rows)
```

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 1100 and j < 9910 and k > 50;

                        QUERY PLAN
-----------------------------------------------------------------------
Append
    ->  Seq Scan on tbl_a1 tbl_a_1
            Filter: ((i >= 990) AND (i <= 1100) AND (j < 9910) AND (k > 50))
    ->  Seq Scan on tbl_a2 tbl_a_2
            Filter: ((i >= 990) AND (i <= 1100) AND (j < 9910) AND (k > 50))
    SQL Hash: 1553185667, Plan Hash: -694232056
    (6 rows)
```

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 2100 and j < 9910 and k > 50;

                QUERY PLAN
-----------------------------------------------------------------------------
 Append
   ->  Seq Scan on tbl_a1 tbl_a_1
         Filter: ((i >= 990) AND (i <= 2100) AND (j < 9910) AND (k > 50))
```

```
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 2100) AND (j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a3 tbl_a_3
         Filter: ((i >= 990) AND (i <= 2100) AND (j < 9910) AND (k > 50))
 SQL Hash: 1553185667, Plan Hash: -694232056
(8 rows)
```

Die folgenden 3 Pläne gelten ebenfalls als identisch, da auf der übergeordneten Ebene die Zugriffsmethoden, Indexnamen ohne Ziffern und Partitionsnamen ohne Ziffern `SeqScan tbl_a` und `IndexScan (i_idx) tbl_a` lauten.

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 1100 and j < 9910 and k > 50;

                                QUERY PLAN
-------------------------------------------------------------------------
 Append
   ->  Seq Scan on tbl_a1 tbl_a_1
         Filter: ((i >= 990) AND (i <= 1100) AND (j < 9910) AND (k > 50))
   ->  Index Scan using tbl_a2_i_idx on tbl_a2 tbl_a_2
         Index Cond: ((i >= 990) AND (i <= 1100))
         Filter: ((j < 9910) AND (k > 50))
 SQL Hash: 1553185667, Plan Hash: -993736942
(7 rows)
```

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 2100 and j < 9910 and k > 50;

                                QUERY PLAN
-------------------------------------------------------------------------
 Append
   ->  Index Scan using tbl_a1_i_idx on tbl_a1 tbl_a_1
         Index Cond: ((i >= 990) AND (i <= 2100))
         Filter: ((j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 2100) AND (j < 9910) AND (k > 50))
   ->  Index Scan using tbl_a3_i_idx on tbl_a3 tbl_a_3
         Index Cond: ((i >= 990) AND (i <= 2100))
         Filter: ((j < 9910) AND (k > 50))
 SQL Hash: 1553185667, Plan Hash: -993736942
(10 rows)
```

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 3100 and j < 9910 and k > 50;

                                QUERY PLAN
------------------------------------------------------------------------
 Append
   ->  Seq Scan on tbl_a1 tbl_a_1
         Filter: ((i >= 990) AND (i <= 3100) AND (j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 3100) AND (j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a3 tbl_a_3
         Filter: ((i >= 990) AND (i <= 3100) AND (j < 9910) AND (k > 50))
   ->  Index Scan using tbl_a4_i_idx on tbl_a4 tbl_a_4
         Index Cond: ((i >= 990) AND (i <= 3100))
         Filter: ((j < 9910) AND (k > 50))
 SQL Hash: 1553185667, Plan Hash: -993736942
(11 rows)
```

Unabhängig von der unterschiedlichen Reihenfolge und Anzahl der Vorkommen in untergeordneten Partitionen sind die Zugriffsmethoden, Indexnamen ohne Ziffern und Partitionsnamen ohne Ziffern auf der übergeordneten Ebene für jeden der oben aufgeführten Pläne konstant.

Die Pläne würden jedoch nicht als identisch gelten, wenn eine der folgenden Bedingungen erfüllt ist:

- Es werden zusätzliche Zugriffsmethoden im Plan verwendet.

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between
 990 and 2100 and j < 9910 and k > 50;

                                QUERY PLAN
------------------------------------------------------------------------
 Append
   ->  Seq Scan on tbl_a1 tbl_a_1
         Filter: ((i >= 990) AND (i <= 2100) AND (j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 2100) AND (j < 9910) AND (k > 50))
   ->  Bitmap Heap Scan on tbl_a3 tbl_a_3
         Recheck Cond: ((i >= 990) AND (i <= 2100))
         Filter: ((j < 9910) AND (k > 50))
         ->  Bitmap Index Scan on tbl_a3_i_idx
               Index Cond: ((i >= 990) AND (i <= 2100))
 SQL Hash: 1553185667, Plan Hash: 1134525070
```

```
(11 rows)
```

- Eine der im Plan enthaltenen Zugriffsmethoden wird nicht mehr verwendet.

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between
 990 and 1100 and j < 9910 and k > 50;

                              QUERY PLAN
-----------------------------------------------------------------------
 Append
   ->  Seq Scan on tbl_a1 tbl_a_1
         Filter: ((i >= 990) AND (i <= 1100) AND (j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 1100) AND (j < 9910) AND (k > 50))
 SQL Hash: 1553185667, Plan Hash: -694232056
(6 rows)
```

- Der einer Indexmethode zugeordnete Index wird geändert.

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between
 990 and 1100 and j < 9910 and k > 50;

                             QUERY PLAN
-----------------------------------------------------------------------
 Append
   ->  Seq Scan on tbl_a1 tbl_a_1
         Filter: ((i >= 990) AND (i <= 1100) AND (j < 9910) AND (k > 50))
   ->  Index Scan using tbl_a2_j_idx on tbl_a2 tbl_a_2
         Index Cond: (j < 9910)
         Filter: ((i >= 990) AND (i <= 1100) AND (k > 50))
 SQL Hash: 1553185667, Plan Hash: -993343726
(7 rows)
```

Erzwingen eines Tabellenpartitionsplans

Genehmigte Pläne für partitionierte Tabellen werden durch Positionskorrespondenz erzwungen. Die Pläne sind nicht spezifisch für die Partitionen und können für andere Partitionen als die in der ursprünglichen Abfrage referenzierten Pläne erzwungen werden. Pläne können auch für Abfragen erzwungen werden, die auf eine andere Anzahl von Partitionen als die ursprünglich genehmigte Gliederung zugreifen.

Beispiel: Die genehmigte Gliederung gilt für den folgenden Plan:

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 2100 and j < 9910 and k > 50;

                                QUERY PLAN
-------------------------------------------------------------------------
 Append
   ->  Index Scan using tbl_a1_i_idx on tbl_a1 tbl_a_1
         Index Cond: ((i >= 990) AND (i <= 2100))
         Filter: ((j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 2100) AND (j < 9910) AND (k > 50))
   ->  Index Scan using tbl_a3_i_idx on tbl_a3 tbl_a_3
         Index Cond: ((i >= 990) AND (i <= 2100))
         Filter: ((j < 9910) AND (k > 50))
 SQL Hash: 1553185667, Plan Hash: -993736942
(10 rows)
```

Dann kann dieser Plan auch für SQL-Abfragen erzwungen werden, die 2, 4 oder mehr Partitionen referenzieren. Die möglichen Pläne, die sich aus diesen Szenarien für den Zugriff auf 2 und 4 Partitionen ergeben könnten, sind folgende:

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 1100 and j < 9910 and k > 50;

                                QUERY PLAN
-------------------------------------------------------------------------------
 Append
   ->  Index Scan using tbl_a1_i_idx on tbl_a1 tbl_a_1
         Index Cond: ((i >= 990) AND (i <= 1100))
         Filter: ((j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 1100) AND (j < 9910) AND (k > 50))
 Note: An Approved plan was used instead of the minimum cost plan.
 SQL Hash: 1553185667, Plan Hash: -993736942, Minimum Cost Plan Hash: -1873216041
(8 rows)
```

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 3100 and j < 9910 and k > 50;

                                QUERY PLAN
-------------------------------------------------------------------------
 Append
```

```
   ->  Index Scan using tbl_a1_i_idx on tbl_a1 tbl_a_1
         Index Cond: ((i >= 990) AND (i <= 3100))
         Filter: ((j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 3100) AND (j < 9910) AND (k > 50))
   ->  Index Scan using tbl_a3_i_idx on tbl_a3 tbl_a_3
         Index Cond: ((i >= 990) AND (i <= 3100))
         Filter: ((j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a4 tbl_a_4
         Filter: ((i >= 990) AND (i <= 3100) AND (j < 9910) AND (k > 50))
 Note: An Approved plan was used instead of the minimum cost plan.
 SQL Hash: 1553185667, Plan Hash: -993736942, Minimum Cost Plan Hash: -1873216041
(12 rows)
```

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 3100 and j < 9910 and k > 50;

                                QUERY PLAN
-------------------------------------------------------------------------------
 Append
   ->  Index Scan using tbl_a1_i_idx on tbl_a1 tbl_a_1
         Index Cond: ((i >= 990) AND (i <= 3100))
         Filter: ((j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 3100) AND (j < 9910) AND (k > 50))
   ->  Index Scan using tbl_a3_i_idx on tbl_a3 tbl_a_3
         Index Cond: ((i >= 990) AND (i <= 3100))
         Filter: ((j < 9910) AND (k > 50))
   ->  Index Scan using tbl_a4_i_idx on tbl_a4 tbl_a_4
         Index Cond: ((i >= 990) AND (i <= 3100))
         Filter: ((j < 9910) AND (k > 50))
 Note: An Approved plan was used instead of the minimum cost plan.
 SQL Hash: 1553185667, Plan Hash: -993736942, Minimum Cost Plan Hash: -1873216041
(14 rows)
```

Betrachten Sie einen anderen genehmigten Plan mit unterschiedlichen Zugriffsmethoden für jede Partition:

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 2100 and j < 9910 and k > 50;

                                QUERY PLAN
-------------------------------------------------------------------------
```

```
 Append
   ->  Index Scan using tbl_a1_i_idx on tbl_a1 tbl_a_1
         Index Cond: ((i >= 990) AND (i <= 2100))
         Filter: ((j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 2100) AND (j < 9910) AND (k > 50))
   ->  Bitmap Heap Scan on tbl_a3 tbl_a_3
         Recheck Cond: ((i >= 990) AND (i <= 2100))
         Filter: ((j < 9910) AND (k > 50))
         ->  Bitmap Index Scan on tbl_a3_i_idx
               Index Cond: ((i >= 990) AND (i <= 2100))
 SQL Hash: 1553185667, Plan Hash: 2032136998
(12 rows)
```

In diesem Fall würde jeder Plan, der aus zwei Partitionen liest, nicht erzwungen werden. Solange nicht alle Kombinationen (Zugriffsmethode, Indexname) aus dem genehmigten Plan verwendet werden können, kann der Plan nicht erzwungen werden. Die folgenden Pläne haben beispielsweise unterschiedliche Plan-Hashes und der genehmigte Plan kann in diesen Fällen nicht erzwungen werden:

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 1900 and j < 9910 and k > 50;

                             QUERY PLAN
--------------------------------------------------------------------------
 Append
   ->  Bitmap Heap Scan on tbl_a1 tbl_a_1
         Recheck Cond: ((i >= 990) AND (i <= 1900))
         Filter: ((j < 9910) AND (k > 50))
         ->  Bitmap Index Scan on tbl_a1_i_idx
               Index Cond: ((i >= 990) AND (i <= 1900))
   ->  Bitmap Heap Scan on tbl_a2 tbl_a_2
         Recheck Cond: ((i >= 990) AND (i <= 1900))
         Filter: ((j < 9910) AND (k > 50))
         ->  Bitmap Index Scan on tbl_a2_i_idx
               Index Cond: ((i >= 990) AND (i <= 1900))
  Note: This is not an Approved plan.  No usable Approved plan was found.
  SQL Hash: 1553185667, Plan Hash: -568647260
(13 rows)
```

```
postgres=>explain (hashes true, costs false) select j, k from tbl_a where i between 990
 and 1900 and j < 9910 and k > 50;
```

```
                              QUERY PLAN
------------------------------------------------------------------------------
 Append
   ->  Index Scan using tbl_a1_i_idx on tbl_a1 tbl_a_1
         Index Cond: ((i >= 990) AND (i <= 1900))
         Filter: ((j < 9910) AND (k > 50))
   ->  Seq Scan on tbl_a2 tbl_a_2
         Filter: ((i >= 990) AND (i <= 1900) AND (j < 9910) AND (k > 50))
 Note: This is not an Approved plan.  No usable Approved plan was found.
 SQL Hash: 1553185667, Plan Hash: -496793743
(8 rows)
```

Namenskonvention

Damit QPM einen Plan mit deklarativ partitionierten Tabellen durchsetzen kann, müssen Sie bestimmte Benennungsregeln für übergeordnete Tabellen, Tabellenpartitionen und Indizes befolgen:

- Namen der übergeordneten Tabellen — Diese Namen müssen sich durch Alphabete oder Sonderzeichen unterscheiden und nicht nur durch Ziffern. Beispielsweise sind tA, tB und tC zulässige Namen für separate übergeordnete Tabellen, t1, t2 und t3 hingegen nicht.
- Namen einzelner Partitionstabellen — Partitionen derselben übergeordneten Partition sollten sich nur durch Ziffern voneinander unterscheiden. Zulässige Partitionsnamen von tA könnten beispielsweise tA1, tA2 oder t1A, t2A oder auch mehrere Ziffern sein.

  Alle anderen Unterschiede (Buchstaben, Sonderzeichen) garantieren das Erzwingen des Plans nicht.
- Indexnamen — Stellen Sie in der Hierarchie der Partitionstabellen sicher, dass alle Indizes eindeutige Namen haben. Das bedeutet, dass die nicht numerischen Teile der Namen unterschiedlich sein müssen. Wenn Sie beispielsweise eine partitionierte Tabelle `tA` mit einem Index benannt haben`tA_col1_idx1`, können Sie keinen anderen Index benennen. `tA_col1_idx2` Sie können jedoch einen Index aufrufen, `tA_a_col1_idx2` da der nichtnumerische Teil des Namens eindeutig ist. Diese Regel gilt für Indizes, die sowohl für die übergeordnete Tabelle als auch für einzelne Partitionstabellen erstellt wurden.

Wenn die oben genannten Namenskonventionen nicht eingehalten werden, kann dies dazu führen, dass die genehmigten Pläne nicht erzwungen werden. Das folgende Beispiel veranschaulicht ein fehlgeschlagenes Erzwingen:

```
postgres=>create table t1(i int, j int, k int, l int, m int) partition by range(i);
CREATE TABLE
postgres=>create table t1a partition of t1 for values from (0) to (1000);
CREATE TABLE
postgres=>create table t1b partition of t1 for values from (1001) to (2000);
CREATE TABLE
postgres=>SET apg_plan_mgmt.capture_plan_baselines TO 'manual';
SET
postgres=>explain (hashes true, costs false) select count(*) from t1 where i > 0;

                           QUERY PLAN
-----------------------------------------------------------------------------
 Aggregate
   ->  Append
         ->  Seq Scan on t1a t1_1
               Filter: (i > 0)
         ->  Seq Scan on t1b t1_2
               Filter: (i > 0)
 SQL Hash: -1720232281, Plan Hash: -1010664377
(7 rows)
```

```
postgres=>SET apg_plan_mgmt.use_plan_baselines TO 'on';
SET
postgres=>explain (hashes true, costs false) select count(*) from t1 where i > 1000;

                           QUERY PLAN
-----------------------------------------------------------------------------
 Aggregate
   ->  Seq Scan on t1b t1
         Filter: (i > 1000)
 Note: This is not an Approved plan. No usable Approved plan was found.
 SQL Hash: -1720232281, Plan Hash: 335531806
(5 rows)
```

Auch wenn die beiden Pläne identisch erscheinen mögen, unterscheiden sich ihre `Plan Hash` Werte aufgrund der Namen der untergeordneten Tabellen. Die Tabellennamen unterscheiden sich nach Alphazeichen und nicht nur nach Ziffern, was dazu führt, dass die Durchsetzung fehlschlägt.

Arbeiten mit Erweiterungen und Fremddaten-Wrappern

Sie können verschiedene PostgreSQL-Erweiterungen installieren und verwenden, um Ihrem DB-Cluster der Aurora-PostgreSQL-kompatiblen Edition einige Funktionen hinzuzufügen. Wenn Ihr Anwendungsfall beispielsweise eine intensive Dateneingabe in sehr großen Tabellen verlangt, können Sie die `pg_partman`-Erweiterung installieren, um Ihre Daten zu partitionieren und damit den Workload zu verteilen.

> **Note**
>
> Ab Aurora PostgreSQL 14.5 unterstützt Aurora PostgreSQL Trusted Language Extensions für PostgreSQL. Diese Funktion ist als Erweiterung `pg_tle` implementiert, die Sie Ihrem Aurora PostgreSQL hinzufügen können. Mithilfe dieser Erweiterung können Entwickler ihre eigenen PostgreSQL-Erweiterungen in einer sicheren Umgebung erstellen, was die Setup- und Konfigurationsanforderungen sowie einen Großteil der Vorabtests für neue Erweiterungen vereinfacht. Weitere Informationen finden Sie unter Arbeiten mit Trusted Language Extensions für PostgreSQL.

In einigen Fällen bietet es sich an, anstatt eine Erweiterung zu installieren, ein bestimmtes Modul zur Liste der `shared_preload_libraries` in der benutzerdefinierten DB-Cluster-Parametergruppe Ihres DB-Clusters von Aurora PostgreSQL hinzuzufügen. In der Regel lädt die standardmäßige DB-Cluster-Parametergruppe nur die `pg_stat_statements`. Es stehen jedoch weitere Module zur Verfügung, die der Liste hinzugefügt werden können. Sie können beispielsweise Planungsfunktionen hinzufügen, indem Sie das `pg_cron`-Modul hinzufügen, wie unter Planen der Wartung mit der PostgreSQL-Erweiterung pg_cron beschrieben. Als weiteres Beispiel können Sie Abfrageausführungspläne protokollieren, indem Sie das `auto_explain`-Modul laden. Weitere Informationen finden Sie unter Protokollieren von Abfrageausführungsplänen im AWS-Wissenscenter.

Eine Erweiterung, die Zugriff auf externe Daten ermöglicht, wird als Fremddaten-Wrapper (FDW) bezeichnet. Zum Beispiel ermöglicht die Erweiterung `oracle_fdw` Ihrem Aurora-PostgreSQL-DB-Cluster die Zusammenarbeit mit Oracle-Datenbanken.

Sie können auch genau angeben, welche Erweiterungen auf Ihrer Aurora PostgreSQL DB-Instance installiert werden können, indem Sie sie im Parameter `rds.allowed_extensions` aufführen. Weitere Informationen finden Sie unter Einschränkung der Installation von PostgreSQL-Erweiterungen.

Im Folgenden finden Sie Informationen zum Einrichten und Verwenden einiger Erweiterungen, Module und FDWs, die für Aurora PostgreSQL verfügbar sind. Der Einfachheit halber werden diese alle als „Erweiterungen“ bezeichnet. Eine Auflistung der Erweiterungen, die Sie mit den aktuell verfügbaren Aurora-PostgreSQL-Versionen verwenden können, finden Sie unter Versionen der Erweiterungen für Amazon Aurora PostgreSQL in Versionshinweise für Aurora PostgreSQL.

- Verwalten großer Objekte mit dem lo-Modul
- Verwalten von Geodaten mit der PostGIS-Erweiterung
- Verwalten von PostgreSQL-Partitionen mit der Erweiterung pg_partman
- Planen der Wartung mit der PostgreSQL-Erweiterung pg_cron
- Verwenden von pgAudit zur Protokollierung der Datenbankaktivität
- Verwenden von pglogical, um Daten zwischen Instances zu synchronisieren
- Arbeiten mit Oracle-Datenbanken unter Verwendung der Erweiterung oracle_fdw
- Arbeiten mit SQL-Server-Datenbanken unter Verwendung der Erweiterung tds_fdw

Verwenden der Unterstützung delegierter Amazon Aurora-Erweiterungen für PostgreSQL

Mithilfe der Unterstützung für delegierte Amazon Aurora-Erweiterungen für PostgreSQL können Sie die Erweiterungsverwaltung an einen Benutzer delegieren, der kein sein muss`rds_superuser`. Mit dieser Unterstützung für delegierte Erweiterungen `rds_extension` wird eine neue Rolle namens erstellt und Sie müssen diese einem Benutzer zuweisen, um andere Erweiterungen zu verwalten. Diese Rolle kann Erweiterungen erstellen, aktualisieren und löschen.

Sie können die Erweiterungen angeben, die auf Ihrer DB-Instance von Aurora PostgreSQL installiert werden können, indem Sie sie im `rds.allowed_extensions` Parameter auflisten. Weitere Informationen finden Sie unter Verwenden von PostgreSQL-Erweiterungen mit Amazon RDS für PostgreSQL.

Sie können die Liste der verfügbaren Erweiterungen einschränken, die vom Benutzer mit der `rds_extension` Rolle mithilfe des `rds.allowed_delegated_extensions` Parameters verwaltet werden können.

Die Unterstützung für delegierte Erweiterungen ist in den folgenden Versionen verfügbar:

- Alle höheren Versionen

- 15.5 und höhere 15-Versionen
- 14.10 und höhere 14-Versionen
- 13.13 und höhere 13-Versionen
- 12.17 und höhere 12-Versionen

Themen

Aktivieren der Unterstützung für das Delegieren von Erweiterungen an einen Benutzer

Sie müssen Folgendes tun, um die Unterstützung der Delegierungserweiterung für einen Benutzer zu aktivieren:

1. **`rds_extension`** Einem Benutzer Rolle gewähren – Stellen Sie als eine Verbindung mit der Datenbank her `rds_superuser` und führen Sie den folgenden Befehl aus:

   ```
   Postgres => grant rds_extension to user_name;
   ```

2. Festlegen der Liste der Erweiterungen, die delegierten Benutzern zur Verwaltung zur Verfügung stehen – `rds.allowed_delegated_extensions` Mit können Sie eine Teilmenge der verfügbaren Erweiterungen mit `rds.allowed_extensions` im DB-Cluster-Parameter angeben. Sie können dies auf einer der folgenden Ebenen durchführen:

   - Im Cluster oder in der Instance-Parametergruppe über die AWS Management Console oder API. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen.

- Verwenden Sie den folgenden Befehl auf Datenbankebene:

```
alter database database_name set rds.allowed_delegated_extensions =
 'extension_name_1,
                    extension_name_2,...extension_name_n';
```

- Verwenden Sie den folgenden Befehl auf Benutzerebene:

```
alter user user_name set rds.allowed_delegated_extensions = 'extension_name_1,
                    extension_name_2,...extension_name_n';
```

> **Note**
>
> Sie müssen die Datenbank nicht neu starten, nachdem Sie den `rds.allowed_delegated_extensions` dynamischen Parameter geändert haben.

3. Erlauben Sie dem delegierten Benutzer Zugriff auf Objekte, die während der Erstellung der Erweiterung erstellt wurden – Bestimmte Erweiterungen erstellen Objekte, für die zusätzliche Berechtigungen erteilt werden müssen, bevor der Benutzer mit der `rds_extension` Rolle darauf zugreifen kann. Der `rds_superuser` muss dem delegierten Benutzer Zugriff auf diese Objekte gewähren. Eine der Optionen besteht darin, einen Ereignisauslöser zu verwenden, um dem delegierten Benutzer automatisch die Berechtigung zu erteilen. Weitere Informationen finden Sie im Beispiel für einen Ereignisauslöser unter Deaktivieren der Unterstützung für die delegierte Erweiterung.

Konfiguration, die in der Unterstützung delegierter Aurora-Erweiterungen für PostgreSQL verwendet wird

Konfig tionsna	Beschreibung	Standardwert	Hinweise	Wer die Berechtig ung ändern oder erteilen kann
`rds.a ed_de ted_e sions`	Dieser Parameter begrenzt die Erweiterungen, die eine rds_exten	Leere Zeichenfolge	• Standardm äßig ist dieser Parameter eine leere	rds_superuser

Konfig tionsna	Beschreibung	Standardwert	Hinweise	Wer die Berechtig ung ändern oder erteilen kann
	sion-Rolle in einer Datenbank verwalten kann. Es muss eine Teilmenge von rds.allowed_extens ions sein.		Zeichenfolge, was bedeutet, dass keine Erweiteru ngen an Benutzer mit delegiert wurden`rds_exten sion` . • Jede unterstüt zte Erweiterung kann hinzugefügt werden, wenn der Benutzer dazu berechtigt ist. Legen Sie dazu den `rds.allow ed_delega ted_exten sions` Parameter auf eine Zeichenfolge von kommagetr ennten Erweiteru ngsnamen fest. Indem Sie diesem Parameter eine Liste von Erweiterungen hinzufügen, identifizieren Sie explizit die Erweiteru ngen, die der Benutzer mit	

Konfigurationsna	Beschreibung	Standardwert	Hinweise	Wer die Berechtigung ändern oder erteilen kann
			der `rds_extension` Rolle installieren kann. • Wenn diese Option auf festgelegt ist*, bedeutet dies, dass alle in aufgeführten Erweiterungen an Benutzer mit `-rds_extension` Rolle delegiert `rds_allowed_extensions` werden. Weitere Informationen zum Einrichten dieses Parameters finden Sie unter Aktivieren der Unterstützung für das Delegieren von Erweiterungen an einen Benutzer.	

Konfigurationsna	Beschreibung	Standardwert	Hinweise	Wer die Berechtigung ändern oder erteilen kann
`rds.allowed_extensions`	Mit diesem Parameter kann der Kunde die Erweiterungen einschränken, die in der DB-Instance von Aurora PostgreSQL installiert werden können. Weitere Informationen finden Sie unter Beschränken der Installation von PostgreSQL-Erweiterungen	"*"	Standardmäßig ist dieser Parameter auf „*“ gesetzt, was bedeutet, dass alle Erweiterungen, die auf RDS für PostgreSQL und Aurora PostgreSQL unterstützt werden, von Benutzern mit den erforderlichen Berechtigungen erstellt werden dürfen. Leer bedeutet, dass in der Aurora PostgreSQL-DB-Instance keine Erweiterungen installiert werden können.	Administrator

Konfig tionsna	Beschreibung	Standardwert	Hinweise	Wer die Berechtig ung ändern oder erteilen kann
`rds-deleg ated_ nsior ow_dr ascac`	Dieser Parameter steuert die Möglichkeit für Benutzer mit `rds_extension` , die Erweiteru ng mithilfe einer Kaskadierungsoptio n zu löschen.	aus	`rds-deleg ated_exte nsion_all ow_drop_c ascade` ist standardmäßig auf `off` festgeleg t. Das bedeutet, dass Benutzer mit `rds_extension` keine Erweiterung mit der Kaskadier ungsoption löschen dürfen. Um diese Fähigkeit zu gewähren, sollte der `rds.deleg ated_exte nsion_all ow_drop_c ascade` Parameter auf gesetzt werdenon.	rds_superuser

Deaktivieren der Unterstützung für die delegierte Erweiterung

Teilweises Ausschalten

Die delegierten Benutzer können keine neuen Erweiterungen erstellen, aber weiterhin vorhandene Erweiterungen aktualisieren.

- Setzen Sie `rds.allowed_delegated_extensions` auf den Standardwert in der DB-Cluster-Parametergruppe zurück.
- Verwenden Sie den folgenden Befehl auf Datenbankebene:

```
alter database database_name reset rds.allowed_delegated_extensions;
```

- Verwenden Sie den folgenden Befehl auf Benutzerebene:

```
alter user user_name reset rds.allowed_delegated_extensions;
```

Vollständiges Ausschalten

Durch das Widerrufen der `rds_extension` Rolle eines Benutzers wird der Benutzer auf Standardberechtigungen zurückgesetzt. Der Benutzer kann keine Erweiterungen mehr erstellen, aktualisieren oder löschen.

```
postgres => revoke rds_extension from user_name;
```

Beispiel für einen Ereignisauslöser

Wenn Sie einem delegierten Benutzer mit erlauben möchten, Erweiterungen `rds_extension` zu verwenden, die das Festlegen von Berechtigungen für seine Objekte erfordern, die bei der Erstellung der Erweiterung erstellt wurden, können Sie das folgende Beispiel eines Ereignisauslösers anpassen und nur die Erweiterungen hinzufügen, für die die delegierten Benutzer Zugriff auf die volle Funktionalität haben sollen. Dieser Ereignisauslöser kann auf template1 (die Standardvorlage) erstellt werden, daher hat jede aus template1 erstellte Datenbank diesen Ereignisauslöser. Wenn ein delegierter Benutzer die Erweiterung installiert, gewährt dieser Auslöser automatisch die Eigentümerschaft an den Objekten, die von der Erweiterung erstellt wurden.

```
CREATE OR REPLACE FUNCTION create_ext()

  RETURNS event_trigger AS $$

DECLARE

  schemaname TEXT;
  databaseowner TEXT;
```

```
  r RECORD;

BEGIN

  IF tg_tag = 'CREATE EXTENSION' and current_user != 'rds_superuser' THEN
    RAISE NOTICE 'SECURITY INVOKER';
    RAISE NOTICE 'user: %', current_user;
    FOR r IN SELECT * FROM pg_event_trigger_ddl_commands()
    LOOP
        CONTINUE WHEN r.command_tag != 'CREATE EXTENSION' OR r.object_type !=
 'extension';

        schemaname = (
            SELECT n.nspname
            FROM pg_catalog.pg_extension AS e
            INNER JOIN pg_catalog.pg_namespace AS n
            ON e.extnamespace = n.oid
            WHERE e.oid = r.objid
        );

        databaseowner = (
            SELECT pg_catalog.pg_get_userbyid(d.datdba)
            FROM pg_catalog.pg_database d
            WHERE d.datname = current_database()
        );
        RAISE NOTICE 'Record for event trigger %, objid: %,tag: %, current_user: %,
 schema: %, database_owenr: %', r.object_identity, r.objid, tg_tag, current_user,
 schemaname, databaseowner;
        IF r.object_identity = 'address_standardizer_data_us' THEN
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE %I.us_gaz TO
 %I WITH GRANT OPTION;', schemaname, databaseowner);
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE %I.us_lex TO
 %I WITH GRANT OPTION;', schemaname, databaseowner);
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE %I.us_rules
 TO %I WITH GRANT OPTION;', schemaname, databaseowner);
        ELSIF r.object_identity = 'dict_int' THEN
            EXECUTE format('ALTER TEXT SEARCH DICTIONARY %I.intdict OWNER TO %I;',
 schemaname, databaseowner);
        ELSIF r.object_identity = 'pg_partman' THEN
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE
 %I.part_config TO %I WITH GRANT OPTION;', schemaname, databaseowner);
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE
 %I.part_config_sub TO %I WITH GRANT OPTION;', schemaname, databaseowner);
```

```
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE
 %I.custom_time_partitions TO %I WITH GRANT OPTION;', schemaname, databaseowner);
        ELSIF r.object_identity = 'postgis_topology' THEN
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON ALL TABLES IN
 SCHEMA topology TO %I WITH GRANT OPTION;', databaseowner);
            EXECUTE format('GRANT USAGE, SELECT ON ALL SEQUENCES IN SCHEMA topology TO
 %I WITH GRANT OPTION;', databaseowner);
            EXECUTE format('GRANT EXECUTE ON ALL FUNCTIONS IN SCHEMA topology TO %I
 WITH GRANT OPTION;', databaseowner);
            EXECUTE format('GRANT USAGE ON SCHEMA topology TO %I WITH GRANT OPTION;',
 databaseowner);
        END IF;
    END LOOP;
  END IF;
END;
$$ LANGUAGE plpgsql SECURITY DEFINER;

CREATE EVENT TRIGGER log_create_ext ON ddl_command_end EXECUTE PROCEDURE create_ext();
```

Vorteile der Verwendung der Unterstützung delegierter Amazon Aurora-Erweiterungen

Durch die Verwendung der Unterstützung der delegierten Erweiterung von Amazon Aurora für PostgreSQL delegieren Sie die Erweiterungsverwaltung sicher an Benutzer, die nicht über die `rds_superuser` Rolle verfügen. Diese Funktion bietet die folgenden Vorteile:

- Sie können die Erweiterungsverwaltung einfach an Benutzer Ihrer Wahl delegieren.
- Dies erfordert keine `rds_superuser` Rolle.
- Bietet die Möglichkeit, verschiedene Erweiterungen für verschiedene Datenbanken im selben DB-Cluster zu unterstützen.

Einschränkung der Unterstützung delegierter Aurora-Erweiterungen für PostgreSQL

- Für Objekte, die während der Erstellung der Erweiterung erstellt wurden, sind möglicherweise zusätzliche Berechtigungen erforderlich, damit die Erweiterung ordnungsgemäß funktioniert.

Erforderliche Berechtigungen für bestimmte Erweiterungen

Um die folgenden Erweiterungen zu erstellen, zu verwenden oder zu aktualisieren, sollte der delegierte Benutzer über die erforderlichen Berechtigungen für die folgenden Funktionen, Tabellen und Schemata verfügen.

Erwe ngen die Eige oder Bere unge benö	Funktion	Tabellen	Schema	Wörterbuch für die Textsuche	Kommentar
addre tanda er_da s		us_gaz, us_lex, us_lex, l.us_rules			
amch	bt_index_check, bt_index_ parent_check				
dict_i				-Indikt	
pg_p n		custom_ti me_partitions, part_config, part_config_sub			
pg_st tatem					
Post(	st_tileenvelope	Geo-ref_sys			
postg aster					

Erwe ngen die Eiger oder Bere unge benö	Funktion	Tabellen	Schema	Wörterbuch für die Textsuche	Kommentar
postg opolo		Topologie, Ebene	Topologie		der delegierte Benutzer Muss der Datenbank besitzer sein
log_f	create_fo reign_tab le_for_log_file				
rds_t	role_pass word_encr yption_type				
postg iger_ oder		geocode_s ettings_default, geocode_s ettings	Tiger		
pg_fr acem	pg_freespace				
pg_vi lity	pg_visibility				

Sicherheitsüberlegungen

Beachten Sie, dass ein Benutzer mit -`rds_extension`Rolle Erweiterungen für alle Datenbanken verwalten kann, für die er über die Verbindungsberechtigung verfügt. Wenn beabsichtigt ist, dass ein delegierter Benutzer die Erweiterung für eine einzelne Datenbank verwaltet, empfiehlt es sich,

alle Rechte öffentlich für jede Datenbank zu widerrufen und dann dem delegierten Benutzer die Verbindungsberechtigung für diese spezifische Datenbank explizit zu erteilen.

Es gibt mehrere Erweiterungen, mit denen ein Benutzer auf Informationen aus mehreren Datenbanken zugreifen kann. Stellen Sie sicher, dass die von Ihnen gewährten Benutzer über datenbankübergreifende Funktionen `rds_extension` verfügen, bevor Sie diese Erweiterungen zu hinzufügen`rds.allowed_delegated_extensions`. Beispielsweise `dblink` bieten `postgres_fdw` und Funktionen zum datenbankübergreifenden Abfragen auf derselben Instance oder Remote-Instances. `log_fdw` liest die Postgres-Engine-Protokolldateien, die für alle Datenbanken in der Instance gelten und möglicherweise langsame Abfragen oder Fehlermeldungen aus mehreren Datenbanken enthalten. `pg_cron` ermöglicht das Ausführen geplanter Hintergrundaufträge auf der DB-Instance und kann Aufträge so konfigurieren, dass sie in einer anderen Datenbank ausgeführt werden.

Entfernen der Erweiterungskaskade deaktiviert

Die Möglichkeit, die Option „Erweiterung mit Kaskade“ von einem Benutzer mit der `rds_extension` Rolle zu löschen, wird durch den `rds.delegated_extension_allow_drop_cascade` Parameter gesteuert. `rds-delegated_extension_allow_drop_cascade` ist standardmäßig auf `off` festgelegt. Das bedeutet, dass Benutzer mit der `rds_extension` Rolle eine Erweiterung nicht mit der Kaskadierungsoption löschen dürfen, wie in der folgenden Abfrage gezeigt.

```
DROP EXTENSION CASCADE;
```

Dadurch werden automatisch Objekte gelöscht, die von der Erweiterung abhängen, und umgekehrt alle Objekte, die von diesen Objekten abhängen. Der Versuch, die Kaskadierungsoption zu verwenden, führt zu einem Fehler.

Um diese Fähigkeit zu gewähren, sollte der `rds.delegated_extension_allow_drop_cascade` Parameter auf gesetzt werdenon.

Das Ändern des `rds.delegated_extension_allow_drop_cascade` dynamischen Parameters erfordert keinen Neustart der Datenbank. Sie können dies auf einer der folgenden Ebenen tun:

- Im Cluster oder in der Instance-Parametergruppe über die AWS Management Console oder API.
- Verwenden Sie den folgenden Befehl auf Datenbankebene:

```
alter database database_name set rds.delegated_extension_allow_drop_cascade = 'on';
```

- Verwenden Sie den folgenden Befehl auf Benutzerebene:

```
alter role tenant_user set rds.delegated_extension_allow_drop_cascade = 'on';
```

Beispielerweiterungen, die mithilfe der Unterstützung delegierter Erweiterungen hinzugefügt werden können

- `rds_tools`

```
extension_test_db=> create extension rds_tools;
CREATE EXTENSION
extension_test_db=> SELECT * from rds_tools.role_password_encryption_type() where
 rolname = 'pg_read_server_files';
ERROR: permission denied for function role_password_encryption_type
```

- `amcheck`

```
extension_test_db=> CREATE TABLE amcheck_test (id int);
CREATE TABLE
extension_test_db=> INSERT INTO amcheck_test VALUES (generate_series(1,100000));
INSERT 0 100000
extension_test_db=> CREATE INDEX amcheck_test_btree_idx ON amcheck_test USING btree
 (id);
CREATE INDEX
extension_test_db=> create extension amcheck;
CREATE EXTENSION
extension_test_db=> SELECT bt_index_check('amcheck_test_btree_idx'::regclass);
ERROR: permission denied for function bt_index_check
extension_test_db=> SELECT bt_index_parent_check('amcheck_test_btree_idx'::regclass);
ERROR: permission denied for function bt_index_parent_check
```

- `pg_freespacemap`

```
extension_test_db=> create extension pg_freespacemap;
CREATE EXTENSION
extension_test_db=> SELECT * FROM pg_freespace('pg_authid');
ERROR: permission denied for function pg_freespace
extension_test_db=> SELECT * FROM pg_freespace('pg_authid',0);
ERROR: permission denied for function pg_freespace
```

- `pg_visibility`

```
extension_test_db=> create extension pg_visibility;
CREATE EXTENSION
extension_test_db=> select * from pg_visibility('pg_database'::regclass);
ERROR: permission denied for function pg_visibility
```

- `postgres_fdw`

```
extension_test_db=> create extension postgres_fdw;
CREATE EXTENSION
extension_test_db=> create server myserver foreign data wrapper postgres_fdw options
 (host 'foo', dbname 'foodb', port '5432');
ERROR: permission denied for foreign-data wrapper postgres_fdw
```

Verwalten großer Objekte mit dem lo-Modul

Das lo-Modul (Erweiterung) richtet sich an Datenbankbenutzer und Entwickler, die mit PostgreSQL-Datenbanken über JDBC- oder ODBC-Treiber arbeiten. Sowohl JDBC als auch ODBC erwarten, dass die Datenbank das Löschen großer Objekte bewältigt, wenn sich Verweise auf sie ändern. PostgreSQL funktioniert jedoch nicht so. PostgreSQL geht nicht davon aus, dass ein Objekt gelöscht werden sollte, wenn sich sein Verweis ändert. Demzufolge verbleiben Objekte auf der Festplatte und sind nicht referenziert. Die Erweiterung lo enthält eine Funktion, mit der bei Referenzänderungen das Löschen von Objekten bei Bedarf ausgelöst wird.

> **Tip**
>
> Wenn Sie feststellen möchten, ob Ihre Datenbank von der lo-Erweiterung profitieren kann, suchen Sie mit dem vakuumlo-Dienstprogramm nach verwaisten großen Objekten. Um die Anzahl von verwaisten großen Objekten zu erhalten, ohne Maßnahmen zu ergreifen, führen Sie das Dienstprogramm mit der `-n` Option (no-op) aus. Weitere Informationen erhalten Sie unter vacuumlo utility.

Das lo-Modul ist für Aurora PostgreSQL 13.7, 12.11, 11.16, 10.21 und höhere Nebenversionen verfügbar.

Zum Installieren des Moduls (Erweiterung) benötigen Sie `rds_superuser`-Berechtigungen. Durch die Installation der lo-Erweiterung wird Ihrer Datenbank Folgendes hinzugefügt:

- `lo` – Dies ist ein Datentyp für große Objekte (lo), den Sie für binäre große Objekte (BLOBs) und andere große Objekte verwenden können. Der `lo`-Datentyp ist eine Domäne des `oid`-Datentyps. Mit anderen Worten, es ist eine Objekt-ID mit optionalen Beschränkungen. Weitere Informationen finden Sie unter Objekt-IDs in der PostgreSQL-Dokumentation. Vereinfacht gesagt, können Sie anhand des `lo`-Datentyps Ihre Datenbankspalten, die große Objektreferenzen enthalten, von anderen Objekt-IDs (OIDs) unterscheiden.
- `lo_manage` – Dies ist eine Funktion, die Sie in Triggern für Tabellenspalten verwenden können, die große Objektreferenzen enthalten. Immer wenn Sie einen Wert löschen oder ändern, der auf ein großes Objekt verweist, hebt der Trigger die Verknüpfung des Objekts (`lo_unlink`) mit seiner Referenz auf. Verwenden Sie den Trigger für eine Spalte nur, wenn die Spalte der einzige Datenbankverweis auf das große Objekt ist.

Weitere Informationen zum Modul für große Objekte erhalten Sie unter lo in der PostgreSQL-Dokumentation.

Installieren der lo-Erweiterung

Stellen Sie vor der Installation der lo-Erweiterung sicher, dass Sie über `rds_superuser`-Berechtigungen verfügen.

So installieren Sie die lo-Erweiterung

1. Verwenden Sie `psql`, um eine Verbindung mit der primären DB-Instance Ihres Aurora-PostgreSQL-DB-Clusters herzustellen.

   ```
   psql --host=your-cluster-instance-1.666666666666.aws-region.rds.amazonaws.com --
   port=5432 --username=postgres --password
   ```

   Geben Sie bei der Aufforderung Ihr Passwort ein. Der `psql`-Client verbindet und zeigt die standardmäßige administrative Verbindungsdatenbank `postgres=>` als Eingabeaufforderung an.

2. Installieren Sie die Erweiterung wie folgt.

   ```
   postgres=> CREATE EXTENSION lo;
   CREATE EXTENSION
   ```

Sie können jetzt den `lo`-Datentyp zum Definieren von Spalten in Ihren Tabellen verwenden. Beispielsweise können Sie eine Tabelle (`images`) erstellen, die Raster-Bilddaten enthält. Sie können den `lo`-Datentyp für eine Spalte `raster` verwenden, wie im folgenden Beispiel, mit dem eine Tabelle erstellt wird, gezeigt.

```
postgres=> CREATE TABLE images (image_name text, raster lo);
```

Verwenden der Triggerfunktion lo_manage zum Löschen von Objekten

Sie können die `lo_manage`-Funktion in einem Trigger in einer `lo` oder anderen großen Objektspalten verwenden, um verwaiste Objekte zu bereinigen (und zu verhindern), wenn `lo` aktualisiert oder gelöscht wird.

So richten Sie Trigger für Spalten ein, die auf große Objekte verweisen

- Führen Sie eine der folgenden Aktionen aus:
  - Erstellen Sie einen BEFORE UPDATE ODER DELETE-Trigger für jede Spalte, damit diese eindeutige Verweise auf große Objekte enthält, wobei der Spaltenname als Argument verwendet wird.

    ```
    postgres=> CREATE TRIGGER t_raster BEFORE UPDATE OR DELETE ON images
        FOR EACH ROW EXECUTE FUNCTION lo_manage(raster);
    ```

  - Wenden Sie einen Trigger nur an, wenn die Spalte aktualisiert wird.

    ```
    postgres=> CREATE TRIGGER t_raster BEFORE UPDATE OF images
        FOR EACH ROW EXECUTE FUNCTION lo_manage(raster);
    ```

Die `lo_manage`-Trigger-Funktion funktioniert nur im Kontext des Einfügens oder Löschens von Spaltendaten, je nachdem, wie Sie den Trigger definieren. Er hat keine Auswirkung, wenn Sie eine `DROP`- oder `TRUNCATE`-Operation in einer Datenbank ausführen. Das bedeutet, dass Sie vor der Verwendung der DROP-Operation Objektspalten aus allen Tabellen löschen sollten, um das Erstellen von verwaisten Objekten zu verhindern.

Angenommen, Sie möchten die Datenbank entfernen, die die Tabelle `images` enthält. Sie löschen die Spalte wie folgt.

```
postgres=> DELETE FROM images COLUMN raster
```

Vorausgesetzt, die `lo_manage`-Funktion ist in dieser Spalte definiert, um Löschvorgänge zu behandeln, können Sie die Tabelle jetzt sicher entfernen.

Verwenden des vacuumlo-Dienstprogramms

Das vakuumlo-Dienstprogramm identifiziert verwaiste große Objekte und kann diese aus Datenbanken entfernen. Dieses Dienstprogramm ist seit PostgreSQL 9.1.24 verfügbar. Wenn Ihre Datenbankbenutzer routinemäßig mit großen Objekten arbeiten, empfehlen wir Ihnen, vakuumlo gelegentlich auszuführen, um verwaiste große Objekte zu bereinigen.

Bevor Sie die lo-Erweiterung installieren, können Sie mit vacuumlo beurteilen, ob Ihr Aurora-PostgreSQL-DB-Cluster davon profitieren kann. Führen Sie dazu `vacuumlo` mit der `-n`-Option (no-op) aus, um zu zeigen, was entfernt würde, wie im Folgenden gezeigt:

```
$ vacuumlo -v -n -h your-cluster-instance-1.666666666666.aws-region.rds.amazonaws.com -
p 5433 -U postgres docs-lab-spatial-db
Password:*****
Connected to database "docs-lab-spatial-db"
Test run: no large objects will be removed!
Would remove 0 large objects from database "docs-lab-spatial-db".
```

Wie die Ausgabe zeigt, stellen verwaiste große Objekte für diese bestimmte Datenbank kein Problem dar.

Weitere Informationen über dieses Dienstprogramm finden Sie unter vacuumlo in der PostgreSQL-Dokumentation.

Verwalten von Geodaten mit der PostGIS-Erweiterung

PostGIS ist eine Erweiterung von PostgreSQL zur Speicherung und Verwaltung von Geodaten. Weitere Informationen zu PostGIS finden Sie unter PostGIS.net.

Ab Version 10.5 unterstützt PostgreSQL die libprotobuf-1.3.0-Bibliothek, die von PostGIS für die Arbeit mit Vektorkacheldaten der Kartenbox verwendet wird.

Für das Einrichten der PostGIS-Erweiterung sind `rds_superuser`-Berechtigungen erforderlich. Wir empfehlen Ihnen, einen Benutzer (Rolle) zum Verwalten der PostGIS-Erweiterung und Ihrer

räumlichen Daten zu erstellen. Die PostGIS-Erweiterung und ihre zugehörigen Komponenten fügen PostgreSQL Tausende von Funktionen hinzu. Erstellen Sie die PostGIS-Erweiterung ggf. in einem eigenen Schema, wenn dies für Ihren Anwendungsfall sinnvoll ist. Das folgende Beispiel zeigt, wie die Erweiterung in einer eigenen Datenbank installiert wird. Dies ist jedoch nicht erforderlich.

Themen

Schritt 1: Erstellen Sie einen Benutzer (Rolle) zum Verwalten der PostGIS-Erweiterung.

Zuerst stellen Sie eine Verbindung mit Ihrer DB-Instance von RDS für PostgreSQL als Benutzer her, der über `rds_superuser`-Berechtigungen verfügt. Wenn Sie beim Einrichten Ihrer Instance den Standardnamen beibehalten haben, stellen Sie eine Verbindung als `postgres` her.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --username=postgres
 --password
```

Erstellen Sie eine separate Rolle (Benutzer), um die PostGIS-Erweiterung zu verwalten.

```
postgres=>  CREATE ROLE gis_admin LOGIN PASSWORD 'change_me';
CREATE ROLE
```

Gewähren Sie dieser Rolle `rds_superuser`-Berechtigungen, damit die Rolle die Erweiterung installieren kann.

```
postgres=> GRANT rds_superuser TO gis_admin;
GRANT
```

Erstellen Sie eine Datenbank, die Sie für Ihre PostGIS-Artefakte verwenden können. Dieser Schritt ist optional. Oder Sie können in Ihrer Benutzerdatenbank ein Schema für die PostGIS-Erweiterungen erstellen, aber das ist auch nicht erforderlich.

```
postgres=> CREATE DATABASE lab_gis;
CREATE DATABASE
```

Gewähren Sie `gis_admin` alle Berechtigungen für die `lab_gis`-Datenbank.

```
postgres=> GRANT ALL PRIVILEGES ON DATABASE lab_gis TO gis_admin;
GRANT
```

Beenden Sie die Sitzung und stellen Sie wieder eine Verbindung mit Ihrer RDS-for-PostgreSQL-DB-Instance als `gis_admin` her.

```
postgres=> psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=gis_admin --password --dbname=lab_gis
Password for user gis_admin:...
lab_gis=>
```

Fahren Sie mit der Einrichtung der Erweiterung fort, wie in den nächsten Schritten beschrieben.

Schritt 2: Laden der PostGIS-Erweiterungen.

Die PostGIS-Erweiterung enthält mehrere verwandte Erweiterungen, die zusammenarbeiten, um Geodatenfunktionen bereitzustellen. Je nach Anwendungsfall benötigen Sie möglicherweise nicht alle Erweiterungen, die Sie in diesem Schritt erstellt haben.

Verwenden Sie `CREATE EXTENSION`-Anweisungen, um die PostGIS-Erweiterungen zu laden.

```
CREATE EXTENSION postgis;
CREATE EXTENSION
CREATE EXTENSION postgis_raster;
CREATE EXTENSION
CREATE EXTENSION fuzzystrmatch;
CREATE EXTENSION
CREATE EXTENSION postgis_tiger_geocoder;
CREATE EXTENSION
CREATE EXTENSION postgis_topology;
CREATE EXTENSION
CREATE EXTENSION address_standardizer_data_us;
```

```
CREATE EXTENSION
```

Sie können die Ergebnisse überprüfen, indem Sie die in dem folgenden Beispiel gezeigte SQL-Abfrage ausführen, in der die Erweiterungen und ihre Besitzer aufgeführt sind.

```
SELECT n.nspname AS "Name",
  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"
  FROM pg_catalog.pg_namespace n
  WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'
  ORDER BY 1;
List of schemas
     Name     |   Owner
--------------+-----------
 public       | postgres
 tiger        | rdsadmin
 tiger_data   | rdsadmin
 topology     | rdsadmin
(4 rows)
```

Schritt 3: Übertragen Sie die Eigentümerschaft der Erweiterungen

Verwenden Sie die ALTER SCHEMA-Anweisungen, um die Eigentümerschaft der Schemata auf die Rolle `gis_admin` zu übertragen.

```
ALTER SCHEMA tiger OWNER TO gis_admin;
ALTER SCHEMA
ALTER SCHEMA tiger_data OWNER TO gis_admin;
ALTER SCHEMA
ALTER SCHEMA topology OWNER TO gis_admin;
ALTER SCHEMA
```

Sie können die Eigentümeränderung bestätigen, indem Sie die folgende SQL-Abfrage ausführen. Oder Sie können den Metabefehl `\dn` über die psql-Befehlszeile verwenden.

```
SELECT n.nspname AS "Name",
  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"
  FROM pg_catalog.pg_namespace n
  WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'
  ORDER BY 1;
```

```
       List of schemas
     Name     |     Owner
--------------+---------------
 public       | postgres
 tiger        | gis_admin
 tiger_data   | gis_admin
 topology     | gis_admin
(4 rows)
```

Schritt 4: Übertragen Sie die Eigentümerschaft der PostGIS-Objekte.

Verwenden Sie die folgende Funktion, um die Eigentümerschaft der PostGIS-Objekte auf die Rolle `gis_admin` zu übertragen. Führen Sie die folgende Anweisung aus der psql-Aufforderung aus, um die Funktion zu erstellen.

```
CREATE FUNCTION exec(text) returns text language plpgsql volatile AS $f$ BEGIN EXECUTE
 $1; RETURN $1; END; $f$;
CREATE FUNCTION
```

Führen Sie als Nächstes die folgende Abfrage aus, um die `exec`-Funktion auszuführen, die wiederum die Anweisungen ausführt und die Berechtigungen ändert.

```
SELECT exec('ALTER TABLE ' || quote_ident(s.nspname) || '.' || quote_ident(s.relname)
 || ' OWNER TO gis_admin;')
  FROM (
    SELECT nspname, relname
    FROM pg_class c JOIN pg_namespace n ON (c.relnamespace = n.oid)
    WHERE nspname in ('tiger','topology') AND
    relkind IN ('r','S','v') ORDER BY relkind = 'S')
s;
```

Schritt 5: Testen der Erweiterungen

Um zu vermeiden, dass der Schemaname angegeben werden muss, fügen Sie das `tiger`-Schema Ihrem Suchpfad unter Verwendung des folgenden Befehls hinzu.

```
SET search_path=public,tiger;
SET
```

Testen Sie das `tiger`-Schema unter Verwendung der folgenden SELECT-Anweisung.

```
SELECT address, streetname, streettypeabbrev, zip
 FROM normalize_address('1 Devonshire Place, Boston, MA 02109') AS na;
address | streetname | streettypeabbrev |  zip
---------+------------+------------------+-------
       1 | Devonshire | Pl               | 02109
(1 row)
```

Weitere Informationen zu dieser Erweiterung finden Sie unter Tiger Geocoder in der PostGIS-Dokumentation.

Testen Sie den Zugriff auf das `topology`-Schema, indem Sie folgende `SELECT`-Anweisung verwenden. Das ruft die `createtopology`-Funktion zum Registrieren eines neuen Topologieobjekts (my_new_topo) mit der angegebenen Raumbezugskennung (26986) und der Standardtoleranz (0,5) auf. Weitere Informationen finden Sie CreateTopologyin der PostGIS-Dokumentation.

```
SELECT topology.createtopology('my_new_topo',26986,0.5);
 createtopology
---------------
              1
(1 row)
```

Schritt 6: Upgrade der PostGIS-Erweiterung

Jede neue Version von PostgreSQL unterstützt eine oder mehrere Versionen der PostGIS-Erweiterung, die mit dieser Version kompatibel sind. Bei einem Upgrade der PostgreSQL-Engine auf eine neue Version wird die PostGIS-Erweiterung nicht automatisch aktualisiert. Vor dem Upgrade der PostgreSQL-Engine aktualisieren Sie PostGIS in der Regel auf die neueste verfügbare Version für die aktuelle PostgreSQL-Version. Details hierzu finden Sie unter PostGIS-Erweiterungsversionen.

Nach dem Upgrade der PostgreSQL-Engine aktualisieren Sie die PostGIS-Erweiterung erneut auf die Version, die für die neu aktualisierte PostgreSQL-Engine-Version unterstützt wird. Weitere Informationen zum Upgrade der PostgreSQL-Engine finden Sie unter Testen eines Upgrades Ihres Produktions-DB-Clusters auf eine neue Hauptversion. .

Sie können jederzeit prüfen, ob eine neue Version der PostGIS-Erweiterung auf dem Aurora-PostgreSQL-DB-Cluster verfügbar ist. Führen Sie dazu den folgenden Befehl aus. Diese Funktion ist mit PostGIS 2.5.0 und höheren Versionen verfügbar.

```
SELECT postGIS_extensions_upgrade();
```

Wenn Ihre Anwendung die neueste PostGIS-Version nicht unterstützt, können Sie weiterhin eine ältere Version von PostGIS installieren, die in Ihrer Hauptversion wie folgt verfügbar ist.

```
CREATE EXTENSION postgis VERSION "2.5.5";
```

Wenn Sie von einer älteren Version auf eine bestimmte PostGIS-Version aktualisieren möchten, können Sie auch den folgenden Befehl verwenden.

```
ALTER EXTENSION postgis UPDATE TO "2.5.5";
```

Abhängig von der Version, von der Sie ein Upgrade durchführen, müssen Sie diese Funktion möglicherweise noch einmal verwenden. Das Ergebnis des ersten Durchlaufs der Funktion bestimmt, ob eine zusätzliche Upgrade-Funktion benötigt wird. Dies ist beispielsweise bei einem Upgrade von PostGIS 2 auf PostGIS 3 der Fall. Weitere Informationen finden Sie unter Upgrade von PostGIS 2 auf PostGIS 3.

Wenn Sie diese Erweiterung aktualisiert haben, um ein Upgrade der Hauptversion der PostgreSQL-Engine vorzubereiten, können Sie mit anderen vorbereitenden Aufgaben fortfahren. Weitere Informationen finden Sie unter Testen eines Upgrades Ihres Produktions-DB-Clusters auf eine neue Hauptversion.

PostGIS-Erweiterungsversionen

Wir empfehlen Ihnen, die Versionen aller Erweiterungen wie PostGIS zu installieren, wie sie unter Extension versions for Aurora PostgreSQL-Compatible Edition (Versionen aller Erweiterungen für Editionen, die mit Aurora PostgreSQL kompatibel sind) in Versionshinweise für Aurora PostgreSQL aufgelistet sind. . Sie können mithilfe des folgenden Befehls auflisten, welche Versionen in Ihrer Version verfügbar sind.

```
SELECT * FROM pg_available_extension_versions WHERE name='postgis';
```

Versionsinformationen finden Sie in den folgenden Abschnitten in den Versionshinweisen zu Aurora PostgreSQL:

- Erweiterungsversionen für Aurora PostgreSQL 14
- Extension versions for Aurora PostgreSQL-Compatible Edition 13 (Versionen aller Erweiterungen für Edition 13, die mit Aurora PostgreSQL kompatibel ist)

- Extension versions for Aurora PostgreSQL-Compatible Edition 12 (Versionen aller Erweiterungen für Edition 12, die mit Aurora PostgreSQL kompatibel ist)
- Extension versions for Aurora PostgreSQL-Compatible Edition 11 (Versionen aller Erweiterungen für Edition 11, die mit Aurora PostgreSQL kompatibel ist)
- Extension versions for Aurora PostgreSQL-Compatible Edition10 (Versionen aller Erweiterungen für Edition 10, die mit Aurora PostgreSQL kompatibel ist)
- Extension versions for Aurora PostgreSQL-Compatible Edition 9.6 (Versionen aller Erweiterungen für Edition 9.6, die mit Aurora PostgreSQL kompatibel ist)

Upgrade von PostGIS 2 auf PostGIS 3

Ab Version 3.0 ist die PostGIS-Raster-Funktionalität jetzt eine separate Erweiterung, `postgis_raster`. Diese Erweiterung hat einen eigenen Installations- und Upgrade-Pfad. Dadurch werden Dutzende von Funktionen, Datentypen und anderen Artefakten, die für die Rasterbildverarbeitung erforderlich sind, aus der `postgis`-Kernerweiterung entfernt. Das heißt, wenn Ihr Anwendungsfall keine Raster-Verarbeitung erfordert, müssen Sie die `postgis_raster`-Erweiterung nicht installieren.

Im folgenden Upgrade-Beispiel extrahiert der erste Upgrade-Befehl die Raster-Funktionalität in die `postgis_raster`-Erweiterung. Ein zweiter Upgrade-Befehl ist dann erforderlich, um ein Upgrade von `postgres_raster` auf die neue Version durchzuführen.

So führen Sie ein Upgrade von PostGIS 2 auf PostGIS 3 durch

1. Identifizieren Sie die Standardversion von PostGIS, die für die PostgreSQL-Version auf Ihrem Aurora-PostgreSQL-DB-Cluster verfügbar ist. Führen Sie dazu die folgende Abfrage durch.

```
SELECT * FROM pg_available_extensions
    WHERE default_version > installed_version;
  name   | default_version | installed_version |                              comment
---------+-----------------+-------------------
+-------------------------------------------------------------
 postgis | 3.1.4           | 2.3.7             | PostGIS geometry and geography
 spatial types and functions
(1 row)
```

2. Identifizieren Sie die Versionen von PostGIS, die in jeder Datenbank auf der Writer-Instance Ihres Aurora-PostgreSQL-DB-Clusters installiert sind. Anders gesagt: Fragen Sie jede Benutzerdatenbank wie folgt ab.

```
SELECT
    e.extname AS "Name",
    e.extversion AS "Version",
    n.nspname AS "Schema",
    c.description AS "Description"
FROM
    pg_catalog.pg_extension e
    LEFT JOIN pg_catalog.pg_namespace n ON n.oid = e.extnamespace
    LEFT JOIN pg_catalog.pg_description c ON c.objoid = e.oid
    AND c.classoid = 'pg_catalog.pg_extension'::pg_catalog.regclass
WHERE
    e.extname LIKE '%postgis%'
ORDER BY
    1;
  Name   | Version | Schema |                            Description
---------+---------+--------
+-------------------------------------------------------------------------
 postgis | 2.3.7   | public | PostGIS geometry, geography, and raster spatial types
 and functions
(1 row)
```

Diese Nichtübereinstimmung zwischen der Standardversion (PostGIS 3.1.4) und der installierten Version (PostGIS 2.3.7) bedeutet, dass Sie die PostGIS-Erweiterung aktualisieren müssen.

```
ALTER EXTENSION postgis UPDATE;
ALTER EXTENSION
WARNING: unpackaging raster
WARNING: PostGIS Raster functionality has been unpackaged
```

3. Führen Sie die folgende Abfrage aus, um sicherzustellen, dass sich die Raster-Funktionalität jetzt in einem eigenen Paket befindet.

```
SELECT
    probin,
    count(*)
FROM
    pg_proc
WHERE
    probin LIKE '%postgis%'
GROUP BY
    probin;
```

```
          probin          | count
--------------------------+-------
 $libdir/rtpostgis-2.3    | 107
 $libdir/postgis-3        | 487
(2 rows)
```

Die Ausgabe zeigt, dass es immer noch einen Unterschied zwischen den Versionen gibt. Die PostGIS-Funktionen sind Version 3 (postgis-3), während die Raster-Funktionen (rtpostgis) Version 2 (rtpostgis-2.3) sind. Um das Upgrade abzuschließen, führen Sie den Upgrade-Befehl erneut wie folgt aus.

```
postgres=> SELECT postgis_extensions_upgrade();
```

Die Warnmeldungen können Sie ohne Bedenken ignorieren. Führen Sie die folgende Abfrage erneut aus, um zu überprüfen, ob das Upgrade abgeschlossen ist. Das Upgrade ist abgeschlossen, wenn PostGIS und alle zugehörigen Erweiterungen nicht als aktualisierungsbedürftig gekennzeichnet sind.

```
SELECT postgis_full_version();
```

4. Verwenden Sie die folgende Abfrage, um den abgeschlossenen Upgrade-Vorgang und die separat gepackten Erweiterungen anzuzeigen und zu überprüfen, ob ihre Versionen übereinstimmen.

```
SELECT
    e.extname AS "Name",
    e.extversion AS "Version",
    n.nspname AS "Schema",
    c.description AS "Description"
FROM
    pg_catalog.pg_extension e
    LEFT JOIN pg_catalog.pg_namespace n ON n.oid = e.extnamespace
    LEFT JOIN pg_catalog.pg_description c ON c.objoid = e.oid
        AND c.classoid = 'pg_catalog.pg_extension'::pg_catalog.regclass
WHERE
    e.extname LIKE '%postgis%'
ORDER BY
    1;
      Name      | Version | Schema |                            Description
----------------+---------+--------
+------------------------------------------------------------------------
```

```
 postgis        | 3.1.5   | public | PostGIS geometry, geography, and raster
 spatial types and functions
 postgis_raster | 3.1.5   | public | PostGIS raster types and functions
(2 rows)
```

Die Ausgabe zeigt, dass die PostGIS-2-Erweiterung auf PostGIS 3 aktualisiert wurde und beide `postgis` und die jetzt getrennte `postgis_raster`-Erweiterungen Version 3.1.5 sind.

Wenn Sie nach Abschluss dieses Upgrades die Raster-Funktionalität nicht verwenden möchten, können Sie die Erweiterung wie folgt löschen.

```
DROP EXTENSION postgis_raster;
```

Verwalten von PostgreSQL-Partitionen mit der Erweiterung pg_partman

Die PostgreSQL-Tabellenpartitionierung bietet ein Framework für den leistungsstarken Umgang mit Dateneingaben und Berichten. Verwenden Sie die Partitionierung für Datenbanken, die eine sehr schnelle Eingabe großer Datenmengen erfordern. Die Partitionierung ermöglicht auch schnellere Abfragen großer Tabellen. Die Partitionierung hilft bei der Verwaltung von Daten, ohne die Datenbank-Instance zu beeinträchtigen, da sie weniger I/O-Ressourcen benötigt.

Durch die Partitionierung können Sie Daten zur Verarbeitung in benutzerdefinierte Blöcke aufteilen. Sie können beispielsweise Zeitreihendaten für Bereiche wie stündlich, täglich, wöchentlich, monatlich, vierteljährlich, jährlich, benutzerdefiniert oder eine beliebige Kombination davon partitionieren. Wenn Sie für ein Beispiel für Zeitreihendaten die Tabelle nach Stunden partitionieren, enthält jede Partition die Daten einer Stunde. Wenn Sie die Zeitreihentabelle nach Tag partitionieren, enthalten die Partitionen die Daten eines Tages und so weiter. Der Partitionsschlüssel steuert die Größe einer Partition.

Wenn Sie den SQL-Befehl `INSERT` oder `UPDATE` für eine partitionierte Tabelle verwenden, leitet die Datenbank-Engine die Daten an die entsprechende Partition weiter. PostgreSQL-Tabellenpartitionen, die die Daten speichern, sind untergeordnete Tabellen der Haupttabelle.

Während der Lesevorgänge der Datenbankabfrage untersucht der PostgreSQL-Optimierer die `WHERE`-Klausel der Abfrage und leitet den Datenbank-Scan nach Möglichkeit nur an die relevanten Partitionen weiter.

Beginnend mit Version 10 verwendet PostgreSQL deklarative Partitionierung, um die Tabellenpartitionierung zu implementieren. Dies wird auch als native PostgreSQL-Partitionierung

bezeichnet. Vor PostgreSQL Version 10 wurden Auslöser verwendet, um Partitionen zu implementieren.

Die PostgreSQL-Tabellenpartitionierung bietet die folgenden Funktionen:

- Erstellung neuer Partitionen zu jeder Zeit.
- Variable Partitionsbereiche.
- Entfernbare und wiederverwendbare Partitionen mit DDL-Anweisungen (Data Definition Language).

  Zum Beispiel sind entfernbare Partitionen nützlich, um Verlaufsdaten aus der Hauptpartition zu entfernen, aber Verlaufsdaten für die Analyse zu behalten.
- Neue Partitionen erben die Eigenschaften der übergeordneten Datenbanktabelle, einschließlich folgender Eigenschaften:
  - Indizes
  - Primärschlüssel, die die Partitionsschlüsselspalte enthalten müssen
  - Fremdschlüssel
  - Einschränkungen prüfen
  - Referenzen
- Erstellen von Indizes für die vollständige Tabelle oder jede spezifische Partition.

Sie können das Schema für eine einzelne Partition nicht ändern. Sie können jedoch die übergeordnete Tabelle ändern (z. B. das Hinzufügen einer neuen Spalte), die auf Partitionen übertragen wird.

Themen

Übersicht über die PostgreSQL-Erweiterung pg_partman

Sie können die PostgreSQL-Erweiterung `pg_partman` verwenden, um die Erstellung und Pflege von Tabellenpartitionen zu automatisieren. Weitere allgemeine Informationen finden Sie unter PG-Partitions-Manager in der `pg_partman`-Dokumentation.

> **Note**
>
> Die Erweiterung `pg_partman` wird auf den Aurora-PostgreSQL-Versionen 12.6 und höher unterstützt.

Anstatt jede Partition manuell erstellen zu müssen, konfigurieren Sie `pg_partman` mit den folgenden Einstellungen:

- Zu partitionierende Tabelle
- Partitionstyp
- Partitionsschlüssel
- Granularität der Partition
- Optionen für die Erstellung und Verwaltung von Partitionen

Nachdem Sie eine partitionierte PostgreSQL-Tabelle erstellt haben, registrieren Sie diese mit `pg_partman`, indem Sie die Funktion `create_parent` aufrufen. Dadurch werden die erforderlichen Partitionen basierend auf den Parametern erstellt, die Sie an die Funktion übergeben.

Die Erweiterung `pg_partman` bietet auch die Funktion `run_maintenance_proc`, die Sie planmäßig aufrufen können, um Partitionen automatisch zu verwalten. Planen Sie, dass diese Funktion regelmäßig (z. B. stündlich) ausgeführt wird, um sicherzustellen, dass die richtigen Partitionen nach Bedarf erstellt werden. Sie können auch sicherstellen, dass Partitionen automatisch gelöscht werden.

Aktivieren der Erweiterung pg_partman

Wenn Sie mehrere Datenbanken innerhalb derselben PostgreSQL-DB-Instance haben, für die Sie Partitionen verwalten möchten, aktivieren Sie die Erweiterung `pg_partman` für jede Datenbank separat. Um die Erweiterung `pg_partman` für eine bestimmte Datenbank zu aktivieren, erstellen Sie das Partitionswartungsschema und dann die Erweiterung `pg_partman` wie folgt:

```
CREATE SCHEMA partman;
CREATE EXTENSION pg_partman WITH SCHEMA partman;
```

> **Note**
>
> Um die Erweiterung pg_partman zu erstellen, müssen Sie sicherstellen, dass Sie über `rds_superuser`-Berechtigungen verfügen.

Wenn Sie einen Fehler wie den folgenden erhalten, erteilen Sie dem Konto die Berechtigungen `rds_superuser` oder verwenden Sie Ihr Superuser-Konto.

```
ERROR: permission denied to create extension "pg_partman"
HINT: Must be superuser to create this extension.
```

Um die Berechtigungen `rds_superuser` zu erteilen, verbinden Sie sich mit Ihrem Superuser-Konto und führen Sie den folgenden Befehl aus.

```
GRANT rds_superuser TO user-or-role;
```

Für die Beispiele, die die Verwendung der Erweiterung pg_partman zeigen, verwenden wir die folgende Beispieldatenbanktabelle und Partition. Diese Datenbank verwendet eine partitionierte Tabelle basierend auf einem Zeitstempel. Ein `data_mart`-Schema enthält eine Tabelle mit dem Namen `events` mit einer Spalte namens `created_at`. Die folgenden Einstellungen sind in der `events`-Tabelle enthalten:

- Primärschlüssel `event_id` und `created_at`, die die Spalte zur Führung der Partition verwenden müssen.
- Eine CHECK-Beschränkung `ck_valid_operation` zum Durchsetzen von Werten für eine `operation`-Tabellenspalte.
- Zwei Fremdschlüssel, wobei einer `fk_orga_membership)` auf die externe Tabelle `organization` verweist und der andere (`fk_parent_event_id`) ein selbst referenzierter Fremdschlüssel ist.
- Zwei Indizes, wobei einer (`idx_org_id`) für den Fremdschlüssel und der andere (`idx_event_type`) für den Ereignistyp steht.

Die folgenden DDL-Anweisungen erstellen diese Objekte, die automatisch auf jeder Partition enthalten sind.

```
CREATE SCHEMA data_mart;
```

```
CREATE TABLE data_mart.organization ( org_id BIGSERIAL,
        org_name TEXT,
        CONSTRAINT pk_organization PRIMARY KEY (org_id)
    );

CREATE TABLE data_mart.events(
        event_id        BIGSERIAL,
        operation       CHAR(1),
        value           FLOAT(24),
        parent_event_id BIGINT,
        event_type      VARCHAR(25),
        org_id          BIGSERIAL,
        created_at      timestamp,
        CONSTRAINT pk_data_mart_event PRIMARY KEY (event_id, created_at),
        CONSTRAINT ck_valid_operation CHECK (operation = 'C' OR operation = 'D'),
        CONSTRAINT fk_orga_membership
            FOREIGN KEY(org_id)
            REFERENCES data_mart.organization (org_id),
        CONSTRAINT fk_parent_event_id
            FOREIGN KEY(parent_event_id, created_at)
            REFERENCES data_mart.events (event_id,created_at)
    ) PARTITION BY RANGE (created_at);

CREATE INDEX idx_org_id     ON  data_mart.events(org_id);
CREATE INDEX idx_event_type ON  data_mart.events(event_type);
```

Konfigurieren von Partitionen mit der create_parent-Funktion

Nachdem Sie die Erweiterung `pg_partman` aktiviert haben, verwenden Sie die `create_parent`-Funktion, um Partitionen innerhalb des Partitionswartungsschemas zu konfigurieren. Im folgenden Beispiel wird das `events`-Tabellenbeispiel verwendet, das in Aktivieren der Erweiterung pg_partman erstellt wurde. Rufen Sie die `create_parent`-Funktion wie folgt auf.

```
SELECT partman.create_parent( p_parent_table => 'data_mart.events',
 p_control => 'created_at',
 p_type => 'native',
 p_interval=> 'daily',
 p_premake => 30);
```

Dabei werden die folgenden Parameter verwendet:

- `p_parent_table` – Die übergeordnete partitionierte Tabelle. Diese Tabelle muss bereits existieren und einschließlich des Schemas vollständig qualifiziert sein.
- `p_control` – Die Spalte, auf der die Partitionierung basieren soll. Der Datentyp muss ganzzahlig oder zeitbasiert sein.
- `p_type` – Der Typ ist entweder `'native'` oder `'partman'`. In der Regel verwenden Sie den `native` Typ für seine Leistungsverbesserungen und Flexibilität. Der `partman`-Typ beruht auf Vererbung.
- `p_interval` – Das Zeitintervall oder der Ganzzahlbereich für jede Partition. Beispielwerte sind `daily`, stündlich und so weiter.
- `p_premake` – Die Anzahl der Partitionen, die im Voraus erstellt werden müssen, um neue Inserts zu unterstützen.

Eine vollständige Beschreibung der Funktion `create_parent` finden Sie in der `pg_partman`-Dokumentation unter Creation Functions (Erstellungsfunktionen).

Konfigurieren der Partitionspflege mit der run_maintenance_proc-Funktion

Sie können Partitionswartungsvorgänge ausführen, um automatisch neue Partitionen zu erstellen, Partitionen zu trennen oder alte Partitionen zu entfernen. Die Partitionspflege beruht auf der Funktion `run_maintenance_proc` von der `pg_partman`-Erweiterung und der Erweiterung `pg_cron`, die einen internen Scheduler initiiert. Der `pg_cron`-Scheduler führt automatisch SQL-Anweisungen, -Funktionen und -Prozesse aus, die in Ihren Datenbanken definiert sind.

Im folgenden Beispiel wird das `events`-Tabellenbeispiel verwendet, das in Aktivieren der Erweiterung pg_partman erstellt wurde, um die automatische Ausführung der Partitionswartung festzulegen. Fügen Sie als Voraussetzung `pg_cron` zum Parameter `shared_preload_libraries` in der Parametergruppe der DB-Instance hinzu.

```
CREATE EXTENSION pg_cron;

UPDATE partman.part_config
SET infinite_time_partitions = true,
    retention = '3 months',
    retention_keep_table=true
WHERE parent_table = 'data_mart.events';
SELECT cron.schedule('@hourly', $$CALL partman.run_maintenance_proc()$$);
```

Nachfolgend finden Sie eine Schritt-für-Schritt-Erklärung für das vorangehende Beispiel:

1. Ändern Sie die mit Ihrer DB-Instance verknüpfte Parametergruppe und fügen Sie `pg_cron` dem `shared_preload_libraries`-Parameterwert hinzu. Diese Änderung erfordert einen Neustart der DB-Instance, damit sie wirksam wird. Weitere Informationen finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.
2. Führen Sie den Befehl `CREATE EXTENSION pg_cron;` mit einem Konto aus, das die `rds_superuser`-Berechtigungen besitzt. Dadurch wird die Erweiterung `pg_cron` aktiviert. Weitere Informationen finden Sie unter Planen der Wartung mit der PostgreSQL-Erweiterung pg_cron.
3. Führen Sie den Befehl `UPDATE partman.part_config` aus, um die `pg_partman`-Einstellungen für die Tabelle `data_mart.events` anzupassen.
4. Führen Sie den Befehl aus `SET . . .` um die `data_mart.events`-Tabelle mit den folgenden Klauseln zu konfigurieren:
   a. `infinite_time_partitions = true,` – Konfiguriert die Tabelle so, dass automatisch neue Partitionen ohne Begrenzung erstellt werden können.
   b. `retention = '3 months',` – Konfiguriert die Tabelle so, dass sie eine maximale Beibehaltung von drei Monaten hat.
   c. `retention_keep_table=true` – Konfiguriert die Tabelle so, dass die Tabelle bei Fälligkeit der Aufbewahrungsfrist nicht automatisch gelöscht wird. Stattdessen werden Partitionen, die älter als die Aufbewahrungsfrist sind, nur von der übergeordneten Tabelle getrennt.
5. Führen Sie den Befehl aus `SELECT cron.schedule . . .` um einen `pg_cron`-Funktionsaufruf zu machen. Dieser Aufruf definiert, wie oft der Scheduler das `pg_partman`-Wartungsverfahren `partman.run_maintenance_proc` ausführt. In diesem Beispiel wird der Prozess stündlich ausgeführt.

Eine vollständige Beschreibung der `run_maintenance_proc`-Funktion finden Sie in der `pg_partman`-Dokumentation unter Maintenance Functions (Wartungsfunktionen).

Planen der Wartung mit der PostgreSQL-Erweiterung pg_cron

Sie können die PostgreSQL-Erweiterung `pg_cron` verwenden, um Wartungsbefehle innerhalb einer PostgreSQL-Datenbank zu planen. Weitere Informationen zu der Erweiterung finden Sie unter Was ist pg_cron? in der pg_cron-Dokumentation.

Die Erweiterung `pg_cron` wird von Aurora-PostgreSQL-Versionen 12.6 und höher unterstützt.

Weitere Informationen zur Verwendung von pg_cron finden Sie unter Planen von Aufträgen mit pg_cron auf RDS für PostgreSQL oder Ihren Datenbanken der mit Aurora PostgreSQL kompatiblen Edition.

Themen

- Einrichten der pg_con-Erweiterung
- Gewähren von Berechtigungen zur Verwendung von pg_cron für Datenbankbenutzer
- Planen von pg_cron-Aufträgen
- Referenz für die pg_cron-Erweiterung

Einrichten der pg_con-Erweiterung

Richten Sie die Erweiterung pg_cron wie folgt ein:

1. Ändern Sie die benutzerdefinierte Parametergruppe, die mit Ihrer PostgreSQL-DB-Instance verknüpft ist, indem Sie pg_cron dem Parameterwert shared_preload_libraries hinzufügen.

   Starten Sie die PostgreSQL-DB-Instance neu, damit die Änderungen an der Parametergruppe in Kraft treten. Weitere Informationen zum Arbeiten mit Parametergruppen finden Sie unter Amazon-Aurora-PostgreSQL-Parameter.
2. Nachdem die PostgreSQL-DB-Instance neu gestartet wurde, führen Sie den folgenden Befehl mit einem Konto aus, das über rds_superuser-Berechtigungen verfügt. Wenn Sie beispielsweise beim Erstellen Ihres Aurora-PostgreSQL-DB-Clusters die Standardeinstellungen verwendet haben, verbinden Sie sich als Benutzer postgres und erstellen Sie die Erweiterung.

   ```
   CREATE EXTENSION pg_cron;
   ```

   Der Scheduler pg_cron ist in der standardmäßigen PostgreSQL-Datenbank mit dem Namen postgres festgelegt. Die Objekte pg_cron werden in dieser postgres-Datenbank erstellt und alle Planungsaktionen werden in dieser Datenbank ausgeführt.
3. Sie können die Standardeinstellungen verwenden oder Aufgaben für die Ausführung in anderen Datenbanken innerhalb Ihrer PostgreSQL-DB-Instance planen. Informationen zum Planen von Aufgaben für andere Datenbanken innerhalb Ihrer PostgreSQL-DB-Instance finden Sie im Beispiel unter Planen einer Cron-Aufgabe für eine andere als die Standard-Datenbank.

Gewähren von Berechtigungen zur Verwendung von pg_cron für Datenbankbenutzer

Zum Installieren der Erweiterung `pg_cron` sind `rds_superuser`-Berechtigungen erforderlich. Berechtigungen zur Verwendung von `pg_cron` können anderen Datenbankbenutzern (von einem Mitglied der Gruppe/Rolle `rds_superuser`) gewährt werden, damit diese ihre eigenen Aufträge planen können. Wir empfehlen Ihnen, dem `cron`-Schema Berechtigungen nur nach Bedarf, wenn es die Abläufe in Ihrer Produktionsumgebung verbessert, zu gewähren.

Führen Sie den folgenden Befehl aus, um einem Datenbankbenutzer Berechtigungen im `cron`-Schema zu erteilen:

```
postgres=> GRANT USAGE ON SCHEMA cron TO db-user;
```

Damit wird die *`db-user`*-Berechtigung für den Zugriff auf das `cron`-Schema gwährt, um cron-Aufträge für die Objekte zu planen, für die sie Zugriffsberechtigungen haben. Wenn der Datenbankbenutzer keine Berechtigungen hat, schlägt der Auftrag fehl, nachdem die Fehlermeldung in der `postgresql.log`-Datei angezeigt wurde, wie nachfolgend dargestellt:

```
2020-12-08 16:41:00 UTC::@:[30647]:ERROR: permission denied for table table-name
2020-12-08 16:41:00 UTC::@:[27071]:LOG: background worker "pg_cron" (PID 30647) exited
 with exit code 1
```

Mit anderen Worten, stellen Sie sicher, dass Datenbankbenutzer, denen Berechtigungen für das `cron` Schema gewährt werden, auch über Berechtigungen für die Objekte (Tabellen, Schemata usw.) verfügen, die sie planen möchten.

Die Details des Cron-Auftrags und dessen Erfolg oder Misserfolg werden ebenfalls in der `cron.job_run_details` Tabelle erfasst. Weitere Informationen finden Sie unter Tabellen zum Planen von Jobs und zur Erfassung des Status .

Planen von pg_cron-Aufträgen

Die folgenden Abschnitte zeigen, wie Sie verschiedene Verwaltungsaufgaben mit `pg_cron`-Aufträgen planen können.

> **Note**
>
> Wenn Sie `pg_cron`-Aufträge erstellen, überprüfen Sie, dass die Einstellung `max_worker_processes` größer ist als die Anzahl von `cron.max_running_jobs`. Ein

pg_cron-Auftrag schlägt fehl, wenn keine Hintergrund-Workerprozesse ausgeführt werden. Die Standardanzahl von pg_cron-Aufträgen ist 5. Weitere Informationen finden Sie unter Parameter für die Verwaltung der pg_cron-Erweiterung.

Themen

- Bereinigen von Tabellen
- Löschen der Verlaufstabelle pg_cron
- Protokollieren von Fehlern nur in der Datei postgresql.log
- Planen einer Cron-Aufgabe für eine andere als die Standard-Datenbank

Bereinigen von Tabellen

Autovacuum übernimmt die Entfernung für die meisten Fälle Möglicherweise möchten Sie jedoch eine Bereinigung für eine bestimmte Tabelle zu einem Zeitpunkt Ihrer Wahl planen.

Es folgt ein Beispiel für die Verwendung der Funktion `cron.schedule` zum Einrichten eines Auftrags, der jeden Tag um 22:00 Uhr (GMT) `VACUUM FREEZE` auf eine bestimmte Tabelle anwenden soll.

```
SELECT cron.schedule('manual vacuum', '0 22 * * *', 'VACUUM FREEZE pgbench_accounts');
 schedule
----------
1
(1 row)
```

Nachdem das vorangehende Beispiel ausgeführt wurde, können Sie den Verlauf in der `cron.job_run_details`-Tabelle wie folgt überprüfen.

```
postgres=> SELECT * FROM cron.job_run_details;
jobid  | runid | job_pid | database | username | command                          |
 status    | return_message | start_time                    | end_time
-------+-------+---------+----------+----------+-------------------------------
+-----------+----------------+-------------------------------
+-------------------------------
 1     | 1     | 3395    | postgres | adminuser| vacuum freeze pgbench_accounts
 | succeeded | VACUUM         | 2020-12-04 21:10:00.050386+00 | 2020-12-04
 21:10:00.072028+00
```

```
(1 row)
```

Im Folgenden finden Sie eine Abfrage der `cron.job_run_details` Tabelle, um die fehlgeschlagenen Aufträge anzuzeigen.

```
postgres=> SELECT * FROM cron.job_run_details WHERE status = 'failed';
jobid | runid | job_pid | database | username | command                        | status
 | return_message                                | start_time                    |
 end_time
------+-------+---------+----------+----------+--------------------------------+--------
+-----------------------------------------------+-------------------------------
+-------------------------------
 5    | 4     | 30339   | postgres | adminuser| vacuum freeze pgbench_account | failed
 | ERROR: relation "pgbench_account" does not exist | 2020-12-04 21:48:00.015145+00 |
 2020-12-04 21:48:00.029567+00
(1 row)
```

Weitere Informationen finden Sie unter Tabellen zum Planen von Jobs und zur Erfassung des Status .

Löschen der Verlaufstabelle pg_cron

Die `cron.job_run_details`-Tabelle enthält einen Verlauf von Cron-Aufgaben, die im Laufe der Zeit sehr groß werden können. Wir empfehlen Ihnen, eine Aufgabe zu planen, die diese Tabelle bereinigt. Beispielsweise kann es für die Fehlerbehebung ausreichen, die Eingaben einer Woche beizubehalten.

Im folgenden Beispiel wird die cron.schedule-Funktion verwendet, um eine Aufgabe zu planen, die jeden Tag um Mitternacht ausgeführt wird, um die `cron.job_run_details`-Tabelle zu bereinigen. Die Aufgabe behält nur die letzten sieben Tage. Verwenden Sie Ihr `rds_superuser`-Konto, um die Aufgabe wie folgt zu planen.

```
SELECT cron.schedule('0 0 * * *', $$DELETE
    FROM cron.job_run_details
    WHERE end_time < now() - interval '7 days'$$);
```

Weitere Informationen finden Sie unter Tabellen zum Planen von Jobs und zur Erfassung des Status .

Protokollieren von Fehlern nur in der Datei postgresql.log

Wenn Sie verhindern möchten, dass in die `cron.job_run_details`-Tabelle geschrieben wird, ändern Sie die mit der PostgreSQL-DB-Instance verknüpfte Parametergruppe und deaktivieren Sie

den Parameter `cron.log_run`. Es werden keine Schreibvorgänge der `pg_cron`-Erweiterung in die Tabelle mehr durchgeführt und nur noch Fehler in der `postgresql.log`-Datei erfasst. Weitere Informationen finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.

Verwenden Sie den folgenden Befehl, um den Wert des `cron.log_run`-Parameters zu überprüfen.

```
postgres=> SHOW cron.log_run;
```

Weitere Informationen finden Sie unter Parameter für die Verwaltung der pg_cron-Erweiterung.

Planen einer Cron-Aufgabe für eine andere als die Standard-Datenbank

Die Metadaten für `pg_cron` werden alle in der PostgreSQL-Standarddatenbank mit dem Namen `postgres` gespeichert. Da Hintergrund-Worker für die Ausführung der Maintenance-Cron-Aufgaben verwendet werden, können Sie eine Aufgabe in jeder Ihrer Datenbanken innerhalb der PostgreSQL-DB-Instance planen.

1. Planen Sie die Aufgabe in der Cron-Datenbank wie gewohnt mit cron.schedule.

   ```
   postgres=> SELECT cron.schedule('database1 manual vacuum', '29 03 * * *', 'vacuum
    freeze test_table');
   ```

2. Aktualisieren Sie als Benutzer mit der `rds_superuser`-Rolle die Datenbankspalte für die soeben erstellte Aufgabe, damit sie in einer anderen Datenbank innerhalb Ihrer PostgreSQL-DB-Instance ausgeführt wird.

   ```
   postgres=> UPDATE cron.job SET database = 'database1' WHERE jobid = 106;
   ```

3. Überprüfen Sie dies, indem Sie die `cron.job`-Tabelle abfragen.

   ```
   postgres=> SELECT * FROM cron.job;
   jobid | schedule    | command                        | nodename  | nodeport |
    database | username  | active | jobname
   ------+-------------+--------------------------------+-----------+----------
   +----------+----------+--------+------------------------
   106   | 29 03 * * * | vacuum freeze test_table       | localhost | 8192     |
    database1| adminuser | t      | database1 manual vacuum
     1   | 59 23 * * * | vacuum freeze pgbench_accounts | localhost | 8192     |
    postgres | adminuser | t      | manual vacuum
   (2 rows)
   ```

> **Note**
>
> In einigen Fällen können Sie eine Cron-Aufgabe hinzufügen, die Sie in einer anderen Datenbank ausführen möchten. Bevor Sie die richtige Datenbankspalte aktualisieren, versucht die Aufgabe in solchen Fällen möglicherweise, in der Standarddatenbank (`postgres`) ausgeführt zu werden. Wenn der Benutzername über Berechtigungen verfügt, wird die Aufgabe erfolgreich in der Standarddatenbank ausgeführt.

Referenz für die pg_cron-Erweiterung

Sie können die folgenden Parameter, Funktionen und Tabellen mit der `pg_cron`-Erweiterung verwenden. Weitere Informationen finden Sie unter Was ist pg_cron? in der pg_cron-Dokumentation.

Themen

- Parameter für die Verwaltung der pg_cron-Erweiterung
- Funktionsreferenz: cron.schedule
- Funktionsreferenz: cron.unschedule
- Tabellen zum Planen von Jobs und zur Erfassung des Status

Parameter für die Verwaltung der pg_cron-Erweiterung

Es folgt eine Liste der Parameter zur Steuerung des Erweiterungsverhaltens von `pg_cron`.

Parameter	Beschreibung
cron.database_name	Die Datenbank, in der `pg_cron`-Metadaten aufbewahrt werden.
`cron.host`	Der Hostname für die Verbindung mit PostgreSQL. Dieser Wert kann nicht verändert werden.
`cron.log_run`	Protokollieren Sie jeden ausgeführten Auftrag in der Tabelle `job_run_details` . Die Werte sind on oder `off`. Weitere Informationen finden

Parameter	Beschreibung
	Sie unter Tabellen zum Planen von Jobs und zur Erfassung des Status .
`cron.log_statement`	Protokolliert alle Cron-Anweisungen, bevor Sie ausgeführt werden. Die Werte sind on oder `off`.
`cron.max_running_jobs`	Die maximale Anzahl von Aufgaben, die gleichzeitig ausgeführt werden können.
`cron.use_background_workers`	Verwenden Sie Hintergrund-Worker anstelle von Client-Sitzungen. Dieser Wert kann nicht verändert werden.

Verwenden Sie den folgenden SQL-Befehl, um diese Parameter und ihre Werte anzuzeigen.

```
postgres=> SELECT name, setting, short_desc FROM pg_settings WHERE name LIKE 'cron.%'
 ORDER BY name;
```

Funktionsreferenz: cron.schedule

Diese Funktion plant eine Cron-Aufgabe. Die Aufgabe ist anfänglich in der `postgres` Standarddatenbank geplant. Die Funktion gibt einen `bigint` Wert zurück, der den Aufgabenbezeichner darstellt. Informationen zum Planen von Aufgaben für die Ausführung in anderen Datenbanken innerhalb Ihrer PostgreSQL-DB-Instance finden Sie im Beispiel unter Planen einer Cron-Aufgabe für eine andere als die Standard-Datenbank.

Die Funktion hat zwei Syntaxformate.

Syntax

```
cron.schedule (job_name,
    schedule,
    command
);

cron.schedule (schedule,
    command
```

```
);
```

Parameter

Parameter	Beschreibung
`job_name`	Der Name der Cron-Aufgabe.
`schedule`	Text, der den Zeitplan für die Cron-Aufgabe angibt. Das Format ist das Standard-Cron-Format.
`command`	Text des auszuführenden Befehls.

Beispiele

```
postgres=> SELECT cron.schedule ('test','0 10 * * *', 'VACUUM pgbench_history');
 schedule
----------
      145
(1 row)

postgres=> SELECT cron.schedule ('0 15 * * *', 'VACUUM pgbench_accounts');
 schedule
----------
      146
(1 row)
```

Funktionsreferenz: cron.unschedule

Diese Funktion löscht eine Cron-Aufgabe. Sie können entweder den `job_name` oder die `job_id` angeben. Eine Richtlinie stellt sicher, dass Sie der Besitzer sind, um den Plan für die Aufgabe zu entfernen. Die Funktion gibt einen Booleschen Wert zurück, der Erfolg oder Misserfolg anzeigt.

Die Funktion weist die folgende Syntax auf.

Syntax

```
cron.unschedule (job_id);
```

```
cron.unschedule (job_name);
```

Parameter

Parameter	Beschreibung
`job_id`	Ein Aufgabenbezeichner, der von der `cron.schedule` Funktion zurückgegeben wurde, als die Cron-Aufgabe geplant wurde.
`job_name`	Der Name einer Cron-Aufgabe, die mit der `cron.schedule` Funktion geplant wurde.

Beispiele

```
postgres=> SELECT cron.unschedule(108);
 unschedule
------------
 t
(1 row)

postgres=> SELECT cron.unschedule('test');
 unschedule
------------
 t
(1 row)
```

Tabellen zum Planen von Jobs und zur Erfassung des Status

Die folgenden Tabellen werden verwendet, um die Cron-Aufgaben zu planen und aufzuzeichnen, wie die Aufgaben abgeschlossen wurden.

Tabelle	Beschreibung
`cron.job`	Enthält die Metadaten zu jeder geplanten Aufgabe. Die meisten Interaktionen mit dieser Tabelle sollten über die Funktionen `cron.schedule` und `cron.unschedule` erfolgen.

Tabelle	Beschreibung
	Important Wir empfehlen, dieser Tabelle keine Aktualisierungs- oder Einfügeberechtigungen zu gewähren. Dies würde es dem Benutzer ermöglichen, die `username`-Spalte zu aktualisieren, die als `rds-superuser` ausgeführt wird.
`cron.job_run_details`	Enthält Verlaufsdaten zu vergangenen geplanten Aufträgen , die ausgeführt wurden. Dies ist nützlich, um den Status, die Rückgabe von Nachrichten sowie die Start- und Endzeit des ausgeführten Auftrags zu untersuchen. **Note** Um zu verhindern, dass diese Tabelle ins Unendliche wächst, bereinigen Sie sie in regelmäßigen Abständen. Ein Beispiel finden Sie unter Löschen der Verlaufstabelle pg_cron.

Verwenden von pgAudit zur Protokollierung der Datenbankaktivität

Finanzinstitute, Behörden und viele Branchen müssen Audit-Protokolle aufbewahren, um die gesetzlichen Bestimmungen zu erfüllen. Durch die Verwendung der PostgreSQL-Audit-Erweiterung (pgAudit) mit Ihrem DB-Cluster von Aurora PostgreSQL können Sie die detaillierten Datensätze erfassen, die normalerweise von Prüfern oder zur Erfüllung gesetzlicher Bestimmungen benötigt werden. Sie können beispielsweise die pgAudit-Erweiterung einrichten, um Änderungen an bestimmten Datenbanken und Tabellen nachzuverfolgen, den Benutzer zu erfassen, der die Änderung vorgenommen hat, und viele andere Details.

Die pgAudit-Erweiterung baut auf der Funktionalität der nativen PostgreSQL-Protokollierungsinfrastruktur auf, indem sie die Protokollmeldungen um Details erweitert. Mit anderen Worten, Sie verwenden für die Anzeige Ihres Audit-Protokolls den gleichen Ansatz wie für die Anzeige von Protokollmeldungen. Weitere Informationen zur PostgreSQL-Protokollierung finden Sie unter Datenbank-Protokolldateien von Aurora PostgreSQL.

Die pgAudit-Erweiterung redigiert sensible Daten wie Klartext-Passwörter aus den Protokollen. Wenn Ihr DB-Cluster von Aurora PostgreSQL so konfiguriert ist, dass Data Manipulation Language (DML)-Anweisungen protokolliert werden, wie in Aktivieren der Abfrageprotokollierung für Ihren DB-Cluster von Aurora PostgreSQL beschrieben, können Sie das Klartext-Passwortproblem mithilfe der PostgreSQL-Audit-Erweiterung vermeiden.

Sie können das Auditing für Ihre Datenbank-Instances mit einem hohen Grad an Spezifität konfigurieren. Sie können alle Datenbanken und alle Benutzer überprüfen. Sie können auch festlegen, dass nur bestimmte Datenbanken, Benutzer und andere Objekte überprüft werden. Bestimmte Benutzer und Datenbanken können Sie auch explizit von der Prüfung ausschließen. Weitere Informationen finden Sie unter Benutzer oder Datenbanken von der Audit-Protokollierung ausschließen.

Angesichts der Menge an Details, die erfasst werden können, empfehlen wir, dass Sie bei Verwendung von pgAudit Ihren Speicherverbrauch überwachen.

Die pgAudit-Erweiterung wird von allen verfügbaren Aurora-PostgreSQL-Versionen unterstützt. Eine Liste der pgAudit-Versionen, die von Aurora PostgreSQL unterstützt werden, finden Sie unter Versionen der Erweiterungen für Amazon Aurora PostgreSQL in den Versionshinweisen für Aurora PostgreSQL.

Themen

- Einrichten der pgAudit-Erweiterung
- Überprüfen von Datenbankobjekten
- Benutzer oder Datenbanken von der Audit-Protokollierung ausschließen
- Referenz für die pgAudit-Erweiterung

Einrichten der pgAudit-Erweiterung

Wenn Sie die pgAudit-Erweiterung auf einrichten möchten, fügen Sie zunächst pgAudit zu den gemeinsam genutzten Bibliotheken in der benutzerdefinierten DB-Cluster-Parametergruppe für Ihren DB-Cluster von Aurora PostgreSQL hinzu. Weitere Informationen über das Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe finden Sie unter Arbeiten mit Parametergruppen. Als Nächstes installieren Sie die pgAudit-Erweiterung. Abschließend geben Sie die Datenbanken und Objekte an, die Sie überprüfen möchten. Die Schritte in diesem Abschnitt veranschaulichen die Vorgehensweise. Sie können die AWS Management Console oder die AWS CLI verwenden.

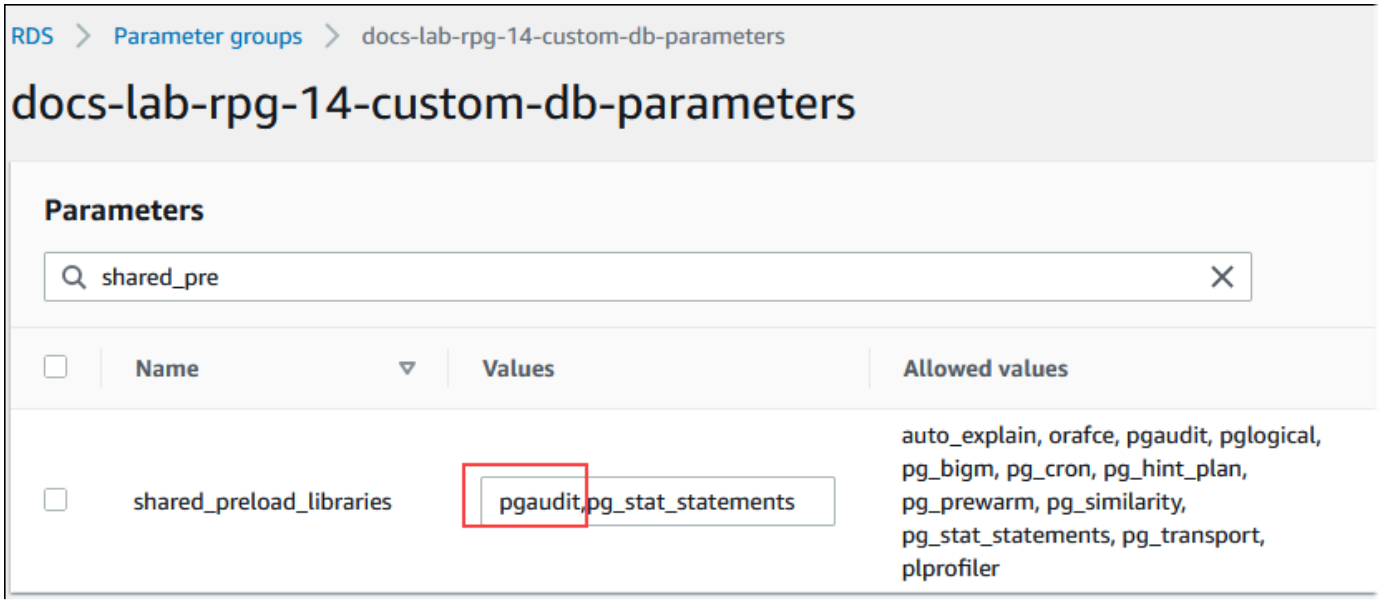
Sie müssen über Berechtigungen als `rds_superuser`-Rolle verfügen, um alle diese Aufgaben ausführen zu können.

Bei den folgenden Schritten wird davon ausgegangen, dass Ihr DB-Cluster von Aurora PostgreSQL einer benutzerdefinierten DB-Cluster -Parametergruppe zugeordnet ist.

Konsole

So richten Sie die pgAudit-Erweiterung ein

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Ihre Writer-Instance des DB-Clusters von Aurora PostgreSQL aus.
3. Öffnen Sie die Registerkarte Configuration (Konfiguration) für Ihre Writer-Instance des DB-Clusters von Aurora PostgreSQL. Suchen Sie in den Instance-Details den Link Parameter group (Parametergruppe).
4. Wählen Sie den Link aus, um die benutzerdefinierten Parameter zu öffnen, die Ihrem DB-Cluster von Aurora PostgreSQL zugeordnet sind.
5. Geben Sie in das Suchfeld Parameters (Parameter) `shared_pre` ein, um den `shared_preload_libraries`-Parameter zu finden.
6. Wählen Sie Edit parameters (Parameter bearbeiten) aus, um auf die Eigenschaftswerte zuzugreifen.
7. Fügen Sie `pgaudit` der Liste im Feld Values (Werte) hinzu. Verwenden Sie ein Komma, um Elemente in der Werteliste zu trennen.



8. Starten Sie die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL neu, damit Ihre Änderung des `shared_preload_libraries`-Parameters wirksam wird.
9. Wenn die Instance verfügbar ist, stellen Sie sicher, dass pgAudit initialisiert wurde. Stellen Sie über `psql` eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her und führen Sie den folgenden Befehl aus.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pgaudit
(1 row)
```

10. Wenn pgAudit initialisiert ist, können Sie jetzt die Erweiterung erstellen. Sie müssen die Erweiterung nach dem Initialisieren der Bibliothek erstellen, da die `pgaudit`-Erweiterung Ereignisauslöser für die Überwachung von Data Definition Language (DDL)-Anweisungen installiert.

```
CREATE EXTENSION pgaudit;
```

11. Schließen Sie die `psql`-Sitzung.

```
labdb=> \q
```

12. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

13. Suchen Sie den `pgaudit.log`-Parameter in der Liste und legen Sie den entsprechenden Wert für Ihren Anwendungsfall fest. Wenn Sie beispielsweise den `pgaudit.log`-Parameter auf `write` festlegen, wie in der folgenden Abbildung gezeigt, werden Einfügungen, Aktualisierungen, Löschungen und einige andere Typänderungen im Protokoll erfasst.

Sie können auch einen der folgenden Werte für den `pgaudit.log`-Parameter auswählen.

- „none“: Dies ist der Standardwert. Es werden keine Datenbankänderungen protokolliert.
- „all“: Es wird alles protokolliert (Lesen, Schreiben, Funktion, Rolle, DDL, Verschiedenes).
- „ddl“: Protokolliert alle Data Definition Language (DDL)-Anweisungen, die nicht in der `ROLE`-Klasse enthalten sind.
- „function“: Protokolliert Funktionsaufrufe und `DO`-Blöcke.
- „misc“: Protokolliert verschiedene Befehle wie `DISCARD`, `FETCH`, `CHECKPOINT`, `VACUUM` und `SET`.
- „read“: Protokolliert `SELECT` und `COPY`, wenn die Quelle eine Beziehung (z. B. eine Tabelle) oder eine Abfrage ist.
- „role“: Protokolliert Anweisungen in Bezug auf Rollen und Berechtigungen wie `GRANT`, `REVOKE`, `CREATE ROLE`, `ALTER ROLE` und `DROP ROLE`.
- „write“: Protokolliert `INSERT`, `UPDATE`, `DELETE`, `TRUNCATE` und `COPY`, wenn das Ziel eine Beziehung (Tabelle) ist.

14. Wählen Sie Änderungen speichern aus.
15. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

16. Wählen Sie aus der Liste der Datenbanken Ihre Writer-Instance des DB-Clusters von Aurora PostgreSQL und dann im Menü „Actions“ (Aktionen) die Option Reboot (Neustart) aus.

AWS CLI

So richten Sie pgAudit ein

Um pgAudit mit der einzurichtenAWS CLI, rufen Sie die -modify-db-parameter-groupOperation auf, um die Audit-Protokollparameter in Ihrer benutzerdefinierten Parametergruppe zu ändern, wie im folgenden Verfahren gezeigt.

1. Verwenden Sie den folgenden AWS CLI-Befehl, um dem `shared_preload_libraries`-Parameter `pgaudit` hinzuzufügen.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=pgaudit,ApplyMethod=pending-
reboot" \
   --region aws-region
```

2. Verwenden Sie den folgendenAWS CLI Befehl, um die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL neu zu starten, sodass die pgaudit-Bibliothek initialisiert wird.

```
aws rds reboot-db-instance \
    --db-instance-identifier writer-instance \
    --region aws-region
```

3. Wenn die Instance verfügbar ist, können Sie überprüfen, ob `pgaudit` initialisiert wurde. Stellen Sie über `psql` eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her und führen Sie den folgenden Befehl aus.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pgaudit
(1 row)
```

   Wenn pgAudit initialisiert ist, können Sie jetzt die Erweiterung erstellen.

```
CREATE EXTENSION pgaudit;
```

4. Schließen Sie die `psql`-Sitzung, damit Sie die AWS CLI verwenden können.

```
labdb=> \q
```

5. Verwenden Sie den folgenden AWS CLI-Befehl, um die Anweisungsklassen anzugeben, die von der Sitzungsüberwachungsprotokollierung erfasst werden sollen. Im Beispiel wird der `pgaudit.log`-Parameter auf `write` festgelegt, wodurch Einfügungen, Aktualisierungen und Löschungen im Protokoll erfasst werden.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=pgaudit.log,ParameterValue=write,ApplyMethod=pending-reboot" \
   --region aws-region
```

Sie können auch einen der folgenden Werte für den `pgaudit.log`-Parameter auswählen.

- „none“: Dies ist der Standardwert. Es werden keine Datenbankänderungen protokolliert.
- „all“: Es wird alles protokolliert (Lesen, Schreiben, Funktion, Rolle, DDL, Verschiedenes).
- „ddl“: Protokolliert alle Data Definition Language (DDL)-Anweisungen, die nicht in der `ROLE`-Klasse enthalten sind.
- „function“: Protokolliert Funktionsaufrufe und `DO`-Blöcke.
- „misc“: Protokolliert verschiedene Befehle wie `DISCARD`, `FETCH`, `CHECKPOINT`, `VACUUM` und `SET`.
- „read“: Protokolliert `SELECT` und `COPY`, wenn die Quelle eine Beziehung (z. B. eine Tabelle) oder eine Abfrage ist.
- „role“: Protokolliert Anweisungen in Bezug auf Rollen und Berechtigungen wie `GRANT`, `REVOKE`, `CREATE ROLE`, `ALTER ROLE` und `DROP ROLE`.
- „write“: Protokolliert `INSERT`, `UPDATE`, `DELETE`, `TRUNCATE` und `COPY`, wenn das Ziel eine Beziehung (Tabelle) ist.

Starten Sie die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL mit dem folgenden AWS CLI-Befehl neu.

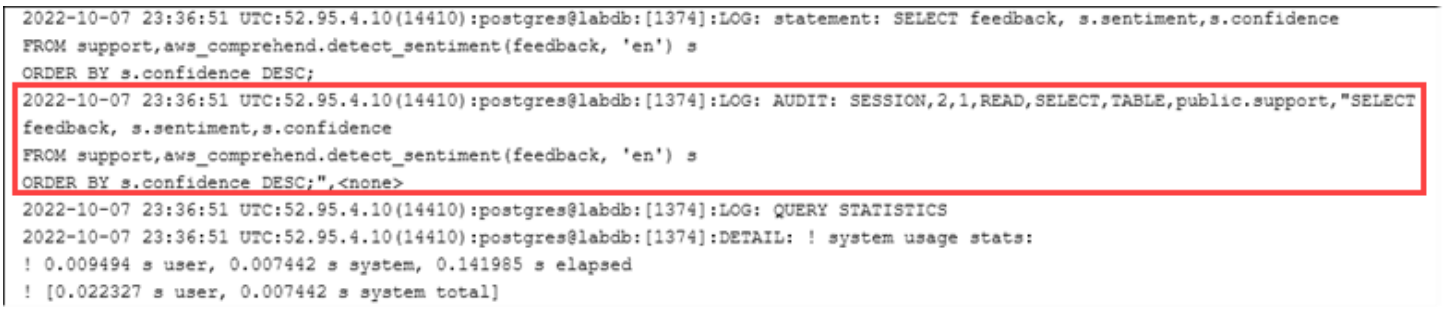
```
aws rds reboot-db-instance \
    --db-instance-identifier writer-instance \
    --region aws-region
```

Überprüfen von Datenbankobjekten

Wenn pgAudit auf Ihrem DB-Cluster von Aurora PostgreSQL eingerichtet und für Ihre Anforderungen konfiguriert ist, werden detailliertere Informationen im PostgreSQL-Protokoll erfasst. Während die PostgreSQL-Standardprotokollierungskonfiguration beispielsweise das Datum und die Uhrzeit angibt, zu der eine Änderung in einer Datenbanktabelle vorgenommen wurde, kann der Protokolleintrag mit der pgAudit-Erweiterung das Schema, den Benutzer, der die Änderung vorgenommen hat, und andere Details enthalten, je nachdem, wie die Erweiterungsparameter konfiguriert sind. Sie können das Auditing einrichten, um Änderungen wie folgt zu verfolgen.

- Für jede Sitzung, nach Benutzer. Auf der Sitzungsebene können Sie den vollständig qualifizierten Befehlstext erfassen.
- Für jedes Objekt, nach Benutzer und nach Datenbank.

Die Objektüberwachungsfunktion wird aktiviert, wenn Sie die `rds_pgaudit`-Rolle in Ihrem System erstellen und diese Rolle dann dem `pgaudit.role`-Parameter in Ihrer benutzerdefinierten Parametergruppe hinzufügen. Standardmäßig ist der `pgaudit.role`-Parameter nicht festgelegt und der einzig zulässige Wert ist `rds_pgaudit`. Bei den folgenden Schritten wird davon ausgegangen, dass `pgaudit` initialisiert wurde und Sie die `pgaudit`-Erweiterung gemäß den Schritten unter Einrichten der pgAudit-Erweiterung erstellt haben.



Wie in diesem Beispiel gezeigt, enthält die Zeile „LOG: AUDIT: SESSION“ unter anderem Informationen über die Tabelle und deren Schema.

So richten Sie die Objektüberwachung ein

1. Stellen Sie über `psql` eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her.

```
psql --host=your-instance-name.aws-region.rds.amazonaws.com --port=5432 --
username=postgrespostgres --password --dbname=labdb
```

2. Erstellen Sie mithilfe des folgenden Befehls eine Datenbankrolle mit dem Namen `rds_pgaudit`.

```
labdb=> CREATE ROLE rds_pgaudit;
CREATE ROLE
labdb=>
```

3. Schließen Sie die `psql`-Sitzung.

```
labdb=> \q
```

   Verwenden Sie in den nächsten Schritten die AWS CLI, um die Audit-Protokollparameter in Ihrer benutzerdefinierten Parametergruppe zu ändern.

4. Verwenden Sie den folgenden AWS CLI-Befehl, um den `pgaudit.role`-Parameter auf `rds_pgaudit` festzulegen. Standardmäßig ist dieser Parameter leer und der einzig zulässige Wert ist `rds_pgaudit`.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=pgaudit.role,ParameterValue=rds_pgaudit,ApplyMethod=pending-reboot"
 \
   --region aws-region
```

5. Starten Sie die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL mit dem folgenden AWS CLI-Befehl neu, damit Ihre Änderungen der Parameter wirksam werden.

```
aws rds reboot-db-instance \
    --db-instance-identifier writer-instance \
    --region aws-region
```

6. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass `pgaudit.role` auf `rds_pgaudit` festgelegt ist.

```
SHOW pgaudit.role;
pgaudit.role
-----------------
rds_pgaudit
```

Um die pgAudit-Protokollierung zu testen, können Sie mehrere Beispielbefehle ausführen, die Sie überprüfen möchten. Sie könnten beispielsweise die folgenden Befehle ausführen.

```
CREATE TABLE t1 (id int);
GRANT SELECT ON t1 TO rds_pgaudit;
SELECT * FROM t1;
id
----
(0 rows)
```

Die Datenbankprotokolle sollten dann einen Eintrag ähnlich dem folgenden enthalten.

```
...
2017-06-12 19:09:49 UTC:...:rds_test@postgres:[11701]:LOG: AUDIT:
OBJECT,1,1,READ,SELECT,TABLE,public.t1,select * from t1;
...
```

Weitere Informationen zur Anzeige der Protokolle finden Sie unter Überwachen von Amazon Aurora-Protokolldateien.

Weitere Informationen zur pgAudit-Erweiterung finden Sie unter pgAudit auf GitHub.

Benutzer oder Datenbanken von der Audit-Protokollierung ausschließen

Wie unter Datenbank-Protokolldateien von Aurora PostgreSQL beschrieben, verbrauchen PostgreSQL-Protokolle Speicherplatz. Die Verwendung der pgAudit-Erweiterung erhöht die in Ihren Protokollen gesammelte Datenmenge je nach den von Ihnen verfolgten Änderungen in unterschiedlichem Maße. Möglicherweise müssen Sie nicht jeden Benutzer oder jede Datenbank in Ihrem DB-Cluster von Aurora PostgreSQL überwachen.

Sie können Benutzer und Datenbanken von der Prüfung ausschließen, um die Auswirkungen auf Ihren Speicher zu minimieren und die unnötige Erfassung von Audit-Datensätzen zu vermeiden. Sie können die Protokollierung auch innerhalb einer bestimmten Sitzung ändern. In den nachstehenden Beispielen wird die Vorgehensweise dazu veranschaulicht.

> **Note**
>
> Parametereinstellungen auf Sitzungsebene haben Vorrang vor den Einstellungen in der benutzerdefinierten DB-Cluster-Parametergruppe der Writer-Instance des DB-Clusters von Aurora PostgreSQL. Wenn Sie nicht möchten, dass Datenbankbenutzer Ihre Konfigurationseinstellungen für die Audit-Protokollierung umgehen, müssen Sie ihre Berechtigungen ändern.

Angenommen, Ihr DB-Cluster von Aurora PostgreSQL ist so konfiguriert, dass derselbe Aktivitätsgrad für alle Benutzer und Datenbanken überprüft wird. Sie entscheiden dann, dass Sie den Benutzer `myuser` nicht überprüfen möchten. Sie können das Auditing für `myuser` mit dem folgenden SQL-Befehl deaktivieren.

```
ALTER USER myuser SET pgaudit.log TO 'NONE';
```

Anschließend können Sie die folgende Abfrage verwenden, um die Spalte `user_specific_settings` auf `pgaudit.log` zu überprüfen und zu bestätigen, dass der Parameter auf `NONE` festgelegt ist.

```
SELECT
    usename AS user_name,
    useconfig AS user_specific_settings
FROM
    pg_user
WHERE
    usename = 'myuser';
```

Die Ausgabe sollte folgendermaßen aussehen.

```
 user_name | user_specific_settings
-----------+-----------------------
 myuser    | {pgaudit.log=NONE}
(1 row)
```

Sie können die Protokollierung für einen bestimmten Benutzer während seiner Datenbanksitzung mit dem folgenden Befehl deaktivieren.

```
ALTER USER myuser IN DATABASE mydatabase SET pgaudit.log TO 'none';
```

Verwenden Sie die folgende Abfrage, um die Einstellungsspalte für eine bestimmte Benutzer- und Datenbankkombination auf pgaudit.log zu überprüfen.

```
SELECT
    usename AS "user_name",
    datname AS "database_name",
    pg_catalog.array_to_string(setconfig, E'\n') AS "settings"
FROM
    pg_catalog.pg_db_role_setting s
    LEFT JOIN pg_catalog.pg_database d ON d.oid = setdatabase
    LEFT JOIN pg_catalog.pg_user r ON r.usesysid = setrole
WHERE
    usename = 'myuser'
    AND datname = 'mydatabase'
ORDER BY
    1,
    2;
```

Die Ausgabe entspricht weitgehend der folgenden.

```
  user_name | database_name |     settings
-----------+---------------+------------------
 myuser    | mydatabase    | pgaudit.log=none
(1 row)
```

Nachdem Sie das Auditing für `myuser` deaktiviert haben, entscheiden Sie, dass Sie Änderungen an `mydatabase` nicht verfolgen möchten. Sie können das Auditing für diese spezifische Datenbank mit dem folgenden Befehl deaktivieren.

```
ALTER DATABASE mydatabase SET pgaudit.log to 'NONE';
```

Verwenden Sie dann die folgende Abfrage, um die Spalte database_specific_settings zu überprüfen und zu bestätigen, dass pgaudit.log auf NONE festgelegt ist.

```
SELECT
a.datname AS database_name,
b.setconfig AS database_specific_settings
FROM
pg_database a
FULL JOIN pg_db_role_setting b ON a.oid = b.setdatabase
```

```
WHERE
a.datname = 'mydatabase';
```

Die Ausgabe sollte folgendermaßen aussehen.

```
 database_name | database_specific_settings
---------------+----------------------------
 mydatabase    | {pgaudit.log=NONE}
(1 row)
```

Verwenden Sie den folgenden Befehl, um die Einstellungen wieder auf die Standardeinstellung für myuser festzulegen:

```
ALTER USER myuser RESET pgaudit.log;
```

Verwenden Sie den folgenden Befehl, um die Einstellungen wieder auf die Standardeinstellung für eine Datenbank festzulegen.

```
ALTER DATABASE mydatabase RESET pgaudit.log;
```

Verwenden Sie den folgenden Befehl, um Benutzer und Datenbank wieder auf die Standardeinstellung festzulegen.

```
ALTER USER myuser IN DATABASE mydatabase RESET pgaudit.log;
```

Sie können auch bestimmte Ereignisse im Protokoll erfassen, indem Sie `pgaudit.log` auf einen der anderen zulässigen Werte für den `pgaudit.log`-Parameter festlegen. Weitere Informationen finden Sie unter Liste der zulässigen Einstellungen für den `pgaudit.log`-Parameter.

```
ALTER USER myuser SET pgaudit.log TO 'read';
ALTER DATABASE mydatabase SET pgaudit.log TO 'function';
ALTER USER myuser IN DATABASE mydatabase SET pgaudit.log TO 'read,function'
```

Referenz für die pgAudit-Erweiterung

Sie können den gewünschten Detaillierungsgrad für Ihr Audit-Protokoll angeben, indem Sie einen oder mehrere der in diesem Abschnitt aufgeführten Parameter ändern.

Steuern des pgAudit-Verhaltens

Sie können die Audit-Protokollierung steuern, indem Sie einen oder mehrere der in der folgenden Tabelle aufgeführten Parameter ändern.

Parameter	Beschreibung
`pgaudit.log`	Gibt die Anweisungsklassen an, die durch die Sitzungs-Audit-Protokollierung erfasst werden. Zulässige Werte sind „ddl“, „function“, „misc“, „read“, „role“, „write“, „none“, „all“. Weitere Informationen finden Sie unter Liste der zulässigen Einstellungen für den `pgaudit.log` -Parameter.
`pgaudit.log_catalog`	Wenn diese Option aktiviert ist (auf 1 festgelegt), werden Anweisungen zum Audit-Trail hinzugefügt, wenn sich alle Beziehungen in einer Anweisung in pg_catalog befinden.
`pgaudit.log_level`	Gibt die Protokollstufe an, die für Protokolleinträge verwendet werden soll. Zulässige Werte: „debug5“, „debug4“, „debug3“, „debug2“, „debug1“, „info“, „notice“, „warning“, „log“
`pgaudit.log_parameter`	Wenn diese Option aktiviert ist (auf 1 festgelegt), werden die mit der Anweisung übergebenen Parameter im Audit-Protokoll erfasst.
`pgaudit.log_relation`	Wenn diese Option aktiviert ist (auf 1 festgelegt), erstellt das Audit-Protokoll für die Sitzung einen separaten Protokolleintrag für jede Beziehung (TABLE, VIEW usw.), auf die in einer SELECT- oder DML-Anweisung verwiesen wird.
`pgaudit.log_statement_once`	Gibt an, ob die Protokollierung den Anweisungstext und die Parameter mit dem ersten Protokolleintrag für eine Kombination aus Anweisung/Unteranweisung oder bei jedem Eintrag enthält.
`pgaudit.role`	Gibt die Hauptrolle an, die für die Objektüberwachungsprotokollierung verwendet werden soll. Der einzig zulässige Eintrag ist `rds_pgaudit` .

Liste der zulässigen Einstellungen für den **`pgaudit.log`**-Parameter

Wert	Beschreibung
none	Dies ist die Standardeinstellung. Es werden keine Datenbankänderungen protokolliert.
all	Protokolliert alles (Lesen, Schreiben, Funktion, Rolle, DDL, Verschied enes).
ddl	Protokolliert alle Data Definition Language (DDL)-Anweisungen, die nicht in der `ROLE`-Klasse enthalten sind.
function	Protokolliert Funktionsaufrufe und `DO`-Blöcke.
misc	Protokolliert verschiedene Befehle wie `DISCARD`, `FETCH`, `CHECKPOINT` , `VACUUM` und `SET`.
read	Protokolliert `SELECT` und `COPY`, wenn die Quelle eine Beziehung (z. B. eine Tabelle) oder eine Abfrage ist.
role	Protokolliert Anweisungen in Bezug auf Rollen und Berechtigungen wie `REVOKE`, `CREATE ROLE`, `ALTER ROLE` und `DROP ROLE`.
write	Protokolliert `INSERT`, `UPDATE`, `DELETE`, `TRUNCATE` und `COPY`, wenn das Ziel eine Beziehung (Tabelle) ist.

Um mehrere Ereignistypen mit der Sitzungsüberwachung zu protokollieren, verwenden Sie eine kommagetrennte Liste. Um alle Ereignistypen zu protokollieren, legen Sie `pgaudit.log` auf `ALL` fest. Starten Sie Ihre DB-Instance neu, um die Änderungen zu übernehmen.

Mit der Objektüberwachung können Sie die Überwachungsprotokollierung verfeinern, um mit bestimmten Beziehungen zu arbeiten. Sie können z. B. angeben, dass Sie eine Audit-Protokollierung für `READ`-Vorgänge in einer oder mehreren Tabellen wünschen.

Verwenden von pglogical, um Daten zwischen Instances zu synchronisieren

Alle derzeit verfügbaren Aurora-PostgreSQL-Versionen unterstützen die `pglogical`-Erweiterung. Die Erweiterung pglogical ist älter als die funktionell ähnliche logische Replikationsfunktion, die von

PostgreSQL in Version 10 eingeführt wurde. Weitere Informationen finden Sie unter Verwenden der logischen Replikation von PostgreSQL mit Aurora.

Die `pglogical`-Erweiterung unterstützt die logische Replikation zwischen zwei oder mehr DB-Cluster von Aurora PostgreSQL. Es unterstützt auch die Replikation zwischen verschiedenen PostgreSQL-Versionen und zwischen Datenbanken, die auf DB-Instances von RDS für PostgreSQL und DB-Clustern von Aurora PostgreSQL laufen. Die `pglogical`-Erweiterung verwendet ein Publish-Subscribe-Modell, um Änderungen an Tabellen und anderen Objekten, z. B. Sequenzen, von einem Herausgeber auf einen Abonnenten zu replizieren. Sie stützt sich auf einen Replikationsslot, um sicherzustellen, dass Änderungen von einem Herausgeberknoten zu einem Abonnentenknoten synchronisiert werden. Dies ist wie folgt definiert.

- Der Herausgeberknoten ist der DB-Cluster von Aurora PostgreSQL, der die Datenquelle ist, die auf andere Knoten repliziert werden soll. Der Herausgeberknoten definiert die Tabellen, die in einem Veröffentlichungssatz repliziert werden sollen.
- Der Abonnentenknoten ist der DB-Cluster von Aurora PostgreSQL, der WAL-Updates vom Herausgeber erhält. Der Abonnent erstellt ein Abonnement, um eine Verbindung zum Herausgeber herzustellen und die dekodierten WAL-Daten abzurufen. Wenn der Abonnent das Abonnement erstellt, wird der Replikationsslot auf dem Herausgeberknoten erstellt.

Im Folgenden erfahren Sie, wie Sie die `pglogical`-Erweiterung einrichten.

Themen

Anforderungen und Einschränkungen für die pglogical-Erweiterung

Alle derzeit verfügbaren Versionen von Aurora PostgreSQL unterstützen die `pglogical`-Erweiterung.

Sowohl der Herausgeberknoten als auch der Abonnentenknoten müssen für die logische Replikation eingerichtet sein.

Die Tabellen, die Sie vom Abonnenten zum Herausgeber replizieren möchten, müssen dieselben Namen und dasselbe Schema haben. Diese Tabellen müssen außerdem dieselben Spalten enthalten und diese müssen dieselben Datentypen verwenden. Sowohl die Herausgeber- als auch die Abonnententabelle müssen dieselben Primärschlüssel haben. Wir empfehlen, nur den PRIMARY KEY als eindeutige Einschränkung zu verwenden.

Die Tabellen auf dem Abonnentenknoten können für CHECK-Einschränkungen und NOT NULL-Einschränkungen großzügigere Einschränkungen haben als die Tabellen auf dem Herausgeberknoten.

Die `pglogical`-Erweiterung bietet Funktionen wie die bidirektionale Replikation, die von der logischen Replikationsfunktion, die in PostgreSQL (Version 10 und höher) integriert ist, nicht unterstützt werden. Weitere Informationen finden Sie unter Die bidirektionale PostgreSQL-Replikation mit pglogical.

Einrichten der pglogical-Erweiterung

Wenn Sie die `pglogical`-Erweiterung auf Ihrem DB-Cluster von Aurora PostgreSQL einrichten möchten, fügen Sie zunächst `pglogical` zu den gemeinsam genutzten Bibliotheken in der benutzerdefinierten DB-Cluster-Parametergruppe für Ihren DB-Cluster von Aurora PostgreSQL hinzu. Sie müssen außerdem den Wert des `rds.logical_replication`-Parameters auf 1 festlegen, um die logische Dekodierung zu aktivieren. Abschließend erstellen Sie die Erweiterung in der Datenbank. Für diese Aufgabe können Sie die AWS Management Console oder die AWS CLI verwenden.

Sie müssen über Berechtigungen als `rds_superuser`-Rolle verfügen, um diese Aufgaben ausführen zu können.

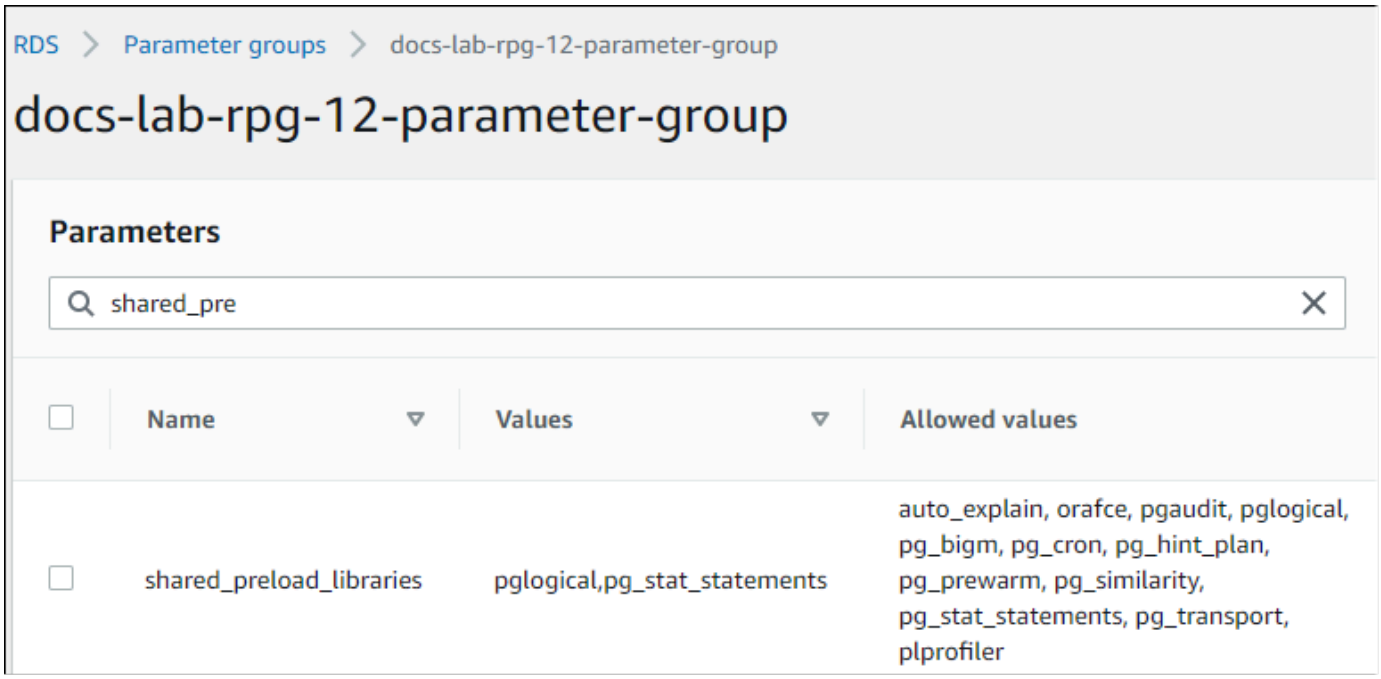
Bei den folgenden Schritten wird davon ausgegangen, dass Ihr DB-Cluster von Aurora PostgreSQL einer benutzerdefinierten DB-Cluster -Parametergruppe zugeordnet ist. Weitere Informationen über das Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe finden Sie unter Arbeiten mit Parametergruppen.

Konsole

So richten Sie die pglogical-Erweiterung ein

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Ihre Writer-Instance des DB-Clusters von Aurora PostgreSQL aus.
3. Öffnen Sie die Registerkarte Configuration (Konfiguration) für Ihre Writer-Instance des DB-Clusters von Aurora PostgreSQL. Suchen Sie in den Instance-Details den Link Parameter group (Parametergruppe).
4. Wählen Sie den Link aus, um die benutzerdefinierten Parameter zu öffnen, die Ihrem DB-Cluster von Aurora PostgreSQL zugeordnet sind.
5. Geben Sie in das Suchfeld Parameters (Parameter) `shared_pre` ein, um den `shared_preload_libraries`-Parameter zu finden.
6. Wählen Sie Edit parameters (Parameter bearbeiten) aus, um auf die Eigenschaftswerte zuzugreifen.
7. Fügen Sie `pglogical` der Liste im Feld Values (Werte) hinzu. Verwenden Sie ein Komma, um Elemente in der Werteliste zu trennen.



8. Suchen Sie den `rds.logical_replication`-Parameter und legen Sie ihn auf 1 fest, um die logische Replikation zu aktivieren.
9. Starten Sie die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL neu, damit Ihre Änderungen wirksam werden.
10. Wenn die Instance verfügbar ist, können Sie über `psql` (oder pgAdmin) eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL herstellen.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

11. Führen Sie den folgenden Befehl aus, um zu überprüfen, dass pglogical initialisiert ist.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pglogical
(1 row)
```

12. Überprüfen Sie die Einstellung, die die logische Dekodierung ermöglicht, wie folgt.

```
SHOW wal_level;
wal_level
-----------
 logical
(1 row)
```

13. Erstellen Sie die Erweiterung wie folgt.

```
CREATE EXTENSION pglogical;
EXTENSION CREATED
```

14. Wählen Sie Änderungen speichern aus.
15. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
16. Wählen Sie aus der Liste der Datenbanken Ihre Writer-Instance des DB-Clusters von Aurora PostgreSQL und dann im Menü „Actions“ (Aktionen) die Option Reboot (Neustart) aus.

AWS CLI

So richten Sie die pglogical-Erweiterung ein

Um pglogical mit der einzurichtenAWS CLI, rufen Sie die -modify-db-parameter-groupOperation auf, um bestimmte Parameter in Ihrer benutzerdefinierten Parametergruppe zu ändern, wie im folgenden Verfahren gezeigt.

1. Verwenden Sie den folgenden AWS CLI-Befehl, um dem `shared_preload_libraries`-Parameter `pglogical` hinzuzufügen.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=pglogical,ApplyMethod=pending-
reboot" \
   --region aws-region
```

2. Verwenden Sie den folgenden AWS CLI-Befehl, um `rds.logical_replication` auf `1` festzulegen und die logische Dekodierungsfunktion für die Writer-Instance des DB-Clusters von Aurora PostgreSQL zu aktivieren.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=rds.logical_replication,ParameterValue=1,ApplyMethod=pending-
reboot" \
   --region aws-region
```

3. Verwenden Sie den folgenden AWS CLI-Befehl, um die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL neu zu starten, sodass die pglogical-Bibliothek initialisiert wird.

```
aws rds reboot-db-instance \
    --db-instance-identifier writer-instance \
    --region aws-region
```

4. Wenn die Instance verfügbar ist, stellen Sie über `psql` eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

5. Erstellen Sie die Erweiterung wie folgt.

```
CREATE EXTENSION pglogical;
EXTENSION CREATED
```

6. Starten Sie die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL mit dem folgenden AWS CLI-Befehl neu.

```
aws rds reboot-db-instance \
    --db-instance-identifier writer-instance \
```

```
    --region aws-region
```

Einrichten der logischen Replikation für den DB-Cluster von Aurora PostgreSQL

Das folgende Verfahren zeigt Ihnen, wie Sie die logische Replikation zwischen zwei DB-Clustern von Aurora PostgreSQL starten. Bei den Schritten wird davon ausgegangen, dass sowohl für die Quelle (Herausgeber) als auch für das Ziel (Abonnent) die `pglogical`-Erweiterung eingerichtet wurde, wie unter Einrichten der pglogical-Erweiterung beschrieben.

So erstellen Sie den Herausgeberknoten und die zu replizierenden Tabellen

Bei diesen Schritten wird vorausgesetzt, dass Ihr DB-Cluster von Aurora PostgreSQL über eine Writer-Instance mit einer Datenbank mit einer oder mehreren Tabellen verfügt, die Sie auf einen anderen Knoten replizieren möchten. Sie müssen die Tabellenstruktur des Herausgebers für den Abonnenten neu erstellen. Rufen Sie daher bei Bedarf zunächst die Tabellenstruktur ab. Verwenden Sie dazu den `psql`-Metabefehl `\d` *`tablename`* und erstellen Sie dann dieselbe Tabelle auf der Abonnenten-Instance. Mit dem folgenden Verfahren wird zu Demonstrationszwecken eine Beispieltabelle für den Herausgeber (Quelle) erstellt.

1. Verwenden Sie `psql`, um eine Verbindung zu der Instance herzustellen, die die Tabelle enthält, die Sie als Quelle für Abonnenten verwenden möchten.

   ```
   psql --host=source-instance.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password --dbname=labdb
   ```

   Wenn Sie noch keine vorhandene Tabelle haben, die Sie replizieren möchten, können Sie wie folgt eine Beispieltabelle erstellen.

   a. Erstellen Sie mit der folgenden SQL-Anweisung eine Beispieltabelle.

      ```
      CREATE TABLE docs_lab_table (a int PRIMARY KEY);
      ```

   b. Füllen Sie die Tabelle mit der folgenden SQL-Anweisung mit generierten Daten auf.

      ```
      INSERT INTO docs_lab_table VALUES (generate_series(1,5000));
      INSERT 0 5000
      ```

   c. Stellen Sie sicher, dass Daten in der Tabelle vorhanden sind, indem Sie die folgende SQL-Anweisung verwenden.

```
SELECT count(*) FROM docs_lab_table;
```

2. Identifizieren Sie diesen DB-Cluster von Aurora PostgreSQL wie folgt als Herausgeberknoten.

```
SELECT pglogical.create_node(
    node_name := 'docs_lab_provider',
    dsn := 'host=source-instance.aws-region.rds.amazonaws.com port=5432
 dbname=labdb');
 create_node
-------------
   3410995529
(1 row)
```

3. Fügen Sie die Tabelle, die Sie replizieren möchten, zum Standardreplikationssatz hinzu. Weitere Informationen zu Replikationssätzen finden Sie unter Replikationssätze in der Dokumentation zur pglogical-Erweiterung.

```
SELECT pglogical.replication_set_add_table('default', 'docs_lab_table', 'true',
 NULL, NULL);
 replication_set_add_table
  --------------------------
  t
  (1 row)
```

Die Einrichtung des Herausgeberknotens ist abgeschlossen. Sie können jetzt den Abonnentenknoten einrichten, um die Updates vom Herausgeber zu erhalten.

So richten Sie den Abonnentenknoten ein und erstellen ein Abonnement für den Empfang von Updates

Bei diesen Schritten wird vorausgesetzt, dass der DB-Cluster von Aurora PostgreSQL mit der `pglogical`-Erweiterung eingerichtet wurde. Weitere Informationen finden Sie unter Einrichten der pglogical-Erweiterung.

1. Verwenden Sie `psql`, um sich mit der Instance zu verbinden, die Updates vom Herausgeber erhalten soll.

```
psql --host=target-instance.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

2. Erstellen Sie auf dem DB-Cluster von Aurora PostgreSQL des Abonnenten dieselbe Tabelle, die auf dem Herausgeber vorhanden ist. In diesem Beispiel heißt die Tabelle `docs_lab_table`. Sie können die Tabelle wie folgt erstellen.

```
CREATE TABLE docs_lab_table (a int PRIMARY KEY);
```

3. Stellen Sie sicher, dass diese Tabelle leer ist.

```
SELECT count(*) FROM docs_lab_table;
 count
-------
  0
(1 row)
```

4. Identifizieren Sie diesen DB-Cluster von Aurora PostgreSQL wie folgt als Abonnentenknoten.

```
SELECT pglogical.create_node(
    node_name := 'docs_lab_target',
    dsn := 'host=target-instance.aws-region.rds.amazonaws.com port=5432
 sslmode=require dbname=labdb user=postgres password=********');
 create_node
-------------
   2182738256
(1 row)
```

5. Erstellen Sie das Abonnement.

```
SELECT pglogical.create_subscription(
   subscription_name := 'docs_lab_subscription',
   provider_dsn := 'host=source-instance.aws-region.rds.amazonaws.com port=5432
 sslmode=require dbname=labdb user=postgres password=*******',
   replication_sets := ARRAY['default'],
   synchronize_data := true,
   forward_origins := '{}' );
 create_subscription
---------------------
1038357190
(1 row)
```

Wenn Sie diesen Schritt abschließen, werden die Daten aus der Tabelle des Herausgeberknotens in der Tabelle auf dem Abonnentenknoten erstellt. Mit der folgenden SQL-Abfrage können Sie überprüfen, ob dies der Fall ist.

```
SELECT count(*) FROM docs_lab_table;
 count
-------
  5000
(1 row)
```

Ab diesem Zeitpunkt werden Änderungen, die an der Tabelle auf dem Herausgeberknoten vorgenommen wurden, auf die Tabelle auf dem Abonnentenknoten repliziert.

Wiederherstellung der logischen Replikation nach einem Hauptversions-Upgrade

Bevor Sie ein Hauptversions-Upgrade eines DB-Clusters von Aurora PostgreSQL durchführen können, der als Herausgeberknoten für die logische Replikation eingerichtet ist, müssen Sie alle Replikationsslots einschließlich der Slots löschen, die nicht aktiv sind. Wir empfehlen, Datenbanktransaktionen vorübergehend vom Herausgeberknoten umzuleiten, die Replikationsslots zu löschen, den DB-Cluster von Aurora PostgreSQL zu aktualisieren und dann die Replikation erneut einzurichten und neu zu starten.

Die Replikationsslots werden nur auf dem Herausgeberknoten gehostet. Der Aurora-PostgreSQL-Abonnentenknoten hat in einem logischen Replikationsszenario keine Slots, die gelöscht werden könnten. Der Upgrade-Prozess für die Hauptversion von Aurora PostgreSQL unterstützt das Upgrade des Abonnenten auf eine neue Hauptversion von PostgreSQL unabhängig vom Herausgeberknoten. Der Upgrade-Prozess unterbricht jedoch den Replikationsprozess und beeinträchtigt die Synchronisation der WAL-Daten zwischen dem Herausgeber- und dem Abonnentenknoten. Sie müssen die logische Replikation zwischen Herausgeber und Abonnent wiederherstellen, nachdem Sie den Herausgeber, den Abonnenten oder beide aktualisiert haben. Im folgenden Verfahren wird gezeigt, wie Sie feststellen, ob die Replikation unterbrochen wurde, und wie Sie das Problem beheben.

Feststellen, dass die logische Replikation unterbrochen wurde

Sie können feststellen, ob der Replikationsprozess unterbrochen wurde, indem Sie entweder den Herausgeberknoten oder den Abonnentenknoten wie folgt abfragen.

So überprüfen Sie den Herausgeberknoten

- Verwenden Sie `psql`, um eine Verbindung mit dem Herausgeberknoten herzustellen, und fragen Sie dann die `pg_replication_slots`-Funktion ab. Notieren Sie sich den Wert in der aktiven Spalte. Normalerweise wird `t` (true) zurückgegeben, was bedeutet, dass die Replikation aktiv ist. Wenn die Abfrage `f` (false) zurückgibt, ist dies ein Hinweis darauf, dass die Replikation an den Abonnenten gestoppt wurde.

```
SELECT slot_name,plugin,slot_type,active FROM pg_replication_slots;
                    slot_name              |      plugin      | slot_type | active
-------------------------------------------+------------------+-----------+--------
 pgl_labdb_docs_labcb4fa94_docs_lab3de412c | pglogical_output | logical   | f
(1 row)
```

So überprüfen Sie den Abonnentenknoten

Auf dem Abonnentenknoten können Sie den Status der Replikation auf drei verschiedene Arten überprüfen.

- Suchen Sie in den PostgreSQL-Protokollen auf dem Abonnentenknoten nach Fehlermeldungen. Das Protokoll identifiziert Fehler mit Meldungen, die den Exit-Code 1 enthalten, wie im Folgenden dargestellt.

```
2022-07-06 16:17:03 UTC::@:[7361]:LOG: background worker "pglogical apply
 16404:2880255011" (PID 14610) exited with exit code 1
2022-07-06 16:19:44 UTC::@:[7361]:LOG: background worker "pglogical apply
 16404:2880255011" (PID 21783) exited with exit code 1
```

- Fragen Sie die `pg_replication_origin`-Funktion ab. Stellen Sie mithilfe von `psql` eine Verbindung mit der Datenbank auf dem Abonnentenknoten her und fragen Sie die `pg_replication_origin`-Funktion wie folgt ab.

```
SELECT * FROM pg_replication_origin;
 roident | roname
---------+--------
(0 rows)
```

  Die leere Ergebnismenge bedeutet, dass die Replikation unterbrochen wurde. Die Ausgabe sollte normalerweise folgendermaßen aussehen.

```
 roident |                       roname
---------+-----------------------------------------------
       1 | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

- Fragen Sie die `pglogical.show_subscription_status`-Funktion wie im folgenden Beispiel veranschaulicht ab.

```
SELECT subscription_name,status,slot_name FROM pglogical.show_subscription_status();
     subscription_name | status |              slot_name
-------+----------------+--------+-----------------------------------
 docs_lab_subscription | down   | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

  Diese Ausgabe zeigt, dass die Replikation unterbrochen wurde. Ihr Status lautet down. Normalerweise zeigt die Ausgabe den Status `replicating` an.

Wenn Ihr logischer Replikationsprozess unterbrochen wurde, können Sie die Replikation wiederherstellen, indem Sie die folgenden Schritte ausführen.

So stellen Sie die logische Replikation zwischen Herausgeber- und Abonnentenknoten wieder her

Um die Replikation wiederherzustellen, trennen Sie zuerst den Abonnenten vom Herausgeberknoten und richten dann das Abonnement erneut ein, wie in diesen Schritten beschrieben.

1. Stellen Sie mit `psql` wie folgt eine Verbindung zum Abonnentenknoten her.

   ```
   psql --host=222222222222.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password --dbname=labdb
   ```

2. Deaktivieren Sie das Abonnement, indem Sie die `pglogical.alter_subscription_disable`-Funktion verwenden.

   ```
   SELECT pglogical.alter_subscription_disable('docs_lab_subscription',true);
    alter_subscription_disable
   ----------------------------
    t
   (1 row)
   ```

3. Rufen Sie die ID des Herausgeberknotens ab, indem Sie `pg_replication_origin` wie folgt abfragen.

```
SELECT * FROM pg_replication_origin;
 roident |               roname
---------+-------------------------------------
       1 | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

4. Verwenden Sie die Antwort aus dem vorherigen Schritt mit dem `pg_replication_origin_create`-Befehl, um die ID zuzuweisen, die vom Abonnement verwendet werden kann, wenn es erneut eingerichtet wurde.

```
SELECT pg_replication_origin_create('pgl_labdb_docs_labcb4fa94_docs_lab3de412c');
  pg_replication_origin_create
------------------------------
                             1
(1 row)
```

5. Aktivieren Sie das Abonnement, indem Sie seinen Namen mit dem Status `true` übergeben, wie im folgenden Beispiel veranschaulicht.

```
SELECT pglogical.alter_subscription_enable('docs_lab_subscription',true);
  alter_subscription_enable
---------------------------
 t
(1 row)
```

Prüfen Sie den Status des Knotens. Sein Status sollte `replicating` wie in diesem Beispiel gezeigt lauten.

```
SELECT subscription_name,status,slot_name
  FROM pglogical.show_subscription_status();
            subscription_name |   status    |              slot_name
------------------------------+-------------+-------------------------------------
 docs_lab_subscription         | replicating |
 pgl_labdb_docs_lab98f517b_docs_lab3de412c
(1 row)
```

Überprüfen Sie den Status des Replikationsslots des Abonnenten auf dem Herausgeberknoten. Die `active`-Spalte des Slots sollte den Wert `t` (true) zurückgeben, was darauf hinweist, dass die Replikation wiederhergestellt wurde.

```
SELECT slot_name,plugin,slot_type,active
  FROM pg_replication_slots;
                   slot_name              |      plugin      | slot_type | active
------------------------------------------+------------------+-----------+--------
 pgl_labdb_docs_lab98f517b_docs_lab3de412c | pglogical_output | logical   | t
(1 row)
```

Verwalten logischer Replikationsslots für Aurora PostgreSQL

Bevor Sie ein Hauptversions-Upgrade eines DB-Clusters von Aurora PostgreSQL durchführen können, der als Herausgeberknoten in einem logischen Replikationsszenario eingerichtet ist, müssen Sie alle Replikationsslots auf der Instance löschen. Bei der Vorabüberprüfung des Hauptversions-Upgrades werden Sie darüber informiert, dass das Upgrade erst fortgesetzt werden kann, wenn die Slots gelöscht wurden.

Um Replikationsslots zu identifizieren, die mit der `pglogical`-Erweiterung erstellt wurden, melden Sie sich bei jeder Datenbank an und rufen Sie die Namen der Knoten ab. Wenn Sie den Abonnentenknoten abfragen, erhalten Sie in der Ausgabe sowohl den Herausgeber- als auch den Abonnentenknoten, wie in diesem Beispiel gezeigt.

```
SELECT * FROM pglogical.node;
node_id   |     node_name
------------+------------------
 2182738256 | docs_lab_target
 3410995529 | docs_lab_provider
(2 rows)
```

Die Details zum Abonnement erhalten Sie mit der folgenden Abfrage.

```
SELECT sub_name,sub_slot_name,sub_target
  FROM pglogical.subscription;
 sub_name |         sub_slot_name          | sub_target
----------+--------------------------------+------------
  docs_lab_subscription     | pgl_labdb_docs_labcb4fa94_docs_lab3de412c | 2182738256
(1 row)
```

Sie können das Abonnement jetzt wie folgt kündigen.

```
SELECT pglogical.drop_subscription(subscription_name := 'docs_lab_subscription');
 drop_subscription
-------------------
                 1
(1 row)
```

Nachdem Sie das Abonnement gekündigt haben, können Sie den Knoten löschen.

```
SELECT pglogical.drop_node(node_name := 'docs-lab-subscriber');
 drop_node
-----------
 t
(1 row)
```

Sie können wie folgt überprüfen, dass der Knoten nicht mehr existiert.

```
SELECT * FROM pglogical.node;
 node_id | node_name
---------+-----------
(0 rows)
```

Parameterreferenz für die pglogical-Erweiterung

In der Tabelle finden Sie Parameter, die der `pglogical`-Erweiterung zugeordnet sind. Parameter wie `pglogical.conflict_log_level` und `pglogical.conflict_resolution` werden verwendet, um Aktualisierungskonflikte zu beheben. Konflikte können auftreten, wenn Änderungen lokal an denselben Tabellen vorgenommen werden, die Änderungen vom Herausgeber abonniert haben. Konflikte können auch in verschiedenen Szenarien auftreten, z. B. bei der bidirektionalen Replikation oder wenn mehrere Abonnenten vom selben Herausgeber replizieren. Weitere Informationen finden Sie unter Die bidirektionale PostgreSQL-Replikation mit pglogical.

Parameter	Beschreibung
pglogical.batch_inserts	Batch-Inserts wenn möglich Standardmäßig nicht festgelegt. In '1' ändern zum Einschalten, in '0' zum Ausschalten.
pglogical.conflict_log_level	Legt die Protokollstufe für die Protokollierung gelöster Konflikte fest. Unterstützte Zeichenfolgenwerte sind debug5, debug4,

Parameter	Beschreibung
	debug3, debug2, debug1, info, notice, warning, error, log, fatal, panic.
pglogical.conflict_resolution	Legt die Methode fest, die verwendet werden soll, um Konflikte zu lösen, die lösbar sind. Unterstützte Zeichenfolgenwerte sind error, apply_remote, keep_local, last_update_wins, first_update_wins.
pglogical.extra_connection_options	Verbindungsoptionen zum Hinzufügen zu allen Peer-Knot enverbindungen
pglogical.synchronous_commit	Spezifischer synchroner Commit-Wert für pglogical
pglogical.use_spi	Verwenden Sie zum Anwenden von Änderungen SPI (Server Programming Interface) anstelle der Low-Level-API. In '1' ändern zum Einschalten, in '0' zum Ausschalten. Weitere Informationen zu SPI finden Sie unter Server Programming Interface in der PostgreSQL-Dokumentation.

Arbeiten mit den unterstützten Fremddaten-Wrapper für Amazon Aurora Postgre SQL

Ein Fremddaten-Wrapper (FDW) ist eine bestimmte Art von Erweiterung, die Zugriff auf externe Daten ermöglicht. Zum Beispiel ermöglicht die Erweiterung `oracle_fdw` Ihrer Aurora-PostgreSQL-DB-Instance die Zusammenarbeit mit Oracle-Datenbanken.

Im Folgenden finden Sie Informationen zu mehreren unterstützten PostgreSQL-Fremddaten-Wrappern.

Themen

- Verwenden der Erweiterung log_fdw für den Zugriff auf das DB-Protokoll mithilfe von SQL
- Verwenden der postgres_fdw-Erweiterung für den Zugriff auf externe Daten
- Arbeiten mit MySQL-Datenbanken mithilfe der Erweiterung mysql_fdw
- Arbeiten mit Oracle-Datenbanken unter Verwendung der Erweiterung oracle_fdw
- Arbeiten mit SQL-Server-Datenbanken unter Verwendung der Erweiterung tds_fdw

Verwenden der Erweiterung log_fdw für den Zugriff auf das DB-Protokoll mithilfe von SQL

Das Aurora-PostgreSQL-DB-Cluster unterstützt die `log_fdw`-Erweiterung, mit der Sie über eine SQL-Schnittstelle auf Ihr Datenbank-Engine-Protokoll zugreifen können. Die `log_fdw`-Erweiterung umfasst zwei neue Funktionen, die das Erstellen von Fremdtabellen für Datenbankprotokolle erleichtern:

- `list_postgres_log_files` führt die Dateien im Datenbankprotokollverzeichnis und die Dateigröße in Bytes auf.
- `create_foreign_table_for_log_file(table_name text, server_name text, log_file_name text)` erstellt eine Fremdtabelle für die angegebene Datei in der aktuellen Datenbank.

Alle durch `log_fdw` erstellten Funktionen gehören `rds_superuser`. Mitglieder der `rds_superuser`-Rolle können anderen Datenbankbenutzern Zugriff auf diese Funktionen gewähren.

Standardmäßig werden die Protokolldateien von Amazon Aurora im `stderr` (Standardfehler)-Format generiert, wie im `log_destination`-Parameter angegeben. Es gibt nur zwei Optionen für diesen Parameter: `stderr` und `csvlog` (Comma Separated Values, CSV). Wenn Sie dem Parameter die Option `csvlog` hinzufügen, generiert Amazon Aurora sowohl `stderr`- als auch `csvlog`-Protokolle. Dies kann die Speicherkapazität Ihres DB-Clusters beeinträchtigen. Daher müssen Sie sich der anderen Parameter bewusst sein, die sich auf die Protokollbehandlung auswirken. Weitere Informationen finden Sie unter Festlegen des Protokollziels (`stderr`, `csvlog`).

Ein Vorteil der Generierung von `csvlog`-Protokollen ist, dass Sie mit der `log_fdw`-Erweiterung Fremdtabellen erstellen können, bei denen die Daten ordentlich in verschiedene Spalten aufgeteilt sind. Dazu muss Ihre Instance einer benutzerdefinierten DB-Parametergruppe zugeordnet sein, damit Sie die Einstellung für `log_destination` ändern können. Weitere Informationen zur Vorgehensweise finden Sie unter Arbeiten mit Parametergruppen.

Im folgenden Beispiel wird angenommen, dass der `log_destination`-Parameter `cvslog` enthält.

So verwenden Sie die Erweiterung log_fdw:

1. Installieren Sie die `log_fdw`-Erweiterung.

```
postgres=> CREATE EXTENSION log_fdw;
CREATE EXTENSION
```

2. Erstellen Sie den Protokollserver als Fremddaten-Wrapper.

```
postgres=> CREATE SERVER log_server FOREIGN DATA WRAPPER log_fdw;
CREATE SERVER
```

3. Wählen Sie aus einer Liste an Protokolldateien "alle" aus.

```
postgres=> SELECT * FROM list_postgres_log_files() ORDER BY 1;
```

Beispiel-Antwort.

```
          file_name           | file_size_bytes
------------------------------+-----------------
 postgresql.log.2023-08-09-22.csv |            1111
 postgresql.log.2023-08-09-23.csv |            1172
 postgresql.log.2023-08-10-00.csv |            1744
 postgresql.log.2023-08-10-01.csv |            1102
(4 rows)
```

4. Erstellen Sie eine Tabelle mit einer einzigen 'log_entry'-Spalte für die ausgewählte Datei.

```
postgres=> SELECT create_foreign_table_for_log_file('my_postgres_error_log',
     'log_server', 'postgresql.log.2023-08-09-22.csv');
```

Die Antwort liefert keine weiteren Details außer, dass die Tabelle jetzt existiert.

```
----------------------------------
(1 row)
```

5. Wählen Sie ein Beispiel der Protokolldatei aus. Mit dem folgenden Code werden die Protokollzeit und die Fehlermeldungsbeschreibung abgerufen.

```
postgres=> SELECT log_time, message FROM my_postgres_error_log ORDER BY 1;
```

Beispiel-Antwort.

```
             log_time             |                                 message
----------------------------------
+-------------------------------------------------------------------------------
Tue Aug 09 15:45:18.172 2023 PDT | ending log output to stderr
Tue Aug 09 15:45:18.175 2023 PDT | database system was interrupted; last known up
 at 2023-08-09 22:43:34 UTC
Tue Aug 09 15:45:18.223 2023 PDT | checkpoint record is at 0/90002E0
Tue Aug 09 15:45:18.223 2023 PDT | redo record is at 0/90002A8; shutdown FALSE
Tue Aug 09 15:45:18.223 2023 PDT | next transaction ID: 0/1879; next OID: 24578
Tue Aug 09 15:45:18.223 2023 PDT | next MultiXactId: 1; next MultiXactOffset: 0
Tue Aug 09 15:45:18.223 2023 PDT | oldest unfrozen transaction ID: 1822, in
 database 1
(7 rows)
```

Verwenden der postgres_fdw-Erweiterung für den Zugriff auf externe Daten

Auf die Daten in einer Tabelle auf einem Remote-Datenbank-Server können Sie mit der Erweiterung postgres_fdw zugreifen. Wenn Sie eine Remote-Verbindung ausgehend von einer PostgreSQL-DB-Instance einrichten, ist der Zugriff auch für das Lesereplikat verfügbar.

Verwenden Sie postgres_fdw wie folgt für den Zugriff auf einen Remote-Datenbank-Server:

1. Installieren Sie die Erweiterung postgres_fdw.

```
CREATE EXTENSION postgres_fdw;
```

2. Erstellen Sie einen Fremddaten-Server mit CREATE SERVER.

```
CREATE SERVER foreign_server
FOREIGN DATA WRAPPER postgres_fdw
OPTIONS (host 'xxx.xx.xxx.xx', port '5432', dbname 'foreign_db');
```

3. Erstellen Sie ein Benutzer-Mapping, um die Rolle zu identifizieren, die auf dem Remote-Server verwendet werden soll.

```
CREATE USER MAPPING FOR local_user
SERVER foreign_server
OPTIONS (user 'foreign_user', password 'password');
```

4. Erstellen Sie eine Tabelle, die der Tabelle auf dem Remote-Server zugewiesen ist.

```
CREATE FOREIGN TABLE foreign_table (
        id integer NOT NULL,
        data text)
SERVER foreign_server
OPTIONS (schema_name 'some_schema', table_name 'some_table');
```

Arbeiten mit MySQL-Datenbanken mithilfe der Erweiterung mysql_fdw

Um von Ihrem Aurora-PostgreSQL-DB-Cluster auf eine MySQL-kompatible Datenbank zuzugreifen, können Sie die `mysql_fdw`-Erweiterung installieren und verwenden. Mit diesem Fremddaten-Wrapper können Sie mit RDS für MySQL, Aurora MySQL, MariaDB und anderen MySQL-kompatiblen Datenbanken arbeiten. Die Verbindung des Aurora-PostgreSQL-DB-Clusters mit der MySQL-Datenbank wird je nach Client- und Serverkonfigurationen bestmöglich verschlüsselt. Sie können die Verschlüsselung jedoch erzwingen, wenn Sie möchten. Weitere Informationen finden Sie unter Verwenden der Verschlüsselung während der Übertragung mit der Erweiterung.

Die `mysql_fdw`-Erweiterung wird in Amazon Aurora PostgreSQL Version 15.4, 14.9, 13.12, 12.16 und neueren Versionen unterstützt. Es werden Auswahlen, Einfügungen, Updates und Löschungen einer RDS-für-PostgreSQL-DB in Tabellen einer MySQL-kompatiblen Datenbank-Instance unterstützt.

Themen

- Einrichten der Aurora-PostgreSQL-DB zur Verwendung der mysql_fdw-Erweiterung
- Beispiel: Arbeiten mit einer Aurora-MySQL--Datenbank von Aurora PostgreSQL
- Verwenden der Verschlüsselung während der Übertragung mit der Erweiterung

Einrichten der Aurora-PostgreSQL-DB zur Verwendung der mysql_fdw-Erweiterung

Das Einrichten der `mysql_fdw`-Erweiterung auf dem Aurora-PostgreSQL-DB-Cluster umfasst das Laden der Erweiterung in den DB-Cluster und das anschließende Erstellen des Verbindungspunkts mit der MySQL-DB-Instance. Für diese Aufgabe benötigen Sie folgende Details zur MySQL-DB-Instance:

- Hostname oder Endpunkt. Sie können den Endpunkt für einen Aurora-MySQL-DB-Cluster mithilfe der Konsole ermitteln. Wählen Sie die Registerkarte „Connectivity & security“ (Konnektivität und Sicherheit) aus und sehen Sie im Abschnitt „Endpoint and port“ (Endpunkt und Port) nach.

- Port-Nummer. Die Standardport-Nummer für MySQL ist 3306.
- Name der Datenbank. Die DB-ID.

Sie müssen auch Zugriff auf die Sicherheitsgruppe oder die Zugriffssteuerungsliste (ACL) für den MySQL-Port 3306 gewähren. Der Aurora-PostgreSQL-DB-Cluster und der Aurora-MySQL-DB-Cluster ebenso wie benötigen Zugriff auf Port 3306. Wenn der Zugriff nicht korrekt konfiguriert ist, wird beim Versuch, eine Verbindung mit einer MySQL-kompatiblen Tabelle herzustellen, eine Fehlermeldung ähnlich wie die folgende angezeigt:

```
ERROR: failed to connect to MySQL: Can't connect to MySQL server on 'hostname.aws-
region.rds.amazonaws.com:3306' (110)
```

Im folgenden Verfahren erstellen Sie (als `rds_superuser`-Konto) den fremden Server. Anschließend gewähren Sie bestimmten Benutzern Zugriff auf den fremden Server. Diese Benutzer erstellen dann ihre eigenen Zuordnungen zu den entsprechenden MySQL-Benutzerkonten zur Zusammenarbeit mit der MySQL-DB-Instance.

So greifen Sie mit mysql_fdw auf einen MySQL-Datenbankserver zu

1. Stellen Sie über ein Konto, das die `rds_superuser`-Rolle enthält, eine Verbindung mit Ihrer PostgreSQL-DB-Instance her. Wenn Sie die Standardwerte beim Erstellen des Aurora-PostgreSQL-DB-Clusters akzeptiert haben, lautet der Benutzername `postgres`. Sie können sich mit dem `psql`-Befehlszeilen-Tool wie folgt verbinden:

   ```
   psql --host=your-DB-instance.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password
   ```

2. Installieren Sie die `mysql_fdw`-Erweiterung wie folgt:

   ```
   postgres=> CREATE EXTENSION mysql_fdw;
   CREATE EXTENSION
   ```

Nachdem die Erweiterung auf dem Aurora-PostgreSQL-DB-Cluster installiert wurde, richten Sie den fremden Server ein, der die Verbindung mit einer MySQL-Datenbank bereitstellt.

So erstellen Sie den fremden Server

Führen Sie diese Aufgaben auf dem Aurora-PostgreSQL-DB-Cluster aus. Die Schritte setzen voraus, dass Sie als Benutzer mit `rds_superuser`-Berechtigungen wie `postgres` verbunden sind.

1. Erstellen Sie einen fremden Server auf dem Aurora-PostgreSQL-DB-Cluster:

```
postgres=> CREATE SERVER mysql-db FOREIGN DATA WRAPPER mysql_fdw OPTIONS (host 'db-
name.111122223333.aws-region.rds.amazonaws.com', port '3306');
CREATE SERVER
```

2. Gewähren Sie den entsprechenden Benutzern Zugriff auf den fremden Server. Dies sollten keine Administratorbenutzer sein, d. h. Benutzer ohne `rds_superuser`-Rolle.

```
postgres=> GRANT USAGE ON FOREIGN SERVER mysql-db to user1;
GRANT
```

PostgreSQL-Benutzer erstellen und verwalten ihre eigenen Verbindungen mit der MySQL-Datenbank über den fremden Server.

Beispiel: Arbeiten mit einer Aurora-MySQL--Datenbank von Aurora PostgreSQL

Angenommen, Sie haben eine einfache Tabelle auf einer Aurora-PostgreSQL-DB-Instance. Ihre Aurora-PostgreSQL-Benutzer möchten (`SELECT`)-, `INSERT`-, `UPDATE`- und `DELETE`-Elemente in dieser Tabelle abfragen. Nehmen wir an, dass die `mysql_fdw`-Erweiterung auf Ihrer RDS-für-PostgreSQL-DB-Instance erstellt wurde, wie im vorherigen Verfahren beschrieben. Nachdem Sie eine Verbindung mit der RDS-für-PostgreSQL-DB-Instance als Benutzer mit `rds_superuser`-Berechtigungen hergestellt haben, können Sie mit den folgenden Schritten fortfahren.

1. Erstellen Sie einen fremden Server in der Aurora-PostgreSQL-DB-Instance:

```
test=> CREATE SERVER mysqldb FOREIGN DATA WRAPPER mysql_fdw OPTIONS (host 'your-
DB.aws-region.rds.amazonaws.com', port '3306');
CREATE SERVER
```

2. Gewähren Sie einem Benutzer, der keine `rds_superuser`-Berechtigungen hat, die Nutzung, zum Beispiel `user1`:

```
test=> GRANT USAGE ON FOREIGN SERVER mysqldb TO user1;
GRANT
```

3. Stellen Sie eine Verbindung als *user1* (Benutzer 1) her und erstellen Sie dann eine Zuordnung zum MySQL-Benutzer:

```
test=> CREATE USER MAPPING FOR user1 SERVER mysqldb OPTIONS (username 'myuser',
 password 'mypassword');
CREATE USER MAPPING
```

4. Erstellen Sie eine fremde Tabelle, die mit der MySQL-Tabelle verknüpft ist:

```
test=> CREATE FOREIGN TABLE mytab (a int, b text) SERVER mysqldb OPTIONS (dbname
 'test', table_name '');
CREATE FOREIGN TABLE
```

5. Führen Sie eine einfache Abfrage mit der fremden Tabelle aus:

```
test=> SELECT * FROM mytab;
a |   b
---+-------
1 | apple
(1 row)
```

6. Sie können der MySQL-Tabelle Daten hinzufügen, ändern und daraus entfernen. Beispiel:

```
test=> INSERT INTO mytab values (2, 'mango');
INSERT 0 1
```

   Führen Sie die SELECT-Abfrage noch einmal aus, um die Ergebnisse zu sehen:

```
test=> SELECT * FROM mytab ORDER BY 1;
 a |   b
---+-------
1 | apple
2 | mango
(2 rows)
```

Verwenden der Verschlüsselung während der Übertragung mit der Erweiterung

Die Verbindung mit MySQL über Aurora PostgreSQL verwendet standardmäßig die Verschlüsselung während der Übertragung (TLS/SSL). Die Verbindung wird jedoch nicht verschlüsselt, wenn sich die Client- und Serverkonfiguration unterscheiden. Sie können die Verschlüsselung für alle

ausgehenden Verbindungen erzwingen, indem Sie die Option `REQUIRE SSL` in den RDS-für-MySQL-Benutzerkonten angeben. Derselbe Ansatz funktioniert auch für MariaDB- und Aurora-MySQL-Benutzerkonten.

Für MySQL-Benutzerkonten, die für `REQUIRE SSL` konfiguriert sind, schlägt der Verbindungsversuch fehl, wenn keine sichere Verbindung hergestellt werden kann.

Um die Verschlüsselung für vorhandene MySQL-Datenbankbenutzerkonten durchzusetzen, können Sie den Befehl `ALTER USER` verwenden. Die Syntax variiert je nach MySQL-Version, wie in der folgenden Tabelle gezeigt. Weitere Informationen finden Sie unter ALTER USER im MySQL-Referenzhandbuch.

MySQL 5.7, MySQL 8.0	MySQL 5.6
`ALTER USER 'user'@'%' REQUIRE SSL;`	`GRANT USAGE ON *.* to 'user'@'%' REQUIRE SSL;`

Weitere Informationen zur Erweiterung `mysql_fdw` finden Sie in der mysql_fdw-Dokumentation.

Arbeiten mit Oracle-Datenbanken unter Verwendung der Erweiterung oracle_fdw

Um von Ihrem Aurora-PostgreSQL-DB-Cluster auf eine Oracle-Datenbank zuzugreifen, können Sie die Erweiterung `oracle_fdw` installieren und verwenden. Diese Erweiterung ist ein Fremddaten-Wrapper für Oracle-Datenbanken. Weitere Informationen zu dieser Erweiterung finden Sie in der oracle_fdw-Dokumentation.

Die Erweiterung `oracle_fdw` wird von Aurora PostgreSQL 12.7, Amazon Aurora Version 4.2) und höheren Versionen unterstützt.

Themen

- Aktivieren der Erweiterung oracle_fdw
- Beispiel: Verwendung eines fremden Servers, der mit einer Amazon RDS for Oracle Database verknüpft ist
- Datenverschlüsselung während der Übertragung
- Informationen zur Ansicht pg_user_mappings und zu Berechtigungen

Aktivieren der Erweiterung oracle_fdw

So verwenden Sie die Erweiterung oracle_fdw:

Aktivieren der Erweiterung oracle_fdw

- Führen Sie den folgenden Befehl mit einem Konto aus, das die `rds_superuser`-Berechtigungen besitzt.

```
CREATE EXTENSION oracle_fdw;
```

Beispiel: Verwendung eines fremden Servers, der mit einer Amazon RDS for Oracle Database verknüpft ist

Das folgende Beispiel zeigt die Verwendung eines fremden Servers, der mit einer Amazon-RDS-für-Oracle-Datenbank verknüpft ist.

So erstellen Sie einen fremden Server, der mit einer RDS-for-Oracle-Datenbank verknüpft ist:

1. Beachten Sie Folgendes auf der RDS-for-Oracle-DB-Instance:
   - Endpunkt
   - Port
   - Datenbankname
2. Erstellen Sie einen fremden Server.

```
test=> CREATE SERVER oradb FOREIGN DATA WRAPPER oracle_fdw OPTIONS (dbserver
 '//endpoint:port/DB_name');
CREATE SERVER
```

3. Gewähren Sie einem Benutzer, der keine `rds_superuser`-Berechtigungen hat, die Nutzung, zum Beispiel `user1`.

```
test=> GRANT USAGE ON FOREIGN SERVER oradb TO user1;
GRANT
```

4. Verbinden Sie sich als `user1` und erstellen Sie ein Mapping zu einem Oracle-Benutzer.

```
test=> CREATE USER MAPPING FOR user1 SERVER oradb OPTIONS (user 'oracleuser',
 password 'mypassword');
```

```
CREATE USER MAPPING
```

5. Erstellen einer fremden Tabelle, die mit einer Oracle-Tabelle verknüpft ist.

```
test=> CREATE FOREIGN TABLE mytab (a int) SERVER oradb OPTIONS (table 'MYTABLE');
CREATE FOREIGN TABLE
```

6. Fragen Sie die fremde Tabelle ab.

```
test=>  SELECT * FROM mytab;
a
---
1
(1 row)
```

Wenn die Abfrage den folgenden Fehler meldet, überprüfen Sie Ihre Sicherheitsgruppe und Zugriffssteuerungsliste (Access Control List, ACL), um sicherzustellen, dass beide Instances kommunizieren können.

```
ERROR: connection for foreign table "mytab" cannot be established
DETAIL: ORA-12170: TNS:Connect timeout occurred
```

Datenverschlüsselung während der Übertragung

Die PostgreSQL-zu-Oracle-Verschlüsselung bei der Übertragung basiert auf einer Kombination von Client- und Server-Konfigurationsparametern. Ein Beispiel für Oracle 21c finden Sie unter Informationen zu den Werten für Verschlüsselung und Integrität in der Oracle-Dokumentation. Der Client, der für oracle_fdw auf Amazon RDS verwendet wird, ist mit `ACCEPTED` konfiguriert, was bedeutet, dass die Verschlüsselung von der Konfiguration des Oracle-Datenbankservers abhängt.

Wenn sich Ihre Datenbank auf RDS for Oracle befindet, finden Sie weitere Informationen zum Konfigurieren der Verschlüsselung unter Oracle Native Network Encryption.

Informationen zur Ansicht pg_user_mappings und zu Berechtigungen

Der PostgreSQL-Katalog `pg_user_mapping` speichert das Mapping eines Benutzers von Aurora PostgreSQL für den Benutzer auf einem fremden Datenserver (Remote). Der Zugriff auf den Katalog ist eingeschränkt, aber Sie verwenden die Ansicht `pg_user_mappings`, um die Mappings zu sehen. Das folgende Beispiel zeigt, wie Berechtigungen für eine Oracle-Beispieldatenbank gelten. Diese Informationen gelten im Allgemeinen für jeden fremden Daten-Wrapper.

In der folgenden Ausgabe finden Sie Rollen und Berechtigungen, die drei verschiedenen Beispielbenutzern zugeordnet sind. Benutzer `rdssu1` und `rdssu2` sind Mitglieder der `rds_superuser`-Rolle und `user1` nicht. In dem Beispiel wird der `psql`-Metabefehl `\du` verwendet, um vorhandene Rollen aufzulisten.

```
test=>  \du
                                                              List of roles
    Role name    |                         Attributes                          |
                 Member of
-----------------+-------------------------------------------------------------
+-----------------------------------------------------------
 rdssu1          |                                                             |
 {rds_superuser}
 rdssu2          |                                                             |
 {rds_superuser}
 user1           |                                                             | {}
```

Alle Benutzer, einschließlich Benutzer mit `rds_superuser`-Berechtigungen, dürfen ihre eigenen Benutzerzuordnungen (`umoptions`) in der `pg_user_mappings`-Tabelle anzeigen. Wie im folgenden Beispiel gezeigt, wird trotz `rdssu1rds_superuser`-Berechtigungen ein Fehler gemeldet, wenn `rdssu1` versucht, alle Benutzerzuordnungen abzurufen:

```
test=> SELECT * FROM pg_user_mapping;
ERROR: permission denied for table pg_user_mapping
```

Im Folgenden sind einige Beispiele aufgeführt.

```
test=> SET SESSION AUTHORIZATION rdssu1;
SET
test=> SELECT * FROM pg_user_mappings;
 umid  | srvid | srvname | umuser | usename    |            umoptions
-------+-------+---------+--------+------------+---------------------------------
 16414 | 16411 | oradb   |  16412 | user1      |
 16423 | 16411 | oradb   |  16421 | rdssu1     | {user=oracleuser,password=mypwd}
 16424 | 16411 | oradb   |  16422 | rdssu2     |
 (3 rows)

test=> SET SESSION AUTHORIZATION rdssu2;
SET
test=> SELECT * FROM pg_user_mappings;
 umid  | srvid | srvname | umuser | usename    |            umoptions
```

```
-------+-------+---------+--------+------------+----------------------------------
 16414 | 16411 | oradb   |  16412 | user1      |
 16423 | 16411 | oradb   |  16421 | rdssu1     |
 16424 | 16411 | oradb   |  16422 | rdssu2     | {user=oracleuser,password=mypwd}
 (3 rows)

test=> SET SESSION AUTHORIZATION user1;
SET
test=> SELECT * FROM pg_user_mappings;
 umid  | srvid | srvname | umuser | usename    |           umoptions
-------+-------+---------+--------+------------+-------------------------------
 16414 | 16411 | oradb   |  16412 | user1      | {user=oracleuser,password=mypwd}
 16423 | 16411 | oradb   |  16421 | rdssu1     |
 16424 | 16411 | oradb   |  16422 | rdssu2     |
 (3 rows)
```

Aufgrund von Unterschieden in der Implementierung von `information_schema._pg_user_mappings` und `pg_catalog.pg_user_mappings` erfordert ein manuell erstelltes `rds_superuser` zusätzliche Berechtigungen zum Anzeigen von Passwörtern in `pg_catalog.pg_user_mappings`.

Es sind keine zusätzlichen Berechtigungen für `rds_superuser` nötig, um Kennwörter in `information_schema._pg_user_mappings` anzuzeigen.

Benutzer, die nicht über die `rds_superuser`-Rolle verfügen können Passwörter in `pg_user_mappings` nur unter den folgenden Bedingungen anzeigen:

- Der aktuelle Benutzer ist der zugeordnete Benutzer und besitzt den Server oder besitzt die `USAGE`-Berechtigung dafür.
- Der aktuelle Benutzer ist der Serverbesitzer und das Mapping ist für `PUBLIC`.

Arbeiten mit SQL-Server-Datenbanken unter Verwendung der Erweiterung tds_fdw

Sie können die PostgreSQL-Erweiterung `tds_fdw` für den Zugriff auf Datenbanken verwenden, die das TDS-Protokoll (Tabular Data Stream) unterstützen, wie Sybase- und Microsoft-SQL-Server-Datenbanken. Mit diesem Fremddaten-Wrapper können Sie sich von Ihrem Aurora-PostgreSQL-DB-Cluster aus mit Datenbanken verbinden, die das TDS-Protokoll verwenden, einschließlich Amazon RDS for Microsoft SQL Server. Weitere Informationen finden Sie in der tds-fdw/tds_fdw-Dokumentation auf GitHub.

Die Erweiterung `tds_fdw` wird von den Amazon-Aurora-PostgreSQL-Versionen 13.6 und höher unterstützt.

Einrichten Ihrer Aurora-PostgreSQL-DB zur Verwendung der tds_fdw-Erweiterung

In den folgenden Verfahren finden Sie ein Beispiel für die Einrichtung und Verwendung der Erweiterung `tds_fdw` mit einem Aurora-PostgreSQL-DB-Cluster. Bevor Sie eine Verbindung mit einer SQL-Server-Datenbank mithilfe von `tds_fdw` herstellen können, benötigen Sie die folgenden Details für die Instance:

- Hostname oder Endpunkt. Sie können den Endpunkt für eine RDS-for-SQL-Server-DB-Instance mithilfe der Konsole ermitteln. Wählen Sie die Registerkarte „Connectivity & security“ (Konnektivität und Sicherheit) aus und sehen Sie im Abschnitt „Endpoint and port“ (Endpunkt und Port) nach.
- Port-Nummer. Die Standardport-Nummer für Microsoft SQL Server ist 1433.
- Name der Datenbank. Die DB-ID.

Sie müssen auch Zugriff auf die Sicherheitsgruppe oder die Zugriffssteuerungsliste (ACL) für den SQL-Server-Port 1433 gewähren. Sowohl der Aurora-PostgreSQL-DB-Cluster als auch die RDS-for-SQL-Server-DB-Instance benötigen Zugriff auf Port 1433. Wenn der Zugriff nicht richtig konfiguriert ist, wird beim Versuch, den Microsoft SQL Server abzufragen, die folgende Fehlermeldung angezeigt:

```
ERROR: DB-Library error: DB #: 20009, DB Msg: Unable to connect:
Adaptive Server is unavailable or does not exist (mssql2019.aws-
region.rds.amazonaws.com), OS #: 0, OS Msg: Success, Level: 9
```

So verbinden Sie sich mit tds_fdw mit einer SQL-Server-Datenbank

1. Verbinden Sie sich mit Ihrer primären Instance des Aurora-PostgreSQL-DB-Clusters über ein Konto mit der `rds_superuser`-Rolle:

   ```
   psql --host=your-cluster-name-instance-1.aws-region.rds.amazonaws.com --port=5432
    --username=test --password
   ```

2. Installieren Sie die `tds_fdw`-Erweiterung.

   ```
   test=> CREATE EXTENSION tds_fdw;
   CREATE EXTENSION
   ```

Nachdem die Erweiterung auf Ihrem Aurora-PostgreSQL-DB-Cluster installiert wurde, richten Sie den fremden Server ein.

So erstellen Sie den fremden Server

Führen Sie diese Aufgaben auf dem Aurora-PostgreSQL-DB-Cluster unter Verwendung eines Kontos mit `rds_superuser`-Berechtigungen aus.

1. Erstellen Sie einen fremden Server auf dem Aurora-PostgreSQL-DB-Cluster:

```
test=> CREATE SERVER sqlserverdb FOREIGN DATA WRAPPER tds_fdw OPTIONS
 (servername 'mssql2019.aws-region.rds.amazonaws.com', port '1433', database
 'tds_fdw_testing');
CREATE SERVER
```

   Um auf Nicht-ASCII-Daten auf der SQLServer-Seite zuzugreifen, erstellen Sie einen Serverlink mit der Option character_set im DB-Cluster von Aurora PostgreSQL:

```
test=> CREATE SERVER sqlserverdb FOREIGN DATA WRAPPER tds_fdw OPTIONS (servername
 'mssql2019.aws-region.rds.amazonaws.com', port '1433', database 'tds_fdw_testing',
 character_set 'UTF-8');
CREATE SERVER
```

2. Gewähren Sie einem Benutzer, der keine `rds_superuser`-Rollenberechtigungen hat, Berechtigungen, zum Beispiel `user1`:

```
test=> GRANT USAGE ON FOREIGN SERVER sqlserverdb TO user1;
```

3. Stellen Sie eine Verbindung als „user1“ (Benutzer 1) her und erstellen Sie dann eine Zuordnung zum SQL-Server-Benutzer:

```
test=> CREATE USER MAPPING FOR user1 SERVER sqlserverdb OPTIONS (username
 'sqlserveruser', password 'password');
CREATE USER MAPPING
```

4. Erstellen Sie eine fremde Tabelle, die mit einer SQL-Server-Tabelle verknüpft ist:

```
test=> CREATE FOREIGN TABLE mytab (a int) SERVER sqlserverdb OPTIONS (table
 'MYTABLE');
CREATE FOREIGN TABLE
```

5. Fragen Sie die fremde Tabelle ab:

```
test=> SELECT * FROM mytab;
 a
---
 1
(1 row)
```

Verwenden der Verschlüsselung während der Übertragung für die Verbindung

Die Verbindung von Aurora PostgreSQL mit SQL Server verwendet je nach SQL-Server-Datenbankkonfiguration die Verschlüsselung während der Übertragung (TLS/SSL). Wenn der SQL Server nicht für die Verschlüsselung konfiguriert ist, bleibt der RDS-für-PostgreSQL-Client, der die Anforderung an die SQL-Server-Datenbank stellt, unverschlüsselt.

Sie können die Verschlüsselung für die Verbindung mit RDS-for-SQL-Server DB-Instances erzwingen, indem Sie den `rds.force_ssl`-Parameter festlegen. Weitere Informationen finden Sie unter Erzwingen von Verbindungen mit Ihrer DB-Instance, um SSL zu verwenden. Weitere Informationen zur SSL/TLS-Konfiguration für RDS for SQL Server finden Sie unter Verwenden von SSL mit einer Microsoft-SQL-Server-DB-Instance.

Arbeiten mit Trusted Language Extensions für PostgreSQL

Trusted Language Extensions für PostgreSQL ist ein Open-Source-Entwicklungskit für die Erstellung von PostgreSQL-Erweiterungen. Es ermöglicht Ihnen, leistungsstarke PostgreSQL-Erweiterungen zu erstellen und diese sicher auf Ihrem DB-Cluster von Aurora PostgreSQL auszuführen. Mithilfe von Trusted Language Extensions (TLE) für PostgreSQL können Sie PostgreSQL-Erweiterungen erstellen, die dem dokumentierten Ansatz zur Erweiterung der PostgreSQL-Funktionalität folgen. Weitere Informationen finden Sie unter Packaging Related Objects in a Extension in der PostgreSQL-Dokumentation.

Ein wesentlicher Vorteil von TLE besteht darin, dass Sie es in Umgebungen verwenden können, die keinen Zugriff auf das der PostgreSQL-Instance zugrunde liegende Dateisystem bieten. Bisher war für die Installation einer neuen Erweiterung Zugriff auf das Dateisystem erforderlich. Mit TLE entfällt diese Einschränkung. Es bietet eine Entwicklungsumgebung für die Erstellung neuer Erweiterungen für jede PostgreSQL-Datenbank, einschließlich solcher, die auf Ihren DB-Clustern von Aurora PostgreSQL ausgeführt werden.

TLE wurde entwickelt, um den Zugriff auf unsichere Ressourcen für die Erweiterungen zu verhindern, die Sie mit TLE erstellen. Die Laufzeitumgebung begrenzt die Auswirkungen eines Erweiterungsdefekts auf eine einzelne Datenbankverbindung. TLE verleiht Datenbankadministratoren auch eine detaillierte Kontrolle darüber, wer Erweiterungen installieren kann, und bietet ein Berechtigungsmodell für deren Ausführung.

TLE wird von Aurora PostgreSQL Version 14.5 und höheren Versionen unterstützt.

Die Entwicklungsumgebung und Laufzeit von Trusted Language Extensions sind als `pg_tle`-PostgreSQL-Erweiterung, Version 1.0.1, verpackt. Es unterstützt die Erstellung von Erweiterungen in Perl JavaScript, Tcl, PL/pgSQL und SQL. Sie installieren die `pg_tle`-Erweiterung in Ihrem DB-Cluster von Aurora PostgreSQL auf die gleiche Weise wie andere PostgreSQL-Erweiterungen. Nach der Einrichtung von `pg_tle` können Entwickler damit neue PostgreSQL-Erweiterungen, sogenannte TLE-Erweiterungen, erstellen.

In den folgenden Themen finden Sie Informationen darüber, wie Sie Trusted Language Extensions einrichten und Ihre eigenen TLE-Erweiterungen erstellen.

Themen

- Einrichten von Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL
- Übersicht über Trusted Language Extensions für PostgreSQL
- Erstellen von TLE-Erweiterungen für Aurora PostgreSQL
- Löschen Ihrer TLE-Erweiterungen aus einer Datenbank
- Deinstallieren von Trusted Language Extensions für PostgreSQL
- Verwenden von PostgreSQL-Haken mit Ihren TLE-Erweiterungen
- Funktionsreferenz für Trusted Language Extensions für PostgreSQL
- Hakenreferenz für Trusted Language Extensions für PostgreSQL

Terminologie

Sehen Sie sich das folgende Glossar und die in diesem Thema verwendeten Begriffe an, damit Sie Trusted Language Extensions besser verstehen.

Trusted Language Extensions für PostgreSQL

: Trusted Language Extensions für PostgreSQL ist der offizielle Name des Open-Source-Entwicklungskits, das als `pg_tle`-Erweiterung verpackt ist. Es ist für die Verwendung in jedem PostgreSQL-System verfügbar. Weitere Informationen finden Sie unter aws/pg_tle on. GitHub

Trusted Language Extensions

: Trusted Language Extensions ist der Kurzname für Trusted Language Extensions für PostgreSQL. Dieser verkürzte Name und seine Abkürzung (TLE) werden ebenfalls in dieser Dokumentation verwendet.

Vertrauenswürdige Sprache

: Eine vertrauenswürdige Sprache ist eine Programmier- oder Skriptsprache mit bestimmten Sicherheitsattributen. Beispielsweise schränken vertrauenswürdige Sprachen in der Regel den Zugriff auf das Dateisystem und die Verwendung bestimmter Netzwerkeigenschaften ein. Das TLE-Entwicklungskit wurde entwickelt, um vertrauenswürdige Sprachen zu unterstützen. PostgreSQL unterstützt verschiedene Sprachen, die verwendet werden, um vertrauenswürdige oder nicht vertrauenswürdige Erweiterungen zu erstellen. Ein Beispiel finden Sie unter Trusted and Untrusted PL/Perl in der PostgreSQL-Dokumentation. Wenn Sie eine Erweiterung mithilfe von Trusted Language Extensions erstellen, verwendet die Erweiterung von sich aus vertrauenswürdige Sprachmechanismen.

TLE-Erweiterung

Eine TLE-Erweiterung ist eine PostgreSQL-Erweiterung, die mithilfe des Trusted Language Extensions (TLE)-Entwicklungskits erstellt wurde.

Anforderungen für die Verwendung von Trusted Language Extensions für PostgreSQL

Beachten Sie die folgenden Anforderungen für die Einrichtung und Verwendung des TLE-Entwicklungskits.

- Aurora-PostgreSQL-Versionen – Trusted Language Extensions wird nur von Aurora-PostgreSQL-Version 14.5, und höheren Versionen unterstützt.
  - Wenn Sie Ihren DB-Cluster von Aurora PostgreSQL aktualisieren müssen, finden Sie weitere Informationen unter Upgrade von DB-Clustern von Amazon Aurora PostgreSQL.
  - Wenn Sie noch keinen Aurora-DB-Cluster für die Ausführung von PostgreSQL haben, können Sie eine/n erstellen. Weitere Informationen finden Sie unter Erstellen eines DB-Clusters von Aurora PostgreSQL und Herstellen einer Verbindung.
- Erfordert **`rds_superuser`**-Berechtigungen – Um die `pg_tle`-Erweiterung einzurichten und zu konfigurieren, muss Ihre Datenbankbenutzerrolle über die Berechtigungen der `rds_superuser`-Rolle verfügen. Diese Rolle wird standardmäßig dem `postgres`-Benutzer zugewiesen, der den DB-Cluster von Aurora PostgreSQL erstellt.
- Erfordert eine benutzerdefinierte DB-Parametergruppe – Ihr DB-Cluster von Aurora PostgreSQL muss mit einer benutzerdefinierten DB-Parametergruppe konfiguriert sein. Sie verwenden die benutzerdefinierte DB-Parametergruppe für die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL.
  - Wenn Ihr DB-Cluster von Aurora PostgreSQL nicht mit einer benutzerdefinierten DB-Parametergruppe konfiguriert ist, sollten Sie eine erstellen und sie der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL zuordnen. Eine kurze Zusammenfassung der Schritte finden Sie unter Erstellen und Anwenden einer benutzerdefinierten DB-Parametergruppe.
  - Wenn Ihr DB-Cluster von Aurora PostgreSQL bereits mit einer benutzerdefinierten DB-Parametergruppe konfiguriert ist, können Sie Trusted Language Extensions einrichten. Details hierzu finden Sie unter Einrichten von Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL.

Erstellen und Anwenden einer benutzerdefinierten DB-Parametergruppe

Verwenden Sie die folgenden Schritte, um eine benutzerdefinierte DB-Parametergruppe zu erstellen und Ihren DB-Cluster von Aurora PostgreSQL für ihre Verwendung zu konfigurieren.

Konsole

So erstellen Sie eine benutzerdefinierte DB-Parametergruppe und verwenden Sie mit Ihrem DB-Cluster von Aurora PostgreSQL

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Menü von Amazon RDS „Parameter groups“ (Parametergruppen) aus.
3. Wählen Sie Parametergruppe erstellen.
4. Geben Sie auf der Seite Parameter group details Parametergruppendetails die folgenden Informationen ein.
   - Wählen Sie unter Parameter group family (Parametergruppenfamilie) die Option aurora-postgresql14 aus.
   - Wählen Sie für Type (Typ) die Option DB Parameter Group (DB-Parametergruppe) aus.
   - Geben Sie Ihrer Parametergruppe unter Group name (Gruppenname) im Kontext Ihrer Operationen einen aussagekräftigen Namen.
   - Geben Sie unter Description (Beschreibung) eine nützliche Beschreibung ein, damit andere Mitglieder Ihres Teams sie leicht finden können.
5. Wählen Sie Erstellen. Ihre benutzerdefinierte DB-Parametergruppe wird in Ihrer AWS-Region erstellt. Sie können jetzt Ihren DB-Cluster von Aurora PostgreSQL ändern, um sie zu verwenden, indem Sie die nächsten Schritte ausführen.
6. Wählen Sie Databases (Datenbanken) im Amazon-RDS-Menü aus.
7. Wählen Sie aus der Liste den DB-Cluster von Aurora PostgreSQL für die Verwendung mit TLE aus und klicken Sie dann auf Modify (Ändern).
8. Suchen Sie auf der Seite zum Ändern der DB-Cluster-Einstellungen nach Database options (Datenbankoptionen) und verwenden Sie die Auswahl, um Ihre benutzerdefinierte DB-Parametergruppe auszuwählen.
9. Wählen Sie Continue (Weiter) aus, um die Änderung zu speichern.
10. Wählen Sie Apply immediately (Sofort anwenden) aus, damit Sie die Einrichtung DB-Clusers von Aurora PostgreSQL zur Verwendung von TLE fortsetzen können.

Informationen zum weiteren Einrichten Ihres Systems für Trusted Language Extensions finden Sie unter Einrichten von Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL.

Weitere Informationen zum Arbeiten mit DB-Clustern und DB-Parametergruppen finden Sie unter Arbeiten mit DB-Cluster-Parametergruppen.

AWS CLI

Sie können die Angabe des `--region`-Arguments vermeiden, wenn Sie CLI-Befehle verwenden, indem Sie Ihre AWS CLI mit Ihrer standardmäßigen AWS-Region konfigurieren. Weitere Informationen finden Sie unter Konfigurationsgrundlagen im AWS Command Line Interface - Benutzerhandbuch.

So erstellen Sie eine benutzerdefinierte DB-Parametergruppe und verwenden Sie mit Ihrem DB-Cluster von Aurora PostgreSQL

1. AWS-RegionBeachten Sie, dass Sie in diesem Schritt eine DB-Parametergruppe zum Anwenden auf die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL erstellen.

   UnixFür, oder: Linux macOS

   ```
   aws rds create-db-parameter-group \
     --region aws-region \
     --db-parameter-group-name custom-params-for-pg-tle \
     --db-parameter-group-family aurora-postgresql14 \
     --description "My custom DB parameter group for Trusted Language Extensions"
   ```

   Windows:

   ```
   aws rds create-db-parameter-group ^
     --region aws-region ^
     --db-parameter-group-name custom-params-for-pg-tle ^
     --db-parameter-group-family aurora-postgresql14 ^
     --description "My custom DB parameter group for Trusted Language Extensions"
   ```

   Ihre benutzerdefinierte DB-Parametergruppe ist in Ihrer AWS-Region verfügbar. Sie können also die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL ändern, um sie zu verwenden.
2. Verwenden Sie den modify-db-instance AWS CLI Befehl, um Ihre benutzerdefinierte DB-Parametergruppe auf die Writer-Instance Ihres Aurora PostgreSQL-DB-Clusters anzuwenden. Mit diesem Befehl wird die aktive Instanz sofort neu gestartet.

FürLinux, odermacOS: Unix

```
aws rds modify-db-instance \
  --region aws-region \
  --db-instance-identifier your-writer-instance-name \
  --db-parameter-group-name custom-params-for-pg-tle \
  --apply-immediately
```

Windows:

```
aws rds modify-db-instance ^
  --region aws-region ^
  --db-instance-identifier your-writer-instance-name ^
  --db-parameter-group-name custom-params-for-pg-tle ^
  --apply-immediately
```

Informationen zum weiteren Einrichten Ihres Systems für Trusted Language Extensions finden Sie unter Einrichten von Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL.

Weitere Informationen finden Sie unter Arbeiten mit DB-Parametergruppen in einer DB-Instance .

Einrichten von Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL

Bei den folgenden Schritten wird davon ausgegangen, dass Ihr DB-Cluster von Aurora PostgreSQL einer benutzerdefinierten DB-Cluster -Parametergruppe zugeordnet ist. Sie können das AWS Management Console oder das AWS CLI für diese Schritte verwenden.

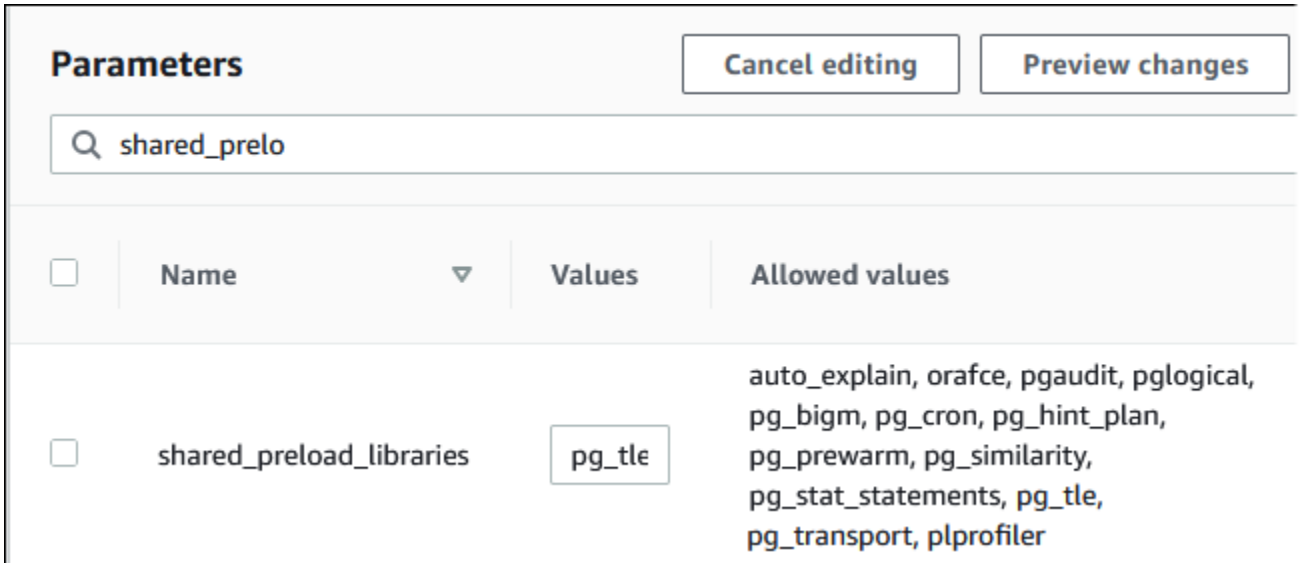
Wenn Sie Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL einrichten, installieren Sie sie in einer bestimmten Datenbank, damit sie von den Datenbankbenutzern verwendet werden kann, die über Berechtigungen für diese Datenbank verfügen.

Konsole

So richten Sie Trusted Language Extensions ein

Führen Sie die folgenden Schritte mit einem Konto aus, das Mitglied der `rds_superuser`-Gruppe (Rolle) ist.

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Ihre Writer-Instance des DB-Clusters von Aurora PostgreSQL aus.
3. Öffnen Sie die Registerkarte Configuration (Konfiguration) für Ihre Writer-Instance des DB-Clusters von Aurora PostgreSQL. Suchen Sie in den Instance-Details den Link Parameter group (Parametergruppe).
4. Wählen Sie den Link aus, um die benutzerdefinierten Parameter zu öffnen, die Ihrem DB-Cluster von Aurora PostgreSQL zugeordnet sind.
5. Geben Sie in das Suchfeld Parameters (Parameter) `shared_pre` ein, um den `shared_preload_libraries`-Parameter zu finden.
6. Wählen Sie Edit parameters (Parameter bearbeiten) aus, um auf die Eigenschaftswerte zuzugreifen.
7. Fügen Sie `pg_tle` der Liste im Feld Values (Werte) hinzu. Verwenden Sie ein Komma, um Elemente in der Werteliste zu trennen.



8. Starten Sie die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL neu, damit Ihre Änderung des `shared_preload_libraries`-Parameters wirksam wird.
9. Wenn die Instance verfügbar ist, überprüfen Sie, ob `pg_tle` initialisiert wurde. Stellen Sie über `psql` eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her und führen Sie den folgenden Befehl aus.

```
SHOW shared_preload_libraries;
shared_preload_libraries
```

```
-------------------------
rdsutils,pg_tle
(1 row)
```

10. Wenn die `pg_tle`-Erweiterung initialisiert ist, können Sie jetzt die Erweiterung erstellen.

```
CREATE EXTENSION pg_tle;
```

Sie können überprüfen, ob die Erweiterung installiert wurde, indem Sie den folgenden `psql`-Metabefehl verwenden.

```
labdb=> \dx
                          List of installed extensions
  Name   | Version |   Schema   |                Description
---------+---------+------------+-------------------------------------------
 pg_tle  | 1.0.1   | pgtle      | Trusted-Language Extensions for PostgreSQL
 plpgsql | 1.0     | pg_catalog | PL/pgSQL procedural language
```

11. Weisen Sie der `pgtle_admin`-Rolle dem primären Benutzernamen zu, den Sie bei der Einrichtung für Ihren DB-Cluster von Aurora PostgreSQL erstellt haben. Wenn Sie die Standardeinstellung akzeptiert haben, lautet der Wert `postgres`.

```
labdb=> GRANT pgtle_admin TO postgres;
GRANT ROLE
```

Wie in folgendem Beispiel veranschaulicht, können Sie anhand des `psql`-Metabefehls überprüfen, ob die Gewährung erfolgt ist. In der Ausgabe werden nur die Rollen `pgtle_admin` und `postgres` angezeigt. Weitere Informationen finden Sie unter Grundlegendes zu PostgreSQL-Rollen und -Berechtigungen.

```
labdb=> \du
                          List of roles
    Role name    |           Attributes            |               Member of
-----------------+---------------------------------
+---------------------------------
pgtle_admin      | Cannot login                     | {}
postgres         | Create role, Create DB          +| {rds_superuser,pgtle_admin}
                 | Password valid until infinity    |...
```

12. Schließen Sie die `psql`-Sitzung mit dem `\q`-Metabefehl.

```
\q
```

Informationen zum Erstellen von TLE-Erweiterungen finden Sie unter Beispiel: Erstellen einer Trusted Language Extension mit SQL.

AWS CLI

Sie können die Angabe des `--region`-Arguments vermeiden, wenn Sie CLI-Befehle verwenden, indem Sie Ihre AWS CLI mit Ihrer standardmäßigen AWS-Region konfigurieren. Weitere Informationen finden Sie unter Konfigurationsgrundlagen im AWS Command Line Interface Benutzerhandbuch.

So richten Sie Trusted Language Extensions ein

1. Verwenden Sie den modify-db-parameter-group AWS CLI Befehl, `pg_tle` um den `shared_preload_libraries` Parameter zu erweitern.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=pg_tle,ApplyMethod=pending-
reboot" \
   --region aws-region
```

2. Verwenden Sie den reboot-db-instance AWS CLI Befehl, um die Writer-Instance Ihrer Aurora neu zu starten und die Bibliothek zu initialisieren. `pg_tle`

```
aws rds reboot-db-instance \
    --db-instance-identifier writer-instance \
    --region aws-region
```

3. Wenn die Instance verfügbar ist, können Sie überprüfen, ob `pg_tle` initialisiert wurde. Stellen Sie über `psql` eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her und führen Sie den folgenden Befehl aus.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pg_tle
```

```
(1 row)
```

Sobald `pg_tle` initialisiert ist, können Sie die Erweiterung erstellen.

```
CREATE EXTENSION pg_tle;
```

4. Weisen Sie der `pgtle_admin`-Rolle dem primären Benutzernamen zu, den Sie bei der Einrichtung für Ihren DB-Cluster von Aurora PostgreSQL erstellt haben. Wenn Sie die Standardeinstellung akzeptiert haben, lautet der Wert `postgres`.

```
GRANT pgtle_admin TO postgres;
GRANT ROLE
```

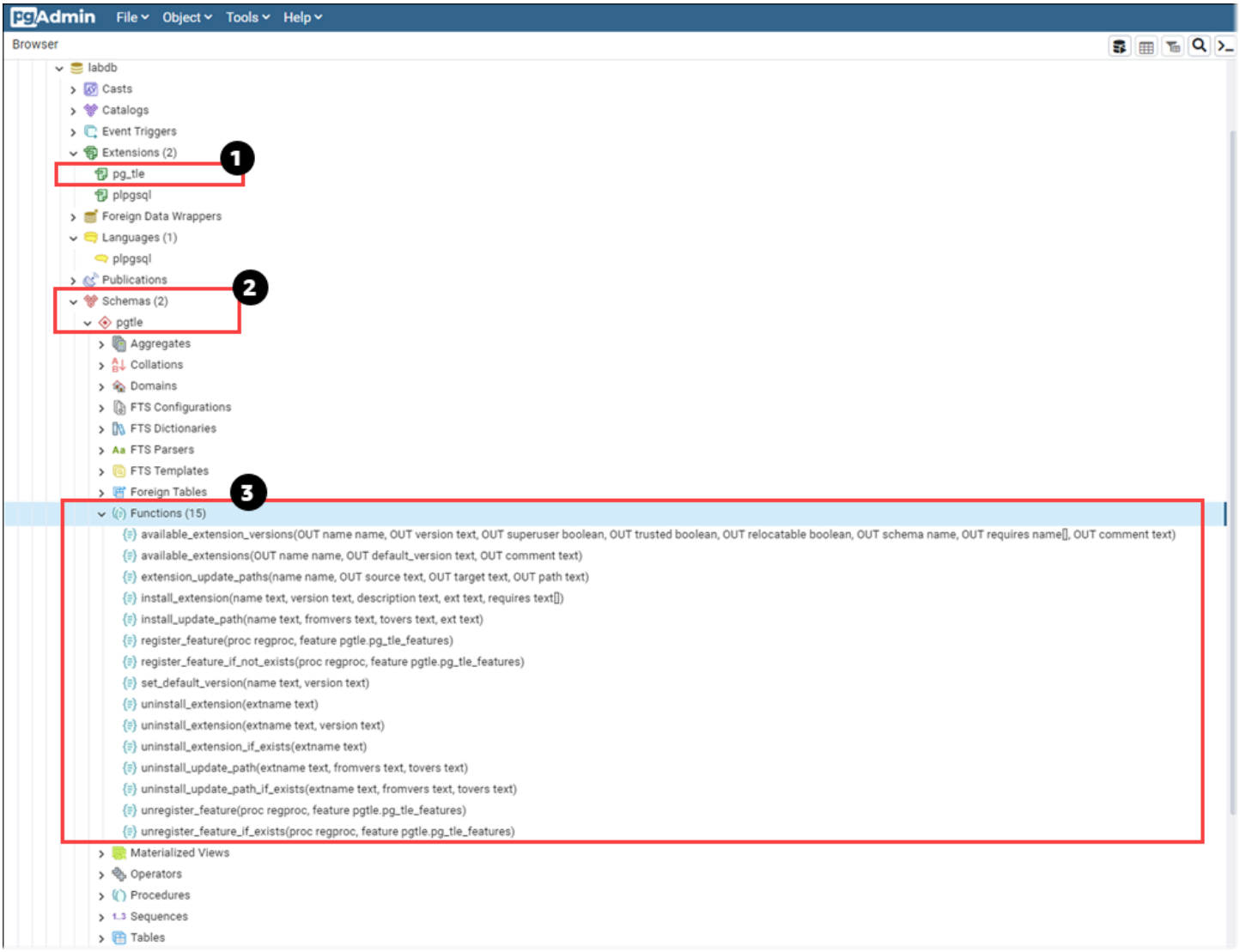
5. Schließen Sie die `psql`-Sitzung wie folgt.

```
labdb=> \q
```

Informationen zum Erstellen von TLE-Erweiterungen finden Sie unter Beispiel: Erstellen einer Trusted Language Extension mit SQL.

Übersicht über Trusted Language Extensions für PostgreSQL

Trusted Language Extensions für PostgreSQL ist eine PostgreSQL-Erweiterung, die Sie in Ihrem DB-Cluster von Aurora PostgreSQL auf die gleiche Weise installieren, wie Sie andere PostgreSQL-Erweiterungen einrichten. In der folgenden Abbildung einer Beispieldatenbank im pgAdmin-Client-Tool können Sie einige der Komponenten sehen, aus denen die `pg_tle`-Erweiterung besteht.



Sie können die folgenden Details sehen.

1. Das Entwicklungskit von Trusted Language Extensions (TLE) für PostgreSQL ist als `pg_tle`-Erweiterung verpackt. Daher wird `pg_tle` den verfügbaren Erweiterungen für die Datenbank hinzugefügt, in der es installiert ist.
2. TLE hat ein eigenes Schema, `pgtle`. Dieses Schema enthält Hilfsfunktionen (3) für die Installation und Verwaltung der von Ihnen erstellten Erweiterungen.
3. TLE bietet über ein Dutzend Hilfsfunktionen für die Installation, Registrierung und Verwaltung Ihrer Erweiterungen. Weitere Informationen zu diesen Funktionen finden Sie unter Funktionsreferenz für Trusted Language Extensions für PostgreSQL.

Das `pg_tle`-Erweiterungspaket umfasst außerdem folgende Komponenten:

- Die **`pgtle_admin`**-Rolle – Die `pgtle_admin`-Rolle wird erstellt, wenn die `pg_tle`-Erweiterung installiert wird. Diese Rolle ist privilegiert und sollte entsprechend behandelt werden. Es wird dringend empfohlen, bei der Gewährung der `pgtle_admin`-Rolle an Datenbankbenutzer dem Prinzip der geringsten Berechtigung zu folgen. Mit anderen Worten, weisen Sie die `pgtle_admin`-Rolle nur Datenbankbenutzern zu, die berechtigt sind, neue TLE-Erweiterungen zu erstellen, zu installieren und zu verwalten, wie z. b. `postgres`.
- Die **`pgtle.feature_info`**-Tabelle – Die `pgtle.feature_info`-Tabelle ist eine geschützte Tabelle, die Informationen über Ihre TLEs, Haken und die von ihnen verwendeten benutzerdefinierten gespeicherten Prozeduren und Funktionen enthält. Wenn Sie über `pgtle_admin`-Berechtigungen verfügen, verwenden Sie die folgenden Funktionen von Trusted Language Extensions, um diese Informationen in der Tabelle hinzuzufügen und zu aktualisieren.
  - pgtle.register_feature
  - pgtle.register_feature_if_not_exists
  - pgtle.unregister_feature
  - pgtle.unregister_feature_if_exists

Erstellen von TLE-Erweiterungen für Aurora PostgreSQL

Sie können alle Erweiterungen, die Sie mit TLE erstellen, in jedem beliebigen DB-Cluster von Aurora PostgreSQL installieren, sofern die die `pg_tle`-Erweiterung darauf installiert ist. Die `pg_tle`-Erweiterung ist auf die PostgreSQL-Datenbank beschränkt, in der sie installiert ist. Die Erweiterungen, die Sie mit TLE erstellen, sind auf dieselbe Datenbank ausgelegt.

Verwenden Sie die verschiedenen `pgtle`-Funktionen, um den Code zu installieren, aus dem Ihre TLE-Erweiterung besteht. Die folgenden Funktionen von Trusted Language Extensions erfordern alle die `pgtle_admin`-Rolle.

- pgtle.install_extension
- pgtle.install_update_path
- pgtle.register_feature
- pgtle.register_feature_if_not_exists
- pgtle.set_default_version
- pgtle.uninstall_extension(name)
- pgtle.uninstall_extension(name, version)

- pgtle.uninstall_extension_if_exists
- pgtle.uninstall_update_path
- pgtle.uninstall_update_path_if_exists
- pgtle.unregister_feature
- pgtle.unregister_feature_if_exists

Beispiel: Erstellen einer Trusted Language Extension mit SQL

Das folgende Beispiel zeigt Ihnen, wie Sie eine TLE-Erweiterung namens `pg_distance` erstellen, die einige SQL-Funktionen für die Berechnung von Entfernungen mit verschiedenen Formeln enthält. In der Liste finden Sie die Funktion zur Berechnung der Manhattan-Distanz und die Funktion zur Berechnung des euklidischen Abstands. Weitere Informationen zum Unterschied zwischen diesen Formeln finden Sie unter Taxi-Geometerie und Euklidische Geometrie in Wikipedia.

Sie können dieses Beispiel in Ihrem eigenen DB-Cluster von Aurora PostgreSQL verwenden, wenn Sie die `pg_tle`-Erweiterung wie unter Einrichten von Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL beschrieben eingerichtet haben.

> **Note**
>
> Sie benötigen die Rechte der `pgtle_admin`-Rolle, um dieses Verfahren ausführen zu können.

So erstellen Sie die TLE-Beispielerweiterung

In den folgenden Schritten wird eine Beispieldatenbank namens `labdb` verwendet. Diese Datenbank gehört dem `postgres`-Hauptbenutzer. Die `postgres`-Rolle verfügt auch über die Berechtigungen der `pgtle_admin`-Rolle.

1. Verwenden Sie `psql`, um eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL herzustellen.

   ```
   psql --host=db-instance-123456789012.aws-region.rds.amazonaws.com
   --port=5432 --username=postgres --password --dbname=labdb
   ```

2. Erstellen Sie eine TLE-Erweiterung mit dem Namen `pg_distance`, indem Sie den folgenden Code kopieren und in Ihre `psql`-Sitzungskonsole einfügen.

```
SELECT pgtle.install_extension
(
 'pg_distance',
 '0.1',
  'Distance functions for two points',
$_pg_tle_$
    CREATE FUNCTION dist(x1 float8, y1 float8, x2 float8, y2 float8, norm int)
    RETURNS float8
    AS $$
      SELECT (abs(x2 - x1) ^ norm + abs(y2 - y1) ^ norm) ^ (1::float8 / norm);
    $$ LANGUAGE SQL;

    CREATE FUNCTION manhattan_dist(x1 float8, y1 float8, x2 float8, y2 float8)
    RETURNS float8
    AS $$
      SELECT dist(x1, y1, x2, y2, 1);
    $$ LANGUAGE SQL;

    CREATE FUNCTION euclidean_dist(x1 float8, y1 float8, x2 float8, y2 float8)
    RETURNS float8
    AS $$
      SELECT dist(x1, y1, x2, y2, 2);
    $$ LANGUAGE SQL;
$_pg_tle_$
);
```

Die Ausgabe sollte folgendermaßen aussehen.

```
install_extension
---------------
 t
(1 row)
```

Die Artefakte, aus denen die `pg_distance`-Erweiterung besteht, sind jetzt in Ihrer Datenbank installiert. Zu diesen Artefakten gehören die Steuerdatei und der Code für die Erweiterung. Diese Elemente müssen vorhanden sein, damit die Erweiterung mit dem `CREATE EXTENSION`-Befehl erstellt werden kann. Mit anderen Worten, Sie müssen die Erweiterung nach wie vor erstellen, um ihre Funktionen Datenbankbenutzern zur Verfügung zu stellen.

3. Um die Erweiterung zu erstellen, verwenden Sie den `CREATE EXTENSION`-Befehl wie für jede andere Erweiterung. Wie bei anderen Erweiterungen muss der Datenbankbenutzer über die `CREATE`-Berechtigungen in der Datenbank verfügen.

```
CREATE EXTENSION pg_distance;
```

4. Um die `pg_distance`-TLE-Erweiterung zu testen, können Sie sie verwenden, um die Manhattan-Distanz zwischen vier Punkten zu berechnen.

```
labdb=> SELECT manhattan_dist(1, 1, 5, 5);
8
```

   Um den euklidischen Abstand zwischen derselben Menge von Punkten zu berechnen, können Sie Folgendes verwenden.

```
labdb=> SELECT euclidean_dist(1, 1, 5, 5);
5.656854249492381
```

Die `pg_distance`-Erweiterung lädt die Funktionen in die Datenbank und stellt sie allen Benutzern mit Berechtigungen für die Datenbank zur Verfügung.

Ändern Ihrer TLE-Erweiterung

Um die Abfrageleistung für die in dieser TLE-Erweiterung enthaltenen Funktionen zu verbessern, fügen Sie ihren Spezifikationen die beiden folgenden PostgreSQL-Attribute hinzu.

- `IMMUTABLE` – Das `IMMUTABLE`-Attribut stellt sicher, dass der Abfrageoptimierer Optimierungen verwenden kann, um die Antwortzeiten von Abfragen zu verbessern. Weitere Informationen finden Sie im Abschnitt Volatilitätskategorien von Funktionen der PostgreSQL-Dokumentation.
- `PARALLEL SAFE` – Das `PARALLEL SAFE`-Attribut ist ein weiteres Attribut, das es PostgreSQL ermöglicht, die Funktion im Parallelmodus auszuführen. Weitere Informationen finden Sie im Abschnitt CREATE FUNCTION der PostgreSQL-Dokumentation.

Im folgenden Beispiel können Sie sehen, wie die `pgtle.install_update_path`-Funktion verwendet wird, um diese Attribute jeder Funktion hinzuzufügen, um eine Version `0.2` der `pg_distance`-TLE-Erweiterung zu erstellen. Weitere Informationen zu dieser Funktion finden

Sie unter pgtle.install_update_path. Sie benötigen die `pgtle_admin` Rolle, um diese Aufgabe auszuführen.

So aktualisieren Sie eine vorhandene TLE-Erweiterung und geben die Standardversion an

1. Stellen Sie über `psql` oder ein anderes Client-Tool wie pgAdmin eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her.

```
psql --host=db-instance-123456789012.aws-region.rds.amazonaws.com
--port=5432 --username=postgres --password --dbname=labdb
```

2. Ändern Sie die vorhandene TLE-Erweiterung, indem Sie den folgenden Code kopieren und in Ihre `psql`-Sitzungskonsole einfügen.

```
SELECT pgtle.install_update_path
(
 'pg_distance',
 '0.1',
 '0.2',
$_pg_tle_$
    CREATE OR REPLACE FUNCTION dist(x1 float8, y1 float8, x2 float8, y2 float8,
 norm int)
    RETURNS float8
    AS $$
      SELECT (abs(x2 - x1) ^ norm + abs(y2 - y1) ^ norm) ^ (1::float8 / norm);
    $$ LANGUAGE SQL IMMUTABLE PARALLEL SAFE;

    CREATE OR REPLACE FUNCTION manhattan_dist(x1 float8, y1 float8, x2 float8, y2
 float8)
    RETURNS float8
    AS $$
      SELECT dist(x1, y1, x2, y2, 1);
    $$ LANGUAGE SQL IMMUTABLE PARALLEL SAFE;

    CREATE OR REPLACE FUNCTION euclidean_dist(x1 float8, y1 float8, x2 float8, y2
 float8)
    RETURNS float8
    AS $$
      SELECT dist(x1, y1, x2, y2, 2);
    $$ LANGUAGE SQL IMMUTABLE PARALLEL SAFE;
$_pg_tle_$
);
```

Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt.

```
install_update_path
--------------------
 t
(1 row)
```

Sie können diese Version der Erweiterung zur Standardversion machen, sodass Datenbankbenutzer keine Version angeben müssen, wenn sie die Erweiterung in ihrer Datenbank erstellen oder aktualisieren.

3. Um anzugeben, dass die modifizierte Version (Version 0.2) Ihrer TLE-Erweiterung die Standardversion ist, verwenden Sie die `pgtle.set_default_version`-Funktion wie im folgenden Beispiel gezeigt.

```
SELECT pgtle.set_default_version('pg_distance', '0.2');
```

Weitere Informationen zu dieser Funktion finden Sie unter pgtle.set_default_version.

4. Wenn der Code vorhanden ist, können Sie die installierte TLE-Erweiterung wie gewohnt aktualisieren, indem Sie den `ALTER EXTENSION ... UPDATE`-Befehl verwenden, wie hier gezeigt:

```
ALTER EXTENSION pg_distance UPDATE;
```

Löschen Ihrer TLE-Erweiterungen aus einer Datenbank

Sie können Ihre TLE-Erweiterungen löschen, indem Sie den `DROP EXTENSION`-Befehl auf die gleiche Weise wie für andere PostgreSQL-Erweiterungen verwenden. Durch das Löschen der Erweiterung werden die Installationsdateien, aus denen die Erweiterung besteht, nicht entfernt, sodass Benutzer die Erweiterung neu erstellen können. Gehen Sie wie folgt in zwei Schritten vor, um die Erweiterung und ihre Installationsdateien zu entfernen.

So löschen Sie die TLE-Erweiterung und entfernen ihre Installationsdateien

1. Stellen Sie über `psql` oder ein anderes Client-Tool eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her.

```
psql --host=cluster-instance-1.111122223333.aws-region.rds.amazonaws.com --
port=5432 --username=postgres --password --dbname=dbname
```

2. Löschen Sie die Erweiterung so wie jede andere PostgreSQL-Erweiterung.

```
DROP EXTENSION your-TLE-extension
```

Wenn Sie die `pg_distance`-Erweiterung beispielsweise wie in beschrieben Beispiel: Erstellen einer Trusted Language Extension mit SQL erstellen, können Sie die Erweiterung wie folgt löschen.

```
DROP EXTENSION pg_distance;
```

Es wird eine Ausgabe angezeigt, die bestätigt, dass die Erweiterung gelöscht wurde, wie im Folgenden gezeigt.

```
DROP EXTENSION
```

Zu diesem Zeitpunkt ist die Erweiterung in der Datenbank nicht mehr aktiv. Die Installationsdateien und die Steuerdatei sind jedoch nach wie vor in der Datenbank verfügbar, sodass Datenbankbenutzer die Erweiterung erneut erstellen können, wenn sie möchten.

- Wenn Sie die Erweiterungsdateien intakt lassen möchten, damit Datenbankbenutzer Ihre TLE-Erweiterung erstellen können, können Sie an dieser Stelle aufhören.
- Wenn Sie alle Dateien, aus denen die Erweiterung besteht, entfernen möchten, fahren Sie mit dem nächsten Schritt fort.

3. Verwenden Sie die `pgtle.uninstall_extension`-Funktion, um alle Installationsdateien für Ihre Erweiterung zu entfernen. Diese Funktion entfernt dne gesamten Code und die Steuerdateien für Ihre Erweiterung.

```
SELECT pgtle.uninstall_extension('your-tle-extension-name');
```

Verwenden Sie beispielsweise den folgenden Befehl, um alle `pg_distance`-Installationsdateien zu entfernen.

```
SELECT pgtle.uninstall_extension('pg_distance');
```

```
 uninstall_extension
---------------------
 t
(1 row)
```

Deinstallieren von Trusted Language Extensions für PostgreSQL

Wenn Sie keine eigenen TLE-Erweiterungen mehr mit TLE erstellen möchten, können Sie die `pg_tle`-Erweiterung löschen und alle Artefakte entfernen. Diese Aktion beinhaltet das Löschen aller TLE-Erweiterungen in der Datenbank und das Entfernen des`pgtle`-Schemas.

So löschen Sie die **`pg_tle`**-Erweiterung und ihr Schema aus einer Datenbank

1. Stellen Sie über `psql` oder ein anderes Client-Tool eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL her.

   ```
   psql --host=cluster-instance-1.111122223333.aws-region.rds.amazonaws.com --
   port=5432 --username=postgres --password --dbname=dbname
   ```

2. Löschen Sie die `pg_tle`-Erweiterung aus der Datenbank. Wenn Ihre eigenen TLE-Erweiterungen noch in der Datenbank laufen, müssen Sie diese Erweiterungen ebenfalls löschen. Dazu können Sie das `CASCADE`-Schlüsselwort verwenden, wie im Folgenden gezeigt.

   ```
   DROP EXTENSION pg_tle CASCADE;
   ```

   Wenn die `pg_tle`-Erweiterung in der Datenbank nicht mehr aktiv ist, müssen Sie das `CASCADE`-Schlüsselwort nicht verwenden.

3. Löschen Sie das `pgtle`-Schema. Mit dieser Aktion werden alle Verwaltungsfunktionen aus der Datenbank entfernt.

   ```
   DROP SCHEMA pgtle CASCADE;
   ```

   Der Befehl gibt nach Abschluss des Vorgangs Folgendes zurück.

   ```
   DROP SCHEMA
   ```

   Die `pg_tle`-Erweiterung, ihr Schema und ihre Funktionen sowie alle Artefakte werden entfernt. Um neue Erweiterungen mit TLE zu erstellen, führen Sie den Einrichtungsvorgang erneut durch.

Weitere Informationen finden Sie unter Einrichten von Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL.

Verwenden von PostgreSQL-Haken mit Ihren TLE-Erweiterungen

Ein Haken ist ein in PostgreSQL verfügbarer Callback-Mechanismus, der es Entwicklern ermöglicht, benutzerdefinierte Funktionen oder andere Routinen während regulärer Datenbankoperationen aufzurufen. Das TLE-Entwicklungskit unterstützt PostgreSQL-Haken, sodass Sie benutzerdefinierte Funktionen zur Laufzeit in das PostgreSQL-Verhalten integrieren können. Sie können beispielsweise einen Haken verwenden, um den Authentifizierungsprozess mit Ihrem eigenen benutzerdefinierten Code zu verknüpfen oder um den Planungs- und Ausführungsprozess für Abfragen Ihren spezifischen Bedürfnissen entsprechend anzupassen.

Ihre TLE-Erweiterungen können Haken verwenden. Wenn ein Haken einen globalen Gültigkeitsbereich hat, gilt er für alle Datenbanken. Wenn Ihre TLE-Erweiterung einen globalen Haken verwendet, müssen Sie Ihre TLE-Erweiterung daher in allen Datenbanken erstellen, auf die Ihre Benutzer zugreifen können.

Wenn Sie die `pg_tle`-Erweiterung verwenden, um Ihre eigenen Trusted Language Extensions zu erstellen, können Sie die verfügbaren Haken einer SQL-API verwenden, um die Funktionen Ihrer Erweiterung zu erstellen. Sie sollten alle Haken bei `pg_tle` registrieren. Für einige Haken müssen Sie möglicherweise auch verschiedene Konfigurationsparameter festlegen. Der `passcode`-Prüfungshaken kann beispielsweise auf ein, aus oder erforderlich festgelegt werden. Weitere Hinweise zu den spezifischen Anforderungen für verfügbare `pg_tle`-Haken finden Sie unter Hakenreferenz für Trusted Language Extensions für PostgreSQL.

Beispiel: Erstellen einer Erweiterung, die einen PostgreSQL-Haken verwendet

Das in diesem Abschnitt besprochene Beispiel verwendet einen PostgreSQL-Haken, um das bei bestimmten SQL-Vorgängen angegebene Passwort zu überprüfen, und verhindert, dass Datenbankbenutzer ihre Passwörter auf eines der in der `password_check.bad_passwords`-Tabelle enthaltenen Passwörter festlegen. Die Tabelle enthält die zehn am häufigsten verwendeten, aber leicht zu knackenden Optionen für Passwörter.

Um dieses Beispiel in Ihrem DB-Cluster von Aurora PostgreSQL einzurichten, müssen Sie Trusted Language Extensions bereits installiert haben. Details hierzu finden Sie unter Einrichten von Trusted Language Extensions in Ihrem DB-Cluster von Aurora PostgreSQL.

So richten Sie das Beispiel für einen Haken für die Passwortüberprüfung ein

1. Verwenden Sie `psql`, um eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL herzustellen.

```
psql --host=db-instance-123456789012.aws-region.rds.amazonaws.com
--port=5432 --username=postgres --password --dbname=labdb
```

2. Kopieren Sie den Code von Liste der Hakencodes für die Passwortüberprüfung und fügen Sie ihn in Ihre Datenbank ein.

```
SELECT pgtle.install_extension (
  'my_password_check_rules',
  '1.0',
  'Do not let users use the 10 most commonly used passwords',
$_pgtle_$
  CREATE SCHEMA password_check;
  REVOKE ALL ON SCHEMA password_check FROM PUBLIC;
  GRANT USAGE ON SCHEMA password_check TO PUBLIC;

  CREATE TABLE password_check.bad_passwords (plaintext) AS
  VALUES
    ('123456'),
    ('password'),
    ('12345678'),
    ('qwerty'),
    ('123456789'),
    ('12345'),
    ('1234'),
    ('111111'),
    ('1234567'),
    ('dragon');
  CREATE UNIQUE INDEX ON password_check.bad_passwords (plaintext);

  CREATE FUNCTION password_check.passcheck_hook(username text, password text,
 password_type pgtle.password_types, valid_until timestamptz, valid_null boolean)
  RETURNS void AS $$
    DECLARE
      invalid bool := false;
    BEGIN
      IF password_type = 'PASSWORD_TYPE_MD5' THEN
        SELECT EXISTS(
          SELECT 1
```

```
          FROM password_check.bad_passwords bp
          WHERE ('md5' || md5(bp.plaintext || username)) = password
        ) INTO invalid;
        IF invalid THEN
          RAISE EXCEPTION 'Cannot use passwords from the common password
 dictionary';
        END IF;
      ELSIF password_type = 'PASSWORD_TYPE_PLAINTEXT' THEN
        SELECT EXISTS(
          SELECT 1
          FROM password_check.bad_passwords bp
          WHERE bp.plaintext = password
        ) INTO invalid;
        IF invalid THEN
          RAISE EXCEPTION 'Cannot use passwords from the common common password
 dictionary';
        END IF;
      END IF;
    END
  $$ LANGUAGE plpgsql SECURITY DEFINER;

  GRANT EXECUTE ON FUNCTION password_check.passcheck_hook TO PUBLIC;

  SELECT pgtle.register_feature('password_check.passcheck_hook', 'passcheck');
$_pgtle_$
);
```

Wenn die Erweiterung in Ihre Datenbank geladen wurde, sehen Sie eine Ausgabe ähnlich wie die folgende.

```
 install_extension
-------------------
 t
(1 row)
```

3. Während Sie noch mit der Datenbank verbunden sind, können Sie jetzt die Erweiterung erstellen.

```
CREATE EXTENSION my_password_check_rules;
```

4. Mit dem folgenden `psql`-Metabefehl können Sie bestätigen, dass die Erweiterung in der Datenbank erstellt wurde.

```
\dx
                        List of installed extensions
          Name           | Version |   Schema   |
 Description
-------------------------+---------+------------
+-------------------------------------------------------------
 my_password_check_rules | 1.0     | public     | Prevent use of any of the top-ten
 most common bad passwords
 pg_tle                  | 1.0.1   | pgtle      | Trusted-Language Extensions for
 PostgreSQL
 plpgsql                 | 1.0     | pg_catalog | PL/pgSQL procedural language
(3 rows)
```

5. Öffnen Sie eine weitere Terminalsitzung, um mit dem zu arbeiten. AWS CLI Sie müssen Ihre benutzerdefinierte DB-Parametergruppe ändern, um den Haken für die Passwortüberprüfung zu aktivieren. Verwenden Sie dazu den modify-db-parameter-groupCLI-Befehl, wie im folgenden Beispiel gezeigt.

```
aws rds modify-db-parameter-group \
    --region aws-region \
    --db-parameter-group-name your-custom-parameter-group \
    --parameters
 "ParameterName=pgtle.enable_password_check,ParameterValue=on,ApplyMethod=immediate"
```

   Es kann einige Minuten dauern, bis die Änderung der Parametergruppe wirksam wird. Dieser Parameter ist jedoch dynamisch, sodass Sie die Writer-Instance des DB-Clusters von Aurora PostgreSQL nicht neu starten müssen, damit die Einstellung wirksam wird.

6. Öffnen Sie die `psql`-Sitzung und fragen Sie die Datenbank ab, um zu überprüfen, ob der password_check-Haken aktiviert wurde.

```
labdb=> SHOW pgtle.enable_password_check;
pgtle.enable_password_check
----------------------------
on
(1 row)
```

Der Haken für die Passwortüberprüfung ist jetzt aktiv. Sie können dies testen, indem Sie eine neue Rolle erstellen und eines der schwachen Passwörter verwenden, wie im folgenden Beispiel gezeigt.

```
CREATE ROLE test_role PASSWORD 'password';
ERROR:  Cannot use passwords from the common password dictionary
CONTEXT:  PL/pgSQL function
 password_check.passcheck_hook(text,text,pgtle.password_types,timestamp with time
 zone,boolean) line 21 at RAISE
SQL statement "SELECT password_check.passcheck_hook(
    $1::pg_catalog.text,
    $2::pg_catalog.text,
    $3::pgtle.password_types,
    $4::pg_catalog.timestamptz,
    $5::pg_catalog.bool)"
```

Die Ausgabe wurde zur besseren Lesbarkeit formatiert.

Das folgende Beispiel zeigt, dass das interaktive `pgsql`-Metabefehlverhalten `\password` auch vom password_check-Haken beeinflusst wird.

```
postgres=> SET password_encryption TO 'md5';
SET
postgres=> \password
Enter new password for user "postgres":*****
Enter it again:*****
ERROR:  Cannot use passwords from the common password dictionary
CONTEXT:  PL/pgSQL function
 password_check.passcheck_hook(text,text,pgtle.password_types,timestamp with time
 zone,boolean) line 12 at RAISE
SQL statement "SELECT password_check.passcheck_hook($1::pg_catalog.text,
 $2::pg_catalog.text, $3::pgtle.password_types, $4::pg_catalog.timestamptz,
 $5::pg_catalog.bool)"
```

Sie können diese TLE-Erweiterung löschen und ihre Quelldateien deinstallieren, wenn Sie möchten. Weitere Informationen finden Sie unter Löschen Ihrer TLE-Erweiterungen aus einer Datenbank.

Liste der Hakencodes für die Passwortüberprüfung

Der hier gezeigte Beispielcode definiert die Spezifikation für die `my_password_check_rules`-TLE-Erweiterung. Wenn Sie diesen Code kopieren und in Ihre Datenbank einfügen, wird der Code für die `my_password_check_rules`-Erweiterung in die Datenbank geladen und der `password_check`-Haken für die Verwendung durch die Erweiterung registriert.

```
SELECT pgtle.install_extension (
  'my_password_check_rules',
```

```
  '1.0',
  'Do not let users use the 10 most commonly used passwords',
$_pgtle_$
  CREATE SCHEMA password_check;
  REVOKE ALL ON SCHEMA password_check FROM PUBLIC;
  GRANT USAGE ON SCHEMA password_check TO PUBLIC;

  CREATE TABLE password_check.bad_passwords (plaintext) AS
  VALUES
    ('123456'),
    ('password'),
    ('12345678'),
    ('qwerty'),
    ('123456789'),
    ('12345'),
    ('1234'),
    ('111111'),
    ('1234567'),
    ('dragon');
  CREATE UNIQUE INDEX ON password_check.bad_passwords (plaintext);

  CREATE FUNCTION password_check.passcheck_hook(username text, password text,
 password_type pgtle.password_types, valid_until timestamptz, valid_null boolean)
  RETURNS void AS $$
    DECLARE
      invalid bool := false;
    BEGIN
      IF password_type = 'PASSWORD_TYPE_MD5' THEN
        SELECT EXISTS(
          SELECT 1
          FROM password_check.bad_passwords bp
          WHERE ('md5' || md5(bp.plaintext || username)) = password
        ) INTO invalid;
        IF invalid THEN
          RAISE EXCEPTION 'Cannot use passwords from the common password dictionary';
        END IF;
      ELSIF password_type = 'PASSWORD_TYPE_PLAINTEXT' THEN
        SELECT EXISTS(
          SELECT 1
          FROM password_check.bad_passwords bp
          WHERE bp.plaintext = password
        ) INTO invalid;
        IF invalid THEN
```

```
          RAISE EXCEPTION 'Cannot use passwords from the common common password
 dictionary';
        END IF;
      END IF;
    END
  $$ LANGUAGE plpgsql SECURITY DEFINER;

  GRANT EXECUTE ON FUNCTION password_check.passcheck_hook TO PUBLIC;

  SELECT pgtle.register_feature('password_check.passcheck_hook', 'passcheck');
$_pgtle_$
);
```

Funktionsreferenz für Trusted Language Extensions für PostgreSQL

Sehen Sie sich die folgende Referenzdokumentation zu den Funktionen an, die in Trusted Language Extensions für PostgreSQL verfügbar sind. Verwenden Sie diese Funktionen, um Ihre TLE-Erweiterungen, d. h. die PostgreSQL-Erweiterungen, die Sie mit dem Trusted Language Extensions Development Kit entwickeln, zu installieren, zu registrieren, zu aktualisieren und zu verwalten.

Themen

pgtle.available_extensions

Die `pgtle.available_extensions`-Funktion ist eine Mengenrückgabefunktion. Sie gibt alle verfügbaren TLE-Erweiterungen in der Datenbank zurück. Jede zurückgegebene Zeile enthält Informationen zu einer einzelnen TLE-Erweiterung.

Funktionsprototyp

```
pgtle.available_extensions()
```

Rolle

Keine.

Argumente

Keine.

Ausgabe

- `name` – Der Name der TLE-Erweiterung.
- `default_version` – Die Version der TLE-Erweiterung, die verwendet werden soll, wenn `CREATE EXTENSION` ohne Angabe einer Version aufgerufen wird.
- `description` – Eine ausführlichere Beschreibung der TLE-Erweiterung.

Verwendungsbeispiel

```
SELECT * FROM pgtle.available_extensions();
```

pgtle.available_extension_versions

Die `available_extension_versions`-Funktion ist eine Mengenrückgabefunktion. Sie gibt eine Liste aller verfügbaren TLE-Erweiterungen und deren Versionen zurück. Jede Zeile enthält Informationen zu einer bestimmten Version der angegebenen TLE-Erweiterung, einschließlich der Frage, ob für sie eine bestimmte Rolle erforderlich ist.

Funktionsprototyp

```
pgtle.available_extension_versions()
```

Rolle

Keine.

Argumente

Keine.

Ausgabe

- `name` – Der Name der TLE-Erweiterung.
- `version` – Die Version der TLE-Erweiterung.
- `superuser` – Dieser Wert ist für Ihre TLE-Erweiterungen immer `false`. Die Berechtigungen, die zum Erstellen oder Aktualisieren der TLE-Erweiterung erforderlich sind, entsprechen denen, die für die Erstellung anderer Objekte in der angegebenen Datenbank notwendig sind.
- `trusted` – Dieser Wert ist für eine TLE-Erweiterung immer `false`.
- `relocatable` – Dieser Wert ist für eine TLE-Erweiterung immer `false`.
- `schema` – Gibt den Namen des Schemas an, in dem die TLE-Erweiterung installiert ist.
- `requires` – Ein Array, das die Namen anderer Erweiterungen enthält, die für diese TLE-Erweiterung benötigt werden.
- `description` – Eine ausführliche Beschreibung der TLE-Erweiterung.

Weitere Informationen zu Ausgabewerten finden Sie unter Packaging Related Objects into an Extension > Extension Files in der PostgreSQL-Dokumentation.

Verwendungsbeispiel

```
SELECT * FROM pgtle.available_extension_versions();
```

pgtle.extension_update_paths

Die `extension_update_paths`-Funktion ist eine Mengenrückgabefunktion. Sie gibt eine Liste aller möglichen Aktualisierungspfade für eine TLE-Erweiterung zurück. Jede Zeile enthält die verfügbaren Upgrades oder Downgrades für diese TLE-Erweiterung.

Funktionsprototyp

```
pgtle.extension_update_paths(name)
```

Rolle

Keine.

Argumente

`name` – Der Name der TLE-Erweiterung, von der die Upgrade-Pfade abgerufen werden sollen.

Ausgabe

- `source` – Die Quellversion für eine Aktualisierung.
- `target` – Die Zielversion für eine Aktualisierung.
- `path` – Der Upgrade-Pfad, der verwendet wird, um eine TLE-Erweiterung von der `source`-Version auf die `target`-Version zu aktualisieren, zum Beispiel `0.1--0.2`.

Verwendungsbeispiel

```
SELECT * FROM pgtle.extension_update_paths('your-TLE');
```

pgtle.install_extension

Mit dieser `install_extension`-Funktion können Sie die Artefakte, aus denen Ihre TLE-Erweiterung besteht, in der Datenbank installieren. Anschließend können sie mit dem `CREATE EXTENSION`-Befehl erstellt werden.

Funktionsprototyp

```
pgtle.install_extension(name text, version text, description text, ext text, requires
 text[] DEFAULT NULL::text[])
```

Rolle

Keine.

Argumente

- `name` – Der Name der TLE-Erweiterung. Dieser Wert wird beim Aufrufen von `CREATE EXTENSION` verwendet.
- `version` – Die Version der TLE-Erweiterung.

- `description` – Eine ausführliche Beschreibung der TLE-Erweiterung. Diese Beschreibung wird im Feld `comment` in `pgtle.available_extensions()` angezeigt.
- `ext` – Der Inhalt der TLE-Erweiterung. Dieser Wert enthält Objekte wie Funktionen.
- `requires` – Ein optionaler Parameter, der Abhängigkeiten für diese TLE-Erweiterung angibt. Die `pg_tle`-Erweiterung wird automatisch als Abhängigkeit hinzugefügt.

Viele dieser Argumente entsprechen denen, die in einer Erweiterungskontrolldatei für die Installation einer PostgreSQL-Erweiterung im Dateisystem einer PostgreSQL-Instance enthalten sind. Weitere Informationen finden Sie unter Extension Files in Packaging Related Objects in a Extension in der PostgreSQL-Dokumentation.

Ausgabe

Diese Funktion gibt bei Erfolg `OK` und bei Fehler `NULL` zurück.

- `OK` – Die TLE-Erweiterung wurde erfolgreich in der Datenbank installiert.
- `NULL` – Die TLE-Erweiterung wurde nicht erfolgreich in der Datenbank installiert.

Verwendungsbeispiel

```
SELECT pgtle.install_extension(
 'pg_tle_test',
 '0.1',
 'My first pg_tle extension',
$_pgtle_$
  CREATE FUNCTION my_test()
  RETURNS INT
  AS $$
    SELECT 42;
  $$ LANGUAGE SQL IMMUTABLE;
$_pgtle_$
);
```

pgtle.install_update_path

Die `install_update_path`-Funktion stellt einen Aktualisierungspfad zwischen zwei verschiedenen Versionen einer TLE-Erweiterung bereit. Mit dieser Funktion können Benutzer Ihrer TLE-Erweiterung ihre Version mithilfe der `ALTER EXTENSION ... UPDATE`-Syntax aktualisieren.

Funktionsprototyp

```
pgtle.install_update_path(name text, fromvers text, tovers text, ext text)
```

Rolle

`pgtle_admin`

Argumente

- `name` – Der Name der TLE-Erweiterung. Dieser Wert wird beim Aufrufen von `CREATE EXTENSION` verwendet.
- `fromvers` – Die Quellversion der TLE-Erweiterung für das Upgrade.
- `tovers` – Die Zielversion der TLE-Erweiterung für das Upgrade.
- `ext` – Der Inhalt der Aktualisierung. Dieser Wert enthält Objekte wie Funktionen.

Ausgabe

Keine.

Verwendungsbeispiel

```
SELECT pgtle.install_update_path('pg_tle_test', '0.1', '0.2',
  $_pgtle_$
    CREATE OR REPLACE FUNCTION my_test()
    RETURNS INT
    AS $$
      SELECT 21;
    $$ LANGUAGE SQL IMMUTABLE;
  $_pgtle_$
);
```

pgtle.register_feature

Die `register_feature`-Funktion fügt der `pgtle.feature_info`-Tabelle das angegebene interne PostgreSQL-Feature hinzu. PostgreSQL-Haken sind ein Beispiel für ein internes PostgreSQL-Feature. Das Trusted Language Extensions Development Kit unterstützt die Verwendung von PostgreSQL-Haken. Derzeit unterstützt diese Funktion das folgende Feature.

- `passcheck` – Registriert den Haken für die Passwortüberprüfung bei Ihrer Prozedur oder Funktion, die das Verhalten von PostgreSQL bei der Passwortüberprüfung anpasst.

Funktionsprototyp

```
pgtle.register_feature(proc regproc, feature pg_tle_feature)
```

Rolle

`pgtle_admin`

Argumente

- `proc` – Der Name einer gespeicherten Prozedur oder Funktion, die für das Feature verwendet werden soll.
- `feature` – Der Name des `pg_tle`-Features (z. B. `passcheck`), das für die Funktion registriert werden soll.

Ausgabe

Keine.

Verwendungsbeispiel

```
SELECT pgtle.register_feature('pw_hook', 'passcheck');
```

pgtle.register_feature_if_not_exists

Die `pgtle.register_feature_if_not_exists`-Funktion fügt der `pgtle.feature_info`-Tabelle das angegebene PostgreSQL-Feature hinzu und identifiziert die TLE-Erweiterung oder eine andere Prozedur oder Funktion, die das Feature verwendet. Weitere Informationen zu Haken und Trusted Language Extensions finden Sie unter Verwenden von PostgreSQL-Haken mit Ihren TLE-Erweiterungen.

Funktionsprototyp

```
pgtle.register_feature_if_not_exists(proc regproc, feature pg_tle_feature)
```

Rolle

`pgtle_admin`

Argumente

- `proc` – Der Name einer gespeicherten Prozedur oder Funktion, die die Logik (Code) enthält, die als Feature für Ihre TLE-Erweiterung verwendet werden soll. Beispielsweise der `pw_hook`-Code.
- `feature` – Der Name des PostgreSQL-Features, das für die TLE-Funktion registriert werden soll. Derzeit ist der `passcheck`-Haken das einzige verfügbare Feature. Weitere Informationen finden Sie unter Haken zur Passwortüberprüfung (Passcheck).

Ausgabe

Gibt `true` zurück, nachdem das Feature für die angegebene Erweiterung registriert wurde. Gibt `false` zurück, wenn das Feature bereits registriert ist.

Verwendungsbeispiel

```
SELECT pgtle.register_feature_if_not_exists('pw_hook', 'passcheck');
```

pgtle.set_default_version

Mit der `set_default_version`-Funktion können Sie eine `default_version` für Ihre TLE-Erweiterung angeben. Mit dieser Funktion können Sie einen Upgrade-Pfad definieren und die Version als Standard für Ihre TLE-Erweiterung festlegen. Wenn Datenbankbenutzer Ihre TLE-Erweiterung in den Befehlen `CREATE EXTENSION` und `ALTER EXTENSION ... UPDATE` angeben, wird diese Version Ihrer TLE-Erweiterung in der Datenbank für diesen Benutzer erstellt.

Diese Funktion gibt bei Erfolg `true` zurück. Wenn die im `name`-Argument angegebene TLE-Erweiterung nicht vorhanden ist, gibt die Funktion einen Fehler zurück. Entsprechend wird ein Fehler zurückgegeben, wenn die `version` der TLE-Erweiterung nicht existiert.

Funktionsprototyp

```
pgtle.set_default_version(name text, version text)
```

Rolle

`pgtle_admin`

Argumente

- `name` – Der Name der TLE-Erweiterung. Dieser Wert wird beim Aufrufen von `CREATE EXTENSION` verwendet.
- `version` – Die Version der TLE-Erweiterung, für die die Standardeinstellung festgelegt werden soll.

Ausgabe

- `true`– Wenn die Standardversion erfolgreich festgelegt wurde, gibt die Funktion `true` zurück.
- `ERROR` – Gibt eine Fehlermeldung zurück, wenn eine TLE-Erweiterung mit dem angegebenen Namen oder der angegebenen Version nicht existiert.

Verwendungsbeispiel

```
SELECT * FROM pgtle.set_default_version('my-extension', '1.1');
```

pgtle.uninstall_extension(name)

Die `uninstall_extension`-Funktion entfernt alle Versionen einer TLE-Erweiterung aus einer Datenbank. Diese Funktion verhindert, dass die TLE-Erweiterung durch künftige Aufrufe von `CREATE EXTENSION` installiert wird. Wenn die TLE-Erweiterung in der Datenbank nicht existiert, wird ein Fehler ausgelöst.

Die `uninstall_extension`-Funktion löscht die TLE-Erweiterung jedoch nicht, wenn diese derzeit in der Datenbank aktiv ist. Zum Löschen einer TLE-Erweiterung, die derzeit aktiv ist, müssen Sie explizit `DROP EXTENSION` aufrufen, um sie zu entfernen.

Funktionsprototyp

```
pgtle.uninstall_extension(extname text)
```

Rolle

`pgtle_admin`

Argumente

- `extname` – Der Name der zu deinstallierenden TLE-Erweiterung. Dieser Name ist derselbe, der mit `CREATE EXTENSION` verwendet wurde, um die TLE-Erweiterung zur Verwendung in einer bestimmten Datenbank zu laden.

Ausgabe

Keine.

Verwendungsbeispiel

```
SELECT * FROM pgtle.uninstall_extension('pg_tle_test');
```

pgtle.uninstall_extension(name, version)

Die `uninstall_extension(name, version)`-Funktion entfernt die angegebene Version der TLE-Erweiterung aus der Datenbank. Diese Funktion verhindert, dass `CREATE EXTENSION` und `ALTER EXTENSION` eine TLE-Erweiterung installieren oder auf die angegebene Version aktualisieren. Diese Funktion entfernt außerdem alle Aktualisierungspfade für die angegebene Version der TLE-Erweiterung. Diese Funktion deinstalliert die TLE-Erweiterung jedoch nicht, wenn diese derzeit in der Datenbank aktiv ist. Sie müssen explizit `DROP EXTENSION` aufrufen, um die TLE-Erweiterung zu entfernen. Informationen zur Deinstallation aller Versionen einer TLE-Erweiterung finden Sie unter pgtle.uninstall_extension(name).

Funktionsprototyp

```
pgtle.uninstall_extension(extname text, version text)
```

Rolle

`pgtle_admin`

Argumente

- `extname` – Der Name der TLE-Erweiterung. Dieser Wert wird beim Aufrufen von `CREATE EXTENSION` verwendet.
- `version` – Die Version der TLE-Erweiterung, die in der Datenbank deinstalliert werden soll.

Ausgabe

Keine.

Verwendungsbeispiel

```
SELECT * FROM pgtle.uninstall_extension('pg_tle_test', '0.2');
```

pgtle.uninstall_extension_if_exists

Die `uninstall_extension_if_exists`-Funktion entfernt alle Versionen einer TLE-Erweiterung aus einer bestimmten Datenbank. Wenn die TLE-Erweiterung nicht existiert, bleibt die Funktion im Hintergrund (es wird keine Fehlermeldung ausgegeben). Wenn die angegebene Erweiterung derzeit in einer Datenbank aktiv ist, wird sie von dieser Funktion nicht gelöscht. Sie müssen `DROP EXTENSION` explizit aufrufen, um die TLE-Erweiterung zu entfernen, bevor Sie diese Funktion verwenden, um ihre Artefakte zu deinstallieren.

Funktionsprototyp

```
pgtle.uninstall_extension_if_exists(extname text)
```

Rolle

`pgtle_admin`

Argumente

- `extname` – Der Name der TLE-Erweiterung. Dieser Wert wird beim Aufrufen von `CREATE EXTENSION` verwendet.

Ausgabe

Die `uninstall_extension_if_exists`-Funktion gibt `true` nach der Deinstallation der angegebenen Erweiterung zurück. Wenn die angegebene Erweiterung nicht vorhanden ist, gibt die Funktion `false` zurück.

- `true` – Gibt `true` nach der Deinstallation der TLE-Erweiterung zurück.
- `false` – Gibt `false` zurück, wenn die TLE-Erweiterung in der Datenbank nicht existiert.

Verwendungsbeispiel

```
SELECT * FROM pgtle.uninstall_extension_if_exists('pg_tle_test');
```

pgtle.uninstall_update_path

Die `uninstall_update_path`-Funktion entfernt den angegebenen Aktualisierungspfad einer TLE-Erweiterung. Dadurch wird verhindert, dass `ALTER EXTENSION ... UPDATE TO` diesen Pfad als Aktualisierungspfad verwendet.

Wenn die TLE-Erweiterung derzeit von einer der Versionen in diesem Aktualisierungspfad verwendet wird, verbleibt sie in der Datenbank.

Wenn der angegebene Aktualisierungspfad nicht vorhanden ist, gibt diese Funktion einen Fehler aus.

Funktionsprototyp

```
pgtle.uninstall_update_path(extname text, fromvers text, tovers text)
```

Rolle

`pgtle_admin`

Argumente

- `extname` – Der Name der TLE-Erweiterung. Dieser Wert wird beim Aufrufen von `CREATE EXTENSION` verwendet.
- `fromvers` – Die Quellversion der TLE-Erweiterung, die im Aktualisierungspfad verwendet wird.
- `tovers` – Die Zielversion der TLE-Erweiterung, die im Aktualisierungspfad verwendet wird.

Ausgabe

Keine.

Verwendungsbeispiel

```
SELECT * FROM pgtle.uninstall_update_path('pg_tle_test', '0.1', '0.2');
```

pgtle.uninstall_update_path_if_exists

Die `uninstall_update_path_if_exists`-Funktion ähnelt `uninstall_update_path` insofern, als sie den angegebenen Aktualisierungspfad aus einer TLE-Erweiterung entfernt. Wenn der Aktualisierungspfad jedoch nicht existiert, löst diese Funktion keine Fehlermeldung aus. Stattdessen gibt die Funktion `false` zurück.

Funktionsprototyp

```
pgtle.uninstall_update_path_if_exists(extname text, fromvers text, tovers text)
```

Rolle

`pgtle_admin`

Argumente

- `extname` – Der Name der TLE-Erweiterung. Dieser Wert wird beim Aufrufen von `CREATE EXTENSION` verwendet.
- `fromvers` – Die Quellversion der TLE-Erweiterung, die im Aktualisierungspfad verwendet wird.
- `tovers` – Die Zielversion der TLE-Erweiterung, die im Aktualisierungspfad verwendet wird.

Ausgabe

- `true` – Die Funktion hat den Pfad für die TLE-Erweiterung erfolgreich aktualisiert.
- `false` – Die Funktion konnte den Pfad für die TLE-Erweiterung nicht aktualisieren.

Verwendungsbeispiel

```
SELECT * FROM pgtle.uninstall_update_path_if_exists('pg_tle_test', '0.1', '0.2');
```

pgtle.unregister_feature

Die `unregister_feature`-Funktion bietet eine Möglichkeit, Funktionen zu entfernen, die für die Verwendung von `pg_tle`-Features wurden, wie z. B. Haken. Weitere Informationen zur Registrierung eines Features erhalten Sie unter pgtle.register_feature.

Funktionsprototyp

```
pgtle.unregister_feature(proc regproc, feature pg_tle_features)
```

Rolle

`pgtle_admin`

Argumente

- `proc` – Der Name einer gespeicherten Funktion, für die ein `pg_tle`-Feature registriert werden soll.
- `feature` – Der Name des `pg_tle`-Features, das für die Funktion registriert werden soll. Beispielsweise ist `passcheck` ein Feature, das für die Verwendung durch die vertrauenswürdigen Spracherweiterungen, die Sie entwickeln, registriert werden kann. Weitere Informationen finden Sie unter Haken zur Passwortüberprüfung (Passcheck).

Ausgabe

Keine.

Verwendungsbeispiel

```
SELECT * FROM pgtle.unregister_feature('pw_hook', 'passcheck');
```

pgtle.unregister_feature_if_exists

Die `unregister_feature`-Funktion bietet eine Möglichkeit, Funktionen zu entfernen, die für die Verwendung von `pg_tle`-Features wurden, wie z. B. Haken. Weitere Informationen finden Sie unter Verwenden von PostgreSQL-Haken mit Ihren TLE-Erweiterungen. Gibt `true` zurück, nachdem die Registrierung der Funktion erfolgreich aufgehoben wurde. Gibt `false` zurück, wenn das Feature nicht registriert wurde.

Informationen zur Registrierung von `pg_tle`-Features für Ihre TLE-Erweiterungen finden Sie unter pgtle.register_feature.

Funktionsprototyp

```
pgtle.unregister_feature_if_exists('proc regproc', 'feature pg_tle_features')
```

Rolle

`pgtle_admin`

Argumente

- `proc` – Der Name der gespeicherten Funktion, für die ein `pg_tle`-Feature registriert wurde.
- `feature` – Der Name des `pg_tle`-Features, das mit der vertrauenswürdigen Spracherweiterung registriert wurde.

Ausgabe

Gibt `true` oder `false` wie folgt zurück.

- `true` – Die Funktion hat die Registrierung des Features in der Erweiterung erfolgreich aufgehoben.
- `false` – Die Funktion konnte die Registrierung des Features in der TLE-Erweiterung nicht aufheben.

Verwendungsbeispiel

```
SELECT * FROM pgtle.unregister_feature_if_exists('pw_hook', 'passcheck');
```

Hakenreferenz für Trusted Language Extensions für PostgreSQL

Trusted Language Extensions für PostgreSQL unterstützt PostgreSQL-Haken. Ein Haken ist ein interner Callback-Mechanismus, der Entwicklern zur Erweiterung der Kernfunktionalität von PostgreSQL zur Verfügung steht. Durch die Verwendung von Haken können Entwickler ihre eigenen Funktionen oder Verfahren zur Verwendung bei verschiedenen Datenbankoperationen implementieren und so das Verhalten von PostgreSQL in gewisser Weise ändern. Sie können beispielsweise einen `passcheck`-Haken verwenden, um anzupassen, wie PostgreSQL die Passwörter behandelt, die beim Erstellen oder Ändern von Passwörtern für Benutzer (Rollen) angegeben werden.

In der folgenden Dokumentation erfahren Sie mehr über die Haken, die für Ihre TLE-Erweiterungen verfügbar sind.

Themen

- Haken zur Passwortüberprüfung (Passcheck)

Haken zur Passwortüberprüfung (Passcheck)

Der `passcheck`-Haken wird verwendet, um das PostgreSQL-Verhalten während der Passwortüberprüfung für die folgenden SQL-Befehle und `psql`-Metabefehle anzupassen.

- `CREATE ROLE username ...PASSWORD` – Weitere Informationen finden Sie im Abschnitt CREATE ROLE der PostgreSQL-Dokumentation.
- `ALTER ROLE username...PASSWORD` – Weitere Informationen finden Sie im Abschnitt ALTER ROLE der PostgreSQL-Dokumentation.
- `\password username` – Dieser interaktive `psql`-Metabefehl ändert das Passwort für den angegebenen Benutzer auf sichere Weise, indem er das Passwort hasht, bevor die `ALTER ROLE ... PASSWORD`-Syntax transparent verwendet wird. Der Metabefehl ist ein sicherer Wrapper für den `ALTER ROLE ... PASSWORD`-Befehl, daher gilt der Haken für das Verhalten des`psql`-Metabefehls.

Ein Beispiel finden Sie unter Liste der Hakencodes für die Passwortüberprüfung.

Funktionsprototyp

```
passcheck_hook(username text, password text, password_type pgtle.password_types,
 valid_until timestamptz, valid_null boolean)
```

Argumente

Eine `passcheck`-Hakenfunktion verwendet die folgenden Argumente.

- `username` – Der Name (als Text) der Rolle (Benutzername), die ein Passwort festlegt.
- `password` – Das Klartext- oder Hash-Passwort. Das eingegebene Passwort sollte dem im `password_type` angegebenen Typ entsprechen.
- `password_type` – Geben Sie das `pgtle.password_type`-Format des Passworts an. Dieses Format kann einer der folgenden Optionen entsprechen.
  - `PASSWORD_TYPE_PLAINTEXT` – Ein Klartext-Passwort.
  - `PASSWORD_TYPE_MD5` – Ein Passwort, das mit dem MD5-Algorithmus (Message Digest 5) gehasht wurde.
  - `PASSWORD_TYPE_SCRAM_SHA_256` – Ein Passwort, das mit dem SCRAM-SHA-256-Algorithmus gehasht wurde.

- `valid_until` – Geben Sie den Zeitpunkt an, am dem das Passwort ungültig wird. Dieses Argument ist optional. Wenn Sie dieses Argument verwenden, geben Sie die Uhrzeit als `timestamptz`-Wert an.
- `valid_null` – Wenn dieser boolesche Wert auf `true` festgelegt ist, wird die `valid_until`-Option auf `NULL` eingestellt.

Konfiguration

Die Funktion `pgtle.enable_password_check` steuert, ob der Passcheck-Haken aktiv ist. Der Passcheck-Haken hat drei mögliche Einstellungen.

- `off` – Schaltet den `passcheck`-Haken für die Passwortüberprüfung aus. Dies ist der Standardwert.
- on – Aktiviert den `passcode`-Haken für die Passwortüberprüfung, sodass Passwörter mit der Tabelle verglichen werden.
- `require` – Erfordert, dass ein Passwortüberprüfungshaken definiert wird.

Nutzungshinweise

Um den `passcheck`-Haken ein- oder auszuschalten, müssen Sie die benutzerdefinierte DB-Parametergruppe für die Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL-DB-Clusters ändern.

Für Linux, macOSoder Unix:

```
aws rds modify-db-parameter-group \
    --region aws-region \
    --db-parameter-group-name your-custom-parameter-group \
    --parameters
 "ParameterName=pgtle.enable_password_check,ParameterValue=on,ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-parameter-group ^
    --region aws-region ^
    --db-parameter-group-name your-custom-parameter-group ^
    --parameters
 "ParameterName=pgtle.enable_password_check,ParameterValue=on,ApplyMethod=immediate"
```

Amazon-Aurora-PostgreSQL-Referenz

Themen

Aurora-PostgreSQL-Kollationen für EBCDIC- und andere Mainframe-Migrationen

Migration von Mainframe-Anwendungen auf neue Plattformen wie AWS bewahrt idealerweise das Anwendungsverhalten. Damit das Anwendungsverhalten auf einer neuen Plattform genauso erhalten bleibt, wie es auf dem Mainframe war, müssen migrierte Daten mit denselben Kollations- und Sortierregeln zusammengetragen werden. Beispielsweise verschieben viele Db2-Migrationslösungen Nullwerte auf u0180 (Unicode-Position 0180), sodass diese Sortierungen zuerst u0180 sortieren. Dies ist ein Beispiel dafür, wie Kollationen von ihrer Mainframe-Quelle abweichen können und warum es notwendig ist, eine Kollation zu wählen, die besser der ursprünglichen EBCDIC-Kollation entspricht.

Aurora PostgreSQL 14.3 und höhere Versionen bieten viele ICU- und EBCDIC-Kollationen, um eine solche Migration nach AWS unter Verwendung der AWS-Mainframe-Modernisierung zu unterstützen. Weitere Informationen zu diesem Service finden Sie unter Was ist AWS Mainframe-Modernisierung?

In der folgenden Tabelle finden Sie von Aurora PostgreSQL bereitgestellte Sortierungen. Diese Sortierungen folgen den EBCDIC-Regeln und stellen sicher, dass Mainframe-Anwendungen auf dieselbe Weise auf AWS funktionieren, wie sie es in der Mainframe-Umgebung getan haben. Der Kollationsname beinhaltet die entsprechende Codepage, (cpnnnn), sodass Sie die passende Sortierung für Ihre Mainframe-Quelle auswählen können. Verwenden Sie z. B. `en-US-cp037-x-icu`, um das Kollationsverhalten für EBCDIC-Daten zu erreichen, die von einer Mainframe-Anwendung stammen, die Codepage 037 verwendete.

EBCDIC-Kollationen	AWS Blue Age	AWS Micro-Focus-Kollationen
da-DK-cp1142-x-icu	da-DK-cp1142b-x-icu	da-DK-cp1142m-x-icu
da-DK-cp277-x-icu	da-DK-cp277b-x-icu	–
de-DE-cp1141-x-icu	de-DE-cp1141b-x-icu	de-DE-cp1141m-x-icu
de-DE-cp273-x-icu	de-DE-cp273b-x-icu	–
en-GB-cp1146-x-icu	en-GB-cp1146b-x-icu	en-GB-cp1146m-x-icu
en-GB-cp285-x-icu	en-GB-cp285b-x-icu	–
en-US-cp037-x-icu	en-US-cp037b-x-icu	–
en-US-cp1140-x-icu	en-US-cp1140b-x-icu	en-US-cp1140m-x-icu
es-ES-cp1145-x-icu	es-ES-cp1145b-x-icu	es-ES-cp1145m-x-icu
es-ES-cp284-x-icu	es-ES-cp284b-x-icu	–
fi-FI-cp1143-x-icu	fi-FI-cp1143b-x-icu	fi-FI-cp1143m-x-icu
fi-FI-cp278-x-icu	fi-FI-cp278b-x-icu	–
fr-FR-cp1147-x-icu	fr-FR-cp1147b-x-icu	fr-FR-cp1147m-x-icu
fr-FR-cp297-x-icu	fr-FR-cp297b-x-icu	–
it-IT-cp1144-x-icu	it-IT-cp1144b-x-icu	it-IT-cp1144m-x-icu
it-IT-cp280-x-icu	it-IT-cp280b-x-icu	–
nl-BE-cp1148-x-icu	nl-BE-cp1148b-x-icu	nl-BE-cp1148m-x-icu
nl-BE-cp500-x-icu	nl-BE-cp500b-x-icu	–

Weitere Informationen über AWS Blu Age finden Sie im Tutorial: Verwaltete Runtime für AWS Blu Age im AWSMainframe-Modernisierung-Benutzerhandbuch.

Weitere Informationen zur Arbeit mit AWS Mikrofokus finden Sie im Tutorial: Verwaltete Runtime für Micro Focus im AWS-Mainframe-Modernisierung-Benutzerhandbuch.

Weitere Informationen zu PostgreSQL und Kollationen finden Sie unter Support für Kollationen in der PostgreSQL-Dokumentation.

In Aurora PostgreSQL unterstützte Sortierungen

Sortierungen sind eine Reihe von Regeln, die bestimmen, wie in der Datenbank gespeicherte Zeichenfolgen sortiert und verglichen werden. Sortierungen spielen eine grundlegende Rolle im Computersystem und sind Teil des Betriebssystems. Sortierungen ändern sich im Laufe der Zeit, wenn neue Zeichen zu Sprachen hinzugefügt werden oder wenn sich die Sortierregeln ändern.

Sortierungsbibliotheken definieren spezifische Regeln und Algorithmen für eine Sortierung. Die beliebtesten Sortierungsbibliotheken, die in PostgreSQL verwendet werden, sind GNU C (glibc) und Internationalization Components for Unicode (ICU). Standardmäßig verwendet Aurora PostgreSQL die Glibc-Sortierung, die Unicode-Zeichensortierreihenfolgen für Multibyte-Zeichensequenzen enthält.

Wenn Sie einen neuen DB-Cluster von Aurora PostgreSQL erstellen, wird das Betriebssystem auf die verfügbare Sortierung überprüft. Die PostgreSQL-Parameter des `CREATE DATABASE`-Befehls `LC_COLLATE` und `LC_CTYPE` werden verwendet, um eine Sortierung anzugeben, die in dieser Datenbank als Standardsortierung gilt. Alternativ können Sie auch den Parameter `LOCALE` in `CREATE DATABASE` verwenden, um diese Parameter festzulegen. Dieser bestimmt die Standardsortierung für Zeichenfolgen in der Datenbank und die Regeln für die Klassifizierung von Zeichen als Buchstaben, Zahlen oder Symbole. Sie können auch eine Sortierung auswählen, die für eine Spalte, einen Index oder eine Abfrage verwendet werden soll.

Aurora PostgreSQL benötigt für die Sortierungsunterstützung die Glibc-Bibliothek im Betriebssystem. Die Instance von Aurora PostgreSQL wird regelmäßig mit den neuesten Versionen des Betriebssystems aktualisiert. Diese Updates umfassen manchmal eine neuere Version der Glibc-Bibliothek. In seltenen Fällen ändern neuere Versionen von Glibc die Sortierreihenfolge oder Sortierung einiger Zeichen, was dazu führen kann, dass die Daten anders sortiert werden oder ungültige Indexeinträge entstehen. Wenn Sie während eines Updates bei der Sortierung Probleme mit der Sortierreihenfolge feststellen, müssen Sie möglicherweise die Indizes neu erstellen.

Damit mögliche Auswirkungen der Glibc-Updates reduziert werden, enthält Aurora PostgreSQL jetzt eine unabhängige Standard-Sortierungsbibliothek. Diese Sortierungsbibliothek ist in Aurora PostgreSQL 14.6, 13.9, 12.13, 11.18 und neueren Nebenversionen verfügbar. Sie ist mit Glibc

2.26-59.amzn2 kompatibel und bietet eine stabile Sortierreihenfolge, um falsche Abfrageergebnisse zu verhindern.

Aurora-PostgreSQL-Funktionsreferenz

Nachfolgend finden Sie eine Liste der Aurora PostgreSQL-Funktionen, die für Ihre Aurora-DB-Cluster verfügbar sind, welche die Aurora PostgreSQL-kompatible Edition-DB-Engine ausführen. Diese Aurora PostgreSQL-Funktionen sind zusätzlich zu den Standard-PostgreSQL-Funktionen. Weitere Informationen zu PostgreSQL-Standardfunktionen finden Sie unter PostgreSQL – Funktionen und Operatoren.

Übersicht

Sie können die folgenden Funktionen für Amazon-RDS-DB-Instances verwenden, auf denen Aurora PostgreSQL ausgeführt wird:

- aurora_db_instance_identifier
- aurora_ccm_status
- aurora_global_db_instance_status
- aurora_global_db_status
- aurora_list_builtins
- aurora_replica_status
- aurora_stat_activity
- aurora_stat_backend_waits
- aurora_stat_bgwriter
- aurora_stat_database
- aurora_stat_dml_activity
- aurora_stat_get_db_commit_latency
- aurora_stat_logical_wal_cache
- aurora_stat_memctx_usage
- aurora_stat_optimized_reads_cache
- aurora_stat_plans
- aurora_stat_reset_wal_cache
- aurora_stat_statements

- aurora_stat_system_waits
- aurora_stat_wait_event
- aurora_stat_wait_type
- aurora_version
- aurora_volume_logical_start_lsn
- aurora_wait_report

aurora_db_instance_identifier

Meldet den Namen der DB-Instance, mit der Sie verbunden sind.

Syntax

```
aurora_db_instance_identifier()
```

Argumente

Keine

Rückgabetyp

VARCHAR-Zeichenfolge

Nutzungshinweise

Diese Funktion zeigt den Namen der DB-Instance des Aurora-PostgreSQL-kompatiblen Edition-Clusters für Ihre Datenbank-Client- oder Anwendungsverbindung an.

Diese Funktion ist ab der Veröffentlichung der PostgreSQL-Versionen 13.7, 12.11, 11.16 und 10.21 und für alle späteren Versionen verfügbar.

Beispiele

Im folgenden Beispiel sehen Sie die Ergebnisse vom Aufruf der Funktion `aurora_db_instance_identifier`.

```
=> SELECT aurora_db_instance_identifier();
```

```
aurora_db_instance_identifier
------------------------------
 test-my-instance-name
```

Sie können die Ergebnisse dieser Funktion mit der `aurora_replica_status`-Funktion verbinden, um Details über die DB-Instance für Ihre Verbindung abzurufen. Die aurora_replica_status allein zeigt Ihnen nicht, welche DB-Instance Sie verwenden. Im folgenden Beispiel wird gezeigt, wie Sie dies tun.

```
=> SELECT *
    FROM aurora_replica_status() rt,
         aurora_db_instance_identifier() di
    WHERE rt.server_id = di;
-[ RECORD 1 ]----------------------+----------------------
server_id                         | test-my-instance-name
session_id                        | MASTER_SESSION_ID
durable_lsn                       | 88492069
highest_lsn_rcvd                  |
current_read_lsn                  |
cur_replay_latency_in_usec        |
active_txns                       |
is_current                        | t
last_transport_error              | 0
last_error_timestamp              |
last_update_timestamp             | 2022-06-03 11:18:25+00
feedback_xmin                     |
feedback_epoch                    |
replica_lag_in_msec               |
log_stream_speed_in_kib_per_second | 0
log_buffer_sequence_number        | 0
oldest_read_view_trx_id           |
oldest_read_view_lsn              |
pending_read_ios                  | 819
```

aurora_ccm_status

Zeigt den Status des Cluster-Cache-Managers an.

Syntax

```
aurora_ccm_status()
```

Argumente

Keine.

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- `buffers_sent_last_minute` – Die Anzahl der Puffer, die in der letzten Minute an den designierten Reader gesendet wurden.
- `buffers_found_last_minute` – Die Anzahl der Puffer, auf die in der letzten Minute häufig zugegriffen wurde.
- `buffers_sent_last_scan` – Die Anzahl der Puffer, die während des letzten vollständigen Scanvorgangs des Puffercaches an den designierten Reader gesendet wurden.
- `buffers_found_last_scan` – Die Anzahl der Puffer, auf die während des letzten vollständigen Scanvorgangs des Puffercaches häufig zugegriffen wurde. Puffer, die bereits im Cache des designierten Readers abgelegt wurden, werden nicht gesendet.
- `buffers_sent_current_scan` – Die Anzahl der Puffer, die während des aktuellen Scanvorgangs gesendet wurden.
- `buffers_found_current_scan` – Die Anzahl der häufig aufgerufenen Puffer, die im aktuellen Scan identifiziert wurden.
- `current_scan_progress` – Die Anzahl der Puffer, die während des aktuellen Scanvorgangs aufgerufen wurden.

Nutzungshinweise

Sie können diese Funktion verwenden, um die Funktion zur Cluster-Cache-Verwaltung (CCM) zu überprüfen und zu überwachen. Diese Funktion ist nur verfügbar, wenn CCM auf Ihrem Aurora-PostgreSQL-DB-Cluster aktiv ist. Zum Verwenden dieser Funktion stellen Sie eine Verbindung mit der Write-DB-Instance Ihres Aurora-PostgreSQL-DB-Clusters her.

Sie aktivieren CCM für einen Aurora-PostgreSQL-DB-Cluster, indem Sie den Wert `apg_ccm_enabled` in der benutzerdefinierten DB-Cluster-Parametergruppe des Clusters auf 1 festlegen. Um zu erfahren wie dies geht, vgl. Konfigurieren der Cluster-Cache-Verwaltung.

Die Cluster-Cache-Verwaltung ist auf einem Aurora-PostgreSQL-DB-Cluster aktiv, wenn der Cluster über eine Aurora-Reader-Instance verfügt, die wie folgt konfiguriert ist:

- Die Aurora-Reader-Instance verwendet den gleichen Typ und die gleiche Größe der DB-Instance-Klasse wie die Writer-Instance des Clusters.
- Die Aurora-Reader-Instance ist für den Cluster als Tier-0 konfiguriert. Wenn der Cluster über mehr als einen Reader verfügt, ist dies der einzige Tier-0-Reader.

Wenn Sie mehr als einen Reader auf Tier-0 einstellen, wird CCM deaktiviert. Wenn CCM deaktiviert ist, wird beim Aufruf dieser Funktion die folgende Fehlermeldung zurückgegeben:

```
ERROR: Cluster Cache Manager is disabled
```

Sie können auch die PostgreSQL-Erweiterung pg_buffercache verwenden, um den Puffercache zu analysieren. Weitere Informationen finden Sie unter pg_buffercache in der PostgreSQL-Dokumentation.

Weitere Informationen finden Sie unter Einführung in die Aurora-PostgreSQL-Cluster-Cache-Verwaltung.

Beispiele

Im folgenden Beispiel sehen Sie die Ergebnisse vom Aufruf der Funktion `aurora_ccm_status`. Dieses erste Beispiel zeigt CCM-Statistiken.

```
=> SELECT * FROM aurora_ccm_status();
 buffers_sent_last_minute | buffers_found_last_minute | buffers_sent_last_scan |
 buffers_found_last_scan | buffers_sent_current_scan | buffers_found_current_scan |
 current_scan_progress
--------------------------+---------------------------+------------------------
+-------------------------+---------------------------+---------------------------
+------------------------
                  2242000 |                   2242003 |               17920442 |
         17923410 |                  14098000 |                   14100964 |
   15877443
```

Für ausführlichere Details können Sie die erweiterte Anzeige verwenden, wie im Folgenden gezeigt:

```
\x
Expanded display is on.
SELECT *  FROM aurora_ccm_status();
[ RECORD 1 ]----------------------+---------
buffers_sent_last_minute          | 2242000
```

```
buffers_found_last_minute          | 2242003
buffers_sent_last_scan             | 17920442
buffers_found_last_scan            | 17923410
buffers_sent_current_scan          | 14098000
buffers_found_current_scan         | 14100964
current_scan_progress              | 15877443
```

Dieses Beispiel zeigt, wie die aktive Rate und der aktive Prozentsatz überprüft werden.

```
=> SELECT buffers_sent_last_minute * 8/60 AS warm_rate_kbps,
100 * (1.0-buffers_sent_last_scan/buffers_found_last_scan) AS warm_percent
FROM aurora_ccm_status ();
 warm_rate_kbps | warm_percent
----------------+--------------
 16523 |        100.0
```

aurora_global_db_instance_status

Zeigt den Status aller Aurora-Instances an, einschließlich Replikaten in einem globalen Aurora-DB-Cluster.

Syntax

```
aurora_global_db_instance_status()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- `server_id` – Die ID der DB-Instance.
- `session_id` – Eindeutiger Bezeichner für die aktuelle Sitzung. Der Wert `MASTER_SESSION_ID` bezeichnet die (primäre) Writer-DB-Instance.
- `aws_region` – Die AWS-Region, in der diese globale DB-Instance ausgeführt wird. Eine Liste der Regionen finden Sie unter Verfügbarkeit in Regionen.
- `durable_lsn` – Die Log-Sequenznummer (LSN), die dauerhaft gespeichert wurde. Eine Log-Sequenznummer (LSN) ist eine eindeutige fortlaufende Nummer, die einen Datensatz im

Datenbank-Transaktionsprotokoll identifiziert. LSNs werden so angeordnet, dass eine größere LSN eine spätere Transaktion darstellt.

- `highest_lsn_rcvd` – Die höchste LSN, die die DB-Instance von der Writer-DB-Instance empfangen hat.
- `feedback_epoch` – Die Epoche, die die DB-Instance beim Erzeugen der Hot-Standby-Informationen verwendet. Ein Hot Standby ist eine DB-Instance, die Verbindungen und Abfragen unterstützt, während sich die primäre DB im Wiederherstellungs- oder Standby-Modus befindet. Die Hot-Standby-Informationen umfassen die Epoche (bestimmter Zeitpunkt) und andere Details über die DB-Instance, die als Hot-Standby verwendet wird. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation zu Hot Standby.
- `feedback_xmin` – Die minimale (älteste) aktive Transaktions-ID, die von der DB-Instance verwendet wird.
- `oldest_read_view_lsn` – Die älteste LSN, die von der DB-Instance zum Lesen aus dem Speicher verwendet wird.
- `visibility_lag_in_msec` – Gibt an (in Millisekunden), wie weit die DB-Instance hinter der Writer-DB-Instance zurückgeblieben ist.

Nutzungshinweise

Diese Funktion gibt Aufschluss über Replikationsstatistiken für einen Aurora-DB-Cluster. Für jede Aurora-PostgreSQL-DB-Instance im Cluster zeigt die Funktion eine Datenreihe an, die regionsübergreifende Replikate in einer globalen Datenbankkonfiguration enthält.

Sie können diese Funktion von jeder Instance in einem Aurora-PostgreSQL-DB-Cluster oder einer globalen Aurora-PostgreSQL-Datenbank ausführen. Die Funktion gibt Details zur Verzögerung für alle Replikat-Instances zurück.

Weitere Informationen über die Überwachung der Verzögerung mithilfe dieser Funktion (`aurora_global_db_instance_status`) oder mit `aurora_global_db_status` finden Sie unter Überwachen von Aurora-PostgreSQL-basierten globalen Datenbanken.

Informationen über globale Aurora-Datenbanken finden Sie unter Übersicht über Amazon Aurora Global Databases.

Informationen zu den ersten Schritten mit globalen Aurora-Datenbanken finden Sie unter Erste Schritte mit globalen Amazon-Aurora-Datenbanken oder Häufig gestellte Fragen zu Amazon Aurora.

Beispiele

Dieses Beispiel zeigt regionsübergreifende Instance-Statistiken.

```
=> SELECT *
  FROM aurora_global_db_instance_status();
               server_id                |              session_id              |
  aws_region  | durable_lsn | highest_lsn_rcvd | feedback_epoch | feedback_xmin |
 oldest_read_view_lsn | visibility_lag_in_msec
----------------------------------------+--------------------------------------
+-------------+-------------+------------------+----------------+---------------
+----------------------+------------------------
 db-119-001-instance-01                  | MASTER_SESSION_ID                    | eu-
west-1    |  2534560273 |           [NULL] |         [NULL] |        [NULL] |
     [NULL] |                [NULL]
 db-119-001-instance-02                  | 4ecff34d-d57c-409c-ba28-278b31d6fc40 | eu-
west-1    |  2534560266 |       2534560273 |              0 |      19669196 |
 2534560266 |                    6
 db-119-001-instance-03                  | 3e8a20fc-be86-43d5-95e5-bdf19d27ad6b | eu-
west-1    |  2534560266 |       2534560273 |              0 |      19669196 |
 2534560266 |                    6
 db-119-001-instance-04                  | fc1b0023-e8b4-4361-bede-2a7e926cead6 | eu-
west-1    |  2534560266 |       2534560273 |              0 |      19669196 |
 2534560254 |                   23
 db-119-001-instance-05                  | 30319b74-3f08-4e13-9728-e02aa1aa8649 | eu-
west-1    |  2534560266 |       2534560273 |              0 |      19669196 |
 2534560254 |                   23
 db-119-001-global-instance-1            | a331ffbb-d982-49ba-8973-527c96329c60 | eu-
central-1 |  2534560254 |       2534560266 |              0 |      19669196 |
 2534560247 |                  996
 db-119-001-global-instance-1            | e0955367-7082-43c4-b4db-70674064a9da | eu-
west-2    |  2534560254 |       2534560266 |              0 |      19669196 |
 2534560247 |                   14
 db-119-001-global-instance-1-eu-west-2a  | 1248dc12-d3a4-46f5-a9e2-85850491a897 | eu-
west-2    |  2534560254 |       2534560266 |              0 |      19669196 |
 2534560247 |                    0
```

Dieses Beispiel veranschaulicht, wie die globale Replikatverzögerung in Millisekunden überprüft wird.

```
=> SELECT CASE
          WHEN 'MASTER_SESSION_ID' = session_id THEN 'Primary'
         ELSE 'Secondary'
      END AS global_role,
```

```
      aws_region,
      server_id,
      visibility_lag_in_msec
  FROM aurora_global_db_instance_status()
  ORDER BY 1, 2, 3;
   global_role |  aws_region  |               server_id                |
 visibility_lag_in_msec
-------------+--------------+----------------------------------------
+------------------------
 Primary     | eu-west-1    | db-119-001-instance-01                 |
 [NULL]
 Secondary   | eu-central-1 | db-119-001-global-instance-1           |
     13
 Secondary   | eu-west-1    | db-119-001-instance-02                 |
     10
 Secondary   | eu-west-1    | db-119-001-instance-03                 |
      9
 Secondary   | eu-west-1    | db-119-001-instance-04                 |
      2
 Secondary   | eu-west-1    | db-119-001-instance-05                 |
     18
 Secondary   | eu-west-2    | db-119-001-global-instance-1           |
     14
 Secondary   | eu-west-2    | db-119-001-global-instance-1-eu-west-2a |
     13
```

Dieses Beispiel zeigt, wie die minimale, maximale und durchschnittliche Verzögerung je AWS-Region im Hinblick auf die globale Datenbankkonfiguration überprüft wird.

```
=> SELECT 'Secondary' global_role,
       aws_region,
       min(visibility_lag_in_msec) min_lag_in_msec,
       max(visibility_lag_in_msec) max_lag_in_msec,
       round(avg(visibility_lag_in_msec),0) avg_lag_in_msec
  FROM aurora_global_db_instance_status()
 WHERE aws_region NOT IN (SELECT   aws_region
                            FROM aurora_global_db_instance_status()
                           WHERE session_id='MASTER_SESSION_ID')
                        GROUP BY aws_region
UNION ALL
SELECT  'Primary' global_role,
        aws_region,
        NULL,
```

```
        NULL,
        NULL
    FROM aurora_global_db_instance_status()
   WHERE session_id='MASTER_SESSION_ID'
ORDER BY 1, 5;
 global_role |  aws_region  | min_lag_in_msec | max_lag_in_msec | avg_lag_in_msec
-------------+--------------+-----------------+-----------------+-----------------
 Primary     | eu-west-1    |          [NULL] |          [NULL] |          [NULL]
 Secondary   | eu-central-1 |             133 |             133 |             133
 Secondary   | eu-west-2    |               0 |             495 |             248
```

aurora_global_db_status

Zeigt Informationen über verschiedene Aspekte der globalen Aurora-Datenbankverzögerung an, insbesondere die Verzögerung des zugrunde liegenden Aurora-Speichers (sogenannte Haltbarkeitsverzögerung) und die Verzögerung zwischen dem Recovery Point Objective (RPO).

Syntax

```
aurora_global_db_status()
```

Argumente

Keine.

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- `aws_region` – Die AWS-Region, in der sich dieser DB-Cluster befindet. Eine vollständige Auflistung von AWS-Regionen nach Engine finden Sie unter Regionen und Availability Zones.
- `highest_lsn_written` – Die höchste Log-Sequenznummer (LSN), die derzeit auf diesem DB-Cluster vorhanden ist. Eine Log-Sequenznummer (LSN) ist eine eindeutige fortlaufende Nummer, die einen Datensatz im Datenbank-Transaktionsprotokoll identifiziert. LSNs werden so angeordnet, dass eine größere LSN eine spätere Transaktion darstellt.
- `durability_lag_in_msec` – Die Differenz zwischen den Zeitstempelwerten der `highest_lsn_written` auf einem sekundären DB-Cluster und der `highest_lsn_written` auf dem primären DB-Cluster. Der Wert -1 identifiziert den primären DB-Cluster der globalen Aurora-Datenbank.

- `rpo_lag_in_msec` – Die RPO-Verzögerung (Recovery Point Objective). Die RPO-Verzögerung ist die Zeit, die benötigt wird, bis die letzte Benutzertransaktion COMMIT auf einem sekundären DB-Cluster gespeichert wird, nachdem sie auf dem primären DB-Cluster einer globalen Aurora-Datenbank abgelegt wurde. Der Wert -1 bezeichnet den primären DB-Cluster (die Verzögerung ist daher nicht relevant).

  Einfach ausgedrückt berechnet diese Metrik das Recovery Point Objective für jeden Aurora-PostgreSQL-DB-Cluster in der globalen Aurora-Datenbank, d. h., wie viele Daten bei einem Ausfall verloren gehen könnten. Wie die Verzögerung wird auch RPO zeitlich gemessen.
- `last_lag_calculation_time` – Der Zeitstempel, der angibt, wann die Werte für `durability_lag_in_msec` und `rpo_lag_in_msec` zuletzt berechnet wurden. Ein Zeitwert wie `1970-01-01 00:00:00+00` bedeutet, dass dies der primäre DB-Cluster ist.
- `feedback_epoch` – Die Epoche, die der sekundäre DB-Cluster beim Erzeugen von Hot-Standby-Informationen verwendet. Ein Hot Standby ist eine DB-Instance, die Verbindungen und Abfragen unterstützt, während sich die primäre DB im Wiederherstellungs- oder Standby-Modus befindet. Die Hot-Standby-Informationen umfassen die Epoche (bestimmter Zeitpunkt) und andere Details über die DB-Instance, die als Hot-Standby verwendet wird. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation zu Hot Standby.
- `feedback_xmin` – Die minimale (älteste) aktive Transaktions-ID, die von einem sekundären DB-Cluster verwendet wird.

Nutzungshinweise

Diese Funktion zeigt Replikationsstatistiken für eine globale Aurora-Datenbank. Sie zeigt eine Zeile für jeden DB-Cluster in einer globalen Aurora-PostgreSQL-Datenbank. Sie können diese Funktion von jeder Instance in Ihrer globalen Aurora-PostgreSQL-Datenbank ausführen.

Informationen zur Auswertung der Replikationsverzögerung der globalen Aurora-Datenbank, die die sichtbare Datenverzögerung darstellt, finden Sie unter aurora_global_db_instance_status.

Weitere Informationen über die Verwendung von `aurora_global_db_status` und `aurora_global_db_instance_status` zur Überwachung der globalen Aurora-Datenbankverzögerung finden Sie unter Überwachen von Aurora-PostgreSQL-basierten globalen Datenbanken. Informationen über globale Aurora-Datenbanken finden Sie unter Übersicht über Amazon Aurora Global Databases.

Beispiele

Dieses Beispiel zeigt, wie regionsübergreifende Speicherstatistiken angezeigt werden.

```
=> SELECT CASE
          WHEN '-1' = durability_lag_in_msec THEN 'Primary'
          ELSE 'Secondary'
       END AS global_role,
       *
  FROM aurora_global_db_status();
 global_role | aws_region | highest_lsn_written | durability_lag_in_msec |
 rpo_lag_in_msec | last_lag_calculation_time  | feedback_epoch | feedback_xmin
-------------+------------+---------------------+------------------------
+-----------------+----------------------------+----------------+--------------
 Primary     | eu-west-1  |           131031557 |                     -1 |
 -1 | 1970-01-01 00:00:00+00     |             0 |             0
 Secondary   | eu-west-2  |           131031554 |                    410 |
  0 | 2021-06-01 18:59:36.124+00 |             0 |         12640
 Secondary   | eu-west-3  |           131031554 |                    410 |
  0 | 2021-06-01 18:59:36.124+00 |             0 |         12640
```

aurora_list_builtins

Listet alle verfügbaren integrierten Aurora-PostgreSQL-Funktionen mit kurzen Beschreibungen und Funktionsdetails auf.

Syntax

```
aurora_list_builtins()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz

Beispiele

Im folgenden Beispiel sehen Sie Ergebnisse vom Aufruf der Funktion `aurora_list_builtins`.

```
=> SELECT *
```

```
FROM aurora_list_builtins();

               Name                | Result data type |                    Argument data
 types                     | Type | Volatility |  Parallel  | Security |
             Description
-----------------------------------+-----------------
+-------------------------------------------------------------+------+------------
+------------+----------
+-------------------------------------------------------------------------
 aurora_version                    | text             |
                           | func | stable     | safe       | invoker  | Amazon Aurora
 PostgreSQL-Compatible Edition version string
 aurora_stat_wait_type             | SETOF record     | OUT type_id smallint, OUT
 type_name text                 | func | volatile   | restricted | invoker  | Lists all
 supported wait types
 aurora_stat_wait_event            | SETOF record     | OUT type_id smallint, OUT
 event_id integer, OUT event_na.| func | volatile   | restricted | invoker  | Lists all
 supported wait events
                                   |                  |.me text
                          |      |            |            |          |
 aurora_list_builtins              | SETOF record     | OUT "Name" text, OUT "Result
 data type" text, OUT "Argum.| func | stable     | safe       | invoker  | Lists all
 Aurora built-in functions
                                   |                  |.ent data types" text, OUT
 "Type" text, OUT "Volatility" .|      |            |            |          |
                                   |                  |.text, OUT "Parallel" text, OUT
 "Security" text, OUT "Des.|      |            |            |          |
                                   |                  |.cription" text
                          |      |            |            |          |
 .
 .
 .
 aurora_stat_file                  | SETOF record     | OUT filename text, OUT
 allocated_bytes bigint, OUT used_.| func | stable     | safe       | invoker  | Lists
 all files present in Aurora storage
                                   |                  |.bytes bigint
                          |      |            |            |          |
 aurora_stat_get_db_commit_latency | bigint           | oid
                           | func | stable     | restricted | invoker  | Per DB commit
 latency in microsecs
```

aurora_replica_status

Zeigt den Status aller Aurora-PostgreSQL-Reader-Knoten an.

Syntax

```
aurora_replica_status()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- `server_id` – Die DB-Instance-ID (Kennung).
- `session_id` – Eine eindeutige ID für die aktuelle Sitzung, die wie folgt für die primäre Instance und Reader-Instances zurückgegeben wird:
  - Für die primäre Instance ist `session_id` immer `` `MASTER_SESSION_ID' ``.
  - Für Reader-Instances ist `session_id` immer die `UUID` (Universally Unique Identifier, eindeutige Kennung) der Reader-Instance.
- `durable_lsn` – Die Log-Sequenznummer (LSN), die im Speicher abgelegt wurde.
  - Für das primäre Volume die dauerhafte LSN des primären Volumes (VDL), die derzeit in Kraft ist.
  - Für alle sekundären Volumes die VDL des primären Volumes, auf das das sekundäre Volume erfolgreich angewendet wurde.

  > **Note**
  >
  > Eine Log-Sequenznummer (LSN) ist eine eindeutige fortlaufende Nummer, die einen Datensatz im Datenbank-Transaktionsprotokoll identifiziert. LSNs werden so angeordnet, dass eine größere LSN eine Transaktion darstellt, die später in der Sequenz auftritt.

- `highest_lsn_rcvd` – Die höchste (neueste) LSN, die die DB-Instance von der Writer-DB-Instance empfangen hat.
- `current_read_lsn` – Die LSN des letzten Snapshots, die auf alle Reader angewendet wurde.
- `cur_replay_latency_in_usec` – Die Anzahl der Mikrosekunden, die voraussichtlich benötigt werden, um das Protokoll auf der sekundären Instance wiederzugeben.

- `active_txns` – Die Anzahl der derzeit aktiven Transaktionen.
- `is_current` – Nicht verwendet.
- `last_transport_error` – Fehlercode für die letzte Replikation.
- `last_error_timestamp` – Zeitstempel des letzten Replikationsfehlers.
- `last_update_timestamp` – Zeitstempel der letzten Aktualisierung auf den Replikatstatus. Ab Aurora PostgreSQL 13.9 ist der `last_update_timestamp`-Wert für die DB-Instance, mit der Sie verbunden sind, auf `NULL` festgelegt.
- `feedback_xmin` – Der Hot Standby feedback_xmin des Replikats. Die minimale (älteste) aktive Transaktions-ID, die von der DB-Instance verwendet wird.
- `feedback_epoch` – Die Epoche, die die DB-Instance beim Erzeugen der Hot-Standby-Informationen verwendet.
- `replica_lag_in_msec` – Zeit, die die Reader-Instance in Millisekunden hinter der Writer-Instance zurückbleibt.
- `log_stream_speed_in_kib_per_second` – Der Durchsatz des Protokollstreams in Kilobyte pro Sekunde.
- `log_buffer_sequence_number` – Die Sequenznummer des Protokollpuffers.
- `oldest_read_view_trx_id` – Nicht verwendet.
- `oldest_read_view_lsn` – Die älteste LSN, die von der DB-Instance zum Lesen aus dem Speicher verwendet wird.
- `pending_read_ios` – Die ausstehenden Seiten-Lesevorgänge, die noch im Replikat anstehen.
- `read_ios` – Die Gesamtzahl der Lesevorgänge auf dem Replikat.
- `iops` – Nicht verwendet.
- `cpu` – Die CPU-Auslastung durch den Replikatprozess. Beachten Sie, dass dies nicht die CPU-Auslastung durch die Instance, sondern durch den Prozess ist. Weitere Informationen zur CPU-Auslastung durch die Instance finden Sie unter Metriken auf Instance-Ebene für Amazon Aurora.

Nutzungshinweise

Die Funktion `aurora_replica_status` gibt Werte aus dem Replikatstatus-Manager eines Aurora-PostgreSQL-DB-Clusters zurück. Sie können diese Funktion verwenden, um Informationen über den Status der Replikation auf Ihrem Aurora-PostgreSQL-DB-Cluster zu erhalten, einschließlich Metriken für alle DB-Instances in Ihrem Aurora-DB-Cluster. Sie können z. B. Folgendes tun:

- Informationen über die Art der Instance (Writer, Reader) im Aurora-PostgreSQL-DB-Cluster abrufen – Diese Informationen erhalten Sie, indem Sie sich die Werte der folgenden Spalten ansehen:
  - `server_id` – Enthält den Namen der Instance, die Sie beim Erstellen der Instance festgelegt haben. In einigen Fällen, z. B. für die primäre (Writer-)Instance, wird der Name normalerweise durch Anhängen von -instance-1 an den Namen, den Sie für Ihren Aurora-PostgreSQL-DB-Cluster festlegen, für Sie erstellt.
  - `session_id` – Das Feld `session_id` gibt an, ob es sich bei der Instance um einen Reader oder einen Writer handelt. Für eine Writer-Instance ist `session_id` immer auf `"MASTER_SESSION_ID"` festgelegt. Für eine Reader-Instance ist `session_id` auf die `UUID` des spezifischen Readers festgelegt.
- Häufige Replikationsprobleme wie Replikatverzögerung, diagnostizieren – Replikatverzögerung ist die Zeit in Millisekunden, die der Seiten-Cache einer Reader-Instance hinter dem Cache der Writer-Instance zurückbleibt. Diese Verzögerung tritt auf, weil Aurora-Cluster eine asynchrone Replikation verwenden, wie unter Replikation mit Amazon Aurorabeschrieben. Diese ist in der Spalte `replica_lag_in_msec` in den von dieser Funktion zurückgegebenen Ergebnissen zu sehen. Verzögerungen können auch auftreten, wenn eine Abfrage aufgrund von Konflikten mit der Wiederherstellung auf einem Standby-Server abgebrochen wird. Unter `pg_stat_database_conflicts()` können Sie nachsehen, ob ein solcher Konflikt die Replikatverzögerung verursacht (oder nicht). Weitere Informationen finden Sie unter Die Statistikerfassung in der PostgreSQL-Dokumentation. Weitere Informationen zu Hochverfügbarkeit und Replikation finden Sie unter Häufig gestellte Fragen zu Amazon Aurora.

  Amazon CloudWatch speichert `replica_lag_in_msec`-Ergebnisse im Laufe der Zeit als `AuroraReplicaLag`-Metrik. Weitere Informationen zur Verwendung der CloudWatch-Metriken für Aurora finden Sie unter Überwachen von Amazon Aurora-Metriken mit Amazon CloudWatch.

Weitere Informationen zur Fehlerbehebung bei Aurora-Lesereplikaten und Neustarts finden Sie unter Warum ist mein Amazon-Aurora-Lesereplikat in den Rückstand geraten und wurde neu gestartet? im AWS Support Center.

Beispiele

Im folgenden Beispiel wird veranschaulicht, wie Sie den Replikationsstatus aller Instances in einem Aurora-PostgreSQL-DB-Cluster abrufen:

```
=> SELECT *
```

```
FROM aurora_replica_status();
```

Das folgende Beispiel zeigt die Writer-Instance im Aurora-PostgreSQL-DB-Cluster `docs-lab-apg-main`:

```
=> SELECT server_id,
    CASE
        WHEN 'MASTER_SESSION_ID' = session_id THEN 'writer'
        ELSE 'reader'
    END AS instance_role
FROM aurora_replica_status()
WHERE session_id = 'MASTER_SESSION_ID';
        server_id       | instance_role
------------------------+---------------
 db-119-001-instance-01 | writer
```

Im folgenden Beispiel werden alle Reader-Instances in einem Cluster aufgeführt:

```
=> SELECT server_id,
    CASE
        WHEN 'MASTER_SESSION_ID' = session_id THEN 'writer'
        ELSE 'reader'
    END AS instance_role
FROM aurora_replica_status()
WHERE session_id <> 'MASTER_SESSION_ID';
        server_id       | instance_role
------------------------+---------------
db-119-001-instance-02  | reader
db-119-001-instance-03  | reader
db-119-001-instance-04  | reader
db-119-001-instance-05  | reader
(4 rows)
```

Im folgenden Beispiel werden alle Instances aufgeführt und es wird angegeben, wie weit jede Instance hinter dem Writer zurückbleibt und wie lange seit dem letzten Update:

```
=> SELECT server_id,
    CASE
        WHEN 'MASTER_SESSION_ID' = session_id THEN 'writer'
        ELSE 'reader'
    END AS instance_role,
    replica_lag_in_msec AS replica_lag_ms,
```

```
    round(extract (epoch FROM (SELECT age(clock_timestamp(), last_update_timestamp))) *
 1000) AS last_update_age_ms
FROM aurora_replica_status()
ORDER BY replica_lag_in_msec NULLS FIRST;
       server_id        | instance_role | replica_lag_ms | last_update_age_ms
------------------------+---------------+----------------+--------------------
 db-124-001-instance-03 | writer        |         [NULL] |               1756
 db-124-001-instance-01 | reader        |             13 |               1756
 db-124-001-instance-02 | reader        |             13 |               1756
(3 rows)
```

aurora_stat_activity

Gibt eine Zeile pro Serverprozess zurück, in der Informationen zur aktuellen Aktivität dieses Prozesses angezeigt werden.

Syntax

```
aurora_stat_activity();
```

Argumente

None

Rückgabetyp

Gibt eine Zeile pro Serverprozess zurück. Zusätzlich zu den `pg_stat_activity` Spalten wird das folgende Feld hinzugefügt:

- planid — Plan-ID

Nutzungshinweise

Eine zusätzliche Ansicht zur `pg_stat_activity` Rückgabe derselben Spalten mit einer zusätzlichen `plan_id` Spalte, die den aktuellen Abfrageausführungsplan zeigt.

`aurora_compute_plan_id`muss aktiviert sein, damit die Ansicht eine plan_id zurückgibt.

Diese Funktion ist ab den Aurora PostgreSQL-Versionen 14.10, 15.5 und für alle anderen späteren Versionen verfügbar.

Beispiele

Die folgende Beispielabfrage aggregiert die Top-Load nach query_id und plan_id.

```
db1=# select count(*), query_id, plan_id
db1-# from aurora_stat_activity() where state = 'active'
db1-# and pid <> pg_backend_pid()
db1-# group by query_id, plan_id
db1-# order by 1 desc;

count |  query_id             |  plan_id
-------+----------------------+-------------
 11    | -5471422286312252535 | -2054628807
 3     | -6907107586630739258 | -815866029
 1     | 5213711845501580017  |  300482084
(3 rows)
```

Wenn sich der für query_id verwendete Plan ändert, wird von aurora_stat_activity eine neue plan_id gemeldet.

```
count  |  query_id            |  plan_id
-------+----------------------+-------------
 10    | -5471422286312252535 | 1602979607
 1     | -6907107586630739258 | -1809935983
 1     | -2446282393000597155 | -207532066
(3 rows)
```

aurora_stat_backend_waits

Zeigt Statistiken für die Warteaktivität für einen bestimmten Backend-Prozess an.

Syntax

```
aurora_stat_backend_waits(pid)
```

Argumente

`pid` – Die ID für den Backend-Prozess. Sie können Prozess-IDs in der Ansicht `pg_stat_activity` abrufen.

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- `type_id` – Eine Zahl, die die Art des Warteereignisses angibt, wie 1 für eine einfache Sperre (`LWLock`), 3 für eine Sperre oder 6 für eine Clientsitzung, um nur einige Beispiele zu nennen. Diese Werte werden aussagekräftig, wenn Sie die Ergebnisse dieser Funktion mit Spalten der Funktion `aurora_stat_wait_type` verbinden, wie in Beispiele gezeigt.
- `event_id` – Eine ID-Nummer für das Warteereignis. Verbinden Sie diesen Wert mit den Spalten von `aurora_stat_wait_event`, um aussagekräftige Ereignisnamen zu erhalten.
- `waits` – Die Anzahl der Warteereignisse, die für die angegebene Prozess-ID aufgelaufen sind.
- `wait_time` – Wartezeit in Millisekunden.

Nutzungshinweise

Sie können diese Funktion verwenden, um bestimmte Backend-Warteereignisse (Sitzung) zu analysieren, die seit dem Öffnen einer Verbindung aufgetreten sind. Aussagekräftigere Informationen über Warteereignisnamen und -typen erhalten Sie, wenn Sie diese Funktion mit `aurora_stat_wait_type` und `aurora_stat_wait_event` kombinieren, indem Sie JOIN verwenden, wie in den Beispielen gezeigt.

Beispiele

Dieses Beispiel zeigt alle Warteereignisse, Typen und Ereignisnamen für die Backend-Prozess-ID 3027.

```
=> SELECT type_name, event_name, waits, wait_time
        FROM aurora_stat_backend_waits(3027)
NATURAL JOIN aurora_stat_wait_type()
NATURAL JOIN aurora_stat_wait_event();
type_name |       event_name       | waits | wait_time
----------+------------------------+-------+------------
 LWLock    | ProcArrayLock          |     3 |         27
 LWLock    | wal_insert             |   423 |      16336
```

```
 LWLock    | buffer_content         | 11840 |    1033634
 LWLock    | lock_manager           | 23821 |    5664506
 Lock      | tuple                  | 10258 |  152280165
 Lock      | transactionid          | 78340 | 1239808783
 Client    | ClientRead             | 34072 |   17616684
 IO        | ControlFileSyncUpdate  |     2 |          0
 IO        | ControlFileWriteUpdate |     4 |         32
 IO        | RelationMapRead        |     2 |        795
 IO        | WALWrite               | 36666 |      98623
 IO        | XactSync               |  4867 |    7331963
```

Dieses Beispiel zeigt aktuelle und kumulative Wartetypen und -ereignisse für alle aktiven Sitzungen (`pg_stat_activity state <> 'idle'`) (aber ohne die aktuelle Sitzung, die die Funktion aufruft (`pid <> pg_backend_pid()`)).

```
=> SELECT a.pid,
            a.usename,
            a.app_name,
            a.current_wait_type,
            a.current_wait_event,
            a.current_state,
            wt.type_name AS wait_type,
            we.event_name AS wait_event,
            a.waits,
            a.wait_time
       FROM (SELECT pid,
                    usename,
                    left(application_name,16) AS app_name,
                    coalesce(wait_event_type,'CPU') AS current_wait_type,
                    coalesce(wait_event,'CPU') AS current_wait_event,
                    state AS current_state,
                    (aurora_stat_backend_waits(pid)).*
               FROM pg_stat_activity
              WHERE pid <> pg_backend_pid()
                AND state <> 'idle') a
NATURAL JOIN aurora_stat_wait_type() wt
NATURAL JOIN aurora_stat_wait_event() we;
  pid  | usename  | app_name | current_wait_type | current_wait_event | current_state |
 wait_type |       wait_event       | waits | wait_time
-------+----------+----------+-------------------+--------------------+---------------
+-----------+------------------------+-------+-----------
 30099 | postgres | pgbench  | Lock              | transactionid      | active        |
 LWLock    | wal_insert             |  1937 |     29975
```

```
30099 | postgres | pgbench  | Lock              | transactionid      | active        |
LWLock    | buffer_content         | 22903 |    760498
30099 | postgres | pgbench  | Lock              | transactionid      | active        |
LWLock    | lock_manager           | 10012 |    223207
30099 | postgres | pgbench  | Lock              | transactionid      | active        |
Lock      | tuple                  | 20315 |  63081529
.
.
.
30099 | postgres | pgbench  | Lock              | transactionid      | active        |
IO        | WALWrite               | 93293 |    237440
30099 | postgres | pgbench  | Lock              | transactionid      | active        |
IO        | XactSync               | 13010 |  19525143
30100 | postgres | pgbench  | Lock              | transactionid      | active        |
LWLock    | ProcArrayLock          |     6 |        53
30100 | postgres | pgbench  | Lock              | transactionid      | active        |
LWLock    | wal_insert             |  1913 |     25450
30100 | postgres | pgbench  | Lock              | transactionid      | active        |
LWLock    | buffer_content         | 22874 |    778005
.
.
.
30109 | postgres | pgbench  | IO                | XactSync           | active        |
LWLock    | ProcArrayLock          |     3 |        71
30109 | postgres | pgbench  | IO                | XactSync           | active        |
LWLock    | wal_insert             |  1940 |     27741
30109 | postgres | pgbench  | IO                | XactSync           | active        |
LWLock    | buffer_content         | 22962 |    776352
30109 | postgres | pgbench  | IO                | XactSync           | active        |
LWLock    | lock_manager           |  9879 |    218826
30109 | postgres | pgbench  | IO                | XactSync           | active        |
Lock      | tuple                  | 20401 |  63581306
30109 | postgres | pgbench  | IO                | XactSync           | active        |
Lock      | transactionid          | 50769 | 211645008
30109 | postgres | pgbench  | IO                | XactSync           | active        |
Client    | ClientRead             | 89901 |  44192439
```

Dieses Beispiel zeigt aktuelle und die drei wichtigsten (3) kumulativen Wartetypen und Warteereignisse für alle aktiven Sitzungen (`pg_stat_activity state <> 'idle'`) ohne die aktuelle Sitzung (`pid <>pg_backend_pid()`).

```
=> SELECT top3.*
       FROM (SELECT a.pid,
```

```
                    a.usename,
                    a.app_name,
                    a.current_wait_type,
                    a.current_wait_event,
                    a.current_state,
                    wt.type_name AS wait_type,
                    we.event_name AS wait_event,
                    a.waits,
                    a.wait_time,
                    RANK() OVER (PARTITION BY pid ORDER BY a.wait_time DESC)
               FROM (SELECT pid,
                            usename,
                            left(application_name,16) AS app_name,
                            coalesce(wait_event_type,'CPU') AS current_wait_type,
                            coalesce(wait_event,'CPU') AS current_wait_event,
                            state AS current_state,
                            (aurora_stat_backend_waits(pid)).*
                       FROM pg_stat_activity
                      WHERE pid <> pg_backend_pid()
                        AND state <> 'idle') a
             NATURAL JOIN aurora_stat_wait_type() wt
             NATURAL JOIN aurora_stat_wait_event() we) top3
 WHERE RANK <=3;
  pid  | usename  | app_name | current_wait_type | current_wait_event | current_state |
 wait_type |   wait_event    |  waits  | wait_time  | rank
-------+----------+----------+-------------------+--------------------+---------------
+-----------+-----------------+---------+------------+------
 20567 | postgres | psql     | CPU               | CPU                | active        |
 LWLock    | wal_insert      |   25000 |   67512003 |    1
 20567 | postgres | psql     | CPU               | CPU                | active        |
 IO        | WALWrite        | 3071758 |    1016961 |    2
 20567 | postgres | psql     | CPU               | CPU                | active        |
 IO        | BufFileWrite    |   20750 |     184559 |    3
 27743 | postgres | pgbench  | Lock              | transactionid      | active        |
 Lock      | transactionid   |  237350 | 1265580011 |    1
 27743 | postgres | pgbench  | Lock              | transactionid      | active        |
 Lock      | tuple           |   93641 |  341472318 |    2
 27743 | postgres | pgbench  | Lock              | transactionid      | active        |
 Client    | ClientRead      |  417556 |  204796837 |    3
 .
 .
 .
 27745 | postgres | pgbench  | IO                | XactSync           | active        |
 Lock      | transactionid   |  238068 | 1265816822 |    1
```

```
 27745 | postgres | pgbench  | IO               | XactSync          | active        |
 Lock      | tuple           |   93210 |  338312247 |    2
 27745 | postgres | pgbench  | IO               | XactSync          | active        |
 Client    | ClientRead      |  419157 |  207836533 |    3
 27746 | postgres | pgbench  | Lock             | transactionid     | active        |
 Lock      | transactionid   |  237621 | 1264528811 |    1
 27746 | postgres | pgbench  | Lock             | transactionid     | active        |
 Lock      | tuple           |   93563 |  339799310 |    2
 27746 | postgres | pgbench  | Lock             | transactionid     | active        |
 Client    | ClientRead      |  417304 |  208372727 |    3
```

aurora_stat_bgwriter

`aurora_stat_bgwriter` ist eine Statistikanzeige mit Informationen über Cache-Schreibvorgänge für optimierte Lesevorgänge.

Syntax

```
aurora_stat_bgwriter()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit allen Spalten von `pg_stat_bgwriter` und den folgenden zusätzlichen Spalten. Weitere Informationen zu den Spalten von `pg_stat_bgwriter` finden Sie unter `pg_stat_bgwriter`.

Sie können die Statistiken für diese Funktion mit `pg_stat_reset_shared("bgwriter")` zurücksetzen.

- `orcache_blks_written` – Gesamtzahl der geschriebenen Cache-Datenblöcke für optimierte Lesevorgänge.
- `orcache_blk_write_time` – Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit, die für das Schreiben von Cache-Datendateiblöcken für optimierte Lesevorgänge aufgewendet wurde, in Millisekunden aufgezeichnet. Weitere Informationen finden Sie unter track_io_timing.

Nutzungshinweise

Diese Funktion steht in folgenden Aurora-PostgreSQL-Versionen zur Verfügung:

- 15.4 und höhere 15-Versionen
- 14.9 und höhere 14-Versionen

Beispiele

```
=> select * from aurora_stat_bgwriter();
-[ RECORD 1 ]-----------------+-----------
orcache_blks_written          | 246522
orcache_blk_write_time        | 339276.404
```

aurora_stat_database

Enthält alle Spalten von pg_stat_database und fügt am Ende neue Spalten hinzu.

Syntax

```
aurora_stat_database()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit allen Spalten von `pg_stat_database` und den folgenden zusätzlichen Spalten. Weitere Informationen zu den Spalten von `pg_stat_database` finden Sie unter `pg_stat_database`.

- `storage_blks_read`: Gesamtzahl der gemeinsam genutzten Blöcke, die aus dem Aurora-Speicher in dieser Datenbank gelesen wurden.
- `orcache_blks_hit`: Gesamtzahl der Treffer im Cache für optimierte Lesevorgänge in dieser Datenbank.
- `local_blks_read`: Gesamtzahl der in dieser Datenbank gelesenen lokalen Blöcke.

- `storage_blk_read_time`: Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit für das Lesen von Datendateiblöcken aus dem Aurora-Speicher in Millisekunden aufgezeichnet. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.
- `local_blk_read_time`: Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit für das Lesen von lokalen Datendateiblöcken in Millisekunden aufgezeichnet. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.
- `orcache_blk_read_time`: Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit für das Lesen von Datendateiblöcken aus dem Cache für optimierte Lesevorgänge in Millisekunden aufgezeichnet. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.

> **Note**
>
> Der Wert von `blks_read` ist die Summe von `storage_blks_read`, `orcache_blks_hit` und `local_blks_read`.
> Der Wert von `blk_read_time` ist die Summe von `storage_blk_read_time`, `orcache_blk_read_time` und `local_blk_read_time`.

Nutzungshinweise

Diese Funktion steht in folgenden Aurora-PostgreSQL-Versionen zur Verfügung:

- 15.4 und höhere 15-Versionen
- 14.9 und höhere 14-Versionen

Beispiele

Das folgende Beispiel zeigt, wie alle Spalten von `pg_stat_database` enthalten sind und am Ende 6 neue Spalten angefügt werden:

```
=> select * from aurora_stat_database() where datid=14717;
-[ RECORD 1 ]------------+------------------------------
datid                    | 14717
datname                  | postgres
numbackends              | 1
xact_commit              | 223
```

```
xact_rollback            | 4
blks_read                | 1059
blks_hit                 | 11456
tup_returned             | 27746
tup_fetched              | 5220
tup_inserted             | 165
tup_updated              | 42
tup_deleted              | 91
conflicts                | 0
temp_files               | 0
temp_bytes               | 0
deadlocks                | 0
checksum_failures        |
checksum_last_failure    |
blk_read_time            | 3358.689
blk_write_time           | 0
session_time             | 1076007.997
active_time              | 3684.371
idle_in_transaction_time | 0
sessions                 | 10
sessions_abandoned       | 0
sessions_fatal           | 0
sessions_killed          | 0
stats_reset              | 2023-01-12 20:15:17.370601+00
orcache_blks_hit         | 425
orcache_blk_read_time    | 89.934
storage_blks_read        | 623
storage_blk_read_time    | 3254.914
local_blks_read          | 0
local_blk_read_time      | 0
```

aurora_stat_dml_activity

Meldet kumulative Aktivitäten für jeden Data-Manipulation-Language-Vorgangstyp (DML) in einer Datenbank in einem Aurora-PostgreSQL-Cluster.

Syntax

```
aurora_stat_dml_activity(database_oid)
```

Argumente

database_oid

Die Objekt-ID (OID) der Datenbank im Aurora-PostgreSQL-Cluster.

Rückgabetyp

SETOF-Datensatz

Nutzungshinweise

Die Funktion `aurora_stat_dml_activity` ist nur mit Version 3.1 von Aurora PostgreSQL verfügbar, die mit der PostgreSQL-Engine 11.6 und höher kompatibel ist.

Verwenden Sie diese Funktion in Aurora-PostgreSQL-Clustern mit einer großen Anzahl von Datenbanken, um zu ermitteln, welche Datenbanken mehr oder langsamere DML-Aktivitäten oder beides haben.

Die Funktion `aurora_stat_dml_activity` gibt die Anzahl der Ausführungen und die kumulative Latenz in Mikrosekunden für SELECT-, INSERT-, UPDATE- und DELETE-Operationen zurück. Der Bericht enthält nur erfolgreiche DML-Operationen.

Mit der PostgreSQL-Statistikzugriffsfunktion `pg_stat_reset` können Sie diese Statistik zurücksetzen. Mit der Funktion `pg_stat_get_db_stat_reset_time` können Sie überprüfen, wann diese Statistik zuletzt zurückgesetzt wurde. Weitere Informationen zu PostgreSQL-Statistikzugriffsfunktionen finden Sie unter Die Statistikerfassung in der PostgreSQL-Dokumentation.

Beispiele

Im folgenden Beispiel wird gezeigt, wie Sie DML-Aktivitätsstatistiken für die verbundene Datenbank melden.

```
--Define the oid variable from connected database by using \gset
=> SELECT oid,
          datname
     FROM pg_database
    WHERE datname=(select current_database()) \gset
=> SELECT *
     FROM aurora_stat_dml_activity(:oid);
select_count | select_latency_microsecs | insert_count | insert_latency_microsecs |
 update_count | update_latency_microsecs | delete_count | delete_latency_microsecs
```

```
--------------+--------------------------+--------------+--------------------------
+--------------+--------------------------+--------------+--------------------------
       178957 |                 66684115 |       171065 |                 28876649 |
    519538 |            1454579206167 |            1 |                        53027


-- Showing the same results with expanded display on
=> SELECT *
     FROM aurora_stat_dml_activity(:oid);
-[ RECORD 1 ]------------+--------------
select_count             | 178957
select_latency_microsecs | 66684115
insert_count             | 171065
insert_latency_microsecs | 28876649
update_count             | 519538
update_latency_microsecs | 1454579206167
delete_count             | 1
delete_latency_microsecs | 53027
```

Im folgenden Beispiel sehen Sie DML-Aktivitätsstatistiken für alle Datenbanken im Aurora-PostgreSQL-Cluster. Dieser Cluster hat zwei Datenbanken, `postgres` und `mydb`. Die durch Komma getrennte Liste entspricht den Feldern `select_count`, `select_latency_microsecs`, `insert_count`, `insert_latency_microsecs`, `update_count`, `update_latency_microsecs`, `delete_count` und `delete_latency_microsecs`.

Aurora PostgreSQL erstellt und verwendet eine Systemdatenbank namens `rdsadmin`, um administrative Vorgänge wie Backups, Wiederherstellungen, Zustandsprüfungen, Replikationen usw. zu unterstützen. Diese DML-Operationen haben keine Auswirkungen auf Ihren Aurora-PostgreSQL-Cluster.

```
=> SELECT oid,
    datname,
    aurora_stat_dml_activity(oid)
    FROM pg_database;
oid  |    datname     |                   aurora_stat_dml_activity
-------+---------------
+-------------------------------------------------------------------
 14006 | template0      | (,,,,,,,)
 16384 | rdsadmin       | (2346623,1211703821,4297518,817184554,0,0,0,0)
     1 | template1      | (,,,,,,,)
```

```
 14007 | postgres       |
(178961,66716329,171065,28876649,519538,1454579206167,1,53027)
 16401 | mydb           | (200246,64302436,200036,107101855,600000,83659417514,0,0)
```

Das folgende Beispiel zeigt DML-Aktivitätsstatistiken für alle Datenbanken, die aus Gründen der Lesbarkeit in Spalten angeordnet sind.

```
SELECT db.datname,
       BTRIM(SPLIT_PART(db.asdmla::TEXT, ',', 1), '()') AS select_count,
       BTRIM(SPLIT_PART(db.asdmla::TEXT, ',', 2), '()') AS select_latency_microsecs,
       BTRIM(SPLIT_PART(db.asdmla::TEXT, ',', 3), '()') AS insert_count,
       BTRIM(SPLIT_PART(db.asdmla::TEXT, ',', 4), '()') AS insert_latency_microsecs,
       BTRIM(SPLIT_PART(db.asdmla::TEXT, ',', 5), '()') AS update_count,
       BTRIM(SPLIT_PART(db.asdmla::TEXT, ',', 6), '()') AS update_latency_microsecs,
       BTRIM(SPLIT_PART(db.asdmla::TEXT, ',', 7), '()') AS delete_count,
       BTRIM(SPLIT_PART(db.asdmla::TEXT, ',', 8), '()') AS delete_latency_microsecs
FROM  (SELECT datname,
              aurora_stat_dml_activity(oid) AS asdmla
         FROM pg_database
      ) AS db;

    datname     | select_count | select_latency_microsecs | insert_count |
 insert_latency_microsecs | update_count | update_latency_microsecs | delete_count |
 delete_latency_microsecs
----------------+--------------+--------------------------+--------------
+--------------------------+--------------+--------------------------+--------------
+--------------------------
 template0      |              |                          |              |
             |              |                          |              |
 rdsadmin       | 4206523      | 2478812333               | 7009414      | 1338482258
             | 0            | 0                        | 0            | 0
 template1      |              |                          |              |
             |              |                          |              |
 fault_test     | 66           | 452099                   | 0            | 0
             | 0            | 0                        | 0            | 0
 db_access_test | 1            | 5982                     | 0            | 0
             | 0            | 0                        | 0            | 0
 postgres       | 42035        | 95179203                 | 5752         | 2678832898
             | 21157        | 441883182488             | 2            | 1520
 mydb           | 71           | 453514                   | 0            | 0
             | 1            | 190                      | 1            | 152
```

Das folgende Beispiel zeigt die durchschnittliche kumulative Latenz (kumulative Latenz geteilt durch die Anzahl) jeder DML-Operation für die Datenbank mit der OID 16401.

```
=> SELECT select_count,
          select_latency_microsecs,
          select_latency_microsecs/NULLIF(select_count,0) select_latency_per_exec,
          insert_count,
          insert_latency_microsecs,
          insert_latency_microsecs/NULLIF(insert_count,0) insert_latency_per_exec,
          update_count,
          update_latency_microsecs,
          update_latency_microsecs/NULLIF(update_count,0) update_latency_per_exec,
          delete_count,
          delete_latency_microsecs,
          delete_latency_microsecs/NULLIF(delete_count,0) delete_latency_per_exec
     FROM aurora_stat_dml_activity(16401);
-[ RECORD 1 ]------------+-------------
select_count             | 451312
select_latency_microsecs | 80205857
select_latency_per_exec  | 177
insert_count             | 451001
insert_latency_microsecs | 123667646
insert_latency_per_exec  | 274
update_count             | 1353067
update_latency_microsecs | 200900695615
update_latency_per_exec  | 148478
delete_count             | 12
delete_latency_microsecs | 448
delete_latency_per_exec  | 37
```

aurora_stat_get_db_commit_latency

Ruft die kumulative Commit-Latenz in Mikrosekunden für Aurora-PostgreSQL-Datenbanken ab. Die Commit-Latenz wird als Zeit zwischen dem Senden einer Commit-Anforderung und dem Empfang der Commit-Bestätigung gemessen.

Syntax

```
aurora_stat_get_db_commit_latency(database_oid)
```

Argumente

database_oid

Die Objekt-ID (OID) der Aurora-PostgreSQL-Datenbank.

Rückgabetyp

SETOF-Datensatz

Nutzungshinweise

Amazon CloudWatch verwendet diese Funktion, um die durchschnittliche Commit-Latenz zu berechnen. Weitere Informationen zu Amazon-CloudWatch-Metriken und zur Behebung einer hohen Commit-Latenz finden Sie unter Anzeigen von Metriken in der Amazon-RDS-Konsole und Making better decisions about Amazon RDS with Amazon CloudWatch metrics.

Mit der PostgreSQL-Statistikzugriffsfunktion `pg_stat_reset` können Sie diese Statistik zurücksetzen. Mit der Funktion `pg_stat_get_db_stat_reset_time` können Sie überprüfen, wann diese Statistik zuletzt zurückgesetzt wurde. Weitere Informationen zu PostgreSQL-Statistikzugriffsfunktionen finden Sie unter Die Statistikerfassung in der PostgreSQL-Dokumentation.

Beispiele

Im folgenden Beispiel wird die kumulative Commit-Latenz für jede Datenbank im Cluster `pg_database` abgerufen.

```
=> SELECT oid,
    datname,
    aurora_stat_get_db_commit_latency(oid)
    FROM pg_database;

  oid  |    datname     | aurora_stat_get_db_commit_latency
-------+----------------+-----------------------------------
 14006 | template0      |                                 0
 16384 | rdsadmin       |                         654387789
     1 | template1      |                                 0
 16401 | mydb           |                            229556
 69768 | postgres       |                             22011
```

Im folgenden Beispiel wird die kumulative Commit-Latenz für die aktuell verbundene Datenbank abgerufen. Vor dem Aufruf der Funktion `aurora_stat_get_db_commit_latency` wird im Beispiel

zuerst `\gset` verwendet, um eine Variable für das Argument `oid` zu definieren und ihren Wert aus der verbundenen Datenbank zu beziehen.

```
--Get the oid value from the connected database before calling
 aurora_stat_get_db_commit_latency
=> SELECT oid
     FROM pg_database
    WHERE datname=(SELECT current_database()) \gset
=> SELECT *
     FROM aurora_stat_get_db_commit_latency(:oid);

 aurora_stat_get_db_commit_latency
-----------------------------------
                        1424279160
```

Im folgenden Beispiel wird die kumulative Commit-Latenz für die mydb-Datenbank im Cluster `pg_database` abgerufen. Dann wird diese Statistik mit der Funktion `pg_stat_reset` zurückgesetzt und die Ergebnisse werden angezeigt. Abschließend wird die Funktion `pg_stat_get_db_stat_reset_time` ausgeführt, um zu überprüfen, wann diese Statistik zuletzt zurückgesetzt wurde.

```
=> SELECT oid,
    datname,
    aurora_stat_get_db_commit_latency(oid)
    FROM pg_database
    WHERE datname = 'mydb';

  oid  |  datname  | aurora_stat_get_db_commit_latency
-------+-----------+-----------------------------------
 16427 | mydb      |                           3320370


=> SELECT pg_stat_reset();
 pg_stat_reset
---------------


=> SELECT oid,
          datname,
          aurora_stat_get_db_commit_latency(oid)
     FROM pg_database
    WHERE datname = 'mydb';
```

```
  oid  |  datname  | aurora_stat_get_db_commit_latency
-------+-----------+-----------------------------------
 16427 | mydb      |                                 6


=> SELECT *
     FROM pg_stat_get_db_stat_reset_time(16427);

 pg_stat_get_db_stat_reset_time
--------------------------------
 2021-04-29 21:36:15.707399+00
```

aurora_stat_logical_wal_cache

Zeigt die Cache-Auslastung für das logische Write-Ahead-Protokoll (WAL) pro Slot an.

Syntax

```
SELECT * FROM aurora_stat_logical_wal_cache()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- `name` – Der Name der Replikationsgruppe.
- `active_pid` – Die ID des Walsender-Prozesses.
- `cache_hit` – Die Gesamtzahl der WAL-Cache-Treffer seit dem letzten Reset.
- `cache_miss` – Die Gesamtzahl der WAL-Cache-Fehler seit dem letzten Reset.
- `blks_read` – Die Gesamtzahl der Wal-Cache-Leseanfragen.
- `hit_rate` – Die WAL-Cache-Trefferrate (cache_hit/blks_read).
- `last_reset_timestamp` – Das letzte Mal, dass der Zähler zurückgesetzt wurde.

Nutzungshinweise

Diese Funktion steht für die folgenden Versionen zur Verfügung.

- Aurora PostgreSQL 14.7
- Aurora PostgreSQL 13.8 und höhere Versionen
- Aurora PostgreSQL 12.12 und höhere Versionen
- Aurora PostgreSQL 11.17 und höhere Versionen

Beispiele

Das folgende Beispiel zeigt zwei Replikations-Slots mit nur einer aktiven `aurora_stat_logical_wal_cache`-Funktion.

```
=> SELECT *
     FROM aurora_stat_logical_wal_cache();
    name    | active_pid | cache_hit | cache_miss | blks_read | hit_rate |
 last_reset_timestamp
------------+------------+-----------+------------+-----------+----------
+-------------------------------
 test_slot1 |      79183 |        24 |          0 |        24 | 100.00%  | 2022-08-05
 17:39:56.830635+00
 test_slot2 |            |         1 |          0 |         1 | 100.00%  | 2022-08-05
 17:34:04.036795+00
(2 rows)
```

aurora_stat_memctx_usage

Meldet die Speicherkontextnutzung für jeden PostgreSQL-Prozess.

Syntax

```
aurora_stat_memctx_usage()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- `pid` – die ID des Prozesses.

- `name` – der Name des Speicherkontexts.
- `allocated` – Die Anzahl der Byte, die der Speicherkontext aus dem zugrunde liegenden Speichersubsystem abgerufen hat.
- `used` – Die Anzahl der an Clients des Speicherkontextes übergebenen Byte.
- `instances` – Die Anzahl der derzeit existierenden Kontexte dieses Typs.

Nutzungshinweise

Diese Funktion zeigt die Speicherkontextnutzung für jeden PostgreSQL-Prozess an. Einige Prozesse sind mit `anonymous` beschriftet. Die Prozesse werden nicht offengelegt, da sie eingeschränkte Schlüsselwörter enthalten.

Diese Funktion steht ab den folgenden Aurora-PostgreSQL-Versionen zur Verfügung:

- 15.3 und höhere 15-Versionen
- 14.8 und höhere 14-Versionen
- 13.11 und höhere 13-Versionen
- 12.15 und höhere 12-Versionen
- 11.20 und höhere 11-Versionen

Beispiele

Im folgenden Beispiel sehen Sie die Ergebnisse vom Aufruf der Funktion `aurora_stat_memctx_usage`.

```
=> SELECT *
     FROM aurora_stat_memctx_usage();

    pid| name                             | allocated |   used  | instances
-------+----------------------------------+-----------+---------+-----------
123864 | Miscellaneous                    |     19520 |   15064 |         3
123864 | Aurora File Context              |      8192 |     616 |         1
123864 | Aurora WAL Context               |      8192 |     296 |         1
123864 | CacheMemoryContext               |    524288 |  422600 |         1
123864 | Catalog tuple context            |     16384 |   13736 |         1
123864 | ExecutorState                    |     32832 |   28304 |         1
123864 | ExprContext                      |      8192 |    1720 |         1
```

```
123864 | GWAL record construction        |      1024 |     832 |         1
123864 | MdSmgr                          |      8192 |     296 |         1
123864 | MessageContext                  |    532480 |  353832 |         1
123864 | PortalHeapMemory                |      1024 |     488 |         1
123864 | PortalMemory                    |      8192 |     576 |         1
123864 | printtup                        |      8192 |     296 |         1
123864 | RelCache hash table entries     |      8192 |    8152 |         1
123864 | RowDescriptionContext           |      8192 |    1344 |         1
123864 | smgr relation context           |      8192 |     296 |         1
123864 | Table function arguments        |      8192 |     352 |         1
123864 | TopTransactionContext           |      8192 |     632 |         1
123864 | TransactionAbortContext         |     32768 |     296 |         1
123864 | WAL record construction         |     50216 |   43904 |         1
123864 | hash table                      |     65536 |   52744 |         6
123864 | Relation metadata               |    191488 |  124240 |        87
104992 | Miscellaneous                   |      9280 |    7728 |         3
104992 | Aurora File Context             |      8192 |     376 |         1
104992 | Aurora WAL Context              |      8192 |     296 |         1
104992 ||Autovacuum Launcher             |      8192 |     296 |         1
104992 | Autovacuum database list        |     16384 |     744 |         2
104992 | CacheMemoryContext              |    262144 |  140288 |         1
104992 | Catalog tuple context           |      8192 |     296 |         1
104992 | GWAL record construction        |      1024 |     832 |         1
104992 | MdSmgr                          |      8192 |     296 |         1
104992 | PortalMemory                    |      8192 |     296 |         1
104992 | RelCache hash table entries     |      8192 |     296 |         1
104992 | smgr relation context           |      8192 |     296 |         1
104992 | Autovacuum start worker (tmp)   |      8192 |     296 |         1
104992 | TopTransactionContext           |     16384 |     592 |         2
104992 | TransactionAbortContext         |     32768 |     296 |         1
104992 | WAL record construction         |     50216 |   43904 |         1
104992 | hash table                      |     49152 |   34024 |         4
(39 rows)
```

Einige eingeschränkte Schlüsselwörter werden ausgeblendet und die Ausgabe sieht wie folgt aus:

```
postgres=>SELECT *
     FROM aurora_stat_memctx_usage();

    pid| name                            | allocated |   used  | instances
-------+---------------------------------+-----------+---------+-----------
  5482 | anonymous                       |      8192 |     456 |         1
  5482 | anonymous                       |      8192 |     296 |         1
```

aurora_stat_optimized_reads_cache

Diese Funktion zeigt mehrstufige Cache-Statistiken an.

Syntax

```
aurora_stat_optimized_reads_cache()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- `total_size` – Gesamtgröße des Cache für optimierte Lesevorgänge
- `used_size` – Verwendete Seitengröße im Cache für optimierte Lesevorgänge

Nutzungshinweise

Diese Funktion steht in folgenden Aurora-PostgreSQL-Versionen zur Verfügung:

- 15.4 und höhere 15-Versionen
- 14.9 und höhere 14-Versionen

Beispiele

Das folgende Beispiel zeigt die Ausgabe für eine r6gd.8xlarge-Instance:

```
=> select pg_size_pretty(total_size) as total_size, pg_size_pretty(used_size)
               as used_size from aurora_stat_optimized_reads_cache();
total_size | used_size
-----------+-----------
1054 GB    | 975 GB
```

aurora_stat_plans

Gibt eine Zeile für jeden verfolgten Ausführungsplan zurück.

Syntax

```
aurora_stat_plans(
    showtext
)
```

Argumente

- showtext — Zeigt den Abfrage- und Plantext an. Gültige Werte sind NULL, wahr oder falsch. Bei True werden die Abfrage und der Plantext angezeigt.

Rückgabetyp

Gibt für jeden verfolgten Plan eine Zeile zurück, die alle Spalten von `aurora_stat_statements` und die folgenden zusätzlichen Spalten enthält.

- planid — Plan-ID
- explain_plan — erklärt den Plantext
- Plantyp:
  - `no plan`- es wurde kein Plan erfasst
  - `estimate`- der Plan wurde mit den geschätzten Kosten erfasst
  - `actual`- mit EXPLAIN ANALYZE erfasster Plan
- plan_captured_time — das letzte Mal, als ein Plan erfasst wurde

Nutzungshinweise

`aurora_compute_plan_id`muss aktiviert sein und `pg_stat_statements` muss aktiviert sein, damit die Pläne nachverfolgt werden können. `shared_preload_libraries`

Die Anzahl der verfügbaren Pläne wird durch den im `pg_stat_statements.max` Parameter festgelegten Wert gesteuert. Wenn diese Option aktiviert `compute_plan_id` ist, können Sie die Pläne bis zu diesem angegebenen Wert in verfolgen`aurora_stat_plans`.

Diese Funktion ist ab den Aurora PostgreSQL-Versionen 14.10, 15.5 und für alle anderen späteren Versionen verfügbar.

Beispiele

Im folgenden Beispiel werden die beiden Pläne für die Abfrage-ID -5471422286312252535 erfasst, und die Statement-Statistiken werden anhand der Planid verfolgt.

```
db1=# select calls, total_exec_time, planid, plan_captured_time, explain_plan
db1-# from aurora_stat_plans(true)
db1-# where queryid = '-5471422286312252535'

calls    |  total_exec_time   |   planid    |      plan_captured_time       |
                explain_plan
---------+--------------------+-------------+-------------------------------
+-----------------------------------------------------------------
 1532632 |  3209846.097107853 |  1602979607 | 2023-10-31 03:27:16.925497+00 | Update on
 pgbench_branches                                      +
         |                    |             |                               |   ->
 Bitmap Heap Scan on pgbench_branches                     +
         |                    |             |                               |
 Recheck Cond: (bid = 76)                                   +
         |                    |             |                               |         -
>  Bitmap Index Scan on pgbench_branches_pkey          +
         |                    |             |                               |
     Index Cond: (bid = 76)
   61365 | 124078.18012200127 | -2054628807 | 2023-10-31 03:20:09.85429+00  | Update on
 pgbench_branches                                      +
         |                    |             |                               |   ->
 Index Scan using pgbench_branches_pkey on pgbench_branches+
         |                    |             |                               |
 Index Cond: (bid = 17)
```

aurora_stat_reset_wal_cache

Setzt den Zähler für den logischen WAL-Cache zurück.

Syntax

So setzen Sie einen bestimmten Slot zurück

```
SELECT * FROM aurora_stat_reset_wal_cache('slot_name')
```

So setzen Sie alle Slots zurück

```
SELECT * FROM aurora_stat_reset_wal_cache(NULL)
```

Argumente

`NULL` oder `slot_name`

Rückgabetyp

Statusmeldung, Textzeichenfolge

- Setzen Sie den logischen WAL-Cache-Zähler zurück – Erfolgsmeldung. Dieser Text wird zurückgegeben, wenn die Funktion erfolgreich ist.
- Der Replikations-Slot wurde nicht gefunden. Bitte versuchen Sie es noch einmal. – Fehlernachricht Dieser Text wird zurückgegeben, wenn die Funktion nicht erfolgreich ist.

Nutzungshinweise

Diese Funktion steht für die folgenden Versionen zur Verfügung.

- Aurora PostgreSQL 14.5 und höher
- Aurora PostgreSQL 13.8 und höhere Versionen
- Aurora PostgreSQL 12.12 und höhere Versionen
- Aurora PostgreSQL 11.17 und höhere Versionen

Beispiele

Im folgenden Beispiel wird die `aurora_stat_reset_wal_cache`-Funktion verwendet, um einen Slot namens `test_results` zurückzusetzen. Anschließend wird versucht, einen Slot zurückzusetzen, der nicht existiert.

```
=> SELECT *
     FROM aurora_stat_reset_wal_cache('test_slot');
aurora_stat_reset_wal_cache
------------------------------------
 Reset the logical wal cache counter.
(1 row)
=> SELECT *
```

```
     FROM aurora_stat_reset_wal_cache('slot-not-exist');
aurora_stat_reset_wal_cache
-----------------------------------------------
 Replication slot not found. Please try again.
(1 row)
```

aurora_stat_statements

Zeigt alle Spalten von `pg_stat_statements` an und fügt am Ende weitere Spalten hinzu.

Syntax

```
aurora_stat_statements(showtext boolean)
```

Argumente

showtext boolescher Wert

Rückgabetyp

SETOF-Datensatz mit allen Spalten von `pg_stat_statements` und den folgenden zusätzlichen Spalten. Weitere Informationen zu den Spalten von `pg_stat_statements` finden Sie unter `pg_stat_statements`.

Sie können die Statistiken für diese Funktion mit `pg_stat_statements_reset()` zurücksetzen.

- `storage_blks_read`: Gesamtzahl der gemeinsam genutzten Blöcke, die von dieser Anweisung aus dem Aurora-Speicher gelesen wurden.
- `orcache_blks_hit`: Gesamtzahl der mit dieser Anweisung erzielten Treffer im Cache für optimierte Lesevorgänge.
- `storage_blk_read_time`: Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit in Millisekunden aufgezeichnet, die die Anweisung für das Lesen von Datendateiblöcken aus dem Aurora-Speicher benötigt hat. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.
- `local_blk_read_time`: Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit in Millisekunden aufgezeichnet, die die Anweisung für das Lesen von lokalen Datendateiblöcken benötigt hat. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.

- `orcache_blk_read_time`: Wenn `track_io_timing` aktiviert ist, wird die Gesamtzeit in Millisekunden aufgezeichnet, die die Anweisung für das Lesen von Datendateiblöcken aus dem Cache für optimierte Lesevorgänge benötigt hat. Andernfalls beträgt der Wert Null. Weitere Informationen finden Sie unter track_io_timing.

Nutzungshinweise

Um die Funktion aurora_stat_statements () verwenden zu können, müssen Sie eine Erweiterung in den Parameter aufnehmen. `pg_stat_statements` `shared_preload_libraries`

Diese Funktion steht in folgenden Aurora-PostgreSQL-Versionen zur Verfügung:

- 15.4 und höhere 15-Versionen
- 14.9 und höhere 14-Versionen

Beispiele

Das folgende Beispiel zeigt, wie alle Spalten von pg_stat_statements enthalten sind und am Ende 5 neue Spalten angefügt werden:

```
=> select * from aurora_stat_statements(true) where queryid=-7342090857217643794;
-[ RECORD 1 ]---------+--------------------------------------------------
userid                | 10
dbid                  | 16419
toplevel              | t
queryid               | -7342090857217643794
query                 | CREATE TABLE quad_point_tbl AS                   +
                      |     SELECT point(unique1,unique2) AS p FROM tenk1
plans                 | 0
total_plan_time       | 0
min_plan_time         | 0
max_plan_time         | 0
mean_plan_time        | 0
stddev_plan_time      | 0
calls                 | 1
total_exec_time       | 571.844376
min_exec_time         | 571.844376
max_exec_time         | 571.844376
mean_exec_time        | 571.844376
stddev_exec_time      | 0
rows                  | 10000
```

```
shared_blks_hit       | 462
shared_blks_read      | 422
shared_blks_dirtied   | 0
shared_blks_written   | 55
local_blks_hit        | 0
local_blks_read       | 0
local_blks_dirtied    | 0
local_blks_written    | 0
temp_blks_read        | 0
temp_blks_written     | 0
blk_read_time         | 170.634621
blk_write_time        | 0
wal_records           | 0
wal_fpi               | 0
wal_bytes             | 0
storage_blks_read     | 47
orcache_blks_hit      | 375
storage_blk_read_time | 124.505772
local_blk_read_time   | 0
orcache_blk_read_time | 44.684038
```

aurora_stat_system_waits

Meldet Warteereignisinformationen für die Aurora-PostgreSQL-DB-Instance.

Syntax

```
aurora_stat_system_waits()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz

Nutzungshinweise

Diese Funktion gibt die kumulative Anzahl der Wartezeiten und die kumulative Wartezeit für jedes Warteereignis zurück, das von der DB-Instance generiert wird, mit der Sie derzeit verbunden sind.

Der zurückgegebene Datensatz enthält die folgenden Felder:

- `type_id` – die ID des Warteereignistyps.
- `event_id` – die ID des Warteereignisses.
- `waits` – die Häufigkeit, mit der das Warteereignis aufgetreten ist.
- `wait_time` – die Gesamtzeit in Mikrosekunden, die auf dieses Ereignis gewartet wurde.

Die von dieser Funktion zurückgegebenen Statistiken werden zurückgesetzt, wenn eine DB-Instance neu gestartet wird.

Beispiele

Im folgenden Beispiel sehen Sie Ergebnisse vom Aufruf der Funktion `aurora_stat_system_waits`.

```
=> SELECT *
    FROM aurora_stat_system_waits();
 type_id | event_id  |   waits   |  wait_time
---------+-----------+-----------+--------------
       1 |  16777219 |        11 |        12864
       1 |  16777220 |       501 |       174473
       1 |  16777270 |     53171 |     23641847
       1 |  16777271 |        23 |       319668
       1 |  16777274 |        60 |        12759
.
.
.
      10 | 167772231 |    204596 |    790945212
      10 | 167772232 |         2 |        47729
      10 | 167772234 |         1 |          888
      10 | 167772235 |         2 |           64
```

Im folgenden Beispiel wird gezeigt, wie Sie diese Funktion mit `aurora_stat_wait_event` und `aurora_stat_wait_type` ausführen können, um besser lesbare Ergebnisse zu erzeugen.

```
=> SELECT type_name,
            event_name,
            waits,
            wait_time
        FROM aurora_stat_system_waits()
NATURAL JOIN aurora_stat_wait_event()
NATURAL JOIN aurora_stat_wait_type();
```

```
 type_name |       event_name       |  waits   |  wait_time
-----------+------------------------+----------+--------------
 LWLock    | XidGenLock             |       11 |        12864
 LWLock    | ProcArrayLock          |      501 |       174473
 LWLock    | buffer_content         |    53171 |     23641847
 LWLock    | rdsutils               |        2 |        12764
 Lock      | tuple                  |    75686 |   2033956052
 Lock      | transactionid          |  1765147 |  47267583409
 Activity  | AutoVacuumMain         |   136868 |  56305604538
 Activity  | BgWriterHibernate      |     7486 |  55266949471
 Activity  | BgWriterMain           |     7487 |   1508909964
.
.
.
 IO        | SLRURead               |        3 |        11756
 IO        | WALWrite               | 52544463 |    388850428
 IO        | XactSync               |   187073 |    597041642
 IO        | ClogRead               |        2 |        47729
 IO        | OutboundCtrlRead       |        1 |          888
 IO        | OutboundCtrlWrite      |        2 |           64
```

aurora_stat_wait_event

Listet alle unterstützten Warteereignisse für Aurora PostgreSQL auf. Informationen zu Aurora PostgreSQL-Warteereignissen finden Sie unter Amazon-Aurora-PostgreSQL-Warteereignisse.

Syntax

```
aurora_stat_wait_event()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- type_id – die ID des Warteereignistyps.
- event_id – die ID des Warteereignisses.

- type_name – Name des Wartetyps
- event_name – Name des Warteereignisses

Nutzungshinweise

Kombinieren Sie diese Funktion mit anderen Funktionen wie `aurora_stat_wait_type` und `aurora_stat_system_waits`, um Ereignisnamen mit Ereignistypen anstelle von IDs anzuzeigen. Namen von Warteereignissen, die von dieser Funktion zurückgegeben werden, sind die gleichen Namen, die von der Funktion `aurora_wait_report` zurückgegeben werden.

Beispiele

Im folgenden Beispiel sehen Sie Ergebnisse vom Aufruf der Funktion `aurora_stat_wait_event`.

```
=>  SELECT *
    FROM aurora_stat_wait_event();

 type_id | event_id  |               event_name
---------+-----------+-----------------------------------------
       1 |  16777216 | <unassigned:0>
       1 |  16777217 | ShmemIndexLock
       1 |  16777218 | OidGenLock
       1 |  16777219 | XidGenLock
.
.
.
       9 | 150994945 | PgSleep
       9 | 150994946 | RecoveryApplyDelay
      10 | 167772160 | BufFileRead
      10 | 167772161 | BufFileWrite
      10 | 167772162 | ControlFileRead
.
.
.
      10 | 167772226 | WALInitWrite
      10 | 167772227 | WALRead
      10 | 167772228 | WALSync
      10 | 167772229 | WALSyncMethodAssign
      10 | 167772230 | WALWrite
      10 | 167772231 | XactSync
.
.
```

```
.
      11 | 184549377 | LsnAllocate
```

Im folgenden Beispiel werden `aurora_stat_wait_type` und `aurora_stat_wait_event` zusammengeführt, um aus Gründen der Lesbarkeit Typnamen und Ereignisnamen zurückzugeben.

```
=> SELECT *
    FROM aurora_stat_wait_type() t
    JOIN aurora_stat_wait_event() e
      ON t.type_id = e.type_id;

 type_id | type_name | type_id | event_id  |                event_name
---------+-----------+---------+-----------+-------------------------------------------
       1 | LWLock    |       1 |  16777216 | <unassigned:0>
       1 | LWLock    |       1 |  16777217 | ShmemIndexLock
       1 | LWLock    |       1 |  16777218 | OidGenLock
       1 | LWLock    |       1 |  16777219 | XidGenLock
       1 | LWLock    |       1 |  16777220 | ProcArrayLock
.
.
.
       3 | Lock      |       3 |  50331648 | relation
       3 | Lock      |       3 |  50331649 | extend
       3 | Lock      |       3 |  50331650 | page
       3 | Lock      |       3 |  50331651 | tuple
.
.
.
      10 | IO        |      10 | 167772214 | TimelineHistorySync
      10 | IO        |      10 | 167772215 | TimelineHistoryWrite
      10 | IO        |      10 | 167772216 | TwophaseFileRead
      10 | IO        |      10 | 167772217 | TwophaseFileSync
.
.
.
      11 | LSN       |      11 | 184549376 | LsnDurable
```

aurora_stat_wait_type

Listet alle unterstützten Wartetypen für Aurora PostgreSQL auf.

Syntax

```
aurora_stat_wait_type()
```

Argumente

Keine

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- type_id – die ID des Warteereignistyps.
- type_name – name des Wartetyps.

Nutzungshinweise

Kombinieren Sie diese Funktion mit anderen Funktionen wie `aurora_stat_wait_event` und `aurora_stat_system_waits`, um Warteereignisnamen mit Warteereignistypen anstelle von IDs anzuzeigen. Namen von Wartetypen, die von dieser Funktion zurückgegeben werden, sind die gleichen Namen, die von der Funktion `aurora_wait_report` zurückgegeben werden.

Beispiele

Im folgenden Beispiel sehen Sie Ergebnisse vom Aufruf der Funktion `aurora_stat_wait_type`.

```
=> SELECT *
     FROM aurora_stat_wait_type();
 type_id | type_name
---------+-----------
       1 | LWLock
       3 | Lock
       4 | BufferPin
       5 | Activity
       6 | Client
       7 | Extension
       8 | IPC
       9 | Timeout
      10 | IO
      11 | LSN
```

aurora_version

Gibt den Zeichenfolgewert der Versionsnummer der PostgreSQL-kompatiblen Edition von Amazon Aurora zurück.

Syntax

```
aurora_version()
```

Argumente

Keine

Rückgabetyp

CHAR- oder VARCHAR-Zeichenfolge

Nutzungshinweise

Diese Funktion zeigt die Version der Datenbank-Engine der PostgreSQL-kompatiblen Edition von Amazon Aurora an. Die Versionsnummer wird als Zeichenfolge zurückgegeben im Format *major.minor.patch*. Weitere Informationen zu den Aurora-PostgreSQL-Versionsnummern erhalten Sie unter Aurora-Versionsnummer.

Sie können auswählen, wann Upgrades von Nebenversionen angewendet werden sollen, indem Sie das Wartungsfenster für Ihren Aurora-PostgreSQL-DB-Cluster festlegen. Um zu erfahren wie, siehe Warten eines Amazon Aurora-DB-Clusters.

Ab der Veröffentlichung der PostgreSQL-Versionen 13.3, 12.8, 11.13 und 10.18 und für alle späteren Versionen sind die Aurora-Versionsnummern genauer auf die PostgreSQL-Versionsnummern abgestimmt. Weitere Informationen zu allen Aurora-PostgreSQL-Versionen finden Sie unter Updates für Amazon Aurora PostgreSQL in den Versionshinweisen für Aurora PostgreSQL.

Beispiele

Das folgende Beispiel zeigt die Ergebnisse des Aufrufs der `aurora_version`-Funktion auf einem Aurora-PostgreSQL-DB-Cluster, der PostgreSQL 12.7, Aurora-PostgreSQL- Version 4.2 ausführt und dann die gleiche Funktion auf einem Cluster mit Aurora-PostgreSQL-Version 13.3 ausführt.

```
=> SELECT * FROM aurora_version();
aurora_version
```

```
----------------
 4.2.2
SELECT * FROM aurora_version();
aurora_version
----------------
 13.3.0
```

Dieses Beispiel zeigt, wie Sie die Funktion mit verschiedenen Optionen verwenden, um mehr über die Aurora-PostgreSQL-Version zu erfahren. Dieses Beispiel verwendet eine Aurora-Versionsnummer, die sich von der PostgreSQL-Versionsnummer unterscheidet.

```
=> SHOW SERVER_VERSION;
 server_version
----------------
 12.7
(1 row)

=> SELECT * FROM aurora_version();
aurora_version
----------------
 4.2.2
(1 row)

=> SELECT current_setting('server_version') AS "PostgreSQL Compatiblility";
PostgreSQL Compatiblility
--------------------------
 12.7
(1 row)

=> SELECT version() AS "PostgreSQL Compatiblility Full String";
PostgreSQL Compatiblility Full String
-------------------------------------------------------------------------------------------------
 PostgreSQL 12.7 on aarch64-unknown-linux-gnu, compiled by aarch64-unknown-linux-gnu-
gcc (GCC) 7.4.0, 64-bit
(1 row)

=> SELECT 'Aurora: '
    || aurora_version()
    || ' Compatible with PostgreSQL: '
    || current_setting('server_version') AS "Instance Version";
Instance Version
------------------------------------------------
```

```
 Aurora: 4.2.2 Compatible with PostgreSQL: 12.7
(1 row)
```

In diesem nächsten Beispiel wird die Funktion mit den gleichen Optionen wie im vorherigen Beispiel verwendet. Dieses Beispiel hat keine Aurora-Versionsnummer, die sich von der PostgreSQL-Versionsnummer unterscheidet.

```
=> SHOW SERVER_VERSION;
server_version
----------------
 13.3

=> SELECT * FROM aurora_version();
aurora_version
---------------
 13.3.0
=> SELECT current_setting('server_version') AS "PostgreSQL Compatiblility";
PostgreSQL Compatiblility
--------------------------
 13.3

=> SELECT version() AS "PostgreSQL Compatiblility Full String";
PostgreSQL Compatiblility Full String
-------------------------------------------------------------------------------------------------
 PostgreSQL 13.3 on x86_64-pc-linux-gnu, compiled by x86_64-pc-linux-gnu-gcc (GCC)
 7.4.0, 64-bit
=> SELECT 'Aurora: '
    || aurora_version()
    || ' Compatible with PostgreSQL: '
    || current_setting('server_version') AS "Instance Version";
Instance Version
-----------------------------------------------------
 Aurora: 13.3.0 Compatible with PostgreSQL: 13.3
```

aurora_volume_logical_start_lsn

Gibt die Log-Sequenznummer (LSN) zurück, die zur Identifizierung des Anfangs eines Datensatzes im Logical Write-Ahead Log (WAL)-Stream des Aurora-Cluster-Volumes verwendet wird.

Syntax

```
aurora_volume_logical_start_lsn()
```

Argumente

Keine

Rückgabetyp

`pg_lsn`

Nutzungshinweise

Diese Funktion identifiziert den Anfang des Datensatzes im logischen WAL-Stream für ein bestimmtes Aurora-Cluster-Volume. Sie können diese Funktion verwenden, während Sie ein Hauptversions-Upgrade durchführen, indem Sie logische Replikation und schnelles Klonen von Aurora verwenden, um zu ermitteln, an welcher LSN ein Snapshot oder ein Datenbankklon erstellt wird. Anschließend können Sie die logische Replikation verwenden, um die neueren Daten, die nach dem LSN aufgezeichnet wurden, kontinuierlich zu streamen und die Änderungen vom Publisher zum Subscriber zu synchronisieren.

Weitere Informationen zur Verwendung der logischen Replikation für ein Hauptversions-Upgrade finden Sie unter Verwenden der logischen Replikation, um ein Hauptversions-Upgrade für Aurora PostgreSQL durchzuführen.

Diese Funktion steht für die folgenden Versionen von Aurora PostgreSQL zur Verfügung:

- 15.2 und höhere 15-Versionen
- 14.3 und höhere 14-Versionen
- 13.6 und höhere 13-Versionen
- 12.10 und höhere 12-Versionen
- 11.15 und höhere 11-Versionen
- 10.20 und höhere 10-Versionen

Beispiele

Sie können die Log-Sequenznummer (LSN) mithilfe der folgenden Abfrage abrufen:

```
postgres=> SELECT aurora_volume_logical_start_lsn();
```

```
aurora_volume_logical_start_lsn
---------------
0/402E2F0
(1 row)
```

aurora_wait_report

Diese Funktion zeigt die Aktivität „Warteereignis“ über einen bestimmten Zeitraum an.

Syntax

```
aurora_wait_report([time])
```

Argumente

Zeit (optional)

Die Zeit in Sekunden. Der Standardwert beträgt 10 Sekunden.

Rückgabetyp

SETOF-Datensatz mit den folgenden Spalten:

- type_name – Name des Wartetyps
- event_name – Name des Warteereignisses
- wait – Anzahl der Warteereignisse
- wait_time – Wartezeit in Millisekunden
- ms_per_wait – durchschnittliche Millisekunden pro Anzahl eines Warteereignisses
- waits_per_xact – durchschnittliche Warteereignisse pro Anzahl einer Transaktion
- ms_per_xact – durchschnittliche Millisekunden nach Anzahl der Transaktionen

Nutzungshinweise

Diese Funktion ist ab Aurora-PostgreSQL-Release 1.1 verfügbar, die mit PostgreSQL 9.6.6 und höheren Versionen kompatibel ist.

Wenn Sie diese Funktion nutzen möchten, müssen Sie zuerst die Aurora-PostgreSQL-Erweiterung `aurora_stat_utils` wie folgt erstellen:

```
=> CREATE extension aurora_stat_utils;
CREATE EXTENSION
```

Weitere Informationen zu verfügbaren Aurora-PostgreSQL-Erweiterungsversionen finden Sie unter Erweiterungsversionen für Amazon Aurora PostgreSQL in den Versionshinweisen für Aurora PostgreSQL.

Diese Funktion berechnet die Warteereignisse auf Instance-Ebene, indem zwei Snapshots von Statistikdaten aus der Funktion aurora_stat_system_waits() und den Postgre-SQL-Statistikansichten pg_stat_database verglichen werden.

Weitere Informationen über `aurora_stat_system_waits()` und `pg_stat_database` finden Sie unter Die Statistikerfassung in der PostgreSQL-Dokumentation.

Wenn diese Funktion ausgeführt wird, erstellt sie einen ersten Snapshot, wartet die angegebene Anzahl von Sekunden und erstellt dann einen zweiten Snapshot. Die Funktion vergleicht die beiden Snapshots und gibt den Unterschied zurück. Dieser Unterschied stellt die Aktivität der Instance für dieses Zeitintervall dar.

In der Writer-Instance zeigt die Funktion auch die Anzahl der Transaktionen, für die ein Commit ausgeführt wurde, und TPS (Transaktionen pro Sekunde) an. Diese Funktion gibt Informationen auf Instance-Ebene zurück und enthält alle Datenbanken in der Instance.

Beispiele

Dieses Beispiel zeigt, wie die Erweiterung aurora_stat_utils erstellt wird, um die Funktion aurora_log_report verwenden zu können.

```
=> CREATE extension aurora_stat_utils;
CREATE EXTENSION
```

Dieses Beispiel zeigt, wie der Wartebericht 10 Sekunden lang überprüft wird.

```
=> SELECT *
     FROM aurora_wait_report();
NOTICE:  committed 34 transactions in 10 seconds (tps 3)
 type_name |    event_name     | waits | wait_time | ms_per_wait | waits_per_xact |
 ms_per_xact
-----------+-------------------+-------+-----------+-------------+----------------
+-------------
```

```
 Client    | ClientRead        |    26 |  30003.00 |    1153.961 |          0.76 |
 882.441
 Activity  | WalWriterMain     |    50 |  10051.32 |     201.026 |          1.47 |
 295.627
 Timeout   | PgSleep           |     1 |  10049.52 |   10049.516 |          0.03 |
 295.574
 Activity  | BgWriterHibernate |     1 |  10048.15 |   10048.153 |          0.03 |
 295.534
 Activity  | AutoVacuumMain    |    18 |   9941.66 |     552.314 |          0.53 |
 292.402
 Activity  | BgWriterMain      |     1 |    201.09 |     201.085 |          0.03 |
   5.914
 IO        | XactSync          |    15 |     25.34 |       1.690 |          0.44 |
   0.745
 IO        | RelationMapRead   |    12 |      0.54 |       0.045 |          0.35 |
   0.016
 IO        | WALWrite          |    84 |      0.21 |       0.002 |          2.47 |
   0.006
 IO        | DataFileExtend    |     1 |      0.02 |       0.018 |          0.03 |
   0.001
```

Dieses Beispiel zeigt, wie der Wartebericht 60 Sekunden lang überprüft wird.

```
=> SELECT *
     FROM aurora_wait_report(60);
NOTICE:  committed 1544 transactions in 60 seconds (tps 25)
 type_name |       event_name       |  waits  | wait_time | ms_per_wait |
 waits_per_xact | ms_per_xact
-----------+------------------------+---------+-----------+-------------
+----------------+-------------
 Lock      | transactionid          |    6422 | 477000.53 |      74.276 |
 4.16 |     308.938
 Client    | ClientRead             |    8265 | 270752.99 |      32.759 |
 5.35 |     175.358
 Activity  | CheckpointerMain       |       1 |  60100.25 |   60100.246 |
 0.00 |      38.925
 Timeout   | PgSleep                |       1 |  60098.49 |   60098.493 |
 0.00 |      38.924
 Activity  | WalWriterMain          |     296 |  60010.99 |     202.740 |
 0.19 |      38.867
 Activity  | AutoVacuumMain         |     107 |  59827.84 |     559.139 |
 0.07 |      38.749
```

```
Activity  | BgWriterMain           |     290 |  58821.83 |     202.834 |
0.19 |      38.097
IO        | XactSync               |    1295 |  55220.13 |      42.641 |
0.84 |      35.764
IO        | WALWrite               | 6602259 |  47810.94 |       0.007 |
4276.07 |      30.966
Lock      | tuple                  |     473 |  29880.67 |      63.173 |
0.31 |      19.353
LWLock    | buffer_mapping         |     142 |   3540.13 |      24.930 |
0.09 |       2.293
Activity  | BgWriterHibernate      |     290 |   1124.15 |       3.876 |
0.19 |       0.728
IO        | BufFileRead            |    7615 |    618.45 |       0.081 |
4.93 |       0.401
LWLock    | buffer_content         |      73 |    345.93 |       4.739 |
0.05 |       0.224
LWLock    | lock_manager           |      62 |    191.44 |       3.088 |
0.04 |       0.124
IO        | RelationMapRead        |      72 |      5.16 |       0.072 |
0.05 |       0.003
LWLock    | ProcArrayLock          |       1 |      2.01 |       2.008 |
0.00 |       0.001
IO        | ControlFileWriteUpdate |       2 |      0.03 |       0.013 |
0.00 |       0.000
IO        | DataFileExtend         |       1 |      0.02 |       0.018 |
0.00 |       0.000
IO        | ControlFileSyncUpdate  |       1 |      0.00 |       0.000 |
0.00 |       0.000
```

Amazon-Aurora-PostgreSQL-Parameter

Sie können Ihr Amazon-Aurora-DB-Cluster auf dieselbe Art und Weise verwalten, wie Sie Ihre anderen Amazon-RDS-DB-Instances verwalten, und zwar indem Sie die Parameter in einer DB-Parametergruppe verwenden. Amazon Aurora unterscheidet sich jedoch von Amazon RDS dadurch, dass ein Aurora-DB-Cluster mehrere DB-Instances hat. Einige der Parameter, mit denen Sie Ihren Amazon-Aurora-DB-Cluster verwalten, werden auf den gesamten Cluster angewendet, andere hingegen werden wie folgt nur auf eine bestimmte DB-Instance im DB-Cluster angewendet:

- DB-Cluster-Parametergruppe – Eine DB-Cluster-Parametergruppe enthält den Satz von Engine-Konfigurationsparametern, die für den gesamten Aurora-DB-Cluster gelten. Beispielsweise ist die Cluster-Cache-Verwaltung ein Feature eines Aurora-DB-Clusters, der von dem Parameter `apg_ccm_enabled` kontrolliert wird, der Teil der DB-Cluster-Parametergruppe ist. Die DB-Cluster-

Parametergruppe enthält auch Standardeinstellungen für die DB-Parametergruppe für die DB-Instances, aus denen der Cluster besteht.

- DB-Parametergruppe – Eine DB-Parametergruppe ist der Satz von Engine-Konfigurationswerten, die für eine bestimmte DB-Instance dieses Engine-Typs gelten. Die DB-Parametergruppen für die PostgreSQL-DB-Engine werden von einer RDS-for-PostgreSQL-DB-Instance und einem Aurora-PostgreSQL-DB-Cluster verwendet. Diese Konfigurationseinstellungen gelten für Eigenschaften, die je nach DB-Instances in einem Aurora-Cluster unterschiedlich sein können, z. B. Größe der Speicherpuffer.

Sie verwalten Parameter auf Clusterebene in DB-Clusterparametergruppen. Sie verwalten Parameter auf Instance-Ebene in DB-Parametergruppen. Sie können Parameter mit der Amazon RDS-Konsole AWS CLI, der oder der Amazon RDS-API verwalten. Es gibt separate Befehle für das Verwalten von Parametern auf der Cluster- und Instance-Ebene.

- Verwenden Sie den Befehl -group, um Parameter auf Clusterebene in einer DB-Cluster-Parametergruppe zu verwalten. modify-db-cluster-parameter AWS CLI
- Verwenden Sie den Befehl, um Parameter auf Instanzebene in einer DB-Parametergruppe für eine DB-Instance in einem DB-Cluster zu verwalten. modify-db-parameter-group AWS CLI

Weitere Informationen zu finden Sie AWS CLI unter Verwenden von AWS CLI im AWS Command Line Interface Benutzerhandbuch.

Weitere Informationen zu Parametergruppen finden Sie unter Arbeiten mit Parametergruppen.

Anzeigen von Aurora-PostgreSQL-DB-Cluster- und DB-Parametern

Sie können alle verfügbaren Standardparametergruppen für RDS-for-PostgreSQL-DB-Instances und für Aurora-PostgreSQL-DB-Cluster in der AWS Management Console anzeigen. Die Standardparametergruppen für alle DB-Engines und DB-Clustertypen und -versionen sind für jede AWS Region aufgeführt. Alle benutzerdefinierten Parametergruppen werden ebenfalls aufgeführt.

Anstatt sie in der anzusehen AWS Management Console, können Sie auch Parameter auflisten, die in DB-Cluster-Parametergruppen und DB-Parametergruppen enthalten sind, indem Sie die AWS CLI oder die Amazon RDS-API verwenden. Um beispielsweise Parameter in einer DB-Cluster-Parametergruppe aufzulisten, verwenden Sie den describe-db-cluster-parameters AWS CLI Befehl wie folgt:

```
aws rds describe-db-cluster-parameters --db-cluster-parameter-group-name
 default.aurora-postgresql12
```

Der Befehl gibt detaillierte JSON-Beschreibungen für jeden Parameter zurück. Sie können die Menge der zurückgegebenen Informationen reduzieren, indem Sie die Option `--query` verwenden. Beispielsweise können Sie den Parameternamen, seine Beschreibung und die zulässigen Werte für die standardmäßige Aurora-PostgreSQL-12-DB-Cluster-Parametergruppe wie folgt abrufen:

Für LinuxmacOS, oderUnix:

```
aws rds describe-db-cluster-parameters --db-cluster-parameter-group-name
 default.aurora-postgresql12 \
    --query 'Parameters[].
[{ParameterName:ParameterName,Description:Description,ApplyType:ApplyType,AllowedValues:Allowed
```

Windows:

```
aws rds describe-db-cluster-parameters --db-cluster-parameter-group-name
 default.aurora-postgresql12 ^
    --query "Parameters[].
[{ParameterName:ParameterName,Description:Description,ApplyType:ApplyType,AllowedValues:Allowed
```

Eine Aurora-DB-Cluster-Parametergruppe umfasst die DB-Instance-Parametergruppe und Standardwerte für eine bestimmte Aurora-DB-Engine. Sie können die Liste der DB-Parameter aus derselben Standardparametergruppe von Aurora PostgreSQL abrufen, indem Sie den folgenden describe-db-parameters AWS CLI Befehl verwenden.

FürLinux, oder: macOS Unix

```
aws rds describe-db-parameters --db-parameter-group-name default.aurora-postgresql12 \
    --query 'Parameters[].
[{ParameterName:ParameterName,Description:Description,ApplyType:ApplyType,AllowedValues:Allowed
```

Windows:

```
aws rds describe-db-parameters --db-parameter-group-name default.aurora-postgresql12 ^
    --query "Parameters[].
[{ParameterName:ParameterName,Description:Description,ApplyType:ApplyType,AllowedValues:Allowed
```

Die vorherigen Befehle geben Listen von Parametern aus dem DB-Cluster oder der DB-Parametergruppe mit Beschreibungen und anderen Details zurück, die in der Abfrage angegeben sind. Nachfolgend finden Sie eine Beispielantwort.


```
[
    [
        {
            "ParameterName": "apg_enable_batch_mode_function_execution",
            "ApplyType": "dynamic",
            "Description": "Enables batch-mode functions to process sets of rows at a
 time.",
            "AllowedValues": "0,1"
        }
    ],
    [
        {
            "ParameterName": "apg_enable_correlated_any_transform",
            "ApplyType": "dynamic",
            "Description": "Enables the planner to transform correlated ANY Sublink
 (IN/NOT IN subquery) to JOIN when possible.",
            "AllowedValues": "0,1"
        }
    ],...
```


Im Folgenden finden Sie Tabellen, die Werte für den standardmäßigen DB-Cluster-Parameter und den DB-Parameter für Aurora-PostgreSQL-Version 14 enthalten.

Aurora-PostgreSQL-Parameter auf Cluster-Ebene

Sie können die für eine bestimmte Aurora PostgreSQL-Version verfügbaren Parameter auf Clusterebene mithilfe der AWS Management-Konsole, der AWS CLI oder der Amazon RDS-API anzeigen. Weitere Informationen zum Anzeigen von Parametern in einer Parametergruppe des DB-Clusters von Aurora PostgreSQL finden Sie unter Anzeigen der Parameterwerte für eine DB-Cluster-Parametergruppe.

Einige Parameter auf Cluster-Ebene sind nicht in allen Versionen verfügbar und manche sind veraltet. Hinweise zum Anzeigen der Parameter einer bestimmten Aurora-PostgreSQL-Version finden Sie unter Anzeigen von Aurora-PostgreSQL-DB-Cluster- und DB-Parametern.

Die folgende Tabelle enthält beispielsweise die Parameter, die in der standardmäßigen DB-Cluster-Parametergruppe für Aurora PostgreSQL Version 14 verfügbar sind. Wenn Sie einen Aurora-PostgreSQL-DB-Cluster erstellen, ohne Ihre eigene benutzerdefinierte DB-Parametergruppe anzugeben, wird Ihr DB-Cluster mit der standardmäßigen Aurora-DB-Cluster-Parametergruppe für die gewählte Version erstellt, z. B. `default.aurora-postgresql14`, `default.aurora-postgresql13` usw.

Eine Auflistung der DB-Instance-Parameter für dieselbe Standard-DB-Cluster-Parametergruppe finden Sie unter Aurora-PostgreSQL-Parameter auf Instance-Ebene.

Parametername	Beschreibung	Standard
ansi_constraint_trigger_ordering	Ändern Sie die Ausführungsreihenfolge von Einschränkungsauslösern für Kompatibilität mit dem ANSI-SQL-Standard.	–
ansi_force_foreign_key_checks	Stellen Sie sicher, dass referenzielle Aktionen wie kaskadiertes Löschen oder kaskadiertes Aktualisieren immer ablaufen, unabhängig von den diversen Auslöserkontexten der Aktion.	–
ansi_qualified_update_set_target	Unterstützt Tabellen- und Schemaqualifizierer in UPDATE … SET-Anweisungen.	–
apg_ccm_enabled	Aktivieren oder deaktivieren Sie die Cluster-Cache-Verwaltung für den Cluster.	–

Parametername	Beschreibung	Standard
apg_enable_batch_mode_function_execution	Aktiviert Batch-Modus-Funktionen, um mehrere Zeilen gleichzeitig zu verarbeiten.	–
apg_enable_correlated_any_transform	Ermöglicht es dem Planer, korrelierte ANY-Sublinks (IN/NOT IN Unterabfrage) nach Möglichkeit in JOIN umzuwandeln.	–
apg_enable_function_migration	Ermöglicht dem Planer, berechtigte Skalarfunktionen in die FROM-Klausel zu migrieren.	–
apg_enable_not_in_transform	Ermöglicht es dem Planer, NOT IN-Unterabfragen nach Möglichkeit in ANTI JOIN umzuwandeln.	–
apg_enable_remove_redundant_inner_joins	Ermöglicht dem Planer, redundante Inner Joins zu entfernen.	–
apg_enable_semijoin_push_down	Ermöglicht die Verwendung von Semijoin-Filtern für Hash-Joins.	–
apg_plan_mgmt.capture_plan_baselines	Baseline-Modus für Planerfassung. Manuell – Planerfassung für jede SQL-Anweisung aktivieren. Aus – Planerfassung deaktivieren. Automatisch – Planerfassung für Anweisungen in pg_stat_statement aktivieren, die die Berechtigungskriterien erfüllen.	aus
apg_plan_mgmt.max_databases	Legt die maximale Anzahl von Datenbanken fest, die Abfragen mit apg_plan_mgmt verwalten können.	10
apg_plan_mgmt.max_plans	Legt die maximale Anzahl von Plänen fest, die von apg_plan_mgmt zwischengespeichert werden können.	10000

Parametername	Beschreibung	Standard
apg_plan_mgmt.plan_retention_period	Maximale Anzahl von Tagen, seit ein Plan zuletzt verwendet wurde, bevor ein Plan automatisch gelöscht wird.	32
apg_plan_mgmt.unapproved_plan_execution_threshold	Geschätzte Gesamtplankosten, unter denen ein nicht genehmigter Plan ausgeführt wird.	0
apg_plan_mgmt.use_plan_baselines	Verwenden Sie nur genehmigte oder feste Pläne für verwaltete Anweisungen.	false
application_name	Legt den Namen der Anwendung fest, der in Statistiken und Protokollen verwendet werden soll.	–
array_nulls	Ermöglicht die Eingabe von NULL-Elementen in Arrays.	–
aurora_compute_plan_id	Überwacht die Ausführungspläne für Abfragen, um die Ausführungspläne zu ermitteln, die zur aktuellen Datenbanklast beitragen, und um Leistungsstatistiken der Ausführungspläne im Zeitverlauf nachzuverfolgen. Weitere Informationen finden Sie unter Überwachen von Abfrageausführungsplänen für Aurora PostgreSQL.	on
authentication_timeout	(s) Legt die Zeit fest, die maximal zulässig ist, um die Client-Authentifizierung durchzuführen.	–
auto_explain.log_analyze	Verwenden Sie EXPLAIN ANALYZE zur Planprotokollierung.	–
auto_explain.log_buffers	Protokollieren der Puffernutzung.	–

Parametername	Beschreibung	Standard
auto_explain.log_format	EXPLAIN-Format, das für die Planprotokollierung verwendet werden soll.	–
auto_explain.log_min_duration	Legt die Mindestausführungszeit fest, ab der Pläne protokolliert werden.	–
auto_explain.log_nested_statements	Protokollieren verschachtelter Anweisungen.	–
auto_explain.log_timing	Erfasst Timing-Daten, nicht nur Zeilenzahlen.	–
auto_explain.log_triggers	Fügt Auslöserstatistiken in Pläne ein.	–
auto_explain.log_verbose	Verwenden Sie EXPLAIN VERBOSE zur Planprotokollierung.	–
auto_explain.sample_rate	Bruchteil der zu verarbeitenden Abfragen.	–
autovacuum	Startet den Untervorgang der Selbstbereinigung.	–
autovacuum_analyze_scale_factor	Anzahl von Tupel-Einfügungen, -Aktualisierungen oder -Löschungen vor der Analyse als Bruchteil von Reltupeln.	0.05
autovacuum_analyze_threshold	Mindestanzahl von Tupel-Einfügungen, -Aktualisierungen oder -Löschungen vor der Analyse.	–
autovacuum_freeze_max_age	Alter, bei dem eine Selbstbereinigung für eine Tabelle ausgeführt werden soll, um einen Transaktions-ID-Wraparound zu verhindern.	–

Parametername	Beschreibung	Standard
autovacuum_max_workers	Legt die maximale Anzahl gleichzeitig ausgeführter Worker-Vorgänge für die Selbstbereinigung fest.	AM BESTEN (DB InstanceClassMemory /64371566592 ,3)
autovacuum_multixact_freeze_max_age	Multixact-Alter, bei dem eine Tabelle sich selbst bereinigt, um Multixact-Wraparound zu verhindern.	–
autovacuum_naptime	(s) Inaktivitätszeit zwischen Selbstbereinigungen.	5
autovacuum_vacuum_cost_delay	(ms) Bereinigungskostenverzögerung in Millisekunden für die Selbstbereinigung.	5
autovacuum_vacuum_cost_limit	Bereinigungskostenbetrag für die Selbstbereinigung, der vor der Inaktivität verfügbar ist.	AM GRÖSSTEN (log (DB /21474836480) *600.200) InstanceClassMemory
autovacuum_vacuum_insert_scale_factor	Anzahl von Tupel-Einfügungen vor der Bereinigung als Bruchteil von Reltupeln.	–
autovacuum_vacuum_insert_threshold	Mindestanzahl von Tupel-Einfügungen vor der Bereinigung oder -1 zum Deaktivieren von Bereinigungen.	–
autovacuum_vacuum_scale_factor	Anzahl von Tupel-Aktualisierungen oder -Löschungen vor der Bereinigung als Bruchteil von Reltupeln.	0.1
autovacuum_vacuum_threshold	Mindestanzahl von Tupel-Aktualisierungen oder -Löschungen vor der Bereinigung.	–
autovacuum_work_mem	(kB) Legt den maximalen Arbeitsspeicher fest, der von jedem Selbstbereinigungs-Worker-Prozess verwendet werden soll.	AM GRÖSSTEN InstanceClassMemory (DB /32768 ,131072)

Parametername	Beschreibung	Standard
babelfishpg_tds.default_server_name	Der Standardname des Babelfish-Servers	Microsoft SQL Server
babelfishpg_tds.listen_adressen	Legt den Host-Namen oder die IP-Adresse(n) fest, die auf TDS überwacht werden sollen.	*
babelfishpg_tds.port	Legt den TDS-TCP-Port fest, den der Server überwacht.	1433
babelfishpg_tds.tds_debug_log_level	Legt die Protokollierungsstufe in TDS fest, 0 deaktiviert die Protokollierung	1
babelfishpg_tds.tds_default_numeric_precision	Legt die Standardgenauigkeit des numerischen Typs fest, der in den Metadaten der TDS-Spalte gesendet werden soll, wenn die Engine keine angibt.	38
babelfishpg_tds.tds_default_numeric_scale	Legt den Standardmaßstab des numerischen Typs fest, der in den Metadaten der TDS-Spalte gesendet werden soll, wenn die Engine keine angibt.	8
babelfishpg_tds.tds_default_packet_size	Legt die Standardpaketgröße für alle SQL.Server-Clients fest, die verbunden werden	4096
babelfishpg_tds.tds_default_protocol_version	Legt eine Standardversion des TDS-Protokolls für alle Clients fest, die verbunden werden	DEFAULT
babelfishpg_tds.tds_ssl_encrypt	Legt die SSL-Verschlüsselungsoption fest	0
babelfishpg_tds.tds_ssl_max_protocol_version	Legt die Höchstversion des SSL/TLS-Protokolls fest, die für die tds-Sitzung verwendet werden soll.	TLSv1.2

Parametername	Beschreibung	Standard
babelfishpg_tds.tds_ssl_min_protocol_version	Legt die Mindestversion des SSL/TLS-Protokolls fest, die für die tds-Sitzung verwendet werden soll.	TLSv1.2 ab Aurora PostgreSQL Version 16, TLSv1 für Versionen älter als Aurora PostgreSQL Version 16
babelfishpg_tsql.default_locale	Standardgebietsschema, das für Sortierungen verwendet wird, die von CREATE COLLATION erstellt wurden.	en-US
babelfishpg_tsql.migration_mode	Legt fest, ob mehrere Benutzerdatenbanken unterstützt werden	Multi-DB von Aurora PostgreSQL Version 16, Single-DB für Versionen älter als Aurora PostgreSQL Version 16
babelfishpg_tsql.server_colation_name	Name der Standardsortierung für den Server	sql_latin1_general_cp1_ci_as
babelfishpg_tsql.version	Legt die Ausgabe der Variablen @@VERSION fest	default
backend_flush_after	(8 Kb) Anzahl der Seiten, nach denen zuvor ausgeführte Schreibvorgänge auf die Festplatte geschrieben werden.	–
backslash_quote	Legt fest, ob \\ in Zeichenfolgeliteralen zulässig ist.	–
backtrace_functions	Protokollrückverfolgung für Fehler in diesen Funktionen.	–
bytea_output	Legt das Ausgabeformat für bytea fest.	–

Parametername	Beschreibung	Standard
check_function_bodies	Überprüft die Funktionstexte während CREATE FUNCTION.	–
client_connection_check_interval	Legt das Zeitintervall zwischen Prüfungen auf Verbindungsabbrüche während der Ausführung von Abfragen fest.	–
client_encoding	Legt die Zeichensatzkodierung des Clients fest.	UTF8
client_min_messages	Legt die Nachrichtenebenen fest, die an den Client gesendet werden.	–
compute_query_id	Abfrage-IDs berechnen.	auto
config_file	Legt die Hauptkonfigurationsdatei des Servers fest.	/rdsdbdata/config/postgresql.conf
constraint_exclusion	Ermöglicht dem Planer die Verwendung von Einschränkungen, um Abfragen zu optimieren.	–
cpu_index_tuple_cost	Legt die Schätzung des Planers für die Kosten der Verarbeitung der einzelnen Indexeinträge während einer Indexprüfung fest.	–
cpu_operator_cost	Legt die Schätzung des Planers für die Kosten der Verarbeitung der einzelnen Operator- oder Funktionsaufrufe fest.	–
cpu_tuple_cost	Legt die Schätzung des Planers für die Kosten der Verarbeitung der einzelnen Tupeln (Zeilen) fest.	–
cron.database_name	Legt die Datenbank fest, um pg_cron-Metadatentabellen zu speichern	postgres
cron.log_run	Protokolliert alle Aufträge in der Tabelle job_run_details	on

Parametername	Beschreibung	Standard
cron.log_statement	Protokolliert alle Cron-Anweisungen vor der Ausführung.	aus
cron.max_running_jobs	Die maximale Anzahl von Aufträgen, die gleichzeitig ausgeführt werden können.	5
cron.use_background_workers	Aktiviert Hintergrund-Workers für pg_cron	on
cursor_tuple_fraction	Legt die Schätzung des Planers für den Bruchteil der Zeilen eines Cursors fest, die abgerufen werden.	–
data_directory	Legt das Datenverzeichnis des Servers fest.	/rdsdbdata/db
datestyle	Legt das Anzeigeformat für Datum- und Uhrzeitwerte fest.	–
db_user_namespace	Aktiviert Benutzernamen pro Datenbank.	–
deadlock_timeout	(ms) Legt die Zeit fest, die während einer Sperre gewartet wird, bevor auf einen Deadlock geprüft wird.	–
debug_pretty_print	Erstellt Einschübe für Analyse- und Planstrukturanzeigen.	–
debug_print_parse	Protokolliert die Analysestruktur der einzelnen Abfragen.	–
debug_print_plan	Protokolliert den Ausführungsplan der einzelnen Abfragen.	–
debug_print_rewritten	Protokolliert die neu geschriebene Analysestruktur der einzelnen Abfragen.	–
default_statistics_target	Legt das Standardstatistikziel fest.	–

Parametername	Beschreibung	Standard
default_tablespace	Legt den Standardtabellenraum fest, in dem Tabellen und Indexe erstellt werden.	–
default_toast_compression	Legt die Standardkomprimierungsmethode für komprimierbare Werte fest.	–
default_transaction_deferrable	Legt den Standardaufschiebbarkeitsstatus neuer Transaktionen fest.	–
default_transaction_isolation	Legt die Transaktionsisolierungsstufe jeder neuen Transaktion fest.	–
default_transaction_read_only	Legt den Standardschreibschutzstatus neuer Transaktionen fest.	–
effective_cache_size	(8 kB) Legt die Annahme des Planers hinsichtlich der Größe des Datenträger-Caches fest.	SUMME (DB /12038, -50003) InstanceClassMemory
effective_io_concurrency	Die Anzahl der gleichzeitigen Anfragen, die durch das Datenträgersubsystem effizient bearbeitet werden können.	–
enable_async_append	Ermöglicht den Planern die Verwendung paralleler Append-Pläne.	–
enable_bitmapscan	Ermöglicht die Verwendung von Bitmap-Prüfungsplänen durch den Planer.	–
enable_gathermerge	Ermöglicht die Verwendung von Gather-Merge-Plänen durch den Planer.	–
enable_hashagg	Ermöglicht die Verwendung von Hash-Aggregationsplänen durch den Planer.	–
enable_hashjoin	Ermöglicht die Verwendung von Hash-Join-Plänen durch den Planer.	–

Parametername	Beschreibung	Standard
enable_incremental_sort	Ermöglicht den Planern die Verwendung inkrementeller Sortierschritte.	–
enable_indexonlyscan	Ermöglicht den Planern die Verwendung von Plänen. index-only-scan	–
enable_indexscan	Ermöglicht die Verwendung von Indexprüfungsplänen durch den Planer.	–
enable_material	Ermöglicht die Verwendung von Materialisierung durch den Planer.	–
enable_memoize	Ermöglicht den Planern die Verwendung der Speicherung	–
enable_mergejoin	Ermöglicht die Verwendung von Merge-Join-Plänen durch den Planer.	–
enable_nestloop	Ermöglicht die Verwendung von Join-Plänen mit verschachtelten Schleifen durch den Planer.	–
enable_parallel_append	Ermöglicht den Planern die Verwendung paralleler Append-Pläne.	–
enable_parallel_hash	Ermöglicht den Planern die Verwendung paralleler Hash-Pläne.	–
enable_partition_pruning	Aktivieren Sie das Bereinigen von Planzeit- und Laufzeitpartitionen.	–
enable_partitionwise_aggregate	Ermöglicht die partitionsweise Aggregation und Gruppierung.	–
enable_partitionwise_join	Aktiviert partitionsweise Joins.	–
enable_seqscan	Ermöglicht die Verwendung von sequenziellen Prüfungsplänen durch den Planer.	–

Parametername	Beschreibung	Standard
enable_sort	Ermöglicht die Verwendung von expliziten Sortierschritten durch den Planer.	–
enable_tidscan	Ermöglicht die Verwendung von TID-Prüfungsplänen durch den Planer.	–
escape_string_warning	Warnt vor Escape-Notierungen mit Backslash in gewöhnlichen Zeichenfolgeliteralen.	–
exit_on_error	Beendet die Sitzung bei einem Fehler.	–
extra_float_digits	Legt die Anzahl der Stellen fest, die für Gleitkommawerte angezeigt werden.	–
force_parallel_mode	Erzwingt die Verwendung paralleler Abfrageeinrichtungen.	–
from_collapse_limit	Legt die Größe der FROM-Liste fest, jenseits der Unterabfragen nicht ausgeblendet werden.	–
geqo	Ermöglicht die genetische Abfrageoptimierung.	–
geqo_effort	GEQO: Der Aufwand, der verwendet wird, um den Standard für andere GEQO-Parameter festzulegen.	–
geqo_generations	GEQO: Die Zahl der Iterationen des Algorithmus.	–
geqo_pool_size	GEQO: Die Anzahl der Personen in der Population.	–
geqo_seed	GEQO: Der Seed für die zufällige Pfadauswahl.	–
geqo_selection_bias	GEQO: Selektiver Druck innerhalb der Population.	–

Parametername	Beschreibung	Standard
geqo_threshold	Legt den Schwellenwert für FROM-Elemente fest, jenseits derer GEQO verwendet wird.	–
gin_fuzzy_search_limit	Legt das maximal zulässige Ergebnis für die exakte Suche durch GIN fest.	–
gin_pending_list_limit	(kB) Legt die maximale Größe der ausstehen den Liste für den GIN-Index fest.	–
hash_mem_multiplier	Vielfaches von work_mem für Hash-Tabellen.	–
hba_file	Legt die hba-Konfigurationsdatei des Servers fest.	/rdsdbdata/config/ pg_hba.conf
hot_standby_feedback	Ermöglicht Feedback von einem Hot Standby zum primären, um Abfragekonflikte zu vermeiden.	on
huge_pages	Reduziert den Overhead, wenn eine DB-Instan ce mit großen, zusammenhängenden Arbeitssp eicherblöcken arbeitet, wie sie von gemeinsam genutzten Puffern verwendet werden. Der Parameter ist standardmäßig für alle DB-Instan ce-Klassen aktiviert, außer t3.medium, db.t3.lar ge, db.t4g.medium, db.t4g.large.	on
ident_file	Legt die ident-Konfigurationsdatei des Servers fest.	/rdsdbdata/config/ pg_ident.conf
idle_in_transactio n_session_timeout	(ms) Legt die maximal zulässige Dauer von Leerlauftransaktionen fest.	86400000
idle_session_timeout	Beendet jede Sitzung, die länger als die angegebene Zeitspanne im Leerlauf ist (d. h. auf eine Client-Abfrage gewartet hat), sich jedoch nicht innerhalb einer offenen Transakti on befindet	–

Parametername	Beschreibung	Standard
intervalstyle	Legt das Anzeigeformat für Intervallwerte fest.	–
join_collapse_limit	Legt die Größe der FROM-Liste fest, jenseits der JOIN-Konstrukte nicht auf eine Ebene gebracht werden.	–
krb_caseins_users	Legt fest, ob Generic Security Service API (GSSAPI)-Benutzernamen ohne Berücksichtigung von Groß- und Kleinschreibung behandelt werden sollen (true) oder nicht. Standardmäßig ist dieser Parameter auf false festgelegt, sodass Kerberos erwartet, dass bei Benutzernamen zwischen Groß- und Kleinschreibung unterschieden wird. Weitere Informationen finden Sie unter GSSAPI-Authentifizierung in der PostgreSQL-Dokumentation.	false
lc_messages	Legt die Sprache fest, in der Nachrichten angezeigt werden.	–
lc_monetary	Legt das Gebietsschema für die Formatierung von monetären Beträgen fest.	–
lc_numeric	Legt das Gebietsschema für die Formatierung von Zahlen fest.	–
lc_time	Legt das Gebietsschema für die Formatierung von Datum- und Uhrzeitwerten fest.	–
listen_addresses	Legt den Host-Namen oder die IP-Adresse(n) fest, auf die gewartet werden soll.	*
lo_compat_privileges	Aktiviert den Abwärtskompatibilitätsmodus für Berechtigungsprüfungen für große Objekte.	0

Parametername	Beschreibung	Standard
log_autovacuum_min_duration	(ms) Legt die Mindestausführungszeit fest, jenseits der Aktionen für die Selbstbereinigung protokolliert werden.	10000
log_connections	Protokolliert jede erfolgreiche Verbindung.	–
log_destination	Legt das Ziel für die Serverprotokollausgabe fest.	stderr
log_directory	Legt das Zielverzeichnis für Protokolldateien fest.	/rdsdbdata/log/error
log_disconnections	Protokolliert das Ende einer Sitzung einschließlich der Dauer.	–
log_duration	Protokolliert die Dauer jeder abgeschlossenen SQL-Anweisung.	–
log_error_verbosity	Legt die Ausführlichkeit protokollierter Nachrichten fest.	–
log_executor_stats	Schreibt die Leistungsstatistik des Executors in das Serverprotokoll.	–
log_file_mode	Legt die Dateiberechtigungen für Protokolldateien fest.	0644
log_filename	Legt das Dateinamenmuster für Protokolldateien fest.	postgresql.log.%Y-%m-%d-%H%M
logging_collector	Startet einen Unterprozess, um die stderr-Ausgabe und/oder csvlogs in Protokolldateien zu erfassen.	1
log_hostname	Protokolliert den Hostnamen in den Verbindungsprotokollen.	0

Parametername	Beschreibung	Standard
logical_decoding_work_mem	(kB) So viel Speicher kann von jedem internen Neuordnungspuffer genutzt werden, bevor er auf die Festplatte geschrieben wird.	–
log_line_prefix	Steuert Informationen, die jeder Protokollzeile vorangestellt sind.	%t:%r:%u@%d:%p]:
log_lock_waits	Protokolliert lange Sperrenwartezeiten.	–
log_min_duration_sample	(ms) Legt die Mindestausführungszeit fest, jenseits der stichprobenartig Anweisungen protokolliert werden. Das Sampling wird durch log_statement_sample_rate bestimmt.	–
log_min_duration_statement	(ms) Legt die Mindestausführungszeit fest, jenseits der Anweisungen protokolliert werden.	–
log_min_error_statement	Veranlasst, dass alle Anweisungen, die einen Fehler auf oder jenseits dieser Stufe generieren, protokolliert werden.	–
log_min_messages	Legt die Nachrichtenebenen fest, die protokolliert werden.	–
log_parameter_max_length	(B) Beim Protokollieren von Anweisungen werden die protokollierten Parameterwerte auf die ersten N Byte beschränkt.	–
log_parameter_max_length_on_error	(B) Bei der Meldung eines Fehlers werden die protokollierten Parameterwerte auf die ersten N Byte beschränkt.	–
log_parser_stats	Schreibt die Leistungsstatistik des Parsers in das Serverprotokoll.	–
log_planner_stats	Schreibt die Leistungsstatistik des Planers in das Serverprotokoll.	–

Parametername	Beschreibung	Standard
log_replication_commands	Protokolliert jeden Replikationsbefehl.	–
log_rotation_age	(min) Die automatische Protokolldateirotation wird nach N Minuten ausgeführt.	60
log_rotation_size	(kB) Die automatische Protokolldateirotation wird nach N Kilobyte ausgeführt.	100000
log_statement	Legt den Typ der protokollierten Anweisungen fest.	–
log_statement_sample_rate	Anteil der Anweisungen, die log_min_duration_sample überschreiten, die protokolliert werden sollen.	–
log_statement_stats	Schreibt kumulative Leistungsstatistiken in das Serverprotokoll.	–
log_temp_files	(kB) Protokolliert die Verwendung temporärer Dateien, die größer als diese Kilobyte-Angabe sind.	–
log_timezone	Legt die Zeitzone fest, die in Protokoll meldungen verwendet werden soll.	UTC
log_transaction_sample_rate	Legt den Anteil der neuen Transaktionen fest, die protokolliert werden sollen.	–
log_truncate_on_rotation	Kürzt vorhandene Protokolldateien mit demselben Namen während der Protokoll rotation.	0
maintenance_io_concurrency	Eine Variante von effective_io_concurrency, die für Wartungsarbeiten verwendet wird.	1

Parametername	Beschreibung	Standard
maintenance_work_mem	(kB) Legt den maximalen Arbeitsspeicher fest, der für Wartungsoperationen verwendet werden darf.	AM BESTEN (DB InstanceClassMemory /63963136 *1024,65536)
max_connections	Legt die maximale Anzahl gleichzeitiger Verbindungen fest.	AM WENIGSTEN (InstanceClassMemoryDB /9531392 .5000)
max_files_per_process	Legt die maximale Anzahl gleichzeitig geöffneter Dateien für die einzelnen Serverprozesse fest.	–
max_locks_per_transaction	Legt die maximale Anzahl von Sperren pro Transaktion fest.	64
max_logical_replication_workers	Maximale Anzahl von Worker-Prozessen für logische Replikation.	–
max_parallel_maintenance_workers	Legt die maximale Anzahl von parallelen Vorgängen pro Wartungsvorgang fest.	–
max_parallel_workers	Legt die maximale Anzahl von parallelen Workers fest, die gleichzeitig aktiv sein können.	GREATEST($DBInstanceVCPU/2, 8)
max_parallel_workers_per_gather	Legt die maximale Anzahl von parallelen Prozessen pro Executor-Knoten fest.	–
max_pred_locks_per_page	Legt die maximale Anzahl von prädikats gesperrten Tupeln pro Seite fest.	–
max_pred_locks_per_relation	Legt die maximale Anzahl von prädikats gesperrten Seiten und Tupeln pro Beziehung fest.	–
max_pred_locks_per_transaction	Legt die maximale Anzahl von Prädikatssperren pro Transaktion fest.	–

Parametername	Beschreibung	Standard
max_prepared_transactions	Legt die maximale Anzahl gleichzeitig vorbereiteter Transaktionen fest.	0
max_replication_slots	Legt die maximale Anzahl von Replikations-Slots fest, die der Server unterstützen kann.	20
max_slot_wal_keep_size	(MB) Replikations-Slots werden als fehlgeschlagen gekennzeichnet und Segmente werden zum Löschen oder Recycling freigegeben, wenn WAL auf der Festplatte so viel Speicherplatz belegt.	–
max_stack_depth	(kB) Legt die maximale Stack-Tiefe in Kilobytes fest.	6144
max_standby_streaming_delay	(ms) Legt die maximale Verzögerung fest, bevor Abfragen storniert werden, wenn ein Hot Standby-Server gestreamte WAL-Daten verarbeitet.	14000
max_sync_workers_per_subscription	Maximale Anzahl von Synchronisations-Workers pro Abonnement	2
max_wal_senders	Legt die maximale Anzahl gleichzeitig ausgeführter WAL-Senderprozesses fest.	10
max_worker_processes	Legt die maximale Anzahl gleichzeitiger Worker-Prozesse fest.	GREATEST($DBInstanceVCPU*2, 8)
min_dynamic_shared_memory	(MB) Menge des dynamischen gemeinsam genutzten Speichers, der beim Start reserviert wurde.	–
min_parallel_index_scan_size	(8 kB) Legt die Mindestmenge an Indexdaten für einen parallelen Scan fest.	–

Parametername	Beschreibung	Standard
min_parallel_table_scan_size	(8 kB) Legt die Mindestmenge an Tabellendaten für einen parallelen Scan fest.	–
old_snapshot_threshold	(min) Zeit, bis ein Snapshot zu alt ist, um Seiten zu lesen, die nach dem Erstellen des Snapshots geändert wurden.	–
orafce.nls_date_format	Emuliert das Datumsausgabeverhalten von Oracle.	–
orafce.timezone	Gibt die für die Funktion sysdate verwendete Zeitzone an.	–
parallel_leader_participation	Steuert, ob Gather und Gather Merge auch Unterpläne ausführen.	–
parallel_setup_cost	Legt die Kostenschätzung des Planers für das Starten von Worker-Prozessen für parallele Abfragen fest.	–
parallel_tuple_cost	Legt die Kostenschätzung des Planers für die Übergabe von Tupeln (Zeilen) von Worker auf Haupt-Backend fest.	–
password_encryption	Verschlüsselt Passwörter.	–
pgaudit.log	Gibt an, welche Klassen von Anweisungen durch die Sitzungsprüfungs-Protokollierung protokolliert werden.	–
pgaudit.log_catalog	Gibt an, dass die Sitzungsprotokollierung aktiviert werden soll, wenn sich alle Beziehungen in einer Anweisung in pg_catalog befinden.	–
pgaudit.log_level	Gibt die Protokollstufe an, die für Protokolleinträge verwendet wird.	–

Parametername	Beschreibung	Standard
pgaudit.log_parameter	Gibt an, dass die Audit-Protokollierung die Parameter enthalten sollte, die mit der Anweisung übergeben wurden.	–
pgaudit.log_relation	Gibt an, ob die Sitzungsprüfungs-Protokollierung für jede Beziehung (TABLE, VIEW usw.), auf die in einer SELECT- oder DML-Anweisung verwiesen wird, einen separaten Protokolleintrag erstellen soll.	–
pgaudit.log_statement_once	Gibt an, ob die Protokollierung den Anweisungstext und die Parameter mit dem ersten Protokolleintrag für eine Kombination aus Anweisung/Unteranweisung oder bei jedem Eintrag enthält.	–
pgaudit.role	Gibt die Hauptrolle an, die für die Objektüberwachungsprotokollierung verwendet werden soll.	–
pg_bigm.enable_recheck	Gibt an, ob Recheck durchgeführt werden soll, was ein interner Prozess der Volltextsuche ist.	on
pg_bigm.gin_key_limit	Gibt die maximale Anzahl von Bigrammen des Suchschlüsselworts an, das für die Volltextsuche verwendet werden soll.	0
pg_bigm.last_update	Meldet das letzte Aktualisierungsdatum des pg_bigm-Moduls.	2013.11.22
pg_bigm.similarity_limit	Es gibt den Mindestschwellenwert an, der von der Ähnlichkeitssuche verwendet wird.	0.3
pg_hint_plan.debug_print	Protokolliert Ergebnisse der Hinweisanalyse.	–

Parametername	Beschreibung	Standard
pg_hint_plan.enable_hint	Zwingt Planer zur Verwendung der Pläne, die im Hinweiskommentar vor der Abfrage angegeben sind.	–
pg_hint_plan.enable_hint_table	Zwingt Planer, Hinweise nicht über Tabellensuchen zu erhalten.	–
pg_hint_plan.message_level	Nachrichtenebene von Debug-Meldungen.	–
pg_hint_plan.parse_messages	Nachrichtenebene von Analysefehlern.	–
pglogical.batch_inserts	Batch-Inserts wenn möglich	–
pglogical.conflict_log_level	Legt die Protokollstufe gelöster Konflikte fest	–
pglogical.conflict_resolution	Legt die Methode zur Konfliktlösung für lösbare Konflikte fest.	–
pglogical.extra_connection_options	Verbindungsoptionen zum Hinzufügen zu allen Peer-Knotenverbindungen	–
pglogical.synchronous_commit	Spezifischer synchroner Commit-Wert für pglogical	–
pglogical.use_spi	Verwenden Sie SPI anstelle der Low-Level-API zum Anwenden von Änderungen	–
pgtle.client_auth_databases_to_skip	Liste der Datenbanken, die für die Clientauth-Funktion übersprungen werden sollen.	–
pgtle.clientauth_db_name	Steuert, welche Datenbank für die Clientauth-Funktion verwendet wird.	–

Parametername	Beschreibung	Standard
pgtle.clientauth_num_parallel_workers	Anzahl der Hintergrund-Worker, die für die Clientauth-Funktion verwendet werden.	–
pgtle.clientauth_users_to_skip	Liste der Benutzer, die für die Clientauth-Funktion übersprungen werden sollen.	–
pgtle.enable_clientauth	Aktiviert die Clientauth-Funktion.	–
pgtle.passcheck_db_name	Legt fest, welche Datenbank für die clusterweite Passcheck-Funktion verwendet wird.	–
pg_prewarm.autoprewarm	Startet den autoprewarm-Worker.	–
pg_prewarm.autoprewarm_interval	Legt das Intervall zwischen Sicherungen freigegebener Puffer fest	–
pg_similarity.block_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.block_threshold	Legt den Schwellenwert fest, der von der Block-Ähnlichkeitsfunktion verwendet wird.	–
pg_similarity.block_tokenizer	Legt den Tokenizer für die Block-Ähnlichkeitsfunktion fest.	–
pg_similarity.cosine_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.cosine_threshold	Legt den Schwellenwert fest, der von der Kosinus-Ähnlichkeitsfunktion verwendet wird.	–
pg_similarity.cosine_tokenizer	Legt den Tokenizer für die Kosinus-Ähnlichkeitsfunktion fest.	–
pg_similarity.dice_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–

Parametername	Beschreibung	Standard
pg_similarity.dice_threshold	Legt den Schwellenwert fest, der vom Dice-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.dice_tokenizer	Legt den Tokenizer für das Dice-Ähnlichkeitsmaß fest.	–
pg_similarity.euclidean_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.euclidean_threshold	Legt den Schwellenwert fest, der vom euklidischen Ähnlichkeitsmaß verwendet wird.	–
pg_similarity.euclidean_tokenizer	Legt den Tokenizer für das euklidische Ähnlichkeitsmaß fest.	–
pg_similarity.hamming_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.hamming_threshold	Legt den Schwellenwert fest, der von der Block-Ähnlichkeitsmetrik verwendet wird.	–
pg_similarity.jaccard_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.jaccard_threshold	Legt den Schwellenwert fest, der vom Jaccard-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.jaccard_tokenizer	Legt den Tokenizer für das Jaccard-Ähnlichkeitsmaß fest.	–
pg_similarity.jaro_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.jaro_threshold	Legt den Schwellenwert fest, der vom Jaro-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.jarowinkler_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–

Parametername	Beschreibung	Standard
pg_similarity.jaro winkler_threshold	Legt den Schwellenwert fest, der vom Jaro-Winkler-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.leve nshtein_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.leve nshtein_threshold	Legt den Schwellenwert fest, der vom Levenshtein-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.matc hing_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.matc hing_threshold	Legt den Schwellenwert fest, der vom Matching-Koeffizient-Ähnlichkeitsmaß verwendet wird.	–
pg_similarity.matc hing_tokenizer	Legt den Tokenizer für das Matching-Koeffizie nt-Ähnlichkeitsmaß fest.	–
pg_similarity.mong eelkan_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.mong eelkan_threshold	Legt den Schwellenwert fest, der vom Monge-Elkan-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.mong eelkan_tokenizer	Legt den Tokenizer für das Monge-Elkan-Ähnlic hkeitsmaß fest.	–
pg_similarity.nw_g ap_penalty	Legt den Lückenabzug fest, der vom Ähnlichke itsmaß Needleman-Wunsch verwendet wird.	–
pg_similarity.nw_i s_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.nw_t hreshold	Legt den Schwellenwert fest, der vom Ähnlichkeitsmaß Needleman-Wunsch verwendet wird.	–

Parametername	Beschreibung	Standard
pg_similarity.overlap_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.overlap_threshold	Legt den Schwellenwert fest, der vom Überschneidungskoeffizient-Ähnlichkeitsmaß verwendet wird.	–
pg_similarity.overlap_tokenizer	Legt den Tokenizer für das Überschneidungskoeffizient-Ähnlichkeitsmaß fest.	–
pg_similarity.qgram_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.qgram_threshold	Legt den Schwellenwert fest, der vom Q-Gram-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.qgram_tokenizer	Legt den Tokenizer für die Q-Gram-Messung fest.	–
pg_similarity.swg_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.swg_threshold	Legt den Schwellenwert fest, der vom Smith-Waterman-Gotoh-Ähnlichkeitsmaß verwendet wird.	–
pg_similarity.sw_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.sw_threshold	Legt den Schwellenwert fest, der vom Smith-Waterman-Ähnlichkeitsmaß verwendet wird	–
pg_stat_statements.max	Legt die maximale Anzahl von Anweisungen fest, die von pg_stat_statements verfolgt werden.	–

Parametername	Beschreibung	Standard
pg_stat_statements.save	Speichert pg_stat_statements-Statistiken über Serverausfälle hinweg.	–
pg_stat_statements.track	Wählt aus, welche Anweisungen von pg_stat_statements verfolgt werden.	–
pg_stat_statements.track_planning	Wählt aus, ob die Planungsdauer von pg_stat_statements verfolgt wird.	–
pg_stat_statements.track_utility	Wählt aus, ob Dienstprogrammbefehle von pg_stat_statements verfolgt werden.	–
plan_cache_mode	Steuert die Planerauswahl des benutzerdefinierten oder generischen Plans.	–
port	Legt den TCP-Port fest, den der Server überwacht.	EndPointPort
postgis.gdal_enabled_drivers	Aktiviert oder deaktiviert GDAL-Treiber, die mit PostGIS in Postgres 9.3.5 und höher verwendet werden.	ENABLE_ALL
quote_all_identifiers	Fügt beim Generieren von SQL-Fragmenten allen Bezeichnern Anführungszeichen hinzu.	–
random_page_cost	Legt die Schätzung des Planers für die Kosten einer nicht sequenziell abgerufenen Datenträgerseite fest.	–
rdkit.dice_threshold	Unterer Schwellenwert der Dice-Ähnlichkeit. Moleküle mit einer Ähnlichkeit unter dem Schwellenwert sind durch die Operation # nicht ähnlich.	–

Parametername	Beschreibung	Standard
rdkit.do_chiral_sss	Ob Stereochemie beim Unterstrukturabgleich berücksichtigt wird. Bei false werden keine Stereochemie-Informationen für den Unterstru kturabgleich verwendet.	–
rdkit.tanimoto_thr eshold	Unterer Schwellenwert der Tanimoto-Ähnlichke it. Moleküle mit einer Ähnlichkeit unter dem Schwellenwert sind durch die Operation % nicht ähnlich.	–
rds.accepted_passw ord_auth_method	Erzwingt die Authentifizierung für Verbindungen mit lokal gespeichertem Passwort.	md5+scram
rds.adaptive_autov acuum	RDS-Parameter zum Aktivieren/Deaktivieren der adaptiven Selbstbereinigung.	1
rds.babelfish_status	RDS-Parameter zum Aktivieren/Deaktivieren von Babelfish-for-Aurora-PostgreSQL.	aus
rds.enable_plan_ma nagement	Aktivieren oder deaktivieren der apg_plan_ mgmt-Erweiterung.	0

Parametername	Beschreibung	Standard
rds.extensions	Liste von Erweiterungen, die RDS zur Verfügung stellt	address_standardizer, address_standardizer_data_us, apg_plan_mgmt, aurora_stat_utils, amcheck, autoinc, aws_commons, aws_ml, aws_s3, aws_lambda, bool_plperl, bloom, btree_gin, btree_gist, citext, cube, dblink, dict_int, dict_xsyn, earthdistance, fuzzystrmatch, hll, hstore, hstore_plperl, insert_username, intagg, intarray, ip4r, isn, jsonb_plperl, lo, log_fdw, ltree, moddatetime, old_snapshot, oracle_fdw, orafce, pgaudit, pgcrypto, pglogical, pgrouting, pgrowlocks, pgstattuple, pgtap, pg_bigm, pg_buffercache, pg_cron, pg_freespacemap, pg_hint_plan, pg_partman, pg_prewarm, pg_proctab, pg_repack, pg_simila

Parametername	Beschreibung	Standard
		rity, pg_stat_s tatements, pg_trgm, pg_visibility, plcoffee, plls, plperl, plpgsql, plprofiler, pltcl, plv8, postgis, postgis_t iger_geocoder, postgis_raster, postgis_topology, postgres_fdw, prefix, rdkit, rds_tools, refint, sslinfo, tablefunc, tds_fdw, test_parser, tsm_system_rows, tsm_system_time, unaccent, uuid-ossp
rds.force_admin_lo gging_level	Siehe Protokollmeldungen für RDS-Admin-Benutzeraktionen in Kundendatenbanken.	–
rds.force_autovacu um_logging_level	Siehe Protokollmeldungen zu Selbstber einigungsvorgängen.	WARNING
rds.force_ssl	SSL-Verbindungen erzwingen.	0

Parametername	Beschreibung	Standard
rds.global_db_rpo	(s) Der Schwellenwert für das Recovery Point Objective in Sekunden, der bei Überschreitungen Commits von Benutzern blockiert. **Important** Dieser Parameter ist für Aurora-PostgreSQL-basierte globale Datenbanken vorgesehen. Belassen Sie für eine nicht-globale Datenbank den Standardwert. Weitere Informationen zur Nutzung dieses Parameters finden Sie unter the section called “Verwalten von RPOs für Aurora PostgreSQL–basierte globale Datenbanken”.	–
rds.logical_replication	Aktiviert die logische Dekodierung.	0
rds.logically_replicate_unlogged_tables	Nicht protokollierte Tabellen werden logisch repliziert.	1
rds.log_retention_period	Amazon RDS löscht PostgreSQL-Protokolle, die älter als N Minuten sind.	4320
rds.pg_stat_ramdisk_size	Größe der Ramdisk-Statistiken in MB. Ein Wert ungleich Null richtet die Ramdisk ein. Dieser Parameter ist nur für Aurora-PostgreSQL-14-Versionen und niedriger verfügbar.	0
rds.rds_superuser_reserved_connections	Legt die Anzahl der Verbindungs-Slots fest, die für rds_superusers reserviert sind. Dieser Parameter ist nur in den Versionen 15 und früher verfügbar. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation für reservierte Verbindungen.	2

Parametername	Beschreibung	Standard
rds.restrict_password_commands	Beschränkt passwortbezogene Befehle auf Mitglieder von rds_password	–
rds.superuser_variables	Liste der reinen Superuser-Variablen, für die wir die Änderungsanweisungen von rds_superuser erhöhen.	session_replication_role
recovery_init_sync_method	Legt die Methode zum Synchronisieren des Datenverzeichnisses vor der Wiederherstellung nach Abstürzen fest.	syncfs
remove_temp_files_after_crash	Entfernt temporäre Dateien nach dem Backend-Absturz.	0
restart_after_crash	Initialisiert den Server nach dem Backend-Absturz neu.	–
row_security	Aktiviert Zeilensicherheit.	–
search_path	Legt die Schemasuchreihenfolge für Namen fest, die nicht schemaqualifiziert sind.	–
seq_page_cost	Legt die Schätzung des Planers für die Kosten einer sequenziell abgerufenen Datenträgerseite fest.	–
session_replication_role	Legt das Sitzungsverhalten für Auslöser und Neuschreibungsregeln fest.	–
shared_buffers	(8 kB) Legt die maximale Anzahl freigegebener Arbeitsspeicherpuffer fest, die vom Server verwendet werden.	SUMME (DBInstanceClassMemory /12038, -50003)
shared_preload_libraries	Listet freigegebene Bibliotheken auf, die in den Server vorgeladen werden.	pg_stat_statements
ssl	Ermöglicht SSL-Verbindungen.	1

Parametername	Beschreibung	Standard
ssl_ca_file	Speicherort der SSL-Server-Zertifizierungss tellendatei.	/rdsdbdata/rds-met adata/ca-cert.pem
ssl_cert_file	Speicherort der SSL-Serverzertifikatdatei.	/rdsdbdata/rds-met adata/server-cert.pem
ssl_ciphers	Legt die Liste der zulässigen TLS-Versc hlüsselungen fest, die für sichere Verbindungen verwendet werden sollen.	–
ssl_crl_dir	Speicherort des Verzeichnisses der SSL-Zerti fikatsperrliste.	/rdsdbdata/rds-met adata/ssl_crl_dir/
ssl_key_file	Speicherort der privaten Schlüsseldatei des SSL-Servers	/rdsdbdata/rds-met adata/server-key.pem
ssl_max_protocol_v ersion	Legt die maximal zulässige SSL-/TLS-Protokoll version fest	–
ssl_min_protocol_v ersion	Legt die zulässige Mindestversion des SSL-/ TLS-Protokolls fest	TLSv1.2
standard_conformin g_strings	Veranlasst Zeichenfolgen „...“, Backslashes als Zeichen zu behandeln.	–
statement_timeout	(ms) Legt die maximal zulässige Dauer von Anweisungen fest.	–
stats_temp_directory	Schreibt temporäre Statistikdateien in das angegebene Verzeichnis.	/rdsdbdata/db/pg_s tat_tmp
superuser_reserved _connections	Legt die Anzahl der Verbindungs-Slots fest, die für Superusers reserviert sind.	3
synchronize_seqsca ns	Ermöglicht synchronisierte sequenzielle Prüfungen.	–

Parametername	Beschreibung	Standard
synchronous_commit	Legt die Synchronisierungsstufe aktueller Transaktionen fest.	on
tcp_keepalives_count	Maximale Anzahl von TCP-Keepalive-Neuü bertragungen.	–
tcp_keepalives_idle	(s) Zeit zwischen der Ausgabe von TCP-Keepa lives.	–
tcp_keepalives_int erval	(s) Zeit zwischen der Ausgabe von TCP-Keepa live-Neuübertragungen.	–
temp_buffers	(8 kB) Legt die maximale Anzahl der temporäre n Puffer fest, die von den einzelnen Sitzungen verwendet werden.	–
temp_file_limit	Schränkt den Gesamtspeicherplatz in Kilobyte ein, den ein bestimmter PostgreSQL-Prozess für temporäre Dateien verwenden kann, ausschließlich von Speicherplatz, der für explizite temporäre Tabellen verwendet wird	-1
temp_tablespaces	Legt die Tabellenräume fest, die für temporäre Tabellen und Sortierdateien verwendet werden sollen.	–
Zeitzone	Legt die Zeitzone für die Anzeige und Interpret ation von Zeitstempeln fest.	UTC
track_activities	Sammelt Informationen zu Befehlen, die ausgeführt werden.	–
track_activity_que ry_size	Legt die für pg_stat_activity.current_query reservierte Größe in Bytes fest.	4096
track_commit_times tamp	Erfasst den Commit-Zeitpunkt der Transaktion.	–

Parametername	Beschreibung	Standard
track_counts	Sammelt Statistiken zur Datenbankaktivität.	–
track_functions	Sammelt Statistiken auf Funktionsebene zur Datenbankaktivität.	pl
track_io_timing	Erfasst Zeitpunktstatistiken zur Datenbank-E/A-Aktivität.	1
track_wal_io_timing	Erfasst Zeitpunktstatistiken zur WAL-E/A-A ktivität.	–
transform_null_equals	Behandelt expr=NULL als expr IS NULL.	–
update_process_title	Aktualisiert den Titel des Vorgangs, um den aktiven SQL-Befehl anzuzeigen.	–
vacuum_cost_delay	(ms) Bereinigungskostenverzögerung in Millisekunden.	–
vacuum_cost_limit	Bereinigungskostenbetrag, der vor der Inaktivit ät verfügbar ist.	–
vacuum_cost_page_d irty	Bereinigungskosten für eine Seite, die durch eine Bereinigung ungültig wurde.	–
vacuum_cost_page_h it	Bereinigungskosten für eine Seite, die im Puffer-Cache gefunden wurde.	–
vacuum_cost_page_m iss	Bereinigungskosten für eine Seite, die nicht im Puffer-Cache gefunden wurde.	0
vacuum_defer_clean up_age	Anzahl der Transaktionen, um die VACUUM und HOT Cleanup aufgeschoben werden sollen, wenn vorhanden.	–
vacuum_failsafe_age	Alter, bei dem der VACUUM-Vorgang die Ausfallsicherheit auslösen sollte, um einen Wraparound-Ausfall zu vermeiden.	1200000000

Parametername	Beschreibung	Standard
vacuum_freeze_min_age	Mindestalter, bei dem der VACUUM-Vorgang eine Tabellenzeile eingefroren werden sollte.	–
vacuum_freeze_table_age	Alter, bei dem der VACUUM-Vorgang eine Tabelle vollständig scannen sollte, um Tupel einzufrieren.	–
vacuum_multixact_failsafe_age	Multixact-Alter, bei dem der VACUUM-Vorgang die Ausfallsicherheit auslösen sollte, um einen Wraparound-Ausfall zu vermeiden.	1200000000
vacuum_multixact_freeze_min_age	Mindestalter, ab dem VACUUM eine Zahl MultiXactId in einer Tabellenzeile einfrieren soll.	–
vacuum_multixact_freeze_table_age	Multixact-Alter, bei dem der VACUUM-Vorgang eine Tabelle vollständig scannen sollte, um Tupel einzufrieren.	–
wal_buffers	(8 kB) Legt die Anzahl von Datenträger-Seiten puffern im freigegebenen Arbeitsspeicher für WAL fest.	–
wal_receiver_create_temp_slot	Legt fest, ob ein WAL-Receiver einen temporären Replikations-Slot erstellen soll, wenn kein permanenter Slot konfiguriert ist.	0
wal_receiver_status_interval	(s) Legt das maximale Intervall zwischen den Statusberichten des WAL-Receivers auf den primären Wert fest.	–
wal_receiver_timeout	(ms) Legt die maximale Wartezeit fest, um Daten von der Primär-Instance zu empfangen.	30000
wal_sender_timeout	(ms) Legt fest, wie lange höchstens auf die WAL-Replikation gewartet wird.	–

Parametername	Beschreibung	Standard
work_mem	(kB) Legt den maximalen Arbeitsspeicher fest, der für Abfrage-Workspaces verwendet werden darf.	–
xmlbinary	Legt die Kodierung von Binärwerten in XML fest.	–
xmloption	Legt fest, ob XML-Daten in impliziten Parsing- und Serialisierungsoperationen als Dokumente oder Inhaltsfragmente betrachtet werden sollen.	–

Aurora-PostgreSQL-Parameter auf Instance-Ebene

Sie können die für eine bestimmte Aurora PostgreSQL-Version verfügbaren Parameter auf Instance-Ebene mithilfe der AWS Management-Konsole, der AWS CLI oder der Amazon RDS-API anzeigen. Weitere Informationen zum Anzeigen von Parametern in einer DB-Parametergruppe von Aurora PostgreSQL finden Sie unter Anzeigen von Parameterwerten für eine DB-Parametergruppe.

Einige Parameter auf Instance-Ebene sind nicht in allen Versionen verfügbar und manche sind veraltet. Hinweise zum Anzeigen der Parameter einer bestimmten Aurora-PostgreSQL-Version finden Sie unter Anzeigen von Aurora-PostgreSQL-DB-Cluster- und DB-Parametern.

In der folgenden Tabelle werden beispielsweise alle Parameter aufgeführt, die für eine bestimmte DB-Instance in einem DB-Cluster von Aurora PostgreSQL gelten. Diese Liste wurde generiert, indem der describe-db-parameters AWS CLI Befehl mit `default.aurora-postgresql14` für den Wert ausgeführt wurde. `--db-parameter-group-name`

Eine Auflistung der DB-Cluster-Parameter für dieselbe Standard-DB-Parametergruppe finden Sie unter Aurora-PostgreSQL-Parameter auf Cluster-Ebene.

Parametername	Beschreibung	Standard
apg_enable_batch_mode_function_execution	Aktiviert Batch-Modus-Funktionen, um mehrere Zeilen gleichzeitig zu verarbeiten.	–
apg_enable_correlated_any_transform	Ermöglicht es dem Planer, korrelierte ANY-Sublinks (IN/NOT IN Unterabfrage) nach Möglichkeit in JOIN umzuwandeln.	–
apg_enable_function_migration	Ermöglicht dem Planer, berechtigte Skalarfunktionen in die FROM-Klausel zu migrieren.	–
apg_enable_not_in_transform	Ermöglicht es dem Planer, NOT IN-Unterabfragen nach Möglichkeit in ANTI JOIN umzuwandeln.	–
apg_enable_remove_redundant_inner_joins	Ermöglicht dem Planer, redundante Inner Joins zu entfernen.	–

Parametername	Beschreibung	Standard
apg_enable_semijoin_push_down	Ermöglicht die Verwendung von Semijoin-Filtern für Hash-Joins.	–
apg_plan_mgmt.capture_plan_baselines	Baseline-Modus für Planerfassung. Manuell – Planerfassung für jede SQL-Anweisung aktivieren. Aus – Planerfassung deaktivieren. Automatisch – Planerfassung für Anweisungen in pg_stat_statement aktivieren, die die Berechtigungskriterien erfüllen.	aus
apg_plan_mgmt.max_databases	Legt die maximale Anzahl von Datenbanken fest, die Abfragen mit apg_plan_mgmt verwalten können.	10
apg_plan_mgmt.max_plans	Legt die maximale Anzahl von Plänen fest, die von apg_plan_mgmt zwischengespeichert werden können.	10000
apg_plan_mgmt.plan_retention_period	Maximale Anzahl von Tagen, seit ein Plan zuletzt verwendet wurde, bevor ein Plan automatisch gelöscht wird.	32
apg_plan_mgmt.unapproved_plan_execution_threshold	Geschätzte Gesamtplankosten, unter denen ein nicht genehmigter Plan ausgeführt wird.	0
apg_plan_mgmt.use_plan_baselines	Verwenden Sie nur genehmigte oder feste Pläne für verwaltete Anweisungen.	false
application_name	Legt den Namen der Anwendung fest, der in Statistiken und Protokollen verwendet werden soll.	–

Parametername	Beschreibung	Standard
aurora_compute_plan_id	Überwacht die Ausführungspläne für Abfragen, um die Ausführungspläne zu ermitteln, die zur aktuellen Datenbanklast beitragen, und um Leistungsstatistiken der Ausführungspläne im Zeitverlauf nachzuverfolgen. Weitere Informationen finden Sie unter Überwachen von Abfrageausführungsplänen für Aurora PostgreSQL.	on
authentication_timeout	(s) Legt die Zeit fest, die maximal zulässig ist, um die Client-Authentifizierung durchzuführen.	–
auto_explain.log_analyze	Verwenden Sie EXPLAIN ANALYZE zur Planprotokollierung.	–
auto_explain.log_buffers	Protokollieren der Puffernutzung.	–
auto_explain.log_format	EXPLAIN-Format, das für die Planprotokollierung verwendet werden soll.	–
auto_explain.log_min_duration	Legt die Mindestausführungszeit fest, ab der Pläne protokolliert werden.	–
auto_explain.log_nested_statements	Protokollieren verschachtelter Anweisungen.	–
auto_explain.log_timing	Erfasst Timing-Daten, nicht nur Zeilenzahlen.	–
auto_explain.log_triggers	Fügt Auslöserstatistiken in Pläne ein.	–
auto_explain.log_verbose	Verwenden Sie EXPLAIN VERBOSE zur Planprotokollierung.	–

Parametername	Beschreibung	Standard
auto_explain.sample_rate	Bruchteil der zu verarbeitenden Abfragen.	–
babelfishpg_tds.listen_adressen	Legt den Host-Namen oder die IP-Adresse(n) fest, die auf TDS überwacht werden sollen.	*
babelfishpg_tds.tds_debug_log_level	Legt die Protokollierungsstufe in TDS fest, 0 deaktiviert die Protokollierung	1
backend_flush_after	(8 Kb) Anzahl der Seiten, nach denen zuvor ausgeführte Schreibvorgänge auf die Festplatte geschrieben werden.	–
bytea_output	Legt das Ausgabeformat für bytea fest.	–
check_function_bodies	Überprüft die Funktionstexte während CREATE FUNCTION.	–
client_connection_check_interval	Legt das Zeitintervall zwischen Prüfungen auf Verbindungsabbrüche während der Ausführung von Abfragen fest.	–
client_min_messages	Legt die Nachrichtenebenen fest, die an den Client gesendet werden.	–
config_file	Legt die Hauptkonfigurationsdatei des Servers fest.	/rdsdbdata/config/postgresql.conf
constraint_exclusion	Ermöglicht dem Planer die Verwendung von Einschränkungen, um Abfragen zu optimieren.	–
cpu_index_tuple_cost	Legt die Schätzung des Planers für die Kosten der Verarbeitung der einzelnen Indexeinträge während einer Indexprüfung fest.	–

Parametername	Beschreibung	Standard
cpu_operator_cost	Legt die Schätzung des Planers für die Kosten der Verarbeitung der einzelnen Operator- oder Funktionsaufrufe fest.	–
cpu_tuple_cost	Legt die Schätzung des Planers für die Kosten der Verarbeitung der einzelnen Tupeln (Zeilen) fest.	–
cron.database_name	Legt die Datenbank fest, um pg_cron-Metadatentabellen zu speichern	postgres
cron.log_run	Protokolliert alle Aufträge in der Tabelle job_run_details	on
cron.log_statement	Protokolliert alle Cron-Anweisungen vor der Ausführung.	aus
cron.max_running_jobs	Die maximale Anzahl von Aufträgen, die gleichzeitig ausgeführt werden können.	5
cron.use_background_workers	Aktiviert Hintergrund-Workers für pg_cron	on
cursor_tuple_fraction	Legt die Schätzung des Planers für den Bruchteil der Zeilen eines Cursors fest, die abgerufen werden.	–
db_user_namespace	Aktiviert Benutzernamen pro Datenbank.	–
deadlock_timeout	(ms) Legt die Zeit fest, die während einer Sperre gewartet wird, bevor auf einen Deadlock geprüft wird.	–
debug_pretty_print	Erstellt Einschübe für Analyse- und Planstruk turanzeigen.	–

Parametername	Beschreibung	Standard
debug_print_parse	Protokolliert die Analysestruktur der einzelnen Abfragen.	–
debug_print_plan	Protokolliert den Ausführungsplan der einzelnen Abfragen.	–
debug_print_rewritten	Protokolliert die neu geschriebene Analysest ruktur der einzelnen Abfragen.	–
default_statistics _target	Legt das Standardstatistikziel fest.	–
default_transactio n_deferrable	Legt den Standardaufschiebbarkeitsstatus neuer Transaktionen fest.	–
default_transactio n_isolation	Legt die Transaktionsisolierungsstufe jeder neuen Transaktion fest.	–
default_transactio n_read_only	Legt den Standardschreibschutzstatus neuer Transaktionen fest.	–
effective_cache_size	(8 kB) Legt die Annahme des Planers hinsichtl ich der Größe des Datenträger-Caches fest.	SUMME (DB) InstanceClassMemor y /12038, -50003
effective_io_concu rrency	Die Anzahl der gleichzeitigen Anfragen, die durch das Datenträgersubsystem effizient bearbeitet werden können.	–
enable_async_append	Ermöglicht den Planern die Verwendung paralleler Append-Pläne.	–
enable_bitmapscan	Ermöglicht die Verwendung von Bitmap-Pr üfungsplänen durch den Planer.	–
enable_gathermerge	Ermöglicht die Verwendung von Gather-Merge-Plänen durch den Planer.	–

Parametername	Beschreibung	Standard
enable_hashagg	Ermöglicht die Verwendung von Hash-Aggregationsplänen durch den Planer.	–
enable_hashjoin	Ermöglicht die Verwendung von Hash-Join-Plänen durch den Planer.	–
enable_incremental_sort	Ermöglicht den Planern die Verwendung inkrementeller Sortierschritte.	–
enable_indexonlyscan	Ermöglicht den Planern die Verwendung von Plänen. index-only-scan	–
enable_indexscan	Ermöglicht die Verwendung von Indexprüfungsplänen durch den Planer.	–
enable_material	Ermöglicht die Verwendung von Materialisierung durch den Planer.	–
enable_memoize	Ermöglicht den Planern die Verwendung der Speicherung	–
enable_mergejoin	Ermöglicht die Verwendung von Merge-Join-Plänen durch den Planer.	–
enable_nestloop	Ermöglicht die Verwendung von Join-Plänen mit verschachtelten Schleifen durch den Planer.	–
enable_parallel_append	Ermöglicht den Planern die Verwendung paralleler Append-Pläne.	–
enable_parallel_hash	Ermöglicht den Planern die Verwendung paralleler Hash-Pläne.	–
enable_partition_pruning	Aktivieren Sie das Bereinigen von Planzeit- und Laufzeitpartitionen.	–
enable_partitionwise_aggregate	Ermöglicht die partitionsweise Aggregation und Gruppierung.	–

Parametername	Beschreibung	Standard
enable_partitionwise_join	Aktiviert partitionsweise Joins.	–
enable_seqscan	Ermöglicht die Verwendung von sequenziellen Prüfungsplänen durch den Planer.	–
enable_sort	Ermöglicht die Verwendung von expliziten Sortierschritten durch den Planer.	–
enable_tidscan	Ermöglicht die Verwendung von TID-Prüfungsplänen durch den Planer.	–
escape_string_warning	Warnt vor Escape-Notierungen mit Backslash in gewöhnlichen Zeichenfolgeliteralen.	–
exit_on_error	Beendet die Sitzung bei einem Fehler.	–
force_parallel_mode	Erzwingt die Verwendung paralleler Abfrageeinrichtungen.	–
from_collapse_limit	Legt die Größe der FROM-Liste fest, jenseits der Unterabfragen nicht ausgeblendet werden.	–
geqo	Ermöglicht die genetische Abfrageoptimierung.	–
geqo_effort	GEQO: Der Aufwand, der verwendet wird, um den Standard für andere GEQO-Parameter festzulegen.	–
geqo_generations	GEQO: Die Zahl der Iterationen des Algorithmus.	–
geqo_pool_size	GEQO: Die Anzahl der Personen in der Population.	–
geqo_seed	GEQO: Der Seed für die zufällige Pfadauswahl.	–

Parametername	Beschreibung	Standard
geqo_selection_bias	GEQO: Selektiver Druck innerhalb der Population.	–
geqo_threshold	Legt den Schwellenwert für FROM-Elemente fest, jenseits derer GEQO verwendet wird.	–
gin_fuzzy_search_limit	Legt das maximal zulässige Ergebnis für die exakte Suche durch GIN fest.	–
gin_pending_list_limit	(kB) Legt die maximale Größe der ausstehen den Liste für den GIN-Index fest.	–
hash_mem_multiplier	Vielfaches von work_mem für Hash-Tabellen.	–
hba_file	Legt die hba-Konfigurationsdatei des Servers fest.	/rdsdbdata/config/ pg_hba.conf
hot_standby_feedback	Ermöglicht Feedback von einem Hot Standby zum primären, um Abfragekonflikte zu vermeiden.	on
ident_file	Legt die ident-Konfigurationsdatei des Servers fest.	/rdsdbdata/config/ pg_ident.conf
idle_in_transactio n_session_timeout	(ms) Legt die maximal zulässige Dauer von Leerlauftransaktionen fest.	86400000
idle_session_timeout	Beendet jede Sitzung, die länger als die angegebene Zeitspanne im Leerlauf ist (d. h. auf eine Client-Abfrage gewartet hat), sich jedoch nicht innerhalb einer offenen Transakti on befindet	–
join_collapse_limit	Legt die Größe der FROM-Liste fest, jenseits der JOIN-Konstrukte nicht auf eine Ebene gebracht werden.	–

Parametername	Beschreibung	Standard
lc_messages	Legt die Sprache fest, in der Nachrichten angezeigt werden.	–
listen_addresses	Legt den Host-Namen oder die IP-Adresse(n) fest, auf die gewartet werden soll.	*
lo_compat_privileges	Aktiviert den Abwärtskompatibilitätsmodus für Berechtigungsprüfungen für große Objekte.	0
log_connections	Protokolliert jede erfolgreiche Verbindung.	–
log_destination	Legt das Ziel für die Serverprotokollausgabe fest.	stderr
log_directory	Legt das Zielverzeichnis für Protokolldateien fest.	/rdsdbdata/log/error
log_disconnections	Protokolliert das Ende einer Sitzung einschlie ßlich der Dauer.	–
log_duration	Protokolliert die Dauer jeder abgeschlossenen SQL-Anweisung.	–
log_error_verbosity	Legt die Ausführlichkeit protokollierter Nachricht en fest.	–
log_executor_stats	Schreibt die Leistungsstatistik des Executors in das Serverprotokoll.	–
log_file_mode	Legt die Dateiberechtigungen für Protokoll dateien fest.	0644
log_filename	Legt das Dateinamenmuster für Protokoll dateien fest.	postgresql.log.%Y-%m-%d-%H%M
logging_collector	Startet einen Unterprozess, um die stderr-Au sgabe und/oder csvlogs in Protokolldateien zu erfassen.	1

Parametername	Beschreibung	Standard
log_hostname	Protokolliert den Hostnamen in den Verbindungsprotokollen.	0
logical_decoding_work_mem	(kB) So viel Speicher kann von jedem internen Neuordnungspuffer genutzt werden, bevor er auf die Festplatte geschrieben wird.	–
log_line_prefix	Steuert Informationen, die jeder Protokollzeile vorangestellt sind.	%t:%r:%u@%d:%p]:
log_lock_waits	Protokolliert lange Sperrenwartezeiten.	–
log_min_duration_sample	(ms) Legt die Mindestausführungszeit fest, jenseits der Anweisungen stichprobenartig protokolliert werden. Das Sampling wird durch log_statement_sample_rate bestimmt.	–
log_min_duration_statement	(ms) Legt die Mindestausführungszeit fest, jenseits der Anweisungen protokolliert werden.	–
log_min_error_statement	Veranlasst, dass alle Anweisungen, die einen Fehler auf oder jenseits dieser Stufe generieren, protokolliert werden.	–
log_min_messages	Legt die Nachrichtenebenen fest, die protokolliert werden.	–
log_parameter_max_length	(B) Beim Protokollieren von Anweisungen werden die protokollierten Parameterwerte auf die ersten N Byte beschränkt.	–
log_parameter_max_length_on_error	(B) Bei der Meldung eines Fehlers werden die protokollierten Parameterwerte auf die ersten N Byte beschränkt.	–
log_parser_stats	Schreibt die Leistungsstatistik des Parsers in das Serverprotokoll.	–

Parametername	Beschreibung	Standard
log_planner_stats	Schreibt die Leistungsstatistik des Planers in das Serverprotokoll.	–
log_replication_commands	Protokolliert jeden Replikationsbefehl.	–
log_rotation_age	(min) Die automatische Protokolldateirotation wird nach N Minuten ausgeführt.	60
log_rotation_size	(kB) Die automatische Protokolldateirotation wird nach N Kilobyte ausgeführt.	100000
log_statement	Legt den Typ der protokollierten Anweisungen fest.	–
log_statement_sample_rate	Anteil der Anweisungen, die log_min_duration_sample überschreiten, die protokolliert werden sollen.	–
log_statement_stats	Schreibt kumulative Leistungsstatistiken in das Serverprotokoll.	–
log_temp_files	(kB) Protokolliert die Verwendung temporärer Dateien, die größer als diese Kilobyte-Angabe sind.	–
log_timezone	Legt die Zeitzone fest, die in Protokoll meldungen verwendet werden soll.	UTC
log_truncate_on_rotation	Kürzt vorhandene Protokolldateien mit demselben Namen während der Protokoll rotation.	0
maintenance_io_concurrency	Eine Variante von effective_io_concurrency, die für Wartungsarbeiten verwendet wird.	1

Parametername	Beschreibung	Standard
maintenance_work_mem	(kB) Legt den maximalen Arbeitsspeicher fest, der für Wartungsoperationen verwendet werden darf.	AM BESTEN (DB /63963136 *1024,65536) InstanceClassMemory
max_connections	Legt die maximale Anzahl gleichzeitiger Verbindungen fest.	AM WENIGSTEN (DB InstanceClassMemory /9531392 .5000)
max_files_per_process	Legt die maximale Anzahl gleichzeitig geöffneter Dateien für die einzelnen Serverprozesse fest.	–
max_locks_per_transaction	Legt die maximale Anzahl von Sperren pro Transaktion fest.	64
max_parallel_maintenance_workers	Legt die maximale Anzahl von parallelen Vorgängen pro Wartungsvorgang fest.	–
max_parallel_workers	Legt die maximale Anzahl von parallelen Workers fest, die gleichzeitig aktiv sein können.	GREATEST($DBInstanceVCPU/2, 8
max_parallel_workers_per_gather	Legt die maximale Anzahl von parallelen Prozessen pro Executor-Knoten fest.	–
max_pred_locks_per_page	Legt die maximale Anzahl von prädikats gesperrten Tupeln pro Seite fest.	–
max_pred_locks_per_relation	Legt die maximale Anzahl von prädikats gesperrten Seiten und Tupeln pro Beziehung fest.	–
max_pred_locks_per_transaction	Legt die maximale Anzahl von Prädikatssperren pro Transaktion fest.	–

Parametername	Beschreibung	Standard
max_slot_wal_keep_size	(MB) Replikationsslots werden als fehlgeschlagen gekennzeichnet und Segmente zum Löschen oder Recycling freigegeben, wenn WAL auf der Festplatte so viel Speicherplatz belegt.	–
max_stack_depth	(kB) Legt die maximale Stack-Tiefe in Kilobyte fest.	6144
max_standby_streaming_delay	(ms) Legt die maximale Verzögerung fest, bevor Abfragen storniert werden, wenn ein Hot-Standby-Server gestreamte WAL-Daten verarbeitet.	14000
max_worker_processes	Legt die maximale Anzahl gleichzeitiger Worker-Prozesse fest.	GREATEST($DBInstanceVCPU*2, 8
min_dynamic_shared_memory	(MB) Menge des dynamischen gemeinsam genutzten Speichers, der beim Start reserviert wurde.	–
min_parallel_index_scan_size	(8 kB) Legt die Mindestmenge an Indexdaten für einen parallelen Scan fest.	–
min_parallel_table_scan_size	(8 kB) Legt die Mindestmenge an Tabellendaten für einen parallelen Scan fest.	–
old_snapshot_threshold	(min) Zeit, bis ein Snapshot zu alt ist, um Seiten zu lesen, die nach dem Erstellen des Snapshots geändert wurden.	–
parallel_leader_participation	Steuert, ob Gather und Gather Merge auch Unterpläne ausführen.	–

Parametername	Beschreibung	Standard
parallel_setup_cost	Legt die Kostenschätzung des Planers für das Starten von Worker-Prozessen für parallele Abfragen fest.	–
parallel_tuple_cost	Legt die Kostenschätzung des Planers für die Übergabe von Tupeln (Zeilen) von Worker auf Haupt-Backend fest.	–
pgaudit.log	Gibt an, welche Klassen von Anweisungen durch die Sitzungsprüfungs-Protokollierung protokolliert werden.	–
pgaudit.log_catalog	Gibt an, dass die Sitzungsprotokollierung aktiviert werden soll, wenn sich alle Beziehungen in einer Anweisung in pg_catalog befinden.	–
pgaudit.log_level	Gibt die Protokollstufe an, die für Protokolleinträge verwendet wird.	–
pgaudit.log_parameter	Gibt an, dass die Audit-Protokollierung die Parameter enthalten sollte, die mit der Anweisung übergeben wurden.	–
pgaudit.log_relation	Gibt an, ob die Sitzungsprüfungs-Protokollierung für jede Beziehung (TABLE, VIEW usw.), auf die in einer SELECT- oder DML-Anweisung verwiesen wird, einen separaten Protokolleintrag erstellen soll.	–
pgaudit.log_statement_once	Gibt an, ob die Protokollierung den Anweisungstext und die Parameter mit dem ersten Protokolleintrag für eine Kombination aus Anweisung/Unteranweisung oder bei jedem Eintrag enthält.	–

Parametername	Beschreibung	Standard
pgaudit.role	Gibt die Hauptrolle an, die für die Objektüberwachungsprotokollierung verwendet werden soll.	–
pg_bigm.enable_recheck	Gibt an, ob Recheck durchgeführt werden soll, was ein interner Prozess der Volltextsuche ist.	on
pg_bigm.gin_key_limit	Gibt die maximale Anzahl von Bigrammen des Suchschlüsselworts an, das für die Volltextsuche verwendet werden soll.	0
pg_bigm.last_update	Meldet das letzte Aktualisierungsdatum des pg_bigm-Moduls.	2013.11.22
pg_bigm.similarity_limit	Es gibt den Mindestschwellenwert an, der von der Ähnlichkeitssuche verwendet wird.	0.3
pg_hint_plan.debug_print	Protokolliert Ergebnisse der Hinweisanalyse.	–
pg_hint_plan.enable_hint	Zwingt Planer zur Verwendung der Pläne, die im Hinweiskommentar vor der Abfrage angegeben sind.	–
pg_hint_plan.enable_hint_table	Zwingt Planer, Hinweise nicht über Tabellensuchen zu erhalten.	–
pg_hint_plan.message_level	Nachrichtenebene von Debug-Meldungen.	–
pg_hint_plan.parse_messages	Nachrichtenebene von Analysefehlern.	–
pglogical.batch_inserts	Batch-Inserts wenn möglich	–

Parametername	Beschreibung	Standard
pglogical.conflict_log_level	Legt die Protokollstufe gelöster Konflikte fest	–
pglogical.conflict_resolution	Legt die Methode zur Konfliktlösung für lösbare Konflikte fest.	–
pglogical.extra_connection_options	Verbindungsoptionen zum Hinzufügen zu allen Peer-Knotenverbindungen	–
pglogical.synchronous_commit	Spezifischer synchroner Commit-Wert für pglogical	–
pglogical.use_spi	Verwenden Sie SPI anstelle der Low-Level-API zum Anwenden von Änderungen	–
pg_similarity.block_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.block_threshold	Legt den Schwellenwert fest, der von der Block-Ähnlichkeitsfunktion verwendet wird.	–
pg_similarity.block_tokenizer	Legt den Tokenizer für die Block-Ähnlichkeits funktion fest.	–
pg_similarity.cosine_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.cosine_threshold	Legt den Schwellenwert fest, der von der Kosinus-Ähnlichkeitsfunktion verwendet wird.	–
pg_similarity.cosine_tokenizer	Legt den Tokenizer für die Kosinus-Ähnlichkeitsfunktion fest.	–
pg_similarity.dice_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.dice_threshold	Legt den Schwellenwert fest, der vom Dice-Ähnlichkeitsmaß verwendet wird	–

Parametername	Beschreibung	Standard
pg_similarity.dice_tokenizer	Legt den Tokenizer für das Dice-Ähnlichkeitsmaß fest.	–
pg_similarity.euclidean_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.euclidean_threshold	Legt den Schwellenwert fest, der vom euklidischen Ähnlichkeitsmaß verwendet wird.	–
pg_similarity.euclidean_tokenizer	Legt den Tokenizer für das euklidische Ähnlichkeitsmaß fest.	–
pg_similarity.hamming_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.hamming_threshold	Legt den Schwellenwert fest, der von der Block-Ähnlichkeitsmetrik verwendet wird.	–
pg_similarity.jaccard_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.jaccard_threshold	Legt den Schwellenwert fest, der vom Jaccard-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.jaccard_tokenizer	Legt den Tokenizer für das Jaccard-Ähnlichkeitsmaß fest.	–
pg_similarity.jaro_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.jaro_threshold	Legt den Schwellenwert fest, der vom Jaro-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.jarowinkler_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.jarowinkler_threshold	Legt den Schwellenwert fest, der vom Jaro-Winkler-Ähnlichkeitsmaß verwendet wird	–

Parametername	Beschreibung	Standard
pg_similarity.levenshtein_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.levenshtein_threshold	Legt den Schwellenwert fest, der vom Levenshtein-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.matching_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.matching_threshold	Legt den Schwellenwert fest, der vom Matching-Koeffizient-Ähnlichkeitsmaß verwendet wird.	–
pg_similarity.matching_tokenizer	Legt den Tokenizer für das Matching-Koeffizient-Ähnlichkeitsmaß fest.	–
pg_similarity.mongeelkan_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.mongeelkan_threshold	Legt den Schwellenwert fest, der vom Monge-Elkan-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.mongeelkan_tokenizer	Legt den Tokenizer für das Monge-Elkan-Ähnlichkeitsmaß fest.	–
pg_similarity.nw_gap_penalty	Legt den Lückenabzug fest, der vom Ähnlichkeitsmaß Needleman-Wunsch verwendet wird.	–
pg_similarity.nw_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.nw_threshold	Legt den Schwellenwert fest, der vom Ähnlichkeitsmaß Needleman-Wunsch verwendet wird.	–
pg_similarity.overlap_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–

Parametername	Beschreibung	Standard
pg_similarity.overlap_threshold	Legt den Schwellenwert fest, der vom Überschneidungskoeffizient-Ähnlichkeitsmaß verwendet wird.	–
pg_similarity.overlap_tokenizer	Legt den Tokenizer für das Überschneidungskoeffizient-Ähnlichkeitsmaß fest.	–
pg_similarity.qgram_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.qgram_threshold	Legt den Schwellenwert fest, der vom Q-Gram-Ähnlichkeitsmaß verwendet wird	–
pg_similarity.qgram_tokenizer	Legt den Tokenizer für die Q-Gram-Messung fest.	–
pg_similarity.swg_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.swg_threshold	Legt den Schwellenwert fest, der vom Smith-Waterman-Gotoh-Ähnlichkeitsmaß verwendet wird.	–
pg_similarity.sw_is_normalized	Legt fest, ob der Ergebniswert normalisiert ist oder nicht.	–
pg_similarity.sw_threshold	Legt den Schwellenwert fest, der vom Smith-Waterman-Ähnlichkeitsmaß verwendet wird	–
pg_stat_statements.max	Legt die maximale Anzahl von Anweisungen fest, die von pg_stat_statements verfolgt werden.	–
pg_stat_statements.save	Speichert pg_stat_statements-Statistiken über Serverausfälle hinweg.	–

Parametername	Beschreibung	Standard
pg_stat_statements.track	Wählt aus, welche Anweisungen von pg_stat_statements verfolgt werden.	–
pg_stat_statements.track_planning	Wählt aus, ob die Planungsdauer von pg_stat_statements verfolgt wird.	–
pg_stat_statements.track_utility	Wählt aus, ob Dienstprogrammbefehle von pg_stat_statements verfolgt werden.	–
postgis.gdal_enabled_drivers	Aktiviert oder deaktiviert GDAL-Treiber, die mit PostGIS in Postgres 9.3.5 und höher verwendet werden.	ENABLE_ALL
quote_all_identifiers	Fügt beim Generieren von SQL-Fragmenten allen Bezeichnern Anführungszeichen hinzu.	–
random_page_cost	Legt die Schätzung des Planers für die Kosten einer nicht sequenziell abgerufenen Datenträgerseite fest.	–
rds.enable_memory_management	Verbessert die Speicherverwaltungsfunktionen in Aurora PostgreSQL 12.17, 13.13, 14.10, 15.5 und höheren Versionen, wodurch Stabilitätsprobleme und Datenbankneustarts aufgrund unzureichenden freien Speichers verhindert werden. Weitere Informationen finden Sie unter Verbesserte Arbeitsspeicherverwaltung in Aurora PostgreSQL.	True
rds.force_admin_logging_level	Siehe Protokollmeldungen für RDS-Admin-Benutzeraktionen in Kundendatenbanken.	–
rds.log_retention_period	Amazon RDS löscht PostgreSQL-Protokolle, die älter als N Minuten sind.	4320

Parametername	Beschreibung	Standard
rds.memory_allocation_guard	Verbessert die Speicherverwaltungsfunktionen in Aurora PostgreSQL 11.21, 12.16, 13.12, 14.9, 15.4 und älteren Versionen, wodurch Stabilitätsprobleme und Datenbank neustarts aufgrund unzureichenden freien Speichers verhindert werden. Weitere Informationen finden Sie unter Verbesserte Arbeitsspeicherverwaltung in Aurora PostgreSQL.	False
rds.pg_stat_ramdisk_size	Größe der Ramdisk-Statistiken in MB. Ein Wert ungleich Null richtet die Ramdisk ein.	0
rds.rds_superuser_reserved_connections	Legt die Anzahl der Verbindungs-Slots fest, die für rds_superusers reserviert sind. Dieser Parameter ist nur in den Versionen 15 und früher verfügbar. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation für reservierte Verbindungen.	2
rds.superuser_variables	Liste der reinen Superuser-Variablen, für die wir die Änderungsanweisungen von rds_superuser erhöhen.	session_replication_role
remove_temp_files_after_crash	Entfernt temporäre Dateien nach dem Backend-Absturz.	0
restart_after_crash	Initialisiert den Server nach dem Backend-Absturz neu.	–
row_security	Aktiviert Zeilensicherheit.	–
search_path	Legt die Schemasuchreihenfolge für Namen fest, die nicht schemaqualifiziert sind.	–
seq_page_cost	Legt die Schätzung des Planers für die Kosten einer sequenziell abgerufenen Datenträgerseite fest.	–

Parametername	Beschreibung	Standard
session_replication_role	Legt das Sitzungsverhalten für Auslöser und Neuschreibungsregeln fest.	–
shared_buffers	(8 kB) Legt die maximale Anzahl freigegebener Arbeitsspeicherpuffer fest, die vom Server verwendet werden.	SUMME (DB) InstanceClassMemory /12038, -50003
shared_preload_libraries	Listet freigegebene Bibliotheken auf, die in den Server vorgeladen werden.	pg_stat_statements
ssl_ca_file	Speicherort der SSL-Server-Zertifizierungsstellendatei.	/rdsdbdata/rds-metadata/ca-cert.pem
ssl_cert_file	Speicherort der SSL-Serverzertifikatdatei.	/rdsdbdata/rds-metadata/server-cert.pem
ssl_crl_dir	Speicherort des Verzeichnisses der SSL-Zertifikatsperrliste.	/rdsdbdata/rds-metadata/ssl_crl_dir/
ssl_key_file	Speicherort der privaten Schlüsseldatei des SSL-Servers	/rdsdbdata/rds-metadata/server-key.pem
standard_conforming_strings	Veranlasst Zeichenfolgen „...“, Backslashes als Zeichen zu behandeln.	–
statement_timeout	(ms) Legt die maximal zulässige Dauer von Anweisungen fest.	–
stats_temp_directory	Schreibt temporäre Statistikdateien in das angegebene Verzeichnis.	/rdsdbdata/db/pg_stat_tmp
superuser_reserved_connections	Legt die Anzahl der Verbindungs-Slots fest, die für Superusers reserviert sind.	3
synchronize_seqscans	Ermöglicht synchronisierte sequenzielle Prüfungen.	–

Parametername	Beschreibung	Standard
tcp_keepalives_count	Maximale Anzahl von TCP-Keepalive-Neuü bertragungen.	–
tcp_keepalives_idle	(s) Zeit zwischen der Ausgabe von TCP-Keepa lives.	–
tcp_keepalives_int erval	(s) Zeit zwischen der Ausgabe von TCP-Keepa live-Neuübertragungen.	–
temp_buffers	(8 kB) Legt die maximale Anzahl der temporäre n Puffer fest, die von den einzelnen Sitzungen verwendet werden.	–
temp_file_limit	Schränkt den Gesamtspeicherplatz in Kilobyte ein, den ein bestimmter PostgreSQL-Prozess für temporäre Dateien verwenden kann, ausschließlich von Speicherplatz, der für explizite temporäre Tabellen verwendet wird	-1
temp_tablespaces	Legt die Tabellenräume fest, die für temporäre Tabellen und Sortierdateien verwendet werden sollen.	–
track_activities	Sammelt Informationen zu Befehlen, die ausgeführt werden.	–
track_activity_que ry_size	Legt die für pg_stat_activity.current_query reservierte Größe in Bytes fest.	4096
track_counts	Sammelt Statistiken zur Datenbankaktivität.	–
track_functions	Sammelt Statistiken auf Funktionsebene zur Datenbankaktivität.	pl
track_io_timing	Erfasst Zeitpunktstatistiken zur Datenbank-E/A-Aktivität.	1

Parametername	Beschreibung	Standard
transform_–_equals	Behandelt expr=– als expr IS –.	–
update_process_title	Aktualisiert den Titel des Vorgangs, um den aktiven SQL-Befehl anzuzeigen.	–
wal_receiver_status_interval	(s) Legt das maximale Intervall zwischen den Statusberichten des WAL-Receivers auf den primären Wert fest.	–
work_mem	(kB) Legt den maximalen Arbeitsspeicher fest, der für Abfrage-Workspaces verwendet werden darf.	–
xmlbinary	Legt die Kodierung von Binärwerten in XML fest.	–
xmloption	Legt fest, ob XML-Daten in impliziten Parsing- und Serialisierungsoperationen als Dokumente oder Inhaltsfragmente betrachtet werden sollen.	–

Amazon-Aurora-PostgreSQL-Warteereignisse

Im Folgenden sind gängige Warteereignisse für Aurora PostgreSQL aufgeführt. Weitere Informationen über Warteereignisse und die Optimierung Ihres Aurora-PostgreSQL-DB-Clusters finden Sie unter Optimierung mit Warteereignissen für Aurora PostgreSQL.

Aktivität: ArchiverMain

Der Archivierungsprozess wartet auf Aktivität.

Aktivität: AutoVacuumMain

Der Autovacuum-Launcher-Prozess wartet auf Aktivität.

Aktivität: BgWriterHibernate

Der Hintergrundschreibprozess befindet sich im Ruhezustand, während er auf Aktivität wartet.

Aktivität: BgWriterMain

Der Hintergrundschreibprozess wartet auf Aktivität.

Aktivität: CheckpointerMain

Der Checkpointer-Prozess wartet auf Aktivität.

Aktivität: LogicalApplyMain

Der Prozess zum Anwenden der logischen Replikation wartet auf Aktivität.

Aktivität: LogicalLauncherMain

Der Startprozess für die logische Replikation wartet auf Aktivität.

Aktivität: PgStatMain

Der Statistikkollektorprozess wartet auf Aktivität.

Aktivität: RecoveryWalAll

Ein Prozess wartet bei der Wiederherstellung auf das Write-Ahead-Log (WAL) von einem Stream.

Aktivität: RecoveryWalStream

Der Startup-Vorgang wartet auf das Eintreffen des Write-Ahead-Log (WAL) während der Streaming-Wiederherstellung.

Aktivität: SysLoggerMain

Der Syslogger-Prozess wartet auf Aktivität.

Aktivität: WalReceiverMain

Der WAL-Receiver-Prozess wartet auf Aktivität.

Aktivität: WalSenderMain

Der WAL-Senderprozess (Write-Ahead-Log) wartet auf Aktivität.

Aktivität: WalWriterMain

Der Write-Ahead-Log (WAL)-Writerprozess wartet auf Aktivität.

BufferPin:BufferPin

Ein Prozess wartet darauf, einen exklusiven Pin an einem Puffer zu erhalten.

Kunde: GSS OpenServer

Ein Prozess wartet darauf, Daten vom Client zu lesen, während er eine GSSAPI-Sitzung (Generic Security Service Application Program Interface) aufbaut.

Kunde: ClientRead

Ein Backend-Prozess wartet darauf, Daten von einem PostgreSQL-Client zu empfangen. Weitere Informationen finden Sie unter Kunde: ClientRead.

Kunde: ClientWrite

Ein Backend-Prozess wartet darauf, weitere Daten an einen PostgreSQL-Client zu senden. Weitere Informationen finden Sie unter Kunde: ClientWrite.

Kunde: Libpq WalReceiverConnect

Ein Prozess wartet im WAL-Receiver darauf, eine Verbindung zum Remote-Server herzustellen.

Kunde: libPQ WalReceiverReceive

Ein Prozess wartet im Write-Ahead-Log (WAL)-Receiver darauf, Daten vom Remote-Server zu empfangen.

Kunde: SSL OpenServer

Ein Prozess wartet auf Secure Sockets Layer (SSL), während er versucht, eine Verbindung herzustellen.

Kunde: WalReceiverWaitStart

Ein Prozess wartet darauf, dass der Startup-Prozess die Anfangsdaten für die Streaming-Replikation sendet.

Kunde: WalSenderWaitFor WAL

Ein Prozess wartet darauf, dass das Write-Ahead-Log (WAL) im WAL-Senderprozess geleert wird.

Kunde: WalSenderWriteData

Ein Prozess wartet auf eine Aktivität, wenn er Antworten vom Write-Ahead-Log (WAL)-Receiver im WAL-Senderprozess verarbeitet.

CPU

Ein Backend-Prozess ist in der CPU aktiv oder wartet auf diese. Weitere Informationen finden Sie unter CPU.

Extension:extension

Ein Backend-Prozess wartet auf eine Bedingung, die von einer Erweiterung oder einem Modul definiert wird.

IO: AuroraOptimizedReadsCacheRead

Ein Prozess wartet auf einen Lesevorgang aus dem mehrstufigen Cache für optimierte Lesevorgänge, da die Seite nicht im gemeinsam genutzten Speicher verfügbar ist.

IO: AuroraOptimizedReads CacheSegmentKürzen

Ein Prozess wartet darauf, dass eine Segmentdatei des gestuften Caches für optimierte Lesevorgänge gekürzt wird.

IO: AuroraOptimizedReadsCacheWrite

Der Hintergrund-Writer-Prozess wartet darauf, in den mehrstufigen Cache für optimierte Lesevorgänge zu schreiben.

IO: AuroraStorageLogAllocate

Eine Sitzung weist Metadaten zu und bereitet einen Schreibvorgang für das Transaktionsprotokoll vor.

IO: BufFileRead

Wenn Vorgänge mehr Speicher benötigen, als durch die Parameter des Arbeitsspeichers definiert ist, erstellt die Engine temporäre Dateien auf der Festplatte. Dieses Warteereignis tritt auf, wenn Vorgänge aus den temporären Dateien gelesen werden. Weitere Informationen finden Sie unter io:BuffileRead und io:BuffileWrite.

IO: BufFileWrite

Wenn Vorgänge mehr Speicher benötigen, als durch die Parameter des Arbeitsspeichers definiert ist, erstellt die Engine temporäre Dateien auf der Festplatte. Dieses Warteereignis tritt auf, wenn Vorgänge in die temporären Dateien schreiben. Weitere Informationen finden Sie unter io:BuffileRead und io:BuffileWrite.

IO: ControlFileRead

Ein Prozess wartet auf das Lesen der `pg_control`-Datei.

IO: ControlFileSync

Ein Prozess wartet darauf, dass die `pg_control`-Datei den dauerhaften Speicher erreicht.

IO: ControlFileSyncUpdate

Ein Prozess wartet auf eine Aktualisierung der `pg_control`-Datei, um einen dauerhaften Speicher zu erreichen.

IO: ControlFileWrite

Ein Prozess wartet auf einen Schreibvorgang in die `pg_control`-Datei.

IO: ControlFileWriteUpdate

Ein Prozess wartet auf einen Schreibvorgang, um die `pg_control`-Datei zu aktualisieren.

IO: CopyFileRead

Ein Prozess wartet auf das Lesen während eines Dateikopiervorgangs.

IO: CopyFileWrite

Ein Prozess wartet während einer Dateikopieroperation auf einen Schreibvorgang.

IO: DataFileExtend

Ein Prozess wartet darauf, dass eine Relationsdatendatei erweitert wird.

IO: DataFileFlush

Ein Prozess wartet darauf, dass eine Relationsdatendatei einen dauerhaften Speicher erreicht.

IO: DataFileImmediateSync

Ein Prozess wartet auf eine sofortige Synchronisierung einer Relationsdatendatei mit einem dauerhaften Speicher.

IO: DataFilePrefetch

Ein Prozess wartet auf einen asynchronen Vorabruf aus einer Relationsdatendatei.

IO: DataFileSync

Ein Prozess wartet darauf, dass Änderungen an einer Relationsdatendatei einen dauerhaften Speicher erreichen.

IO: DataFileRead

Ein Backend-Prozess hat versucht, eine Seite in den freigegebenen Puffern zu finden, hat sie jedoch nicht gefunden und sie daher aus dem Speicher gelesen. Weitere Informationen finden Sie unter IO:DataFileRead.

IO: DataFileTruncate

Ein Prozess wartet darauf, dass eine Relationsdatendatei abgeschnitten wird.

IO: DataFileWrite

Ein Prozess wartet auf einen Schreibvorgang in eine Relationsdatendatei.

IO: DSM FillZeroWrite

Ein Prozess wartet darauf, null Bytes in eine dynamische Shared Memory-Backing-Datei zu schreiben.

IO: LockFileAddToDataDirRead

Ein Prozess wartet auf das Lesen, während er der Datenverzeichnis-Sperrdatei eine Zeile hinzufügt.

IO: LockFileAddToDataDirSync

Ein Prozess wartet darauf, dass Daten einen dauerhaften Speicher erreichen, während er der Datenverzeichnis-Sperrdatei eine Zeile hinzufügt.

IO: LockFileAddToDataDirWrite

Ein Prozess wartet auf einen Schreibvorgang, während er der Datenverzeichnis-Sperrdatei eine Zeile hinzufügt.

IO: LockFileCreateRead

Ein Prozess wartet auf das Lesen, während er die Datenverzeichnis-Sperrdatei erstellt.

IO: LockFileCreateSync

Ein Prozess wartet darauf, dass Daten einen dauerhaften Speicher erreichen, während er die Datenverzeichnis-Sperrdatei erstellt.

IO: LockFileCreateWrite

Ein Prozess wartet auf einen Schreibvorgang, während er die Datenverzeichnis-Sperrdatei erstellt.

IO: LockFileReCheckDataDirRead

Ein Prozess wartet während der erneuten Überprüfung der Datenverzeichnis-Sperrdatei auf das Lesen.

IO: LogicalRewriteCheckpointSync

Ein Prozess wartet darauf, dass logische Rewrite-Mappings während eines Checkpoints dauerhaften Speicher erreichen.

IO: LogicalRewriteMappingSync

Ein Prozess wartet darauf, dass Mapping-Daten während eines logischen Neuschreibens einen dauerhaften Speicher erreichen.

IO: LogicalRewriteMappingWrite

Ein Prozess wartet während eines logischen Rewrite auf ein Schreiben von Mapping-Daten.

IO: LogicalRewriteSync

Ein Prozess wartet auf logische Rewrite-Zuordnungen, um dauerhaften Speicher zu erreichen.

IO: LogicalRewriteTruncate

Ein Prozess wartet auf das Abschneiden von Mapping-Daten während eines logischen Neuschreibens.

IO: LogicalRewriteWrite

Ein Prozess wartet auf einen Schreibvorgang von logischen Rewrite-Mappings.

IO: RelationMapRead

Ein Prozess wartet auf das Lesen der Relation Map-Datei.

IO: RelationMapSync

Ein Prozess wartet darauf, dass die Relationszuordnungsdatei einen dauerhaften Speicher erreicht.

IO: RelationMapWrite

Ein Prozess wartet auf einen Schreibvorgang in die Relation Map-Datei.

IO: ReorderBufferRead

Ein Prozess wartet während der Neuordnungs-Pufferverwaltung auf das Lesen.

IO: ReorderBufferWrite

Ein Prozess wartet während der Neuordnungs-Pufferverwaltung auf einen Schreibvorgang.

IO: ReorderLogicalMappingRead

Ein Prozess wartet während der Neuordnungspufferverwaltung auf das Lesen einer logischen Abbildung.

IO: ReplicationSlotRead

Ein Prozess wartet auf das Lesen aus einer Replikations-Slot-Steuerungsdatei.

IO: ReplicationSlotRestoreSync

Ein Prozess wartet darauf, dass eine Replikations-Slot-Steuerungsdatei einen dauerhaften Speicher erreicht, während sie im Arbeitsspeicher wiederhergestellt wird.

IO: ReplicationSlotSync

Ein Prozess wartet darauf, dass eine Replikations-Slot-Steuerdatei einen dauerhaften Speicher erreicht.

IO: ReplicationSlotWrite

Ein Prozess wartet auf einen Schreibvorgang in eine Replikations-Slot-Steuerdatei.

IO: SLRU FlushSync

Ein Prozess wartet darauf, dass einfache, selten verwendete Daten (SLRU-Daten) während eines Prüfpunkts oder beim Herunterfahren der Datenbank in einem dauerhaften Speicher abgelegt werden.

IO:SLRURead

Ein Prozess wartet auf das Lesen einer einfachen, selten verwendeten Seite (SLRU-Seite).

IO:SLRUSync

Ein Prozess wartet darauf, dass einfache, selten verwendete Daten (SLRU-Daten) nach einem Seitenschreibvorgang in einem dauerhaften Speicher abgelegt werden.

IO:SLRUWrite

Ein Prozess wartet auf den Schreibvorgang einer einfachen, selten verwendeten Seite (SLRU-Seite).

IO: SnapbuildRead

Ein Prozess wartet auf das Lesen eines serialisierten historischen Katalog-Snapshots.

IO: SnapbuildSync

Ein Prozess wartet darauf, dass ein serialisierter historischer Katalog-Snapshot einen dauerhaften Speicher erreicht.

IO: SnapbuildWrite

Ein Prozess wartet auf das Schreiben eines serialisierten historischen Katalog-Snapshots.

IO: TimelineHistoryFileSync

Ein Prozess wartet darauf, dass eine Zeitachsenverlaufsdatei, die über die Streaming-Replikation empfangen wurde, im dauerhaften Speicher abgelegt wird.

IO: TimelineHistoryFileWrite

Ein Prozess wartet auf das Schreiben einer Zeitachsenverlaufsdatei, die über die Streaming-Replikation empfangen wurde.

IO: TimelineHistoryRead

Ein Prozess wartet auf das Lesen einer Zeitachsenverlaufsdatei.

IO: TimelineHistorySync

Ein Prozess wartet darauf, dass eine neu erstellte Zeitachsenverlaufsdatei einen dauerhaften Speicher erreicht.

IO: TimelineHistoryWrite

Ein Prozess wartet auf das Schreiben einer neu erstellten Zeitachsenverlaufsdatei.

IO: TwophaseFileRead

Ein Prozess wartet auf das Lesen einer Zweiphasen-Statusdatei.

IO: TwophaseFileSync

Ein Prozess wartet darauf, dass eine zweiphasige Zustandsdatei einen dauerhaften Speicher erreicht.

IO: TwophaseFileWrite

Ein Prozess wartet auf das Schreiben einer Zweiphasen-Zustandsdatei.

IO: WAL BootstrapSync

Ein Prozess wartet darauf, dass das Write-Ahead-Log (WAL) während des Bootstrapping im dauerhaften Speicher abgelegt wird.

IO: WAL BootstrapWrite

Ein Prozess wartet während des Bootstrapping auf das Schreiben einer WAL-Seite.

IO: WAL CopyRead

Ein Prozess wartet auf das Lesen, wenn ein neues Write-Ahead-Log (WAL)-Segment erstellt wird, indem ein vorhandenes kopiert wird.

IO: WAL CopySync

Ein Prozess wartet auf ein neues WAL-Segment (Write-Ahead-Log), das durch Kopieren eines vorhandenen Segments erstellt wurde, um dauerhaften Speicher zu erreichen.

IO: WAL CopyWrite

Ein Prozess wartet auf einen Schreibvorgang, wenn er ein neues WAL-Segment (Write-Ahead-Log) erstellt, indem er ein vorhandenes kopiert.

IO: WAL InitSync

Ein Prozess wartet darauf, dass eine neu initialisierte Write-Ahead-Log-Datei (WAL) im dauerhaften Speicher abgelegt wird.

IO: WAL InitWrite

Ein Prozess wartet auf einen Schreibvorgang, während er eine neue Write-Ahead-Protokolldatei (WAL) initialisiert.

IO:WALRead

Ein Prozess wartet auf das Lesen aus einer Write-Ahead-Protokolldatei (WAL).

IO: WAL SenderTimelineHistoryRead

Ein Prozess wartet während eines WAL-Sender-Zeitachsenbefehls auf das Lesen aus einer Zeitachsenverlaufsdatei.

IO:WALSync

Ein Prozess wartet darauf, dass eine Write-Ahead-Protokolldatei (WAL) einen dauerhaften Speicher erreicht.

IO: WAL SyncMethodAssign

Ein Prozess wartet darauf, dass Daten einen dauerhaften Speicher erreichen, während er eine neue WAL-Synchronisierungsmethode (Write-Ahead-Log) zuweist.

IO:WALWrite

Ein Prozess wartet auf einen Schreibvorgang in eine Write-Ahead-Protokolldatei (WAL).

IO: XactSync

Ein Backend-Prozess wartet darauf, dass das Aurora-Speichersubsystem den Commit einer regulären Transaktion oder den Commit oder das Rollback einer vorbereiteten Transaktion bestätigt. Weitere Informationen finden Sie unter IO:XactSync.

IPC: BackupWaitWalArchive

Ein Prozess wartet auf Write-Ahead-Log-Dateien (WAL), die für eine erfolgreiche Archivierung einer Sicherung erforderlich sind.

IPC: AuroraOptimizedReadsCacheWriteStop

Ein Prozess wartet darauf, dass der Hintergrund-Writer das Schreiben in den mehrstufigen Cache von Optimized Reads beendet.

IPC: BgWorkerShutdown

Ein Prozess wartet darauf, dass ein Arbeitsprozess im Hintergrund heruntergefahren wird.

IPC: BgWorkerStartup

Ein Prozess wartet darauf, dass ein Hintergrund-Worker gestartet wird.

IPC: BtreePage

Ein Prozess wartet darauf, dass die Seitennummer, die zum Fortsetzen einer parallelen B-Baum-Abtastung benötigt wird, verfügbar wird.

IPC: CheckpointDone

Ein Prozess wartet darauf, dass ein Checkpoint abgeschlossen wird.

IPC: CheckpointStart

Ein Prozess wartet auf den Start eines Checkpoints.

IPC: ClogGroupUpdate

Ein Prozess wartet darauf, dass der Gruppenleiter den Transaktionsstatus am Ende einer Transaktion aktualisiert.

IPC: DamRecordTxAck

Ein Backend-Prozess hat ein Ereignis für Datenbank-Aktivitätsströme generiert und wartet darauf, dass das Ereignis dauerhaft wird. Weitere Informationen finden Sie unter IPC:DamRecordTxAck.

IPC: ExecuteGather

Ein Prozess wartet auf Aktivitäten von einem untergeordneten Prozess, während er einen Gather-Plan-Knoten ausführt.

IPC:Hash/Batch/Allocating

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer eine Hash-Tabelle zuweist.

IPC:Hash/Batch/Electing

Ein Prozess wählt einen parallelen Hash-Teilnehmer aus, um eine Hash-Tabelle zuzuweisen.

IPC:Hash/Batch/Loading

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer das Laden einer Hash-Tabelle abgeschlossen haben.

IPC:Hash/Build/Allocating

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer die anfängliche Hash-Tabelle zuweist.

IPC:Hash/Build/Electing

Ein Prozess wählt einen parallelen Hash-Teilnehmer aus, um die anfängliche Hash-Tabelle zuzuweisen.

IPC: hash/build/ HashingInner

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer das Hashing der inneren Beziehung abgeschlossen haben.

IPC: hash/build/ HashingOuter

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer die Partitionierung der äußeren Beziehung abschließen.

GrowBatchesipc:hash/ /Zuweisen

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer weitere Batches zuweist.

ipc:hash/ GrowBatches /Deciding

Ein Prozess wählt einen parallelen Hash-Teilnehmer aus, um über zukünftiges Batch-Wachstum zu entscheiden.

ipc:hash/ /Electing GrowBatches

Ein Prozess wählt einen parallelen Hash-Teilnehmer aus, um mehr Batches zuzuweisen.

ipc:hash/ /Finishing GrowBatches

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer über zukünftiges Batch-Wachstum entscheidet.

ipc:hash/ GrowBatches /Repartitionierung

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer die Neupartitionierung abgeschlossen haben.

ipc:hash/ /Zuweisen GrowBuckets

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer die Zuweisung weiterer Buckets abgeschlossen hat.

ipc:hash/ /Electing GrowBuckets

Ein Prozess wählt einen parallelen Hash-Teilnehmer aus, um mehr Buckets zuzuweisen.

ipc:hash/ /Erneut einfügen GrowBuckets

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer das Einfügen von Tupeln in neue Buckets abgeschlossen haben.

IPC: HashBatchAllocate

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer eine Hash-Tabelle zuweist.

IPC: HashBatchElect

Ein Prozess wartet darauf, einen parallelen Hash-Teilnehmer auszuwählen, um eine Hash-Tabelle zuzuweisen.

IPC: HashBatchLoad

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer das Laden einer Hash-Tabelle abgeschlossen haben.

IPC: HashBuildAllocate

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer die anfängliche Hash-Tabelle zuweist.

IPC: HashBuildElect

Ein Prozess wartet darauf, einen parallelen Hash-Teilnehmer auszuwählen, um die anfängliche Hash-Tabelle zuzuweisen.

IPC: HashBuildHashInner

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer das Hashing der inneren Beziehung abgeschlossen haben.

IPC: 'HashBuildHashOuter

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer die Partitionierung der äußeren Beziehung abschließen.

IPC: HashGrowBatchesAllocate

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer weitere Batches zuweist.

IPC: 'HashGrowBatchesDecide

Ein Prozess wartet darauf, einen parallelen Hash-Teilnehmer auszuwählen, um über das zukünftige Batch-Wachstum zu entscheiden.

IPC: HashGrowBatchesElect

Ein Prozess wartet darauf, einen parallelen Hash-Teilnehmer auszuwählen, um weitere Batches zuzuweisen.

IPC: HashGrowBatchesFinish

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer über zukünftiges Batch-Wachstum entscheidet.

IPC: HashGrowBatchesRepartition

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer die Neupartitionierung beenden.

IPC: HashGrowBucketsAllocate

Ein Prozess wartet darauf, dass ein gewählter paralleler Hash-Teilnehmer die Zuweisung weiterer Buckets abgeschlossen hat.

IPC: HashGrowBucketsElect

Ein Prozess wartet darauf, einen parallelen Hash-Teilnehmer auszuwählen, um weitere Buckets zuzuweisen.

IPC: HashGrowBucketsReinsert

Ein Prozess wartet darauf, dass andere parallele Hash-Teilnehmer das Einfügen von Tupeln in neue Buckets abgeschlossen haben.

IPC: LogicalSyncData

Ein Prozess wartet darauf, dass ein Remote-Server für die logische Replikation Daten für die anfängliche Tabellensynchronisierung sendet.

IPC: LogicalSyncStateChange

Ein Prozess wartet darauf, dass ein logischer Replikations-Remote-Server seinen Status ändert.

IPC: MessageQueueInternal

Ein Prozess wartet darauf, dass ein anderer Prozess an eine gemeinsam genutzte Nachrichtenwarteschlange angehängt wird.

IPC: MessageQueuePutMessage

Ein Prozess wartet darauf, eine Protokollnachricht in eine gemeinsam genutzte Nachrichtenwarteschlange zu schreiben.

IPC: MessageQueueReceive

Ein Prozess wartet darauf, Bytes aus einer gemeinsam genutzten Nachrichtenwarteschlange zu empfangen.

IPC: MessageQueueSend

Ein Prozess wartet darauf, Bytes an eine gemeinsam genutzte Nachrichtenwarteschlange zu senden.

IPC: ParallelBitmapScan

Ein Prozess wartet darauf, dass ein paralleler Bitmap-Scan initialisiert wird.

IPC: ParallelCreateIndexScan

Ein Prozess wartet darauf, dass parallele CREATE INDEX-Arbeitsprozesse einen Heap-Scan abschließen.

IPC: ParallelFinish

Ein Prozess wartet darauf, dass parallele Arbeitsprozesse die Berechnung abgeschlossen haben.

IPC: ProcArrayGroupUpdate

Ein Prozess wartet darauf, dass der Gruppenleiter die Transaktions-ID am Ende einer parallelen Operation löscht.

IPC: ProcSignalBarrier

Ein Prozess wartet darauf, dass ein Barriere-Ereignis von allen Backends verarbeitet wird.

IPC:Promote

Ein Prozess wartet auf die Standby-Heraufstufung.

IPC: RecoveryConflictSnapshot

Ein Prozess wartet auf die Lösung des Wiederherstellungskonflikts für eine Vakuumbereinigung.

IPC: RecoveryConflictTablespace

Ein Prozess wartet auf die Lösung eines Wiederherstellungskonflikts, um einen Tablespace zu löschen.

IPC: RecoveryPause

Ein Prozess wartet darauf, dass die Wiederherstellung fortgesetzt wird.

IPC: ReplicationOriginDrop

Ein Prozess wartet darauf, dass ein Replikationsursprung inaktiv wird, damit er gelöscht werden kann.

IPC: ReplicationSlotDrop

Ein Prozess wartet darauf, dass ein Replikations-Slot inaktiv wird, damit er gelöscht werden kann.

IPC: SafeSnapshot

Ein Prozess wartet darauf, einen gültigen Snapshot für eine READ ONLY DEFERRABLE-Transaktion abzurufen.

IPC: SyncRep

Ein Prozess wartet während der synchronen Replikation auf die Bestätigung eines Remote-Servers.

IPC: XactGroupUpdate

Ein Prozess wartet darauf, dass der Gruppenleiter den Transaktionsstatus am Ende einer Parallelоperation aktualisiert.

Lock:advisory

Ein Backend-Prozess hat eine Advisory-Sperre angefordert und wartet darauf. Weitere Informationen finden Sie unter Lock:advisory.

Lock:extend

Ein Backend-Prozess wartet darauf, dass eine Sperre freigegeben wird, damit er eine Relation erweitern kann. Diese Sperre wird benötigt, da jeweils nur ein Backend-Prozess eine Relation erweitern kann. Weitere Informationen finden Sie unter Lock:extend.

Lock:frozenid

Ein Prozess wartet darauf, `pg_database.datfrozenxid` und `pg_database.datminmxid` zu aktualisieren.

Lock:object

Ein Prozess wartet darauf, eine Sperre für ein Objekt einer nichtrelationalen Datenbank zu erhalten.

Lock:page

Ein Prozess wartet darauf, eine Sperre für eine Seite einer Relation zu erhalten.

Lock:Relation

Ein Backend-Prozess wartet darauf, eine Sperre für eine Relation zu erlangen, die durch eine andere Transaktion gesperrt ist. Weitere Informationen finden Sie unter Lock:Relation.

Lock:spectoken

Ein Prozess wartet darauf, eine spekulative Einfügesperre zu erhalten.

Lock:speculative token

Ein Prozess wartet darauf, eine spekulative Einfügesperre zu erlangen.

Lock:transactionid

Eine Transaktion wartet auf eine Sperre auf Zeilenebene. Weitere Informationen finden Sie unter Lock:transactionid.

Lock:tuple

Ein Backend-Prozess wartet darauf, eine Sperre für ein Tupel zu erlangen, während ein anderer Backend-Prozess eine widersprüchliche Sperre für dasselbe Tupel hält. Weitere Informationen finden Sie unter Lock:tuple.

Lock:userlock

Ein Prozess wartet darauf, eine Benutzersperre zu erhalten.

Lock:virtualxid

Ein Prozess wartet darauf, eine virtuelle Transaktions-ID-Sperre zu erhalten.

Schleuse: AddinShmemInit

Ein Prozess wartet darauf, die Speicherplatzzuweisung einer Erweiterung im gemeinsam genutzten Speicher zu verwalten.

LW-Schloss: AddinShmemInitLock

Ein Prozess wartet darauf, die Speicherplatzzuweisung im gemeinsam genutzten Speicher zu verwalten.

LWLock:async

Ein Prozess wartet auf I/O in einem asynchronen (Benachrichtigungs-)Puffer.

LW-Schloss: AsyncCtlLock

Ein Prozess wartet darauf, einen freigegebenen Benachrichtigungsstatus zu lesen oder zu aktualisieren.

LW-Schloss: AsyncQueueLock

Ein Prozess wartet darauf, Benachrichtigungen zu lesen oder zu aktualisieren.

LW-Schloss: AuroraOptimizedReadsCacheMapping

Ein Prozess wartet darauf, einen Datenblock mit einer Seite im mehrstufigen Cache für optimierte Lesevorgänge zu verknüpfen.

LW-Schloss: AutoFile

Ein Prozess wartet darauf, die Datei `postgresql.auto.conf` zu aktualisieren.

LW-Schloss: AutoFileLock

Ein Prozess wartet darauf, die Datei `postgresql.auto.conf` zu aktualisieren.

LWLock:Autovacuum

Ein Prozess wartet darauf, den aktuellen Status der Autovacuum-Arbeitsprozesse zu lesen oder zu aktualisieren.

LW-Schloss: AutovacuumLock

Ein Autovacuum-Worker oder ein Startprogramm wartet darauf, den aktuellen Status der Autovacuum-Worker zu aktualisieren oder zu lesen.

LW-Schloss: AutovacuumSchedule

Ein Prozess wartet, um sicherzustellen, dass eine für den Autovaccuum-Prozess ausgewählte Tabelle noch bereinigt werden muss.

LW-Schloss: AutovacuumScheduleLock

Ein Prozess wartet, um sicherzustellen, dass eine für den Autovakcuum-Prozess ausgewählte Tabelle noch bereinigt werden muss.

LW-Schloss: BackendRandomLock

Ein Prozess wartet darauf, eine Zufallszahl zu generieren.

LW-Schloss: BackgroundWorker

Ein Prozess wartet darauf, den Hintergrund-Worker-Status zu lesen oder zu aktualisieren.

LW-Schloss: BackgroundWorkerLock

Ein Prozess wartet darauf, den Hintergrund-Worker-Status zu lesen oder zu aktualisieren.

LW-Schloss: BtreeVacuum

Ein Prozess wartet darauf, vacuumbezogene Informationen für einen B-Baum-Index zu lesen oder zu aktualisieren.

LW-Schloss: BtreeVacuumLock

Ein Prozess wartet darauf, auf die Bereinigung bezogene Informationen für einen B-Baum-Index zu lesen oder zu aktualisieren.

LWLock:buffer_content

Ein Backend-Prozess wartet darauf, eine einfache Sperre für den Inhalt eines gemeinsam genutzten Speicherpuffers zu erlangen. Weitere Informationen finden Sie unter LWLock:buffer_content (BufferContent).

LWLock:buffer_mapping

Ein Backend-Prozess wartet darauf, einen Datenblock mit einem Puffer im gemeinsam genutzten Pufferpool zu verknüpfen. Weitere Informationen finden Sie unter LWLock:buffer_mapping.

LWLock:BufferIO

Ein Backend-Prozess möchte eine Seite in den gemeinsam genutzten Speicher einlesen. Der Prozess wartet darauf, dass andere Prozesse ihre I/O für die Seite beenden. Weitere Informationen finden Sie unter LWLock:BufferIO (IPC:BufferIO).

LWLock:Checkpoint

Ein Prozess wartet darauf, einen Checkpoint zu starten.

LW-Schloss: CheckpointLock

Ein Prozess wartet darauf, einen Checkpoint auszuführen.

LW-Schloss: CheckpointerComm

Ein Prozess wartet darauf, `fsync` Anfragen zu verwalten.

LW-Schloss: CheckpointerCommLock

Ein Prozess wartet darauf, `fsync` Anfragen zu verwalten.

LWLock:clog

Ein Prozess wartet auf I/O in einem Clog (Transaktionsstatus)-Puffer.

lWlock: C LogControlLock

Ein Prozess wartet darauf, den Transaktionsstatus zu lesen oder zu aktualisieren.

lWlock:C LogTruncationLock

Ein Prozess wartet darauf, `txid_status` auszuführen oder die älteste verfügbare Transaktions-ID zu aktualisieren.

LWLock:commit_timestamp

Ein Prozess wartet auf I/O in einem Commit-Zeitstempelpuffer.

LWlock: CommitTs

Ein Prozess wartet darauf, den letzten für einen Transaktions-Commit-Zeitstempel festgelegten Wert zu lesen oder zu aktualisieren.

LW-Schloss: CommitTsBuffer

Ein Prozess wartet auf I/O in einem einfachen, selten verwendeten Puffer (SLRU-Puffer) für einen Commit-Zeitstempel.

LW-Schloss: CommitTsControlLock

Ein Prozess wartet darauf, Transaktions-Commit-Zeitstempel zu lesen oder zu aktualisieren.

LW-Schloss: CommitTsLock

Ein Prozess wartet darauf, den letzten für den Transaktionszeitstempel festgelegten Wert zu lesen oder zu aktualisieren.

lWlock: SLRU CommitTs

Ein Prozess wartet auf den Zugriff auf den einfachen, selten verwendeten Cache (SLRU-Cache) für einen Commit-Zeitstempel.

LWlock: ControlFile

Ein Prozess wartet darauf, die Datei `pg_control` zu lesen oder zu aktualisieren oder eine neue Write-Ahead-Log-Datei (WAL) zu erstellen.

LW-Schloss: ControlFileLock

Ein Prozess wartet darauf, die Steuerdatei zu lesen oder zu aktualisieren oder eine neue Write-Ahead-Protokolldatei (WAL) zu erstellen.

LW-Schloss: DynamicSharedMemoryControl

Ein Prozess wartet darauf, Informationen zur Zuordnung des dynamischen gemeinsamen Speichers zu lesen oder zu aktualisieren.

LW-Schloss: DynamicSharedMemoryControlLock

Ein Prozess wartet darauf, den Status des dynamischen gemeinsam genutzten Speichers zu lesen oder zu aktualisieren.

LWLock:lock_manager

Ein Backend-Prozess wartet darauf, Sperren für Backend-Prozesse hinzuzufügen oder zu untersuchen. Oder er wartet darauf, einer Sperrgruppe beizutreten oder diese zu verlassen, die von der parallelen Abfrage verwendet wird. Weitere Informationen finden Sie unter LWLock:lock_manager.

LW-Schloss: LockFastPath

Ein Prozess wartet darauf, die Informationen zur Fast-Path-Sperre eines Prozesses zu lesen oder zu aktualisieren.

LW-Schloss: LogicalRepWorker

Ein Prozess wartet darauf, den Status der logischen Replikations-Arbeitsprozesse zu lesen oder zu aktualisieren.

LW-Schloss: LogicalRepWorkerLock

Ein Prozess wartet darauf, dass eine Aktion auf einem logischen Replikations-Worker beendet wird.

LWLock:multixact_member

Ein Prozess wartet auf I/O in einem multixact_member-Puffer.

LWLock:multixact_offset

Ein Prozess wartet auf I/O in einem Multixact-Offset-Puffer.

LW-Schloss: MultiXactGen

Ein Prozess wartet darauf, den freigegebenen multixact-Status zu lesen oder zu aktualisieren.

LW-Schloss: MultiXactGenLock

Ein Prozess wartet darauf, einen gemeinsam genutzten multixact-Zustand zu lesen oder zu aktualisieren.

LW-Schloss: MultiXactMemberBuffer

Ein Prozess wartet auf I/O in einem einfachen, selten verwendeten Puffer (SLRU-Puffer) für ein Multixact-Mitglied. Weitere Informationen finden Sie unter LWLockMultiXact:.

LW-Schloss: MultiXactMemberControlLock

Ein Prozess wartet darauf, Multixact-Mitgliederzuordnungen zu lesen oder zu aktualisieren.

lWlock: SLRU MultiXactMember

– Ein Prozess wartet darauf, auf den einfachen, selten verwendeten Cache (SLRU-Cache) für ein Multixact-Mitglied zuzugreifen. Weitere Informationen finden Sie unter LWLockMultiXact:.

LWlock: MultiXactOffsetBuffer

– Ein Prozess wartet auf I/O in einem einfachen, selten verwendeten Puffer (SLRU-Puffer) für ein Multixact-Offset. Weitere Informationen finden Sie unter LWLockMultiXact:.

LW-Schloss: MultiXactOffsetControlLock

Ein Prozess wartet darauf, multixact Offset-Mappings zu lesen oder zu aktualisieren.

lWlock: SLRU MultiXactOffset

– Ein Prozess wartet darauf, auf den einfachen, selten verwendeten Cache (SLRU-Cache) für ein Multixact-Offset zuzugreifen. Weitere Informationen finden Sie unter LWLockMultiXact:.

LWlock: MultiXactTruncation

Ein Prozess wartet darauf, multixact-Informationen zu lesen oder abzuschneiden.

LW-Schloss: MultiXactTruncationLock

Ein Prozess wartet darauf, multixact-Informationen zu lesen oder abzuschneiden.

LW-Schloss: NotifyBuffer

Ein Prozess wartet auf I/O im einfachen, selten verwendeten Puffer (SLRU-Puffer) für eine NOTIFY-Nachricht.

LW-Schloss: NotifyQueue

Ein Prozess wartet darauf, NOTIFY-Nachrichten zu lesen oder zu aktualisieren.

LW-Schloss: NotifyQueueTail

Ein Prozess wartet darauf, einen Grenzwert für den NOTIFY-Nachrichtenspeicher zu aktualisieren.

LW-Schloss: NotifyQueueTailLock

Ein Prozess wartet darauf, das Limit für den Speicher von Benachrichtigungsnachrichten zu aktualisieren.

LWLock:NotifySLRU

Ein Prozess wartet darauf, auf den einfachen, selten verwendeten Cache (SLRU-Cache) für eine NOTIFY-Nachricht zuzugreifen.

LW-Schloss: OidGen

Ein Prozess wartet darauf, eine neue Objekt-ID (OID) zuzuweisen.

LW-Schloss: OidGenLock

Ein Prozess wartet darauf, eine Objekt-ID (OID) zuzuweisen oder zuzuweisen.

LWLock:oldserxid

Ein Prozess wartet auf I/O in einem Oldserxid-Puffer.

LW-Schloss: OldSerXidLock

Ein Prozess wartet darauf, in Konflikt stehende serialisierbare Transaktionen zu lesen oder aufzuzeichnen.

LW-Schloss: OldSnapshotTimeMap

Ein Prozess wartet darauf, alte Snapshot-Steuerungsinformationen zu lesen oder zu aktualisieren.

LW-Schloss: OldSnapshotTimeMapLock

Ein Prozess wartet darauf, alte Snapshot-Steuerungsinformationen zu lesen oder zu aktualisieren.

LWLock:parallel_append

Ein Prozess wartet darauf, während der parallelen Ausführung des Anhänge-Plans den nächsten Unterplan auszuwählen.

LWLock:parallel_hash_join

Ein Prozess wartet darauf, während einer parallelen Hash-Plan-Ausführung einen Speicherblock zuzuweisen oder auszutauschen oder Zähler zu aktualisieren.

LWLock:parallel_query_dsa

Ein Prozess wartet auf eine Sperre für die dynamische Shared Memory-Zuweisung für eine parallele Abfrage.

LW-Schloss: ParallelAppend

Ein Prozess wartet darauf, während der parallelen Ausführung des Anhänge-Plans den nächsten Unterplan auszuwählen.

LW-Schloss: ParallelHashJoin

Ein Prozess wartet darauf, während der Planausführung Worker für einen parallelen Hash-Join zu synchronisieren.

Lwlock: DSA ParallelQuery

Ein Prozess wartet auf eine dynamische Shared Memory-Zuweisung für eine parallele Abfrage.

Lwlock: DSA PerSession

Ein Prozess wartet auf eine dynamische Shared Memory-Zuweisung für eine parallele Abfrage.

Lwlock: PerSessionRecordType

Ein Prozess wartet darauf, auf die Informationen einer parallelen Abfrage zu zusammengesetzten Typen zuzugreifen.

Lwlock: PerSessionRecordTypmod

Ein Prozess wartet darauf, auf die Informationen einer parallelen Abfrage über Typmodifizierer zuzugreifen, die anonyme Datensatztypen identifizieren.

Lwlock: PerXactPredicateList

Ein Prozess wartet darauf, während einer parallelen Abfrage auf die Liste der Prädikatssperren zuzugreifen, die von der aktuellen serialisierbaren Transaktion gehalten werden.

Lwlock:predicate_lock_manager

Ein Prozess wartet darauf, Informationen zur Prädikatsperre hinzuzufügen oder zu untersuchen.

Lwlock: PredicateLockManager

Ein Prozess wartet darauf, auf Prädikats-Sperrinformationen zuzugreifen, die von serialisierbaren Transaktionen verwendet werden.

Lwlock:proc

Ein Prozess wartet darauf, die Fast-Path-Sperrinformationen zu lesen oder zu aktualisieren.

Lwlock: ProcArray

Ein Prozess wartet darauf, auf die freigegebenen prozessbezogenen Datenstrukturen zuzugreifen (normalerweise um einen Snapshot zu erhalten oder die Transaktions-ID einer Sitzung zu melden).

LW-Schloss: ProcArrayLock

Ein Prozess wartet darauf, einen Snapshot zu erhalten oder eine Transaktions-ID am Ende einer Transaktion zu löschen.

LW-Schloss: RelationMapping

Ein Prozess wartet darauf, eine `pg_filenode.map`-Datei zu lesen oder zu aktualisieren (wird verwendet, um die Dateiknotenzuordnungen bestimmter Systemkataloge zu verfolgen).

LW-Schloss: RelationMappingLock

Ein Prozess wartet darauf, die Relation-Map-Datei zu aktualisieren, die zum Speichern der catalog-to-file-node Zuordnung verwendet wird.

LWlock: RelCacheInit

Ein Prozess wartet darauf, eine `pg_internal.init`-Datei zu lesen oder zu aktualisieren (eine Initialisierungsdatei für den Beziehungscache).

LW-Schloss: RelCacheInitLock

Ein Prozess wartet darauf, eine Initialisierungsdatei für den Beziehungscache zu lesen oder zu schreiben.

LWLock:replication_origin

Ein Prozess wartet darauf, den Replikationsfortschritt zu lesen oder zu aktualisieren.

LWLock:replication_slot_io

Ein Prozess wartet auf I/O in einem Replikations-Slot.

LW-Schloss: ReplicationOrigin

Ein Prozess wartet darauf, einen Replikationsursprung zu erstellen, zu löschen oder zu verwenden.

LW-Schloss: ReplicationOriginLock

Ein Prozess wartet darauf, einen Replikationsursprung einzurichten, zu löschen oder zu verwenden.

LW-Schloss: ReplicationOriginState

Ein Prozess wartet darauf, den Fortschritt eines Replikationsursprungs zu lesen oder zu aktualisieren.

LW-Schloss: ReplicationSlotAllocation

Ein Prozess wartet darauf, einen Replikations-Slot zuzuweisen oder freizugeben.

LW-Schloss: ReplicationSlotAllocationLock

Ein Prozess wartet darauf, einen Replikations-Slot zuzuweisen oder freizugeben.

LW-Schloss: ReplicationSlotControl

Ein Prozess wartet darauf, einen Replikations-Slot-Status zu lesen oder zu aktualisieren.

LW-Schloss: ReplicationSlotControlLock

Ein Prozess wartet darauf, den Status des Replikations-Slots zu lesen oder zu aktualisieren.

lWlock: Ja ReplicationSlot

Ein Prozess wartet auf I/O in einem Replikations-Slot.

LWlock: SerialBuffer

Ein Prozess wartet auf I/O in einem einfachen, selten verwendeten Puffer (SLRU-Puffer) für einen serialisierbaren Transaktionskonflikt.

LW-Schloss: SerializableFinishedList

Ein Prozess wartet darauf, auf die Liste der abgeschlossenen serialisierbaren Transaktionen zuzugreifen.

LW-Schloss: SerializableFinishedListLock

Ein Prozess wartet darauf, auf die Liste der abgeschlossenen serialisierbaren Transaktionen zuzugreifen.

LW-Schloss: SerializablePredicateList

Ein Prozess wartet darauf, auf die Liste der Prädikatssperren zuzugreifen, die von serialisierbaren Transaktionen gehalten werden.

LW-Schloss: SerializablePredicateLockListLock

Ein Prozess wartet darauf, eine Operation für eine Liste von Sperren auszuführen, die von serialisierbaren Transaktionen gehalten werden.

LW-Schloss: SerializableXactHash

Ein Prozess wartet darauf, Informationen zu serialisierbaren Transaktionen zu lesen oder zu aktualisieren.

LW-Schloss: SerializableXactHashLock

Ein Prozess wartet darauf, Informationen zu serialisierbaren Transaktionen abzurufen oder zu speichern.

LWLock:SerialSLRU

Ein Prozess wartet auf den Zugriff auf den einfachen, selten verwendeten Cache (SLRU-Cache) für einen serialisierbaren Transaktionskonflikt.

LW-Schloss: SharedTidBitmap

Ein Prozess wartet darauf, während einer parallelen Bitmap-Indexabtastung auf eine Bitmap mit gemeinsam genutzten Tupelidentifizierern (TID) zuzugreifen.

LW-Schloss: SharedTupleStore

Ein Prozess wartet während einer parallelen Abfrage darauf, auf einen gemeinsam genutzten Tupelspeicher zuzugreifen.

LW-Schloss: ShmemIndex

Ein Prozess wartet darauf, Speicherplatz im gemeinsam genutzten Speicher zu finden oder zuzuweisen.

LW-Schloss: ShmemIndexLock

Ein Prozess wartet darauf, Speicherplatz im gemeinsam genutzten Speicher zu finden oder zuzuweisen.

lWlocks: InvalRead

Ein Prozess wartet darauf, Nachrichten aus der freigegebenen Katalog-Invalidierungswarteschlange abzurufen.

Lwlocks: InvalReadLock

Ein Prozess wartet darauf, Nachrichten aus einer gemeinsam genutzten Invalidierungswarteschlange abzurufen oder zu entfernen.

Lwlocks: InvalWrite

Ein Prozess wartet darauf, der gemeinsam genutzten Katalog-Invalidierungswarteschlange eine Nachricht hinzuzufügen.

Lwlocks: InvalWriteLock

Ein Prozess wartet darauf, eine Nachricht in eine gemeinsam genutzte Invalidierungswarteschlange hinzuzufügen.

LWLock:subtrans

Ein Prozess wartet auf I/O in einem Subtransaktionspuffer.

LW Lock: SubtransBuffer

Ein Prozess wartet auf I/O in einem einfachen, selten verwendeten Puffer (SLRU-Puffer) für eine Subtransaktion.

LW-Schloss: SubtransControlLock

Ein Prozess wartet darauf, Subtransaktionsinformationen zu lesen oder zu aktualisieren.

LWLock:SubtransSLRU

Ein Prozess wartet darauf, auf den einfachen, selten verwendeten Cache (SLRU-Cache) für eine Untertransaktion zuzugreifen.

LW-Schloss: SyncRep

Ein Prozess wartet darauf, Informationen zum Status der synchronen Replikation zu lesen oder zu aktualisieren.

LW-Schloss: SyncRepLock

Ein Prozess wartet darauf, Informationen zu synchronen Replikaten zu lesen oder zu aktualisieren.

LW-Schloss: SyncScan

Ein Prozess wartet darauf, den Startort eines synchronisierten Tabellenscans auszuwählen.

LW-Schloss: SyncScanLock

Ein Prozess wartet darauf, die Startposition eines Scans in einer Tabelle für synchronisierte Scans abzurufen.

LW-Schloss: TablespaceCreate

Ein Prozess wartet darauf, einen Tablespace zu erstellen oder zu löschen.

LW-Schloss: TablespaceCreateLock

Ein Prozess wartet darauf, den Tablespace zu erstellen oder zu löschen.

LWLock:tbm

Ein Prozess wartet auf eine gemeinsame Iteratorsperre für eine Baum-Bitmap (TBM).

LW-Schloss: TwoPhaseState

Ein Prozess wartet darauf, den Status vorbereiteter Transaktionen zu lesen oder zu aktualisieren.

LW-Schloss: TwoPhaseStateLock

Ein Prozess wartet darauf, den Status vorbereiteter Transaktionen zu lesen oder zu aktualisieren.

LWLock:wal_insert

Ein Prozess wartet darauf, das Write-Ahead-Log (WAL) in einen Speicherpuffer einzufügen.

LWlock: WAL BufMapping

Ein Prozess wartet darauf, eine Seite in Write-Ahead-Log(WAL)-Puffern zu ersetzen.

Lwlock: WAL BufMappingLock

Ein Prozess wartet darauf, eine Seite in Write-Ahead-Log(WAL)-Puffern zu ersetzen.

LWLock:WALInsert

Ein Prozess wartet darauf, Write-Ahead-Protokolldaten (WAL) in einen Speicherpuffer einzufügen.

LWLock:WALWrite

Ein Prozess wartet darauf, dass Write-Ahead-Protokoll-Puffer (WAL) auf die Platte geschrieben werden.

Lwlock: WAL WriteLock

Ein Prozess wartet darauf, dass Write-Ahead-Protokoll-Puffer (WAL) auf die Platte geschrieben werden.

LWlock: WrapLimitsVacuum

Ein Prozess wartet darauf, die Limits für Transaktions-ID und Multixact-Verbrauch zu aktualisieren.

LW-Schloss: WrapLimitsVacuumLock

Ein Prozess wartet darauf, die Limits für Transaktions-ID und Multixact-Verbrauch zu aktualisieren.

LW-Schloss: XactBuffer

Ein Prozess wartet auf I/O in einem einfachen, selten verwendeten Puffer (SLRU-Puffer) für einen Transaktionsstatus.

LWLock:XactSLRU

Ein Prozess wartet darauf, für einen Transaktionsstatus auf den einfachen, selten verwendeten Cache (SLRU-Cache) zuzugreifen.

LW-Schloss: XactTruncation

Ein Prozess wartet darauf, pg_xact_status auszuführen oder die älteste verfügbare Transaktions-ID zu aktualisieren.

LW-Schloss: XidGen

Ein Prozess wartet darauf, eine neue Transaktions-ID zuzuweisen.

LW-Schloss: XidGenLock

Ein Prozess wartet darauf, eine Transaktions-ID zu vergeben oder zuzuweisen.

Auszeit: BaseBackupThrottle

Ein Prozess wartet während der Basissicherung, wenn die Aktivität gedrosselt wird.

Auszeit: PgSleep

Ein Backend-Prozess hat die Funktion pg_sleep aufgerufen und wartet auf das Ablaufen des Sleep-Timeouts. Weitere Informationen finden Sie unter Timeout:PgSleep.

Auszeit: RecoveryApplyDelay

Ein Prozess wartet aufgrund einer Verzögerungseinstellung darauf, während der Wiederherstellung ein Write-Ahead-Protokoll (WAL) anzuwenden.

Auszeit: RecoveryRetrieveRetryInterval

Ein Prozess wartet während der Wiederherstellung, wenn Write-Ahead-Protokoll-Daten (WAL) von keiner Quelle (pg_wal, Archiv oder Stream) verfügbar sind.

Auszeit: VacuumDelay

Ein Prozess wartet in einem preis-basierten Vakuum-Verzögerungspunkt.

Eine vollständige Liste der PostgreSQL-Warteereignisse finden Sie unter Der Statistikkollektor > Warteereignistabellen in der PostgreSQL-Dokumentation.

Amazon Aurora PostgreSQL-Aktualisierungen

Nachstehend finden Sie Informationen zu Versionen und Aktualisierungen der Amazon-Aurora-PostgreSQL-Engine. Sie erfahren auch, wie Sie Ihre Aurora-PostgreSQL-Engine aktualisieren. Weitere Informationen zu Aurora-Versionen im Allgemeinen finden Sie unter Amazon-Aurora-Versionen.

> **Tip**
>
> Sie können die für ein DB-Cluster-Upgrade erforderlichen Ausfallzeiten minimieren, indem Sie eine Blau/Grün-Bereitstellung verwenden. Weitere Informationen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen für Datenbankaktualisierungen.

Themen

Identifizieren der Versionen von Amazon Aurora PostgreSQL

Amazon Aurora enthält bestimmte Funktionen, die für Aurora allgemein sind und für alle Aurora-DB-Cluster verfügbar sind. Amazon Aurora umfasst andere Funktionen, die spezifisch für eine bestimmte Datenbank-Engine sind, die Aurora unterstützt. Diese Funktionen stehen nur denjenigen Aurora-DB-Clustern zur Verfügung, die diese Datenbank-Engine verwenden, wie z. B. Aurora PostgreSQL.

Eine Aurora-Datenbank-Version hat normalerweise zwei Versionsnummern, die Aurora-Versionsnummer und die Versionsnummer der Datenbank-Engine. Wenn eine Aurora-PostgreSQL-Version eine Aurora-Versionsnummer hat, befindet sie sich in der Amazon Aurora PostgreSQL Releases und Engine Versionen-Auflistung hinter der Engine-Versionsnummer.

Aurora-Versionsnummer

Aurora-Versionsnummern verwenden das Namensschema *major.minor.patch* (Haupt.Neben.Patch). Eine Aurora-Patch-Version enthält wichtige Bugfixes, die einer Nebenversion

nach ihrer Veröffentlichung hinzugefügt werden. Weitere Informationen zu Haupt-, Neben- und Patch-Versionen von Amazon Aurora finden Sie unter Amazon-Aurora-Hauptversionen, Amazon-Aurora-Nebenversionen und Amazon-Aurora-Patchversionen.

Sie können die Aurora-Versionsnummer Ihrer Aurora-PostgreSQL-DB-Instance mit der folgenden SQL-Abfrage herausfinden:

```
postgres=> SELECT aurora_version();
```

Ab der Veröffentlichung der PostgreSQL-Versionen 13.3, 12.8, 11.13 und 10.18 und für alle späteren Versionen sind die Aurora-Versionsnummern genauer auf die PostgreSQL-Engine-Version abgestimmt. Wenn Sie beispielsweise einen Aurora-PostgreSQL-13.3-DB-Cluster abfragen, wird Folgendes zurückgegeben:

```
aurora_version
----------------
 13.3.1
(1 row)
```

Frühere Versionen, wie Aurora-PostgreSQL-10.14-DB-Cluster, liefern Versionsnummern wie folgende:

```
aurora_version
----------------
 2.7.3
(1 row)
```

Versionsnummern der PostgreSQL-Engine

Ab PostgreSQL 10 verwenden PostgreSQL-Datenbank-Engine-Versionen das Nummernschema *Haupt*.*Neben* für alle Releases. Beispiele: PostgreSQL 10.18, PostgreSQL 12.7 und PostgreSQL 13.3.

Releases vor PostgreSQL 10 verwendeten das Nummernschema *Haupt*.*Haupt*.*Neben*, in dem die ersten beiden Ziffern die Nummer der Hauptversion und die dritte Ziffer die Nebenversion angeben. PostgreSQL 9.6 war beispielsweise eine Hauptversion, wobei die Nebenversionen 9.6.21 oder 9.6.22 durch die dritte Ziffer gekennzeichnet waren.

> **Note**
>
> Die PostgreSQL-Engine-Version 9.6 wird nicht mehr unterstützt. Informationen zum Upgrade finden Sie unter Upgrade von DB-Clustern von Amazon Aurora PostgreSQL. Versionsrichtlinien und Release-Zeitpläne finden Sie unter Wie lange bleiben Amazon-Aurora-Hauptversionen verfügbar?.

Sie können die PostgreSQL-Datenbank-Engine-Versionsnummer mit der folgenden SQL-Abfrage herausfinden:

```
postgres=> SELECT version();
```

Für einen Aurora-PostgreSQL-13.3-DB-Cluster sind die Ergebnisse wie folgt:

```
version
-----------------------------------------------------------------------------------------------------
 PostgreSQL 13.3 on x86_64-pc-linux-gnu, compiled by x86_64-pc-linux-gnu-gcc (GCC)
 7.4.0, 64-bit
(1 row)
```

Amazon Aurora PostgreSQL Releases und Engine Versionen

Versionen der Amazon Aurora PostgreSQL-kompatiblen Edition werden regelmäßig aktualisiert. Updates werden auf Aurora-PostgreSQL-DB-Cluster während des Wartungszeitraums angewendet. Wann Aktualisierungen angewendet werden, hängt von der Art der Aktualisierung, der AWS-Region, der Einstellung für das Wartungsfenster und der Einstellung für den DB-Cluster ab. Viele der aufgelisteten Versionen enthalten sowohl eine PostgreSQL-Versionsnummer als auch eine Amazon-Aurora-Versionsnummer. Ab der Veröffentlichung der PostgreSQL-Versionen 13.3, 12.8, 11.13, 10.18 und für alle anderen späteren Versionen werden jedoch keine Aurora-Versionsnummern mehr verwendet. Zum Ermitteln der Versionsnummern Ihrer Aurora PostgreSQL-Datenbank siehe Identifizieren der Versionen von Amazon Aurora PostgreSQL.

Hinweise zu Erweiterungen und Modulen finden Sie unter Erweiterungsversionen für Amazon Aurora PostgreSQL.

> **Note**
>
> Informationen zu den Versionsrichtlinien und Veröffentlichungszeitplänen von Amazon Aurora finden Sie unter Wie lange bleiben Amazon-Aurora-Hauptversionen verfügbar?.

Informationen zu Support für Amazon Aurora finden Sie unter Häufig gestellte Fragen zu Amazon RDS.

Um festzustellen, welche Aurora PostgreSQL-DB-Engine-Versionen in einer AWS-Region verfügbar sind, verwenden Sie den AWS CLI-Befehl describe-db-engine-versions. Beispiel:

```
aws rds describe-db-engine-versions --engine aurora-postgresql --query '*[].
[EngineVersion]' --output text --region aws-region
```

Eine Liste der AWS-Regionen finden Sie unter Aurora PostgreSQL-Verfügbarkeit in Regionen.

Weitere Informationen zu den PostgreSQL-Versionen, die in Aurora PostgreSQL verfügbar sind, finden Sie in den Versionshinweisen für Aurora PostgreSQL.

Erweiterungsversionen für Amazon Aurora PostgreSQL

Sie können verschiedene PostgreSQL-Erweiterungen installieren und konfigurieren, um sie mit Aurora-PostgreSQL-DB-Clustern zu verwenden. Sie können beispielsweise die PostgreSQL-Erweiterung `pg_partman` verwenden, um die Erstellung und Pflege von Tabellenpartitionen zu automatisieren. Weitere Informationen über diese und andere für Aurora PostgreSQL verfügbare Erweiterungen finden Sie unter Arbeiten mit Erweiterungen und Fremddaten-Wrappern.

Weitere Informationen zu den PostgreSQL-Erweiterungen, die von Aurora PostgreSQL unterstützt werden, finden Sie unter Versionen der Erweiterungen für Amazon Aurora PostgreSQL in den Versionshinweisen für Aurora PostgreSQL.

Upgrade von DB-Clustern von Amazon Aurora PostgreSQL

Amazon Aurora stellt neue Versionen des PostgreSQL-Datenbankmoduls AWS-Regionen erst nach umfangreichen Tests zur Verfügung. Sie können Ihre Aurora-PostgreSQL-DB-Cluster auf die neue Version aktualisieren, wenn diese in Ihrer Region verfügbar ist.

Abhängig von der Version von Aurora PostgreSQL, die Ihr DB-Cluster derzeit ausführt, ist ein Upgrade auf die neue Version entweder ein Nebenversions- oder ein Hauptversions-Upgrade. Zum

Beispiel ist das Upgrade eines DB-Clusters von Aurora PostgreSQL 11.15 auf Aurora PostgreSQL 13.6 ein Hauptversions-Upgrade. Das Upgrade eines DB-Clusters von Aurora PostgreSQL 13.3 auf Aurora PostgreSQL 13.7 hingegen ist ein Nebenversions-Upgrade. In den folgenden Themen finden Sie Informationen darüber, wie beide Arten von Upgrades durchgeführt werden.

Inhalt

Übersicht über die Upgrade-Prozesse für Aurora-PostgreSQL

Zwischen Haupt- und Nebenversions-Upgrades gibt es folgende Unterschiede:

Nebenversions-Upgrades und -Patches

Nebenversions-Upgrades und -Patches enthalten nur Änderungen, die mit bestehenden Anwendungen abwärtskompatibel sind. Nebenversions-Upgrades und -Patches stehen Ihnen erst zur Verfügung, nachdem Aurora PostgreSQL sie getestet und genehmigt hat.

Nebenversions-Upgrades können von Aurora automatisch angewendet werden. Wenn Sie einen neuen Aurora-PostgreSQL-DB-Cluster erstellen, ist die Option Enable minor version upgrade (Nebenversions-Upgrade aktivieren) vorausgewählt. Wenn Sie diese Option nicht deaktivieren, werden Upgrades von Nebenversionen während des geplanten Wartungsfensters automatisch angewendet. Weitere Informationen zur Option für das automatische Nebenversions-Upgrade (Automatic Minor Version Upgrade, AmVU) und darüber, wie Sie Ihren Aurora-DB-Cluster ändern,

um diese verwenden zu können, finden Sie unter Automatische Nebenversions-Upgrades für Aurora-DB-Cluster.

Wenn die Option für das automatische Upgrade der Nebenversion für Ihren Aurora-PostgreSQL-DB-Cluster nicht festgelegt ist, wird Aurora PostgreSQL nicht automatisch auf die neue Nebenversion aktualisiert. Stattdessen fordert Aurora Sie zu einem Upgrade auf, wenn eine neue Nebenversion in Ihrem veröffentlicht wird AWS-Region und Ihr Aurora PostgreSQL-DB-Cluster eine ältere Nebenversion ausführt. Dazu wird den Wartungsaufgaben für Ihren Cluster eine Empfehlung hinzugefügt.

Patches gelten nicht als Upgrade und werden nicht automatisch angewendet. Aurora PostgreSQL fordert Sie auf, alle Patches anzuwenden, indem es den Wartungsaufgaben für Ihren Aurora-PostgreSQL-DB-Cluster eine Empfehlung hinzufügt. Weitere Informationen finden Sie unter So führen Sie Upgrades von Nebenversionen durch und wenden Patches an.

> **Note**
>
> Patches, die Sicherheits- oder andere kritische Probleme lösen, werden ebenfalls als Wartungsaufgaben hinzugefügt. Diese Patches sind jedoch erforderlich. Stellen Sie sicher, dass Sie Sicherheitspatches auf Ihren Aurora-PostgreSQL-DB-Cluster anwenden, wenn diese in Ihren ausstehenden Wartungsaufgaben verfügbar sind.

Beim Upgrade-Prozess kann es zu kurzen Ausfällen kommen, während jede Instance im Cluster auf die neue Version aktualisiert wird. Nach den Aurora-PostgreSQL-Versionen 14.3.3, 13.7.3, 12.11.3, 11.16.3, 10.21.3 und anderen höheren Versionen dieser Nebenversionen verwendet der Upgrade-Prozess jedoch die Zero Downtime Patching (ZDP)-Funktion. Diese Funktion minimiert Ausfälle und eliminiert sie in den meisten Fällen vollständig. Weitere Informationen finden Sie unter Nebenversions-Upgrades und Zero-Downtime-Patching.

> **Note**
>
> ZDP wird in folgenden Fällen nicht unterstützt:
>
> - Wenn DB-Cluster von Aurora PostgreSQL als Aurora Serverless v1 konfiguriert sind.
> - Wenn Aurora PostgreSQL-DB-Cluster als globale Aurora-Datenbank in der Sekundärdatenbank konfiguriert sind. AWS-Regionen
> - Während des Upgrades von Reader-Instances in der globalen Aurora-Datenbank.
> - Während Betriebssystem-Patches und Betriebssystem-Upgrades.

ZDP wird für Aurora PostgreSQL-DB-Cluster unterstützt, die als konfiguriert sind. Aurora Serverless v2

Hauptversions-Upgrades

Im Gegensatz zu Upgrades und Patches für Nebenversionen verfügt Aurora PostgreSQL über keine automatische Upgrade-Option für Hauptversionen. Hauptversions-Upgrades können Datenbankänderungen enthalten, die mit vorhandenen Anwendungen nicht abwärtskompatibel sind. Neue Funktionalität kann dazu führen, dass Ihre vorhandenen Anwendungen nicht mehr ordnungsgemäß funktionieren.

Zur Vermeidung von Problemen empfehlen wir dringend, dem in Testen eines Upgrades Ihres Produktions-DB-Clusters auf eine neue Hauptversion beschriebenen Verfahren zu folgen, bevor Sie die DB-Instances in Ihren Aurora-PostgreSQL-DB-Clustern upgraden. Stellen Sie zunächst sicher, dass Ihre Anwendungen mit der neuen Version ausgeführt werden können, indem Sie diesem Verfahren folgen. Dann können Sie Ihren Aurora-PostgreSQL-DB-Cluster manuell auf die neue Version aktualisieren.

Der Upgrade-Prozess beinhaltet die Möglichkeit eines kurzen Ausfalls, wenn alle Instances im Cluster auf die neue Version aktualisiert werden. Der vorläufige Planungsprozess braucht ebenfalls Zeit. Wir empfehlen Ihnen, Upgrade-Aufgaben immer während des Wartungsfensters Ihres Clusters oder bei minimalem Betrieb auszuführen. Weitere Informationen finden Sie unter Durchführen eines Hauptversions-Upgrades.

> **Note**
>
> Sowohl Upgrades von Neben- als auch von Hauptversionen können kurze Ausfälle verursachen. Aus diesem Grund empfehlen wir dringend, dass Sie Upgrades während Ihres Wartungsfensters oder in anderen Zeiträumen geringer Auslastung durchführen oder planen.

DB-Cluster von Aurora PostgreSQL erfordern gelegentlich Betriebssystem-Updates. Diese Updates können eine neuere Version der Glibc-Bibliothek umfassen. Bei solchen Updates empfehlen wir Ihnen, die unter In Aurora PostgreSQL unterstützte Sortierungen beschriebenen Richtlinien zu befolgen.

Sie erhalten eine Liste der verfügbaren Versionen in Ihrem AWS-Region

Sie können eine Liste aller Engine-Versionen abrufen, die als Upgrade-Ziele für Ihren Aurora PostgreSQL-DB-Cluster verfügbar sind, indem Sie Sie AWS-Region mit dem describe-db-engine-versions AWS CLI folgenden Befehl abfragen.

FürLinux, oder: macOS Unix

```
aws rds describe-db-engine-versions \
  --engine aurora-postgresql \
  --engine-version version-number \
  --query 'DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}' \
  --output text
```

Windows:

```
aws rds describe-db-engine-versions ^
  --engine aurora-postgresql ^
  --engine-version version-number ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" ^
  --output text
```

Um beispielsweise die gültigen Upgrade-Ziele für einen Aurora PostgreSQL-DB-Cluster der Version 12.10 zu identifizieren, führen Sie den folgenden Befehl aus: AWS CLI

FürLinux, oder: macOS Unix

```
aws rds describe-db-engine-versions \
  --engine aurora-postgresql \
  --engine-version 12.10 \
  --query 'DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}' \
  --output text
```

Windows:

```
aws rds describe-db-engine-versions ^
  --engine aurora-postgresql ^
  --engine-version 12.10 ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" ^
  --output text
```

In der Tabelle finden Sie die Haupt- und Unterversions-Upgrades, die für verschiedene Aurora-PostgreSQL-DB-Versionen verfügbar sind.

Aktue Quell ion	Upgrade-Ziele
16.1	16
15,6	16
15,5	16 16 15
15,4	16 16 15 15
15,3	16 16 15 15 15
15,2	16 16 15 15 15 15
14,11	16 15
14,10	16 16 15 15
14,9	16 16 15 15 15 14 14
14,8	16 16 15 15 15 15 15 14 14 14
14,7	16 16 15 15 15 15 15 14 14 14 14
14,6	16 16 15 15 15 15 15 14 14 14 14 14
14,5	16 16 15 15 15 15 15 14 14 14 14 14 14
14,4	16 16 15 15 15 15 15 14 14 14 14 14 14 14
14,3	16 16 15 15 15 15 15 14 14 14 14 14 14 14 14
13,14	16 15 14
13,13	16 16 15 15 14 14

Aktue Quell ion	Upgrade-Ziele
13,12	16 16 15 15 15 14 14 14
13,11	16 16 15 15 15 15 14 14 14 14
13,10	16 16 15 15 15 15 15 14 14 14 14 14 13 13 13 13
13,9	16 16 15 15 15 15 15 14 14 14 14 14 14 13 13 13
13,8	16 16 15 15 15 15 15 14 14 14 14 14 14 14 13 13 13 13 13 13
13,7	16 16 15 15 15 15 15 14 14 14 14 14 14 14 14 14 13 13 13 13 13 13 13
12,18	16 15 14 13
12,17	16 16 15 15 14 14 13
12,16	16 16 15 15 15 14 14 14 13 13 13
12,15	16 16 15 15 15 15 14 14 14 14 13 13 13 13
12,14	16 16 15 15 15 15 15 15 14 14 14 14 14 13 13 13 13 13 12
12,13	16 16 15 15 15 15 15 14 14 14 14 14 14 13 13 13 13 13 13 12 12 12 12
12,12	16 16 15 15 15 15 15 14 14 14 14 14 14 14 13 13 13 13 13 13 12 12 12 13 12 12 12
12,11	16 16 15 15 15 15 15 14 14 14 14 14 14 14 14 13 13 13 13 13 13 13 13 13 12 12 12 12
12,9	16 16 15 15 15 15 15 14 14 14 14 14 13 13 13 13 13 13 13 13 12 12 12 12 12 12 12
11,12	16 16 15 15 15 14 14 14 13 13 13 12 12
11.9	16 16 15 15 15 15 15 14 14 14 14 14 14 13 13 13 13 13 13 12 12 12 12 12 12 12 12 11,21

Überprüfen Sie für jede Version, die Sie in Betracht ziehen, immer die Verfügbarkeit der DB-Instance-Klasse Ihres Clusters. Beispielsweise wird `db.r4` für Aurora PostgreSQL 13 nicht unterstützt. Wenn Ihr DB-Cluster von Aurora PostgreSQL derzeit eine db.r4-Instance-Klasse verwendet, müssen Sie auf

db.r5 umstellen, bevor Sie ein Upgrade ausführen. Weitere Informationen zu DB-Instance-Klassen, einschließlich der Frage, welche Graviton2-basiert und welche Intel-basiert sind, finden Sie unter Aurora DB-Instance-Klassen.

Durchführen eines Hauptversions-Upgrades

Hauptversions-Upgrades können Datenbankänderungen enthalten, die möglicherweise nicht mit früheren Versionen der Datenbank abwärtskompatibel sind. Neue Funktionalität einer neuen Version kann dazu führen, dass Ihre vorhandenen Anwendungen nicht mehr ordnungsgemäß funktionieren. Zur Vermeidung von Problemen wendet Amazon Aurora Hauptversions-Upgrades nicht automatisch an. Wir empfehlen vielmehr, dass Sie ein Hauptversions-Upgrade sorgfältig planen, indem Sie die folgenden Schritte ausführen:

1. Wählen Sie die gewünschte Hauptversion aus der Liste der verfügbaren Ziele aus, die für Ihre Version in der Tabelle aufgeführt sind. Eine genaue Liste der in Ihrer AWS-Region aktuellen Version verfügbaren Versionen erhalten Sie mit dem AWS CLI. Details hierzu finden Sie unter Sie erhalten eine Liste der verfügbaren Versionen in Ihrem AWS-Region.
2. Stellen Sie sicher, dass Ihre Anwendungen bei einer Testbereitstellung der neuen Version erwartungsgemäß funktionieren. Weitere Informationen zum vollständigen Prozess finden Sie unter Testen eines Upgrades Ihres Produktions-DB-Clusters auf eine neue Hauptversion.
3. Nachdem Sie überprüft haben, dass Ihre Anwendungen bei der Testbereitstellung wie erwartet funktionieren, können Sie Ihren Cluster aktualisieren. Details hierzu finden Sie unter Upgrade der Aurora-PostgreSQL-Engine auf eine neue Hauptversion.

> **Note**
>
> Sie können ein Hauptversions-Upgrade von auf Babelfish für Aurora PostgreSQL 13 basierende Versionen ab 13.6 auf Versionen durchführen, die auf Aurora PostgreSQL 14 basieren, und zwar ab 14.6. Babelfish für Aurora PostgreSQL 13.4 und 13.5 unterstützen kein Hauptversions-Upgrade.

Sie können eine Liste der Engine-Versionen abrufen, die als Haupt-Versions-Upgrade-Ziele für Ihren Aurora PostgreSQL-DB-Cluster verfügbar sind, indem Sie Sie AWS-Region mit dem describe-db-engine-versions AWS CLI folgenden Befehl abfragen.

FürLinux, oder: macOS Unix

```
aws rds describe-db-engine-versions \
  --engine aurora-postgresql \
  --engine-version version-number \
  --query 'DBEngineVersions[].ValidUpgradeTarget[?IsMajorVersionUpgrade == `true`].
{EngineVersion:EngineVersion}' \
  --output text
```

Windows:

```
aws rds describe-db-engine-versions ^
  --engine aurora-postgresql ^
  --engine-version version-number ^
  --query "DBEngineVersions[].ValidUpgradeTarget[?IsMajorVersionUpgrade == `true`].
{EngineVersion:EngineVersion}" ^
  --output text
```

In einigen Fällen ist die Version, auf die Sie upgraden möchten, kein Ziel für Ihre aktuelle Version. Verwenden Sie in solchen Fällen die Informationen in versions table, um Nebenversions-Upgrades durchzuführen, bis sich Ihr Cluster in einer Version befindet, die Ihr ausgewähltes Ziel in seiner Zielzeile enthält.

Testen eines Upgrades Ihres Produktions-DB-Clusters auf eine neue Hauptversion

Jede neue Hauptversion enthält Verbesserungen am Abfrageoptimierer, die auf Leistungssteigerung ausgelegt sind. Ihr Workload kann jedoch Abfragen enthalten, die in der neuen Version zu einem Plan mit schlechter Leistung führen. Aus diesem Grund empfehlen wir Ihnen, die Leistung zu testen und zu überprüfen, bevor Sie ein Upgrade in der Produktion durchführen. Sie können die Stabilität des Abfrageplans über Versionen hinweg verwalten, indem Sie die Erweiterung Query Plan Management (QPM) verwenden, wie in Sicherstellen der Planstabilität nach einem größeren Versions-Upgrade ausführlich beschrieben.

Bevor Sie Ihre Produktions-DB-Cluster von Aurora PostgreSQL auf eine neue Hauptversion upgraden, wird dringend empfohlen, das Upgrade zu testen, um sicherzustellen, dass alle Ihre Anwendungen ordnungsgemäß funktionieren:

1. Halten Sie eine versionskompatible Parametergruppe bereit.

   Wenn Sie eine benutzerdefinierte DB-Instance- oder DB-Cluster-Parametergruppe verwenden, haben Sie zwei Möglichkeiten:

a. Geben Sie die Standard-DB-Instance, die DB-Cluster-Parametergruppe oder beides für die neue DB-Engine-Version an.

b. Erstellen Sie eine eigene benutzerdefinierte Parametergruppe für die neue DB-Engine-Version.

Wenn Sie eine neue DB-Instance- oder eine neue DB-Cluster-Parametergruppe als Teil der Upgrade-Anforderung zuordnen, stellen Sie sicher, dass Sie die Datenbank nach Abschluss des Upgrades neu starten, um die Parameter anzuwenden. Wenn eine DB-Instance neu gestartet werden muss, um die Änderungen der Parametergruppe zu übernehmen, wird als Parametergruppenstatus der Instance angegebe `pending-reboot`. Sie können den Parametergruppenstatus einer Instance in der Konsole oder mithilfe eines CLI-Befehls wie describe-db-instancesoder anzeigen describe-db-clusters.

2. Auf nicht unterstützte Verwendung prüfen:

- Übernehmen Sie oder machen Sie alle offenen vorbereiteten Transaktionen rückgängig, bevor Sie ein Upgrade durchführen. Mit der folgenden Abfrage können Sie sicherstellen, dass für Ihre Instance keine geöffneten vorbereiteten Transaktionen vorhanden sind.

```
SELECT count(*) FROM pg_catalog.pg_prepared_xacts;
```

- Entfernen Sie alle Anwendungen der reg*-Datentypen, bevor Sie versuchen, einen Upgrade durchzuführen. Bis auf `regtype` und `regclass` ist kein Upgrade der reg*-Datentypen möglich. Das Dienstprogramm pg_upgrade (das von Amazon Aurora zur Durchführung des Upgrades verwendet wird) kann diesen Datentyp nicht beibehalten. Weitere Informationen zu diesem Dienstprogramm finden Sie unter pg_upgrade in der PostgreSQL-Dokumentation.

  Um zu überprüfen, dass keine Anwendungen der nicht unterstützten reg*-Datentypen vorhanden sind, geben Sie für jede Datenbank die folgende Abfrage aus.

```
SELECT count(*) FROM pg_catalog.pg_class c, pg_catalog.pg_namespace n,
 pg_catalog.pg_attribute a
  WHERE c.oid = a.attrelid
      AND NOT a.attisdropped
      AND a.atttypid IN ('pg_catalog.regproc'::pg_catalog.regtype,
                         'pg_catalog.regprocedure'::pg_catalog.regtype,
                         'pg_catalog.regoper'::pg_catalog.regtype,
                         'pg_catalog.regoperator'::pg_catalog.regtype,
                         'pg_catalog.regconfig'::pg_catalog.regtype,
                         'pg_catalog.regdictionary'::pg_catalog.regtype)
      AND c.relnamespace = n.oid
```

```
      AND n.nspname NOT IN ('pg_catalog', 'information_schema');
```

- Wenn Sie ein Upgrade eines DB-Clusters mit Aurora PostgreSQL Version 10.18 oder höher durchführen, für den die Erweiterung `pgRouting` installiert ist, entfernen Sie diese Erweiterung, bevor Sie auf Version 12.4 oder höher aktualisieren.

  Wenn Sie ein Upgrade eines DB-Clusters mit Aurora-PostgreSQL-Version 10.x oder höher durchführen, für die die Erweiterung `pg_repack` Version 1.4.3 installiert ist, entfernen Sie diese Erweiterung, bevor Sie auf eine höhere Version aktualisieren.

3. Suchen Sie nach den Datenbanken Template1 und Template0.

   Für ein erfolgreiches Upgrade müssen die Datenbanken Template 1 und Template 0 vorhanden sein und sollten als Vorlage aufgeführt werden. Verwenden Sie den folgenden Befehl, um dies zu überprüfen:

```
SELECT datname, datistemplate FROM pg_database;

datname    | datistemplate
-----------+---------------
template0  | t
rdsadmin   | f
template1  | t
postgres   | f
```

   In der Befehlsausgabe sollte der Wert `datistemplate` für die Datenbanken template1 und template0 `t` lauten.

4. Entfernen von logischen Replikations-Slots.

   Der Upgrade-Vorgang kann nicht fortgesetzt werden, wenn der Aurora PostgreSQL DB-Cluster logische Replikations-Slots verwendet. Logische Replikationssteckplätze werden in der Regel für kurzfristige Datenmigrationsaufgaben verwendet, z. B. für die Migration von Daten mithilfe von AWS DMS oder für die Replikation von Tabellen aus der Datenbank in Data Lakes, BI-Tools oder andere Ziele. Vergewissern Sie sich vor dem Upgrade, dass Sie den Zweck der vorhandenen logischen Replikations-Slots kennen, und bestätigen Sie, dass sie gelöscht werden dürfen. Sie können mit der folgenden Abfrage nach logischen Replikationssteckplätzen suchen:

```
SELECT * FROM pg_replication_slots;
```

Wenn die logischen Replikations-Slots noch verwendet werden, sollten Sie sie nicht löschen, und Sie können mit dem Upgrade nicht fortfahren. Wenn die logischen Replikations-Slots jedoch nicht benötigt werden, können Sie sie mit folgendem SQL-Befehl löschen:

```
SELECT pg_drop_replication_slot(slot_name);
```

Für logische Replikationsszenarien, die die `pglogical`-Erweiterung verwenden, müssen außerdem Slots vom Herausgeberknoten gelöscht werden, damit ein Hauptversions-Upgrade auf diesem Knoten erfolgreich durchgeführt werden kann. Sie können den Replikationsprozess jedoch nach dem Upgrade vom Abonnentenknoten aus neu starten. Weitere Informationen finden Sie unter Wiederherstellung der logischen Replikation nach einem Hauptversions-Upgrade.

5. Führen Sie ein Backup durch.

   Der Aktualisierungsprozess erstellt während des Upgrades einen DB-Cluster-Snapshot des DB-Clusters. Wenn Sie vor dem Upgrade auch ein manuelles Backup durchführen möchten, finden Sie weitere Informationen unter Erstellen eines DB-Cluster-Snapshots.

6. Aktualisieren Sie bestimmte Erweiterungen auf die neueste verfügbare Version, bevor Sie das Upgrade der Hauptversion durchführen. Zu den Erweiterungen, die aktualisiert werden sollen, gehören folgende:

   - `pgRouting`
   - `postgis_raster`
   - `postgis_tiger_geocoder`
   - `postgis_topology`
   - `address_standardizer`
   - `address_standardizer_data_us`

   Führen Sie den folgenden Befehl für jede derzeit installierte Erweiterung aus.

   ```
   ALTER EXTENSION PostgreSQL-extension UPDATE TO 'new-version';
   ```

   Weitere Informationen finden Sie unter Aktualisieren von PostgreSQL-Erweiterungen. Weitere Informationen zum Aktualisieren von PostGIS finden Sie unterSchritt 6: Upgrade der PostGIS-Erweiterung.

7. Wenn Sie ein Upgrade auf Version 11.x durchführen, löschen Sie die Erweiterungen, die nicht unterstützt werden, bevor Sie das Upgrade der Hauptversion durchführen. Die zu löschenden Erweiterungen umfassen:
   - `chkpass`
   - `tsearch2`
8. Löschen Sie `unknown`-Datentypen, abhängig von Ihrer Zielversion.

   PostgreSQL-Version 10 unterstützt den Datentyp `unknown` nicht. Wenn eine Datenbank der Version 9.6 den Datentyp `unknown` verwendet, wird bei einem Upgrade auf Version 10 eine Fehlermeldung wie die folgende angezeigt.

   ```
   Database instance is in a state that cannot be upgraded: PreUpgrade checks failed:
   The instance could not be upgraded because the 'unknown' data type is used in user
    tables.
   Please remove all usages of the 'unknown' data type and try again."
   ```

   Verwenden Sie den folgenden SQL-Code für jede Datenbank, um den `unknown`-Datentyp in Ihrer Datenbank zu finden, damit Sie solche Spalten entfernen oder in unterstützte Datentypen ändern können.

   ```
   SELECT n.nspname, c.relname, a.attname
       FROM pg_catalog.pg_class c,
       pg_catalog.pg_namespace n,
       pg_catalog.pg_attribute a
       WHERE c.oid = a.attrelid AND NOT a.attisdropped AND
       a.atttypid = 'pg_catalog.unknown'::pg_catalog.regtype AND
       c.relkind IN ('r','m','c') AND
       c.relnamespace = n.oid AND
       n.nspname !~ '^pg_temp_' AND
       n.nspname !~ '^pg_toast_temp_' AND n.nspname NOT IN ('pg_catalog',
    'information_schema');
   ```
9. Führen Sie ein Test-Upgrade durch.

   Es wird dringend empfohlen, das Upgrade der Hauptversion auf einem Duplikat Ihrer Produktionsdatenbank zu testen, bevor Sie versuchen, das Upgrade für Ihre Produktionsdatenbank auszuführen. Sie können die Ausführungspläne auf der duplizierten Testinstance auf mögliche Regressionen des Ausführungsplans überwachen und deren Leistung bewerten. Um ein Duplikat der Test-Instance zu erstellen, können Sie Ihre Datenbank

entweder aus einem aktuellen Snapshot wiederherstellen oder Ihre Datenbank klonen. Weitere Informationen finden Sie unter Wiederherstellung aus einem Snapshot oder Klonen eines Volumes für einen Amazon-Aurora-DB-Cluster.

Weitere Informationen finden Sie unter Upgrade der Aurora-PostgreSQL-Engine auf eine neue Hauptversion.

10 Aktualisieren Sie Ihre Produktionsinstance.

Wenn das Hauptversions-Upgrade für den Testlauf erfolgreich ist, sollten Sie jetzt in der Lage sein, Ihre Produktionsdatenbank sicher zu aktualisieren. Weitere Informationen finden Sie unter Upgrade der Aurora-PostgreSQL-Engine auf eine neue Hauptversion.

> **Note**
>
> Während des Upgrade-Prozesses erstellt Aurora PostgreSQL einen DB-Cluster-Snapshot, wenn die Backup-Aufbewahrungszeit des Clusters größer als 0 ist. Während dieses Vorgangs können Sie Ihren Cluster nicht point-in-time wiederherstellen. Später können Sie die Zeiten vor Beginn des Upgrades und nach Abschluss des automatischen Snapshots Ihrer Instance point-in-time wiederherstellen. Sie können jedoch keine point-in-time Wiederherstellung auf eine frühere Nebenversion durchführen.

Für Informationen zu einem laufenden Upgrade können Sie mit Amazon RDS zwei Protokolle anzeigen, die von dem pg_upgrade-Dienstprogramm erstellt werden. Diese sind `pg_upgrade_internal.log` und `pg_upgrade_server.log`. Amazon Aurora hängt einen Zeitstempel an den Dateinamen für diese Protokolle an. Sie können diese Protokolle wie jedes andere Protokoll einsehen. Weitere Informationen finden Sie unter Überwachen von Amazon Aurora-Protokolldateien.

11 Aktualisieren Sie PostgreSQL-Erweiterungen. Bei einem PostgreSQL-Upgrade-Prozess werden keine PostgreSQL-Erweiterungen aktualisiert. Weitere Informationen finden Sie unter Aktualisieren von PostgreSQL-Erweiterungen.

Nachdem Sie ein Upgrade der Hauptversion abgeschlossen haben, empfehlen wir Folgendes:

- Führen Sie die `ANALYZE`-Operation aus, um die Tabelle `pg_statistic` zu aktualisieren. Führen Sie diesen Schritt für jede Datenbank auf all Ihren PostgreSQL-DB-Instances durch. Optimizer-

Statistiken werden während eines Hauptversionsupgrades nicht übertragen, daher müssen Sie alle Statistiken neu generieren, um Leistungsprobleme zu vermeiden. Führen Sie den Befehl ohne Parameter aus, um Statistiken für alle regulären Tabellen in der aktuellen Datenbank wie folgt zu generieren:

```
ANALYZE VERBOSE;
```

Das Flag `VERBOSE` ist optional, aber wenn Sie es verwenden, wird Ihnen der Fortschritt angezeigt. Weitere Informationen finden Sie unter ANALYZE in der PostgreSQL-Dokumentation.

> **Note**
>
> Führen Sie ANALYZE nach dem Upgrade auf Ihrem System aus, um Leistungsprobleme zu vermeiden.

- Wenn Sie auf PostgreSQL Version 10 aktualisiert haben, führen Sie `REINDEX` auf allen Hash-Indizes aus, die Sie besitzen. Hash-Indizes wurden in Version 10 geändert und müssen neu erstellt werden. Um ungültige Hash-Indizes zu finden, führen Sie die folgende SQL-Anweisung für jede Datenbank aus, die Hash-Indizes enthält.

```
SELECT idx.indrelid::regclass AS table_name,
   idx.indexrelid::regclass AS index_name
FROM pg_catalog.pg_index idx
   JOIN pg_catalog.pg_class cls ON cls.oid = idx.indexrelid
   JOIN pg_catalog.pg_am am ON am.oid = cls.relam
WHERE am.amname = 'hash'
AND NOT idx.indisvalid;
```

- Wir empfehlen, dass Sie Ihre Anwendung auf der aktualisierten Datenbank mit ähnlicher Workload testen, um sicherzustellen, dass alles wie erwartet funktioniert. Nachdem das Upgrade bestätigt wurde, können Sie diese Testinstance löschen.

Upgrade der Aurora-PostgreSQL-Engine auf eine neue Hauptversion

Wenn Sie den Upgrade-Prozess auf eine neue Hauptversion einleiten, erstellt Aurora PostgreSQL einen Snapshot des Aurora-DB-Clusters, bevor er Änderungen an Ihrem Cluster vornimmt. Dieser Snapshot wird nur für Hauptversions-Upgrades erstellt, nicht für Nebenversions-Upgrades. Wenn der Upgrade-Vorgang abgeschlossen ist, finden Sie diesen Snapshot unter den manuellen Snapshots, die unter Snapshots in der RDS-Konsole aufgeführt sind. Der Snapshot-Name enthält `preupgrade`

als Präfix, den Namen Ihres Aurora-PostgreSQL-DB-Clusters, die Quellversion, die Zielversion sowie das Datum und den Zeitstempel, wie im folgenden Beispiel gezeigt.

```
preupgrade-docs-lab-apg-global-db-12-8-to-13-6-2022-05-19-00-19
```

Nach Abschluss des Upgrades können Sie den Snapshot, den Aurora erstellt und in Ihrer manuellen Snapshot-Liste erstellt und gespeichert hat, verwenden, um den DB-Cluster gegebenenfalls auf seine vorherige Version wiederherzustellen.

> **Tip**
>
> Im Allgemeinen bieten Snapshots viele Möglichkeiten, Ihren Aurora-DB-Cluster zu verschiedenen Zeitpunkten wiederherzustellen. Weitere Informationen hierzu finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot und Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit. Aurora PostgreSQL unterstützt jedoch nicht die Verwendung eines Snapshots für die Wiederherstellung auf eine frühere Nebenversion.

Während des Hauptversions-Upgrades weist Aurora ein Volume zu und klont den Quell-DB-Cluster von Aurora PostgreSQL. Wenn das Upgrade aus irgendeinem Grund fehlschlägt, verwendet Aurora PostgreSQL den Klon, um das Upgrade zurückzusetzen. Nachdem mehr als 15 Klone eines Quell-Volumes zugewiesen wurden, werden nachfolgende Klone zu vollständigen Kopien und dauern länger. Dies kann dazu führen, dass der Upgrade-Prozess ebenfalls länger dauert. Wenn Aurora PostgreSQL das Upgrade zurücksetzt, beachten Sie Folgendes:

- Möglicherweise sehen Sie Fakturierungseinträge und Metriken sowohl für das ursprüngliche Volume als auch für das geklonte Volume, das während des Upgrades zugewiesen wurde. Aurora PostgreSQL bereinigt das zusätzliche Volume, nachdem das Aufbewahrungsfenster für Cluster-Backups den Zeitpunkt des Upgrades überschritten hat.
- Die nächste regionsübergreifende Snapshot-Kopie aus diesem Cluster ist eine vollständige Kopie anstelle einer inkrementellen Kopie.

Um die DB-Instances, aus denen Ihr Cluster besteht, sicher zu aktualisieren, verwendet Aurora PostgreSQL das Dienstprogramm pg_upgrade. Nach Abschluss des Writer-Upgrades kommt es zu einem kurzen Ausfall aller Reader-Instances, während sie auf die neue Hauptversion aktualisiert werden. Weitere Informationen zu diesem PostgreSQL-Dienstprogramm finden Sie unter pg_upgrade in der PostgreSQL-Dokumentation.

Sie können Ihren Aurora PostgreSQL-DB-Cluster auf eine neue Version aktualisieren, indem Sie die AWS Management Console AWS CLI, oder die RDS-API verwenden.

Konsole

So führen Sie ein Upgrade der Engine-Version eines DB-Clusters durch

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann den DB-Cluster aus, den Sie upgraden möchten.
3. Wählen Sie Ändern aus. Die Seite DB-Cluster ändern wird angezeigt.
4. Wählen Sie für Motorversion die neue Version.
5. Klicken Sie auf Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.
6. Wählen Sie Apply immediately, um die Änderungen sofort anzuwenden. Die Auswahl dieser Option kann in einigen Fällen einen Ausfall verursachen. Weitere Informationen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.
7. Überprüfen Sie auf der Bestätigungsseite Ihre Änderungen. Wenn sie korrekt sind, wählen Sie Modify Cluster (Cluster ändern) aus, um Ihre Änderungen zu speichern.

   Oder klicken Sie auf Zurück, um Ihre Änderungen zu bearbeiten, oder auf Abbrechen, um Ihre Änderungen zu verwerfen.

AWS CLI

Verwenden Sie den modify-db-cluster AWS CLI Befehl, um die Engine-Version eines DB-Clusters zu aktualisieren. Geben Sie die folgenden Parameter an:

- `--db-cluster-identifier` – der Name des DB-Clusters.
- `--engine-version` – die Versionsnummer der Datenbank-Engine, auf die das Upgrade durchgeführt wird Verwenden Sie den AWS CLI describe-db-engine-versionsBefehl, um Informationen zu gültigen Engine-Versionen zu erhalten.
- `--allow-major-version-upgrade` – ein erforderliches Flag, wenn die Hauptversion des `--engine-version`-Parameters von der aktuellen Hauptversion des DB-Clusters abweicht
- `--no-apply-immediately` – Änderungen im nächsten Wartungszeitraum anwenden Verwenden Sie , um Änderungen sofort anzuwende `--apply-immediately`.

Example

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --engine-version new_version \
    --allow-major-version-upgrade \
    --no-apply-immediately
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --engine-version new_version ^
    --allow-major-version-upgrade ^
    --no-apply-immediately
```

RDS-API

Sie können die Engine-Version eines DB-Clusters upgraden, indem Sie die Operation ModifyDBCluster aufrufen. Geben Sie die folgenden Parameter an:

- `DBClusterIdentifier` – der Name des DB-Clusters, z. B *`mydbcluster`*
- `EngineVersion` – die Versionsnummer der Datenbank-Engine, auf die das Upgrade durchgeführt wird Verwenden Sie den Vorgang DescribeDB, um Informationen zu gültigen Engine-Versionen zu EngineVersions erhalten.
- `AllowMajorVersionUpgrade` – ein erforderliches Flag, wenn die Hauptversion des `EngineVersion`-Parameters von der aktuellen Hauptversion des DB-Clusters abweicht
- `ApplyImmediately` – Änderungen sofort oder während des nächsten Wartungszeitraums anwenden Legen Sie den Wert auf fest, um Änderungen sofort anzuwende `true`. Legen Sie den Wert auf fest, um Änderungen im nächsten Wartungszeitraum durchzuführe `false`.

Hauptversions-Upgrades für globale Datenbanken

Bei einem globalen Aurora-Datenbank-Cluster aktualisiert der Upgrade-Prozess alle DB-Cluster, aus denen Ihre globale Aurora-Datenbank besteht, gleichzeitig. Damit wird sichergestellt, dass jeder dieselbe Aurora-PostgreSQL-Version ausführt. Außerdem wird sichergestellt, dass Änderungen an Systemtabellen, Datendateiformaten usw. automatisch auf alle sekundären Cluster repliziert werden.

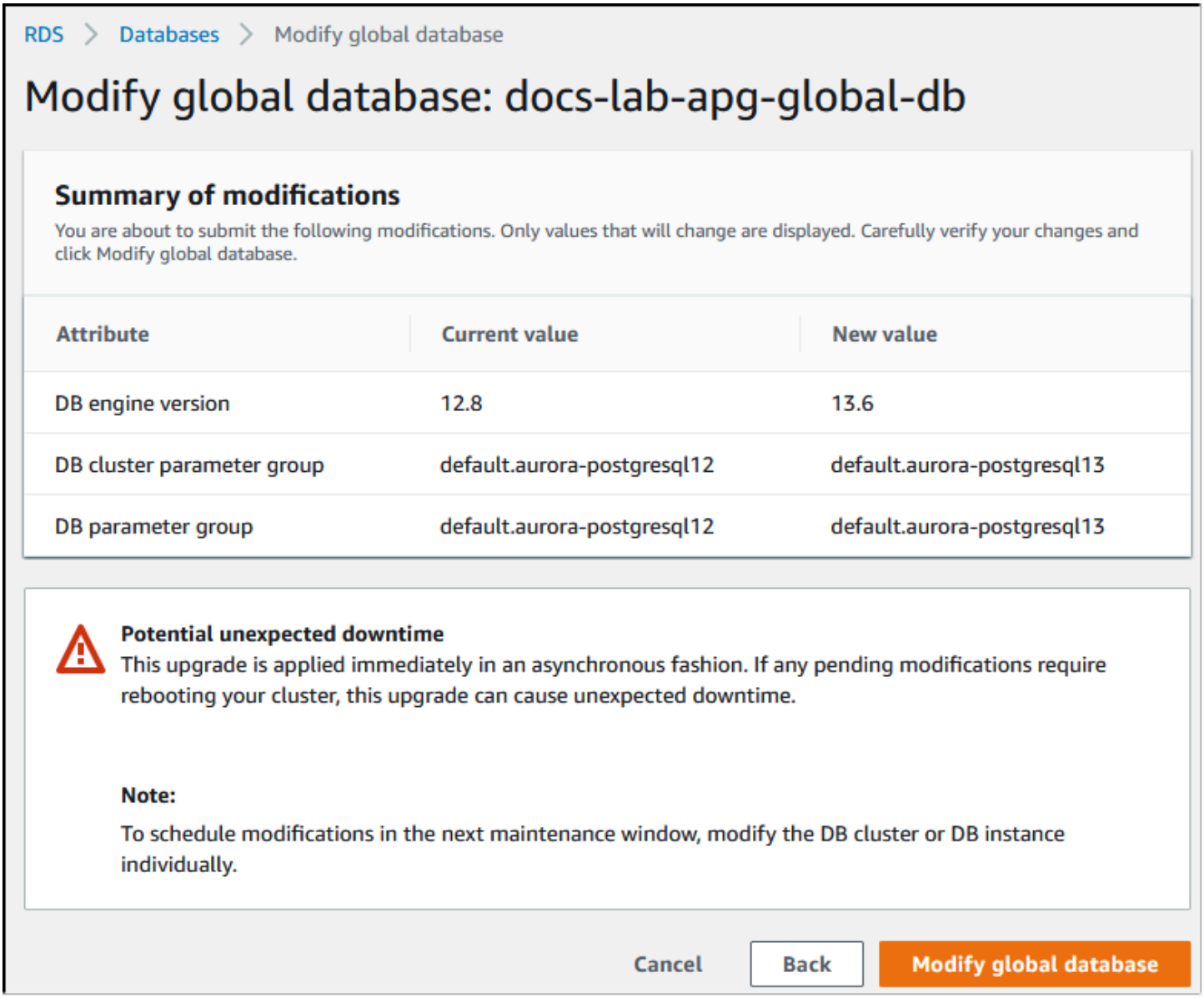
Wenn Sie einen globalen Datenbank-Cluster auf eine neue Hauptversion von Aurora PostgreSQL aktualisieren möchten, empfehlen wir Ihnen, Ihre Anwendungen auf der aktualisierten Version zu testen, wie in Testen eines Upgrades Ihres Produktions-DB-Clusters auf eine neue Hauptversion ausführlich beschrieben. Stellen Sie sicher, dass Sie Ihre DB-Cluster-Parametergruppe und die DB-Parametergruppen-Einstellungen für jeden AWS-Region in Ihrer globalen Aurora-Datenbank vor dem Upgrade vorbereiten, wie unter beschriebenTesten eines Upgrades Ihres Produktions-DB-Clusters auf eine neue Hauptversion. step 1.

Wenn für den Aurora-PostgreSQL-Datenbank-Cluster ein Recovery Point Objective (RPO) für den Parameter `rds.global_db_rpo` festgelegt ist, müssen Sie den Parameter zurücksetzen, bevor Sie das Upgrade durchführen. Der Hauptversions-Upgrade-Prozess funktioniert nicht, wenn das RPO aktiviert ist. Dieser Parameter ist standardmäßig deaktiviert. Weitere Informationen über globale Aurora-PostgreSQL-Datenbanken und RPO finden Sie unter Verwalten von RPOs für Aurora PostgreSQL–basierte globale Datenbanken.

Nachdem Sie überprüft haben, dass Ihre Anwendungen bei der Testbereitstellung der neuen Version erwartungsgemäß ausgeführt werden, können Sie den Upgrade-Prozess starten. Lesen Sie dazu den Abschnitt Upgrade der Aurora-PostgreSQL-Engine auf eine neue Hauptversion. Wählen Sie unbedingt das Element Global database (Globale Datenbank) auf der obersten Ebene der Liste Databases (Datenbanken) in der RDS-Konsole aus, wie in der folgenden Abbildung dargestellt.

DB identifier	Role	Engine	Region & AZ	Size
docs-lab-apg-aiml	Regional cluster	Aurora PostgreSQL	us-west-1	2 instances
docs-lab-apg-global-db	Global database	Aurora PostgreSQL	2 regions	2 clusters
docs-lab-apg-global-12-7	Primary cluster	Aurora PostgreSQL	us-west-1	2 instances
docs-lab-apg-global-12-7-instance-1	Writer instance	Aurora PostgreSQL	us-west-1c	db.r6g.large
docs-lab-apg-global-12-7-instance-1-us-west-1a	Reader instance	Aurora PostgreSQL	us-west-1a	db.r6g.large
docs-lab-apg-global-db-cluster-northwest	Secondary cluster	Aurora PostgreSQL	us-west-2	2 instances
docs-lab-apg-global-db-instance-north	Reader instance	Aurora PostgreSQL	us-west-2c	db.r6g.large
docs-lab-apg-global-db-instance-north-us-west-2b	Reader instance	Aurora PostgreSQL	us-west-2b	db.r6g.large
docs-lab-apg-main	Regional cluster	Aurora PostgreSQL	us-west-1	2 instances
docs-lab-apg-sless-test-aws-s3	Serverless	Aurora PostgreSQL	us-west-1	0 capacity units

Wie bei jeder Änderung können Sie bestätigen, dass der Prozess fortgesetzt werden soll, wenn Sie dazu aufgefordert werden.



Anstatt die Konsole zu verwenden, können Sie den Upgrade-Vorgang mit der AWS CLI oder der RDS-API starten. Wie bei der Konsole arbeiten Sie wie folgt auf dem globalen Aurora-Datenbankcluster und nicht auf einem seiner Bestandteile:

- Verwenden Sie den modify-global-cluster AWS CLI Befehl, um das Upgrade für Ihre globale Aurora-Datenbank zu starten, indem Sie den verwenden AWS CLI.
- Verwenden Sie die ModifyGlobalClusterAPI, um das Upgrade zu starten.

Vor der Durchführung eines kleineren Versions-Upgrades

Wir empfehlen Ihnen, die folgenden Aktionen durchzuführen, um die Ausfallzeit während eines Upgrades einer Nebenversion zu reduzieren:

- Die Wartung des Aurora-DB-Clusters sollte in Zeiten mit geringem Datenverkehr durchgeführt werden. Verwenden Sie Performance Insights, um diese Zeiträume zu identifizieren und die Wartungsfenster korrekt zu konfigurieren. Weitere Informationen zu Performance Insights finden Sie unter Überwachen der DB-Auslastung mit Performance Insights auf Amazon RDS. Weitere Informationen zum Wartungsfenster für DB-Cluster finden Sie unterAnpassen des bevorzugten DB-Cluster-Wartungsfensters.
- Verwenden Sie als AWS bewährte Methode SDKs, die exponentielles Backoff und Jitter unterstützen. Weitere Informationen finden Sie unter Exponentieller Backoff und Jitter.

So führen Sie Upgrades von Nebenversionen durch und wenden Patches an

Kleinere Versions-Upgrades und Patches sind AWS-Regionen erst nach gründlichen Tests verfügbar. Vor der Veröffentlichung von Upgrades und Patches testet Aurora PostgreSQL, um sicherzustellen, dass bekannte Sicherheitsprobleme, Fehler und andere Probleme, die nach der Veröffentlichung der Community-Nebenversion auftreten, die allgemeine Stabilität der Aurora PostgreSQL-Flotte nicht beeinträchtigen.

Sobald Aurora PostgreSQL neue Nebenversionen zur Verfügung stellt, können die Instances, aus denen Ihr Aurora-PostgreSQL-DB-Cluster besteht, während des angegebenen Wartungsfensters automatisch aktualisiert werden. Dazu muss für Ihren Aurora-PostgreSQL-DB-Cluster die Option Enable auto minor version upgrade (Automatische Aktualisierung von Nebenversionen aktivieren) ausgewählt sein. Für alle DB-Instances, aus denen Ihr Aurora-PostgreSQL-DB-Cluster besteht, muss die Option für das automatische Nebenversions-Upgrade (AmVU) aktiviert sein, damit das Nebenversions-Upgrade im gesamten Cluster angewendet werden kann.

> **Tip**
>
> Stellen Sie sicher, dass die Option Enable auto minor version upgrade (Automatische Aktualisierung von Nebenversionen aktivieren) für alle PostgreSQL-DB-Instances ausgewählt ist, aus denen Ihr Aurora-PostgreSQL-DB-Cluster besteht. Diese Option muss aktiviert sein, damit jede Instance im DB-Cluster funktioniert. Informationen zum Festlegen der Einstellung Automatisches Unterversion-Upgrade und zur Funktionsweise der Einstellung,

wenn sie auf Cluster- und Instance-Ebene angewendet wird, finden Sie unter Automatische Nebenversions-Upgrades für Aurora-DB-Cluster.

Sie können den Wert der Option auto Upgrade der Nebenversion aktivieren für alle Ihre Aurora PostgreSQL-DB-Cluster überprüfen, indem Sie den describe-db-instances AWS CLI Befehl mit der folgenden Abfrage verwenden.

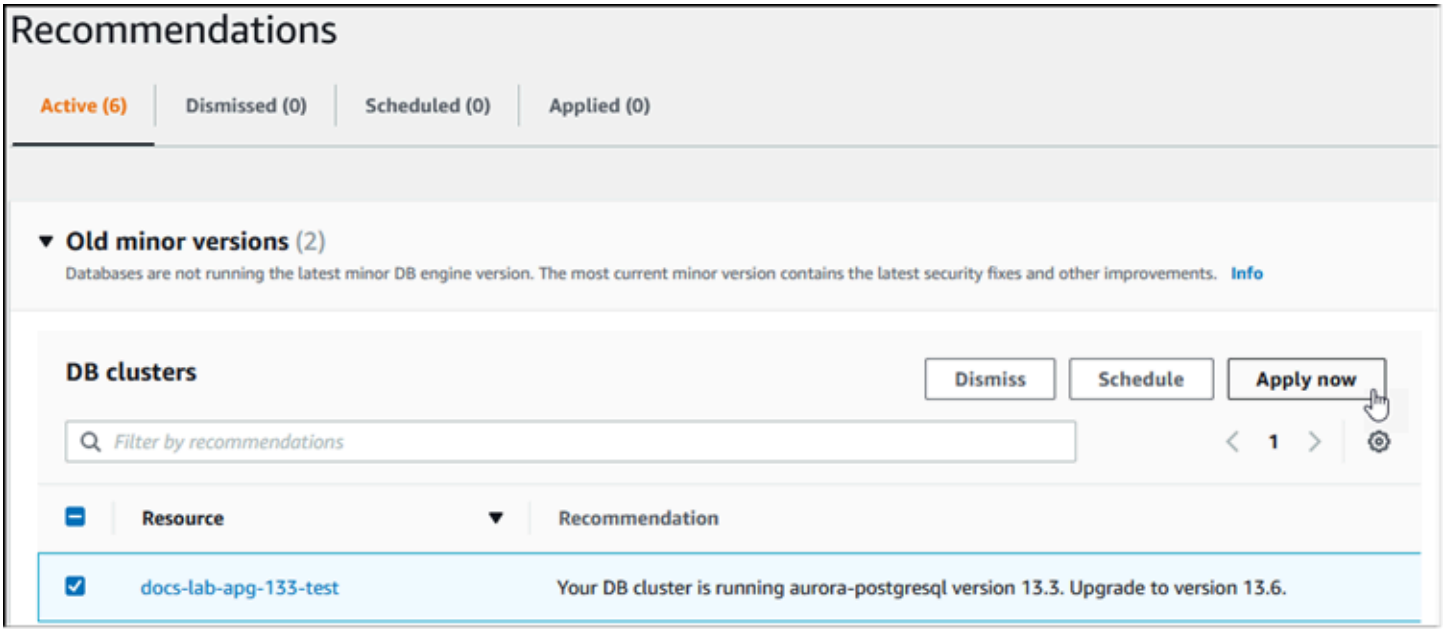
```
aws rds describe-db-instances \
  --query '*[].
{DBClusterIdentifier:DBClusterIdentifier,DBInstanceIdentifier:DBInstanceIdentifier,AutoMinorVer
```

Diese Abfrage gibt eine Liste aller Aurora-DB-Cluster und ihrer Instances mit dem Wert `true` oder `false` für den Status der Einstellung `AutoMinorVersionUpgrade` zurück. Bei dem abgebildeten Befehl wird davon ausgegangen, dass Sie Ihre AWS CLI Konfiguration so konfiguriert haben, dass sie auf Ihre Standardeinstellung abzielt. AWS-Region

Weitere Informationen zur AmVU-Option und darüber, wie Sie Ihren Aurora-DB-Cluster ändern, um diese u verwenden zu können, finden Sie unter Automatische Nebenversions-Upgrades für Aurora-DB-Cluster.

Sie können Ihren Aurora-PostgreSQL-DB-Cluster auf neue Nebenversionen aktualisieren, indem Sie entweder auf Wartungsaufgaben reagieren oder den Cluster so ändern, dass er die neue Version verwendet.

Sie können alle verfügbaren Upgrades oder Patches für Ihre Aurora-PostgreSQL-DB-Cluster identifizieren, indem Sie die RDS-Konsole verwenden und das Menü Recommendations (Empfehlungen) öffnen. Dort finden Sie eine Liste verschiedener Wartungsprobleme wie Old minor versions (Alte Nebenversionen) aus. Abhängig von Ihrer Produktionsumgebung können Sie mit Schedule (Planen) das Upgrade planen oder mit Apply now (Jetzt anwenden) sofort Maßnahmen ergreifen, wie im Folgenden gezeigt.



Weitere Informationen zum Verwalten eines Aurora-DB-Clusters, einschließlich der manuellen Anwendung von Patches und Nebenversions-Upgrades, finden Sie unter Warten eines Amazon Aurora-DB-Clusters.

Nebenversions-Upgrades und Zero-Downtime-Patching

Beim Upgrade eines AuroraPostgreSQL-DB-Clusters kann es zu einem Ausfall kommen. Beim Upgrade-Prozess wird die Datenbank heruntergefahren, während sie aktualisiert wird. Wenn Sie das Upgrade starten, während die Datenbank ausgelastet ist, verlieren Sie alle Verbindungen und Transaktionen, die der DB-Cluster verarbeitet. Wenn Sie warten, bis die Datenbank im Leerlauf ist, um das Upgrade durchzuführen, müssen Sie möglicherweise lange warten.

Die Funktion „Null-Downtime Patching“ (ZDP, Patchen ohne Ausfallzeiten) verbessert den Upgrade-Prozess. Mit dem ZDP können sowohl Upgrades als auch Patches mit minimalen Auswirkungen auf Ihren Aurora-PostgreSQL-DB-Cluster angewendet werden. ZDP wird verwendet, wenn Patches oder neuere Upgrades von Nebenversionen auf Aurora-PostgreSQL-Versionen und anderen höheren Versionen dieser Nebenversionen und neueren Hauptversionen angewendet werden. Das heißt, bei einem Upgrade auf neue Nebenversionen nach einer dieser Versionen wird ZDP verwendet.

Die folgende Tabelle zeigt die Aurora-PostgreSQL-Versionen und DB-Instance-Klassen, in denen ZDP verfügbar ist:

Version	db.r*-Instance-Klassen	db.t*-Instance-Klassen	db.x*-Instance-Klassen	db.serverless-Instance-Klasse
10.21.0 und höhere 10.21-Versionen	Ja	Ja	Ja	N/A
11.16.0 und höhere 11.16-Versionen	Ja	Ja	Ja	N/A
11.17 und höhere Versionen	Ja	Ja	Ja	N/A
12.11.0 und höhere 12.11-Versionen	Ja	Ja	Ja	N/A
12.12 und höhere Versionen	Ja	Ja	Ja	N/A
13.7.0 und höhere 13.7-Versionen	Ja	Ja	Ja	N/A
13.8 und höhere Versionen	Ja	Ja	Ja	Ja
14.3.1 und höhere 14.3-Versionen	Ja	Ja	Ja	N/A
14.4.0 und höhere 14.4-Versionen	Ja	Ja	Ja	N/A

Version	db.r*-Instance-Klassen	db.t*-Instance-Klassen	db.x*-Instance-Klassen	db.serverless-Instance-Klasse
14.5 und höhere Versionen	Ja	Ja	Ja	Ja
15.3 und höhere Versionen	Ja	Ja	Ja	Ja

ZDP arbeitet, indem es die aktuellen Client-Verbindungen zu Ihrem Aurora-PostgreSQL-DB-Cluster während des Aurora-PostgreSQL-Upgrade-Prozesses beibehält. In den folgenden Fällen werden die Verbindungen jedoch unterbrochen, damit ZDP den Vorgang abschließen kann:

- Wenn lang dauernde Abfragen oder Transaktionen ausgeführt werden.
- Data Definition Language (DDL)-Anweisungen werden ausgeführt.
- Es werden temporäre Tabellen verwendet oder Tabellensperren sind aktiv.
- Alle Sitzungen überwachen Benachrichtigungskanäle.
- Ein Cursor mit dem Status 'WITH HOLD' wird verwendet.
- Es werden TLSv1.3- oder TLSv1.1-Verbindungen verwendet.

Während des Upgrade-Vorgangs mit ZDP sucht die Datenbank-Engine nach einem ruhigen Punkt, um alle neuen Transaktionen anzuhalten. Diese Aktion schützt die Datenbank bei Patches und Upgrades. Um sicherzustellen, dass Ihre Anwendungen bei unterbrochenen Transaktionen reibungslos laufen, empfehlen wir, die Logik für Wiederholversuche in Ihren Code zu integrieren. Dieser Ansatz stellt sicher, dass das System kurze Ausfallzeiten ohne Fehler bewältigen und die neuen Transaktionen nach dem Upgrade erneut versuchen kann.

Wenn ZDP erfolgreich abgeschlossen wird, werden Anwendungssitzungen, mit Ausnahme von Sitzungen mit unterbrochenen Verbindungen, beibehalten und die Datenbank-Engine wird während des laufenden Upgrades neu gestartet. Der Neustart der Datenbank-Engine kann zwar zu einem vorübergehenden Abfall des Durchsatzes führen, dieser dauert jedoch normalerweise nur wenige Sekunden oder maximal etwa 1 Minute.

In einigen Fällen ist das Zero-Downtime-Patching (ZDP) möglicherweise nicht erfolgreich. Parameteränderungen, die sich auf Ihrem DB-Cluster von Aurora PostgreSQL oder dessen Instances im Status `pending` befinden, beeinträchtigen ebenfalls ZDP.

Metriken und Ereignisse für ZDP-Operationen finden Sie auf der Seite Events (Ereignisse) in der Konsole. Zu den Ereignissen gehören der Start des ZDP-Upgrades und der Abschluss des Upgrades. In diesem Fall können Sie feststellen, wie lange der Prozess gedauert hat und wie viele Verbindungen während des Neustarts aufrecht erhalten und abgebrochen wurden. Details finden Sie in Ihrem Datenbank-Fehlerprotokoll.

Durchführen eines Upgrades der Aurora-PostgreSQL-Engine auf eine neue Nebenversion

Sie können Ihren Aurora PostgreSQL-DB-Cluster mithilfe der Konsole, der oder der RDS-API auf eine neue Nebenversion aktualisieren. AWS CLI Bevor Sie das Aktualisieren durchführen, wird das Befolgen der selben bewährten Methoden empfohlen, die für Upgrades der Hauptversion empfohlen wird. Wie bei neuen Hauptversionen können auch neue Nebenversionen Optimizer-Verbesserungen aufweisen, z. B. Korrekturen, die Regressionen des Abfrageplans verursachen können. Um die Stabilität des Plans zu gewährleisten, wird die Verwendung der Erweiterung Query Plan Management (QPM) empfohlen, wie inSicherstellen der Planstabilität nach einem größeren Versions-Upgrade.

Konsole

So aktualisieren Sie die Engine-Version Ihres Aurora-PostgreSQL-DB-Clusters.

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann den DB-Cluster aus, den Sie upgraden möchten.
3. Wählen Sie Ändern aus. Die Seite DB-Cluster ändern wird angezeigt.
4. Wählen Sie für Motorversion die neue Version.
5. Klicken Sie auf Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.
6. Wählen Sie Apply immediately, um die Änderungen sofort anzuwenden. Die Auswahl dieser Option kann in einigen Fällen einen Ausfall verursachen. Weitere Informationen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.
7. Überprüfen Sie auf der Bestätigungsseite Ihre Änderungen. Wenn sie korrekt sind, wählen Sie Modify Cluster (Cluster ändern) aus, um Ihre Änderungen zu speichern.

   Oder klicken Sie auf Zurück, um Ihre Änderungen zu bearbeiten, oder auf Abbrechen, um Ihre Änderungen zu verwerfen.

AWS CLI

Um die Engine-Version eines DB-Clusters zu aktualisieren, verwenden Sie den modify-db-cluster AWS CLI Befehl mit den folgenden Parametern:

- `--db-cluster-identifier` – Der Name Ihres Aurora-PostgreSQL-DB-Clusters.
- `--engine-version` – die Versionsnummer der Datenbank-Engine, auf die das Upgrade durchgeführt wird Verwenden Sie den AWS CLI describe-db-engine-versionsBefehl, um Informationen zu gültigen Engine-Versionen zu erhalten.
- `--no-apply-immediately` – Änderungen im nächsten Wartungszeitraum anwenden Verwenden Sie `--apply-immediately`, um Änderungen sofort anzuwenden.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --engine-version new_version \
    --no-apply-immediately
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --engine-version new_version ^
    --no-apply-immediately
```

RDS-API

Sie können die Engine-Version eines DB-Clusters upgraden, indem Sie die Operation ModifyDBCluster aufrufen. Geben Sie die folgenden Parameter an:

- `DBClusterIdentifier` – der Name des DB-Clusters, z. B *`mydbcluster`*
- `EngineVersion` – die Versionsnummer der Datenbank-Engine, auf die das Upgrade durchgeführt wird Verwenden Sie den Vorgang DescribeDB, um Informationen zu gültigen Engine-Versionen zu EngineVersions erhalten.
- `ApplyImmediately` – Änderungen sofort oder während des nächsten Wartungszeitraums anwenden Legen Sie den Wert auf fest, um Änderungen sofort anzuwende `true`. Legen Sie den Wert auf fest, um Änderungen im nächsten Wartungszeitraum durchzuführe `false`.

Aktualisieren von PostgreSQL-Erweiterungen

Wenn Sie Ihren DB-Cluster von Aurora PostgreSQL auf eine neue Haupt- oder Nebenversion aktualisieren, werden die PostgreSQL-Erweiterungen nicht gleichzeitig aktualisiert. Bei den meisten Erweiterungen aktualisieren Sie die Erweiterung, nachdem das Upgrade der Haupt- oder Nebenversion abgeschlossen ist. In einigen Fällen aktualisieren Sie die Erweiterung jedoch vor dem Upgrade der Aurora-PostgreSQL-DB-Engine. Weitere Informationen finden Sie unter list of extensions to update in Testen eines Upgrades Ihres Produktions-DB-Clusters auf eine neue Hauptversion.

Zum Installieren von PostgreSQL-Erweiterungen sind `rds_superuser`-Berechtigungen erforderlich. In der Regel delegiert ein `rds_superuser` Berechtigungen über bestimmte Erweiterungen an relevante Benutzer (Rollen), um die Verwaltung einer bestimmten Erweiterung zu erleichtern. Das heißt, dass die Aufgabe, alle Erweiterungen in Ihrem Aurora-PostgreSQL-DB-Cluster zu aktualisieren, viele verschiedene Benutzer (Rollen) betreffen kann. Beachten Sie dies, insbesondere wenn Sie den Upgrade-Prozess mithilfe von Skripten automatisieren möchten. Weitere Informationen über PostgreSQL-Berechtigungen und -Rollen finden Sie unter Sicherheit in Amazon Aurora PostgreSQL.

> **Note**
>
> Hinweise zum Aktualisieren der PostGIS-Erweiterung finden Sie unter Verwalten von Geodaten mit der PostGIS-Erweiterung (Schritt 6: Upgrade der PostGIS-Erweiterung).
> Um die `pg_repack`-Erweiterung zu aktualisieren, entfernen Sie die Erweiterung und erstellen Sie eine neue Version in der aktualisierten DB-Instance. Weitere Informationen finden Sie unter pg_repack installation in der `pg_repack`-Dokumentation.

Verwenden Sie zur Aktualisierung einer Erweiterung nach einem Upgrade der Engine den Befehl `ALTER EXTENSION UPDATE`.

```
ALTER EXTENSION extension_name UPDATE TO 'new_version';
```

Um Ihre derzeit installierten Erweiterungen aufzulisten, verwenden Sie den PostgreSQL-Katalog pg_extension in dem folgenden Befehl.

```
SELECT * FROM pg_extension;
```

Um eine Liste der spezifischen Erweiterungsversionen anzuzeigen, die zur Installation verfügbar sind, verwenden Sie die PostgreSQL-Ansicht pg_available_extension_versions in dem folgenden Befehl.

```
SELECT * FROM pg_available_extension_versions;
```

Alternatives Blau/Grün-Upgradeverfahren

In einigen Situationen ist es Ihre oberste Priorität, eine sofortige Umstellung vom alten auf einen aktualisierten Cluster durchzuführen. In solchen Situationen können Sie einen mehrstufigen Prozess verwenden, der die alten und neuen Cluster ausführt. side-by-side Hier replizieren Sie Daten vom alten auf den neuen Cluster, bis der neuen Cluster zur Übernahme bereit ist. Details hierzu finden Sie unter Verwendung von Blau/Grün-Bereitstellungen für Datenbankaktualisierungen.

Aurora PostgreSQL Long-Term Support- (LTS, Langzeit-Support) Versionen

Jede neue Aurora-PostgreSQL-Version bleibt für eine bestimmte Zeit zum Erstellen oder Aktualisieren eines DB-Clusters verfügbar. Nach diesem Zeitraum müssen Sie alle Cluster aktualisieren, die diese Version verwenden. Sie können Ihren Cluster vor Ablauf des Supportzeitraums manuell aktualisieren, oder Aurora kann ihn automatisch für Sie aktualisieren, wenn die Aurora-PostgreSQL-Version nicht mehr unterstützt wird.

Aurora bezeichnet bestimmte Aurora-PostgreSQL-Versionen als „Long-term Support“ (LTS, Langzeitsupport)-Versionen. Datenbank-Cluster, die LTS-Versionen verwenden, können länger dieselbe Version nutzen und weniger Upgradezyklen durchlaufen als Cluster, die Nicht-LTS-Versionen verwenden. LTS-Nebenversionen enthalten nur Fehlerbehebungen (über Patch-Versionen); eine LTS-Version enthält keine neuen Funktionen, die nach ihrer Einführung veröffentlicht wurden.

Einmal im Jahr werden DB-Cluster, die auf einer LTS-Nebenversion ausgeführt werden, auf die neueste Patch-Version der LTS-Version gepatcht. Wir führen diese Patches durch, um sicherzustellen, dass Sie von kumulativen Sicherheits- und Stabilitätsbehebungen profitieren. Wir können eine LTS-Nebenversion häufiger patchen, wenn kritische Fehlerbehebungen, z. B. für die Sicherheit, angewendet werden müssen.

> **Note**
>
> Um für die Dauer ihres Lebenszyklus auf einer LTS-Nebenversion zu bleiben, stellen Sie sicher, dass Sie das automatische Upgrade der Nebenversion für Ihre DB-Instances deaktivieren. Um zu vermeiden, dass Ihr DB-Cluster automatisch von der LTS-Nebenversion

aktualisiert wird, setzen Sie das Automatische Nebenversions-Upgrade für alle DB-Instances in Ihrem Aurora-Cluster auf Keines.

Wir empfehlen, dass Sie für die meisten Ihrer Aurora-PostgreSQL-Cluster auf die neueste Version upgraden, anstatt die LTS-Version zu verwenden. Auf diese Weise wird Aurora als Managed verwalteter Service genutzt und Sie erhalten Zugriff auf die neuesten Funktionen und Bugfixes. Die LTS-Releases sind für Cluster mit folgenden Merkmalen gedacht:

- Sie können sich, abgesehen von seltenen Fällen, keine Upgrade-Ausfallzeiten Ihrer Aurora-PostgreSQL-Anwendung für kritische Patches leisten.
- Der Testzyklus für den Cluster und die zugehörigen Anwendungen dauert bei einer Aktualisierung der Aurora-PostgreSQL-Datenbank-Engine sehr lange.
- Die Datenbankversion für Ihren Aurora-PostgreSQL-Cluster enthält alle Funktionen der DB-Engine und Fehlerbehebungen, die Ihre Anwendung benötigt.

Die aktuellen LTS-Versionen für Aurora PostgreSQL lauten wie folgt:

- PostgreSQL 14.6. Es wurde am 20. Januar 2023 veröffentlicht. Weitere Informationen finden Sie unter PostgreSQL 14.6 in den Versionshinweisen für Aurora PostgreSQL.
- PostgreSQL 13.9. Es wurde am 20. Januar 2023 veröffentlicht. Weitere Informationen finden Sie unter PostgreSQL 13.9 in den Versionshinweisen für Aurora PostgreSQL.
- PostgreSQL 12.9. Sie wurde am 25. Februar 2022 veröffentlicht. Weitere Informationen finden Sie unter PostgreSQL 12.9 in den Versionshinweisen für Aurora PostgreSQL.
- PostgreSQL 11.9 (Aurora PostgreSQL Version 3.4. Sie wurde am 11. Dezember 2020 veröffentlicht. Weitere Informationen zu dieser Version finden Sie unter PostgreSQL 11.9, Aurora PostgreSQL Version 3.4 in den Versionshinweisen für Aurora PostgreSQL.

Hinweise zum Identifizieren von Aurora- und Datenbank-Engine-Versionen finden Sie unter Identifizieren der Versionen von Amazon Aurora PostgreSQL.

Verwenden von Amazon Aurora Global Databases

Globale Amazon-Aurora-Datenbanken umfassen mehrere AWS-Regionen, was globale Lesevorgänge mit niedriger Latenz ermöglicht und eine schnelle Wiederherstellung nach einem seltenen Ausfall ermöglicht, der sich auf ein gesamtes auswirken könnte AWS-Region. Eine globale Aurora-Datenbank hat einen primären DB-Cluster in einer Region und bis zu fünf sekundäre DB-Cluster in verschiedenen Regionen.

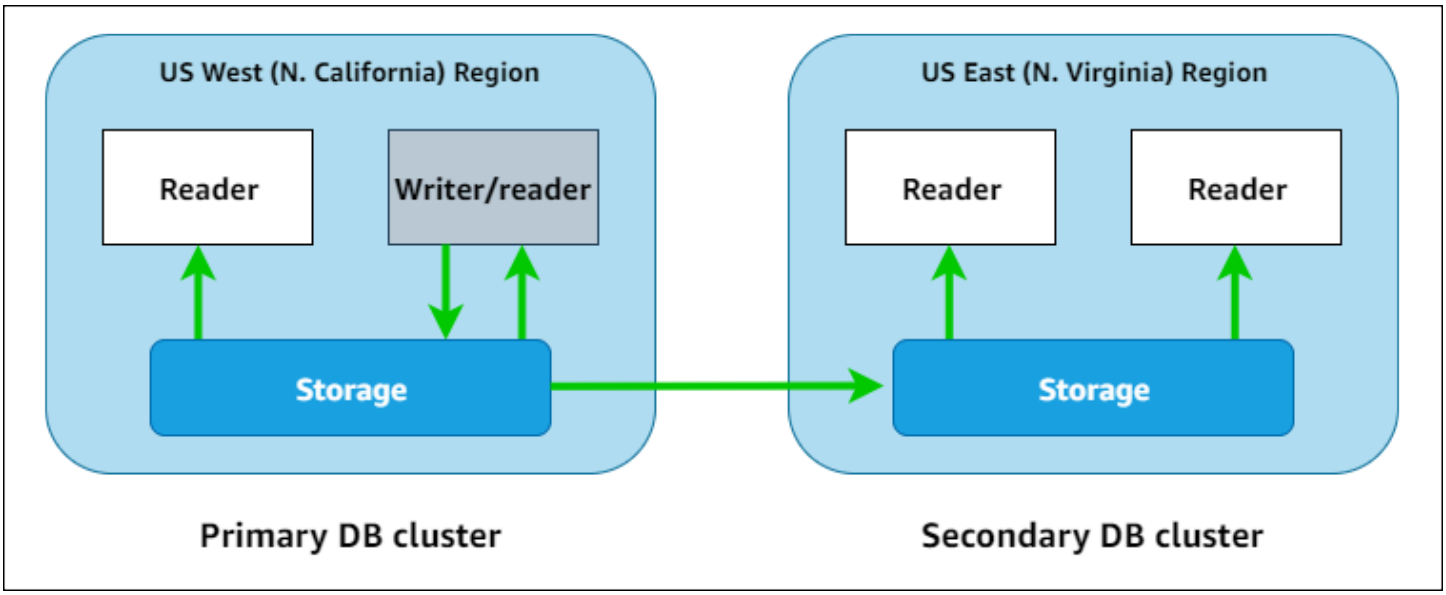
Themen

Übersicht über Amazon Aurora Global Databases

Durch die Verwendung einer globalen Amazon-Aurora-Datenbank können Sie Ihre global verteilten Anwendungen mit einer einzigen Aurora-Datenbank ausführen, die mehrere AWS-Regionen umfasst.

Eine globale Aurora-Datenbank besteht aus einer primären AWS-Region , in die Ihre Daten geschrieben werden, und bis zu fünf schreibgeschützten sekundären AWS-Regionen. Schreibvorgänge erfolgen direkt auf den primären DB-Cluster in der primären AWS-Region. Aurora repliziert Daten AWS-Regionen mithilfe einer dedizierten Infrastruktur auf den sekundären Cluster, wobei die Latenz normalerweise unter einer Sekunde liegt.

Im folgenden Diagramm finden Sie ein Beispiel für eine globale Aurora-Datenbank, die sich über zwei erstreckt AWS-Regionen.



Sie können jeden sekundären Cluster unabhängig hochskalieren, indem Sie eine oder mehrere Aurora-Replicas (schreibgeschützte Aurora-DB-Instances) zum Verarbeiten schreibgeschützter Workloads hinzufügen.

Nur der primäre Cluster führt Schreibvorgänge aus. Clients, die Schreibvorgänge ausführen, stellen eine Verbindung mit dem DB-Cluster-Endpunkt des primären DB-Clusters her. Wie im Diagramm dargestellt, verwendet die globale Aurora-Datenbank für die Replikation das Cluster-Speichervolume und nicht die Datenbank-Engine. Weitere Informationen hierzu finden Sie unter Übersicht über Amazon-Aurora-Speicher.

Globale Aurora-Datenbanken sind für Anwendungen mit weltweiter Präsenz konzipiert. Mit den schreibgeschützten sekundären DB-Clustern (AWS-Regionen) können Sie Lesevorgänge näher an Anwendungsbenutzern unterstützen. Mit dem Feature zur Schreibweiterleitung können Sie globale Aurora-Datenbanken auch so konfigurieren, dass sekundäre Cluster Daten an primäre Cluster senden. Weitere Informationen finden Sie unter Verwenden der Schreibweiterleitung in einer Amazon Aurora globalen Datenbank.

Eine globale Aurora-Datenbank unterstützt je nach Szenario zwei verschiedene Operationen zum Ändern der Region Ihres primären DB-Clusters: globale Datenbank-Umstellung und globales Datenbank-Failover.

- Verwenden Sie für geplante operative Verfahren wie die regionale Rotation die globale Datenbank-Umstellung (früher als „verwaltetes geplantes Failover“ bezeichnet). Mit dieser Funktion können Sie

den primären Cluster einer fehlerfreien globalen Aurora-Datenbank ohne Datenverlust in eine der sekundären Regionen verschieben. Weitere Informationen hierzu finden Sie unter Durchführen von Umstellungen für Amazon Aurora Global Databases.

- Um Ihre globale Aurora-Datenbank nach einem Ausfall in der primären Region wiederherzustellen, verwenden Sie das globale Datenbank-Failover. Mit dieser Funktion führen Sie ein Failover ihres primären DB-Clusters auf eine andere Region durch (regionsübergreifendes Failover). Weitere Informationen hierzu finden Sie unter Ausführen von verwalteten geplanten Failovers für globale Aurora-Datenbanken.

Vorteile von Amazon Aurora Global Databases

Durch die Verwendung globaler Aurora-Datenbanken profitieren Sie von folgenden Vorteilen:

- Globale Lesevorgänge mit lokaler Latenz – Wenn Sie Niederlassungen auf der ganzen Welt haben, können Sie eine globale Aurora-Datenbank nutzen, um die wichtigsten Datenquellen in der primären AWS-Region auf dem neuesten Stand zu halten. Niederlassungen in Ihren anderen Regionen können mit lokaler Latenz auf die Daten in ihrer eigenen Region zugreifen.
- Skalierbare sekundäre Aurora-DB-Cluster – Sie können Ihre sekundären Cluster skalieren, indem Sie einer sekundären AWS-Region weitere schreibgeschützte Instances (Aurora-Replikate) hinzufügen. Der sekundäre Cluster ist schreibgeschützt und kann daher bis zu 16 schreibgeschützte Aurora-Replica-Instances anstelle dem üblichen Limit von 15 für einen einzelnen Aurora-Cluster unterstützen.
- Schnelle Replikation von primären zu sekundären Aurora-DB-Clustern – Die von einer Aurora globalen Datenbank ausgeführte Replikation führt zu geringen Leistungseinbußen auf dem primären DB-Cluster. Die Ressourcen der DB-Instances werden ausschließlich für Lese- und Schreib-Workloads von Anwendungen genutzt.
- Wiederherstellung nach regionsweiten Ausfällen –Die sekundären Cluster ermöglichen Ihnen, eine globale Aurora-Datenbank in einer neuen primären AWS-Region schneller (niedrigere RTO) und mit weniger Datenverlust (niedrigerer RPO) als herkömmliche Replikationslösungen verfügbar zu machen.

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Aurora-Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen

zur Verfügbarkeit von Versionen und Regionen im Zusammenhang mit Aurora und globalen Datenbanken finden Sie unter Unterstützte Regionen und DB-Engines für globale Aurora-Datenbanken.

Einschränkungen von globalen Amazon Aurora-Datenbanken

Für globale Aurora-Datenbanken gelten aktuell die folgenden Einschränkungen:

- Globale Aurora-Datenbanken sind in bestimmten AWS-Regionen und nur für bestimmte Aurora MySQL- und Aurora PostgreSQL-Versionen verfügbar. Weitere Informationen finden Sie unter Unterstützte Regionen und DB-Engines für globale Aurora-Datenbanken.
- Globale Aurora-Datenbanken haben bestimmte Konfigurationsanforderungen für unterstützte Aurora-DB-Instance-Klassen, eine maximale Anzahl von AWS-Regionen usw. Weitere Informationen finden Sie unter Anforderungen an die Konfiguration einer Amazon Aurora globalen Datenbank.
- Für Aurora MySQL mit MySQL 5.7-Kompatibilität erfordern globale Aurora-Datenbankumstellungen Version 2.09.1 oder eine höhere Nebenversion.
- Sie können verwaltete regionsübergreifende Umstellungen oder Failovers für eine globale Aurora-Datenbank nur durchführen, wenn die primären und sekundären DB-Cluster dieselben Engine-Haupt-, Neben- und Patch-Level-Versionen haben. Die Patch-Level können jedoch unterschiedlich sein, wenn es sich bei den Nebenversionen der Engine um eine der folgenden Versionen handelt.

Datenbank-Engine	Engine-Nebenversionen
Aurora PostgreSQL	• Version 14.5 und höhere Unterversionen • Version 13.8 und höhere Unterversionen • Version 12.12 und höhere Unterversionen • Version 11.17 und höhere Unterversionen

  Weitere Informationen finden Sie unter Patch-Level-Kompatibilität für verwaltete regionsübergreifende Umstellungen und Failovers.
- Globale Aurora-Datenbanken unterstützen derzeit die folgenden Aurora-Funktionen nicht:
  - Aurora Serverless v1
  - Rückverfolgung in Aurora

- Einschränkungen bei der Verwendung der RDS-Proxy-Funktion mit globalen Datenbanken finden Sie unter Einschränkungen für RDS Proxy mit globalen Datenbanken.
- Die automatische Aktualisierung von Unterversionen gilt nicht für Aurora-MySQL- und Aurora-PostgreSQL-Cluster, die Teil einer globalen Aurora-Datenbank sind. Beachten Sie, dass Sie diese Einstellung für eine DB-Instanz angeben können, die Teil eines globalen Datenbank-Clusters ist, aber die Einstellung hat keine Auswirkungen.
- Globale Aurora-Datenbanken unterstützen derzeit kein Aurora Auto Scaling für sekundäre DB-Cluster.
- Um Datenbankaktivitäts-Streams in globalen Aurora-Datenbanken zu verwenden, auf denen Aurora MySQL 5.7 ausgeführt wird, muss die Engine-Version Version 2.08 oder höher sein. Hinweise zu Datenbankaktivitäts-Streams finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.
- Für den Upgrade von globalen Aurora-Datenbanken gelten aktuell die folgenden Einschränkungen:
  - Sie können keine benutzerdefinierte Parametergruppe auf den globalen Datenbank-Cluster anwenden, während Sie ein Hauptversions-Upgrade dieser globalen Aurora-Datenbank durchführen. Sie erstellen Ihre benutzerdefinierten Parametergruppen in jeder Region des globalen Clusters und wenden sie nach dem Upgrade manuell auf die regionalen Cluster an.
  - Mit einer globalen Aurora-Datenbank, die auf Aurora MySQL basiert, können Sie kein direktes Upgrade von Aurora MySQL Version 2 auf Version 3 durchführen, wenn der `lower_case_table_names`-Parameter aktiviert ist. Weitere Informationen zu den möglichen Verfahren finden Sie unter Hauptversions-Upgrades.
  - Mit einer globalen Aurora-Datenbank, die auf Aurora PostgreSQL basiert, können Sie kein Hauptversions-Upgrade der Aurora-DB-Engine durchführen, wenn die Recovery Point Objective (RPO)-Funktion aktiviert ist. Weitere Informationen über RPO-Funktion finden Sie unter Verwalten von RPOs für Aurora PostgreSQL–basierte globale Datenbanken.
  - Mit einer globalen Aurora-Datenbank, die auf Aurora MySQL basiert, können Sie kein Hauptversions-Upgrade von Version 3.01 oder 3.02 auf 3.03 oder höher durchführen, indem Sie den Standardprozess verwenden. Weitere Informationen zu dem zu verwendenden Prozess finden Sie unter Upgrade von Aurora MySQL durch Ändern der Engine-Version.

  Informationen zum Upgrade einer globalen Aurora-Datenbank finden Sie unter Aktualisieren einer Amazon Aurora Global Database.
- Sie können die Aurora-DB-Cluster in Ihrer globalen Aurora-Datenbank nicht einzeln anhalten oder starten. Weitere Informationen hierzu finden Sie unter Stoppen und Starten eines Amazon Aurora-DB-Clusters.

- Aurora Replicas, die mit dem sekundären Aurora-DB-Cluster verbunden sind, können unter bestimmten Umständen neu gestartet werden. Wenn die Writer-DB- AWS-RegionInstance des primären neu gestartet wird oder ein Failover durchführt, werden Aurora-Replikate in sekundären Regionen ebenfalls neu gestartet. Der sekundäre Cluster ist erst dann verfügbar, wenn alle Replikate wieder mit der Writer-Instance des primären DB-Clusters synchronisiert sind. Das Verhalten des primären Clusters beim Neustart oder beim Failover ist dasselbe wie bei einem einzelnen, nicht globalen DB-Cluster. Weitere Informationen finden Sie unter Replikation mit Amazon Aurora.

  Stellen Sie sicher, dass Sie die Auswirkungen auf Ihre globale Aurora-Datenbank verstehen, bevor Sie Änderungen an Ihrem primären DB-Cluster vornehmen. Weitere Informationen hierzu finden Sie unter Wiederherstellen einer globalen Amazon Aurora-Datenbank nach einem ungeplanten Ausfall.
- Globale Aurora-Datenbanken unterstützen derzeit den `inaccessible-encryption-credentials-recoverable` Status nicht, wenn Amazon Aurora den Zugriff auf den AWS KMS Schlüssel für den DB-Cluster verliert. In diesen Fällen wechselt der verschlüsselte DB-Cluster direkt in den Beendigungszustand `inaccessible-encryption-credentials`. Weitere Informationen zu diesen Zuständen finden Sie unter Anzeigen des DB-Clusterstatus.
- Aurora-PostgreSQL-basierte DB-Cluster, die in einer globalen Aurora-Datenbank ausgeführt werden, haben folgende Einschränkungen:
  - Die Verwaltung des Cluster-Cache wird für Aurora-PostgreSQL-DB-Cluster, die Teil der globalen Aurora-Datenbanken sind, nicht unterstützt.
  - Wenn der primäre DB-Cluster Ihrer Aurora globalen Datenbank auf eine, Replikat einer Amazon-RDS-PostgreSQL-Instance basiert, können Sie keinen sekundären Cluster erstellen. Versuchen Sie nicht, mithilfe der AWS Management Console, der AWS CLIoder der `CreateDBCluster`-API-Operation aus diesem Cluster ein sekundäres zu erstellen. Solche Versuche werden unterbrochen und der sekundäre Cluster wird nicht erstellt.

Wir empfehlen, dass Sie sekundäre DB-Cluster für Ihre globalen Aurora-Datenbanken erstellen, indem Sie dieselbe Version der Aurora-DB-Engine wie für den primären Cluster verwenden. Weitere Informationen finden Sie unter Erstellen einer Amazon Aurora Global Database.

Erste Schritte mit globalen Amazon-Aurora-Datenbanken

Um mit globalen Aurora-Datenbanken zu beginnen, entscheiden Sie zunächst, welche Aurora-DB-Engine Sie verwenden möchten und in welchen AWS-Regionen. Nur bestimmte Versionen

der Aurora-MySQL- und Aurora-PostgreSQL-Datenbank-Engines in bestimmten AWS-Regionen unterstützen globale Aurora-Datenbanken. Die vollständige Liste finden Sie unter Unterstützte Regionen und DB-Engines für globale Aurora-Datenbanken.

Sie können eine Aurora globale Datenbank auf eine der folgenden Arten erstellen:

- Erstellen Sie eine neue globale Aurora-Datenbank mit neuen Aurora-DB-Clustern und Aurora-DB-Instances – sie können dies tun, indem Sie die unter Erstellen einer Amazon Aurora Global Database beschriebenen Schritte ausführen. Nachdem Sie den primären Aurora-DB-Cluster erstellt haben, fügen Sie die sekundäre AWS-Region hinzu, indem Sie die unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank beschriebenen Schritte ausführen.
- Verwenden Sie einen vorhandenen Aurora-DB-Cluster, der die globale Aurora-Datenbankfunktion unterstützt, und fügen Sie ihm eine AWS-Region hinzu – Das können Sie nur tun, wenn Ihr vorhandener Aurora-DB-Cluster eine DB-Engine-Version verwendet, die den globalen Aurora-Modus unterstützt oder global kompatibel ist. Für einige DB-Engine-Versionen ist dieser Modus explizit, für andere jedoch nicht.

  Überprüfen Sie, ob Sie in Region hinzufügen als Aktion auf AWS Management Console auswählen können, wenn Ihr Aurora-DB-Cluster ausgewählt ist. Wenn das möglich ist, können Sie diesen Aurora-DB-Cluster als globalen Aurora-Cluster verwenden. Weitere Informationen finden Sie unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank.

Bevor Sie eine Aurora globale Datenbank erstellen, empfehlen wir Ihnen, alle Konfigurationsanforderungen zu verstehen.

Themen

- Anforderungen an die Konfiguration einer Amazon Aurora globalen Datenbank
- Erstellen einer Amazon Aurora Global Database
- Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank
- Erstellen eines Aurora-Headless-DB-Clusters in einer sekundären Region
- Verwenden eines Snapshot für Ihre globale Amazon-Aurora-Datenbank

Anforderungen an die Konfiguration einer Amazon Aurora globalen Datenbank

Eine globale Aurora-Datenbank umfasst mindestens zwei AWS-Regionen. Die primäre AWS-Region unterstützt einen Aurora-DB-Cluster mit einer Writer-Aurora-DB-Instance. Eine sekundäre AWS-Region führt einen schreibgeschützten Aurora-DB-Cluster aus, der vollständig aus Aurora-Replikaten besteht. Mindestens eine sekundäre AWS-Region ist erforderlich, aber eine Aurora Global Database kann bis zu fünf sekundäre AWS-Regionen haben. In der Tabelle sind die maximal zulässigen Aurora-DB-Cluster, Aurora-DB-Instances und Aurora-Replicas aufgeführt, die in einer globalen Aurora-Datenbank zulässig sind.

Beschreibung	Primär AWS-Region	Sekundär AWS-Regionen
Aurora-DB-Cluster	1	5 (maximal)
Writer-Inst	1	0
Schreibgeschützte Instances (Aurora-Replicas) pro Aurora-DB-Cluster	15 (Max.)	16 (Total)
Schreibgeschützte Instances (maximal zulässig, bei tatsächli cher Anzahl von sekundären Regionen)	15 - s	s = Gesamtzahl der sekundären AWS-Regionen

Die Aurora-DB-Cluster, aus denen eine globale Aurora-Datenbank besteht, haben die folgenden spezifischen Anforderungen:

- DB-Instance-Klassenanforderungen – Eine globale Aurora-Datenbank erfordert DB-Instance-Klassen, die für speicherintensive Anwendungen optimiert sind. Weitere Informationen zu den arbeitsspeicheroptimierten DB-Instance-Klassen finden Sie unter DB-Instance-Klassen. Wir empfehlen, db.r5 oder eine höhere Instance-Klasse zu nutzen.
- AWS-Region-Anforderungen – Eine globale Aurora-Datenbank benötigt einen primären Aurora-DB-Cluster in einer AWS-Region und mindestens einen sekundären Aurora-DB-Cluster in einer anderen Region. Sie können bis zu fünf sekundäre (schreibgeschützte) Aurora-DB-Cluster erstellen, und jeder muss sich in einer anderen Region befinden. Mit anderen Worten, es können

sich keine zwei Aurora-DB-Cluster in einer globalen Aurora-Datenbank in derselben AWS-Region befinden.

- Benennungsanforderungen – Die Namen, die Sie für jeden Ihrer Aurora-DB-Cluster auswählen, müssen in allen AWS-Regionen eindeutig sein. Sie können nicht denselben Namen für verschiedene Aurora-DB-Cluster verwenden, obwohl sie sich in verschiedenen Regionen befinden.
- Kapazitätsanforderungen für Aurora Serverless v2 – Für eine globale Datenbank mit Aurora Serverless v2 beträgt die Mindestkapazität, die für den DB-Cluster in der primären AWS-Region erforderlich ist, 8 ACUs.

Bevor Sie die in diesem Abschnitt beschriebenen Verfahren befolgen können, benötigen Sie ein AWS-Konto. Schließen Sie die Einrichtungsaufgaben für die Arbeit mit Amazon Aurora ab. Weitere Informationen finden Sie unter Einrichten Ihrer Umgebung für Amazon Aurora. Sie müssen auch andere vorab erforderliche Schritte zum Erstellen eines Aurora-DB-Clusters ausführen. Weitere Informationen hierzu finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Erstellen einer Amazon Aurora Global Database

In einigen Fällen haben Sie möglicherweise einen vorhandenen bereitgestellten Aurora-DB-Cluster, auf dem eine global kompatible Aurora-Datenbank-Engine ausgeführt wird. In diesem Fall können Sie eine weitere AWS-Region hinzufügen, um Ihre globale Aurora-Datenbank zu erstellen. Lesen Sie dazu den Abschnitt Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank.

Führen Sie die folgenden Schritte aus, um eine globale Aurora-Datenbank mit der AWS Management Console, der AWS CLI oder der RDS-API zu erstellen.

Konsole

Die Schritte zum Erstellen einer globalen Aurora-Datenbank beginnen mit der Anmeldung bei einer AWS-Region, die die globale Aurora-Datenbankfunktion unterstützt. Eine vollständige Liste finden Sie hier: Unterstützte Regionen und DB-Engines für globale Aurora-Datenbanken.

Einer der folgenden Schritte ist die Auswahl einer Virtual Private Cloud (VPC), die auf Amazon VPC für Ihren Aurora-DB-Cluster basiert. Um Ihre eigene VPC zu verwenden, empfehlen wir Ihnen, diese im Voraus zu erstellen, damit sie von Ihnen ausgewählt werden kann. Erstellen Sie gleichzeitig alle zugehörigen Subnetze und nach Bedarf eine Subnetz- und Sicherheitsgruppe. Weitere Informationen erhalten Sie unter Tutorial: Erstellen eines Amazon VPC zur Verwendung mit einer DB-Instance.

Allgemeine Informationen zum Erstellen eines Aurora-DB-Clusters finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

So erstellen Sie eine globale Aurora-Datenbank

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Datenbank erstellen aus. Gehen Sie auf der Seite Datenbank erstellen wie folgt vor:
   - Wählen Sie als Datenbankerstellungsmethode Standarderstellung aus. Wählen Sie nicht Einfache Erstellung.
   - Wählen Sie für `Engine type` im Abschnitt Engine-Optionen den entsprechenden Engine-Typ, Aurora (MySQL-kompatibel) oder Aurora (PostgreSQL-kompatibel).
3. Fahren Sie fort mit dem Erstellen der globalen Datenbank, indem Sie den Schritten aus den folgenden Verfahren folgen:

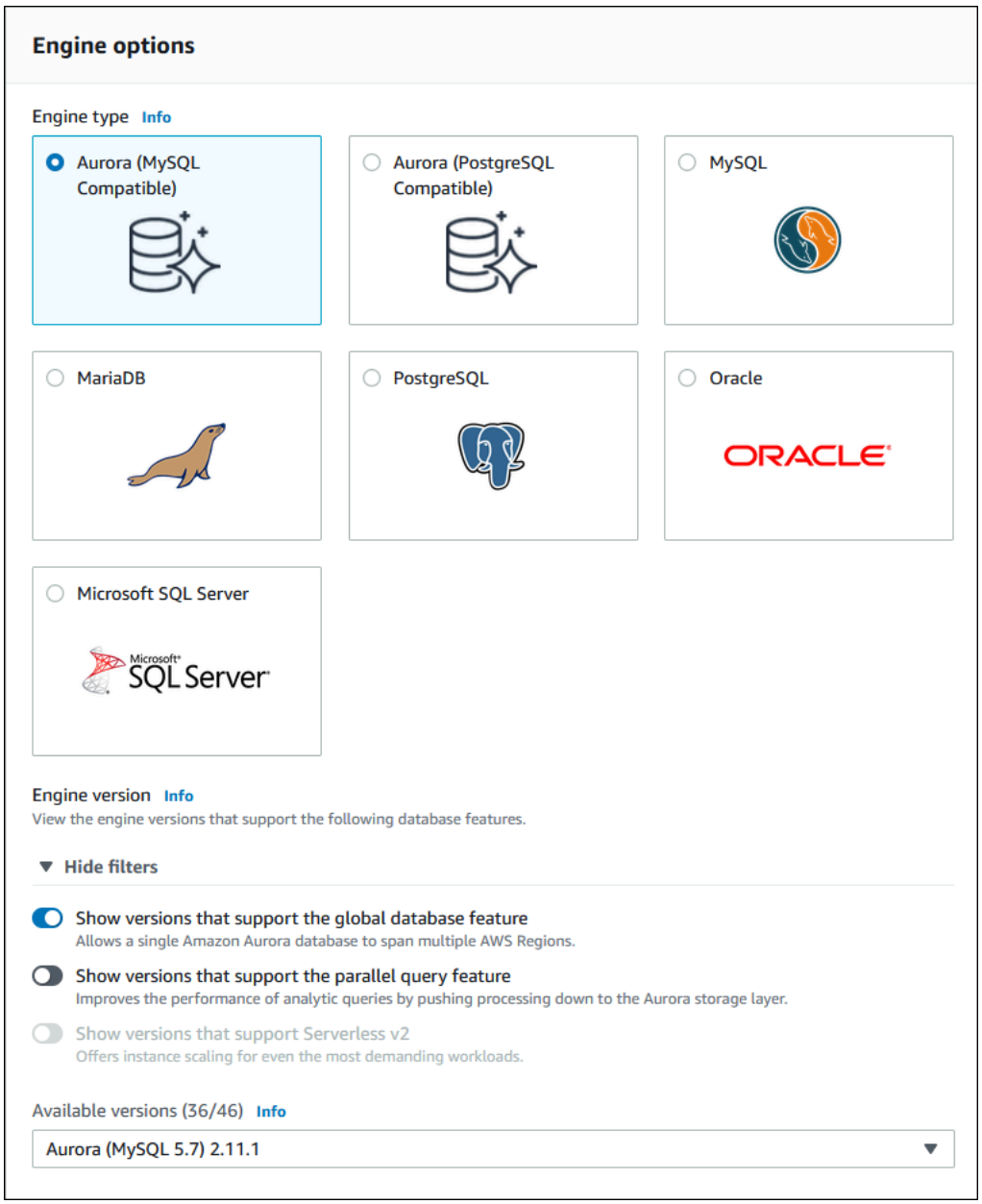
Erstellen einer globalen Datenbank mit Aurora MySQL

Die folgenden Schritte gelten für alle Versionen von Aurora MySQL.

So erstellen Sie eine globale Aurora-Datenbank mit Aurora MySQL:

Füllen Sie die Seite Datenbank erstellen aus.

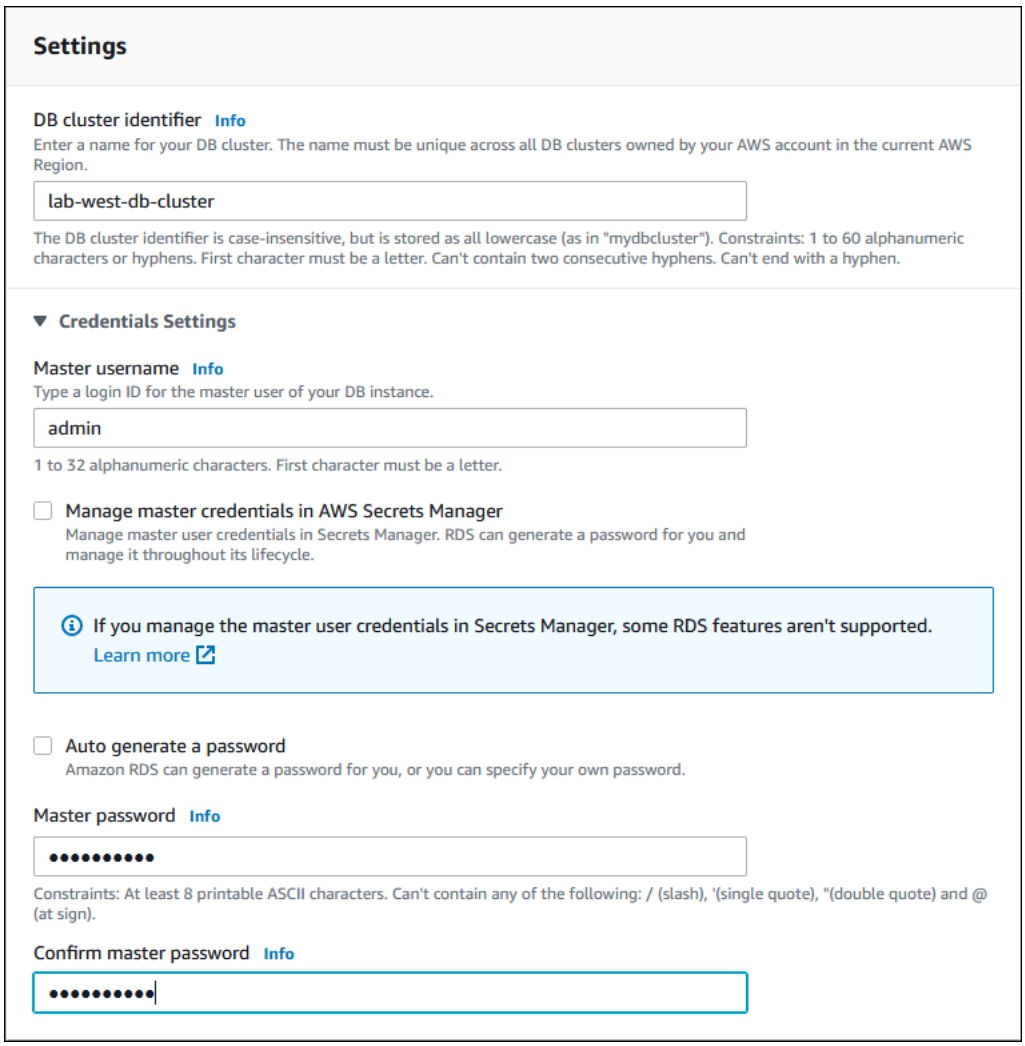
1. Wählen Sie unter Engine-Optionen Folgendes aus:
   a. Erweitern Sie Filter anzeigen und aktivieren Sie dann Versionen anzeigen, die die Funktion für globale Datenbanken unterstützen.
   b. Wählen Sie für Engine-Version die Version von Aurora MySQL, die Sie für Ihre globale Aurora-Datenbank verwenden möchten.



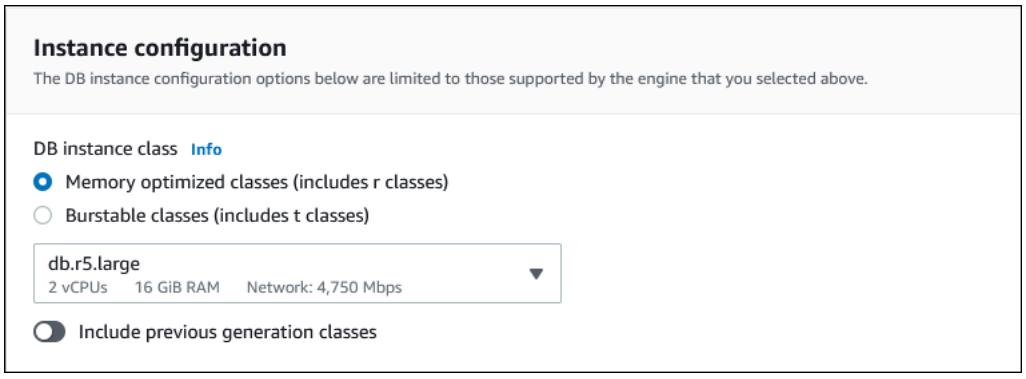
2. Wählen Sie für VorlagenProduktion. Oder Sie können Dev/Test wählen, falls dies für Ihren Anwendungsfall geeignet ist. Verwenden Sie Dev/Test nicht in Produktionsumgebungen.
3. Für Settings (Einstellungen) nehmen Sie folgendes vor:

   a. Geben Sie einen aussagekräftigen Namen für die DB-Cluster-ID ein. Wenn Sie mit dem Erstellen der Aurora globalen Datenbank fertig sind, identifiziert dieser Name den primären DB-Cluster.

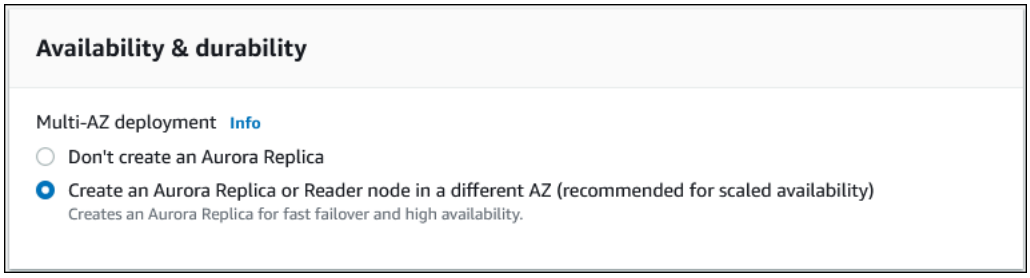
   b. Geben Sie Ihr eigenes Passwort für das `admin`-Benutzerkonto für die DB-Instance ein oder lassen Sie Aurora eines für Sie erstellen. Wenn Sie ein Passwort automatisch generieren, erhalten Sie die Option zum Kopieren des Passworts.



4. Wählen Sie für DB instance class (DB-Instance-Klasse) `db.r5.large` oder eine andere arbeitsspeicheroptimierte DB-Instance-Klasse aus. Wir empfehlen, db.r5 oder eine höhere Instance-Klasse zu nutzen.



5. Für Verfügbarkeit und Haltbarkeit empfehlen wir Ihnen, Aurora für die Erstellung einer Aurora-Replica in einer anderen Availability Zone (AZ) zu wählen. Wenn Sie jetzt keine Aurora-Replica erstellen, müssen Sie dies später tun.



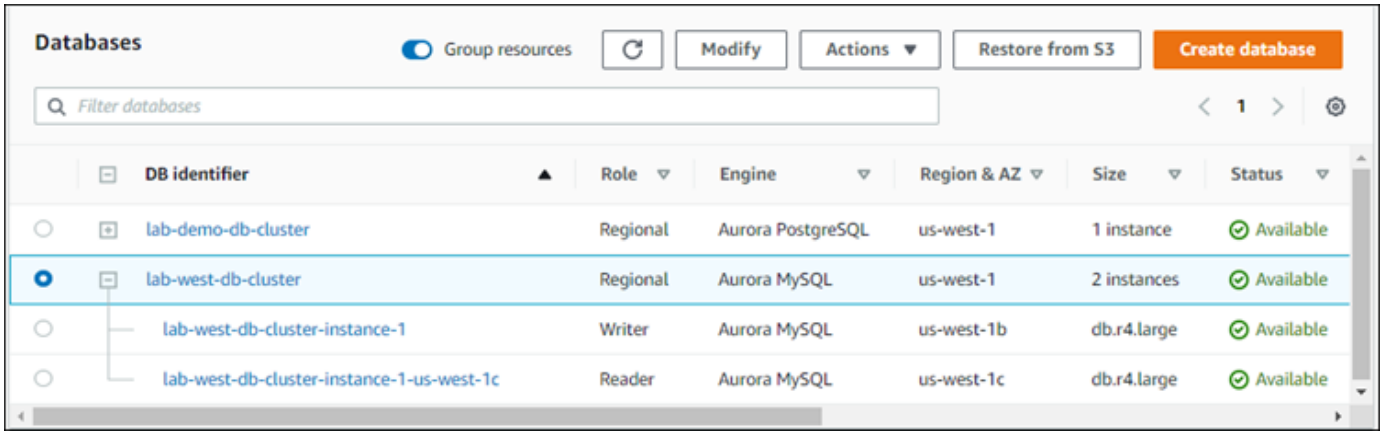
6. Wählen Sie bei Anbindung die auf Amazon VPC basierende Virtual Private Cloud (VPC) aus, die die virtuelle Netzwerkumgebung für diese DB-Instance definiert. Sie können die Standardwerte auswählen, um diese Aufgabe zu vereinfachen.
7. Schließen Sie die Einstellungen für die Datenbankauthentifizierung ab. Um den Prozess zu vereinfachen, können Sie jetzt Passwort-Authentifizierung wählen und AWS Identity and Access Management (IAM) später einrichten.
8. Für Zusätzliche Konfiguration führen Sie die folgenden Schritte aus:

   a. Geben Sie einen Namen für Anfänglicher Datenbankname ein, um die primäre Aurora-DB-Instance für diesen Cluster zu erstellen. Dies ist der Writer-Knoten für den Aurora primären DB-Cluster.

      Belassen Sie die für die DB-Clusterparametergruppe und die DB-Parametergruppe ausgewählten Standardwerte, es sei denn, Sie haben Ihre eigenen benutzerdefinierten Parametergruppen, die Sie verwenden möchten.

   b. Deaktivieren Sie das Kontrollkästchen Rückverfolgung aktivieren, wenn es aktiviert ist. Globale Datenbanken von Aurora unterstützen keine Rückverfolgung. Sie können andernfalls die anderen Standardeinstellungen für die Zusätzliche Konfiguration akzeptieren.
9. Wählen Sie Create database (Datenbank erstellen) aus.

   Es kann einige Minuten dauern, bis Aurora den Prozess zum Erstellen der Aurora-DB-Instance, ihrer Aurora Replica und des Aurora-DB-Clusters abgeschlossen hat. Sie können anhand des Status feststellen, wann der Aurora-DB-Cluster als primärer DB-Cluster in einer globalen Aurora-Datenbank verwendet werden kann. Wenn dies der Fall ist, lautet der Status und der des Writer- und Replikat-Knotens Verfügbar, wie nachstehend gezeigt.



Wenn Ihr primärer DB-Cluster verfügbar ist, erstellen Sie die globale Aurora-Datenbank, indem Sie einen sekundären Cluster hinzufügen. Befolgen Sie dafür die unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank beschriebenen Schritte.

Erstellen einer globalen Datenbank mit Aurora PostgreSQL

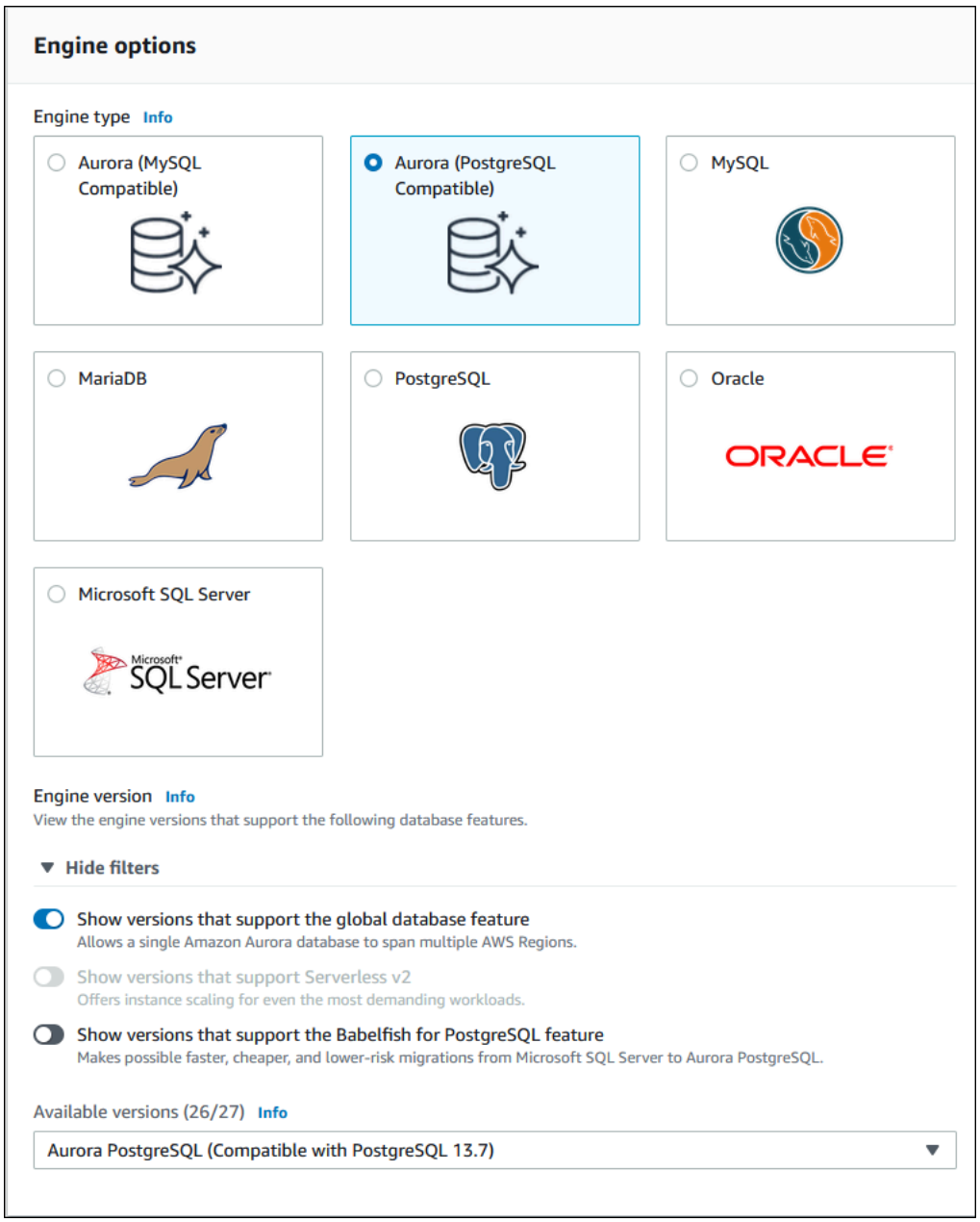
So erstellen Sie eine globale Aurora-Datenbank mit Aurora PostgreSQL

Füllen Sie die Seite Datenbank erstellen aus.

1. Wählen Sie unter Engine-Optionen Folgendes aus:

    a. Erweitern Sie Filter anzeigen und aktivieren Sie dann Versionen anzeigen, die die Funktion für globale Datenbanken unterstützen.

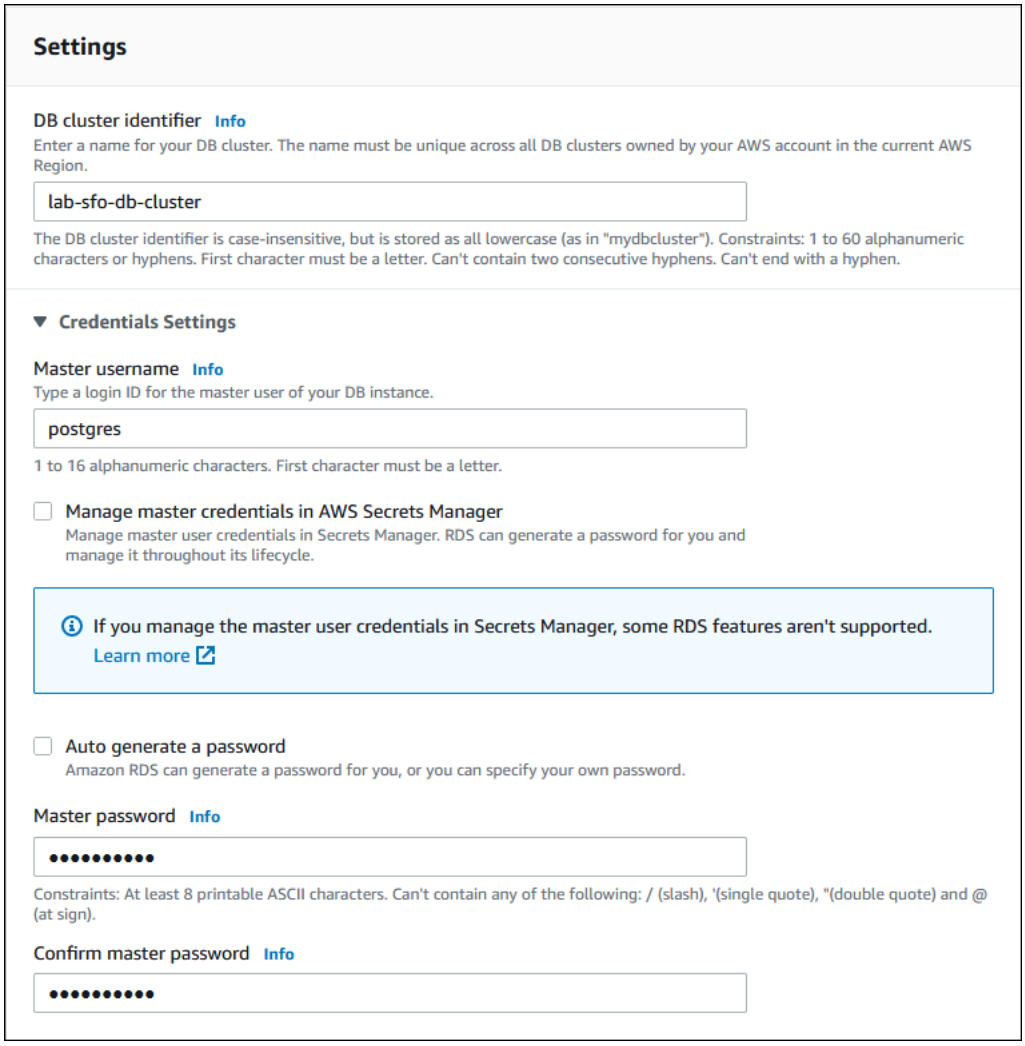
    b. Wählen Sie für Engine-Version die Version von Aurora PostgreSQL, die Sie für Ihre Aurora globale Datenbank verwenden möchten.



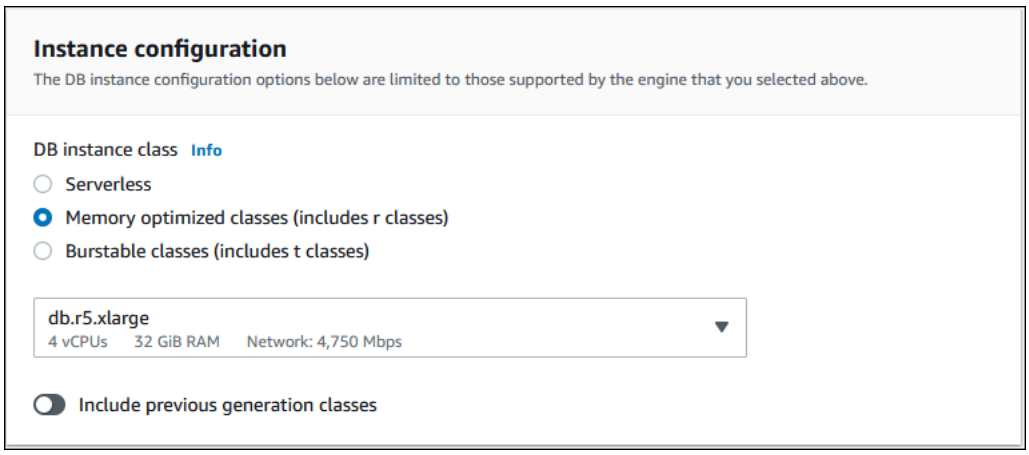
2. Wählen Sie für VorlagenProduktion. Oder Sie können Dev/Test wählen, falls dies geeignet ist. Verwenden Sie Dev/Test nicht in Produktionsumgebungen.
3. Für Settings (Einstellungen) nehmen Sie folgendes vor:

   a. Geben Sie einen aussagekräftigen Namen für die DB-Cluster-ID ein. Wenn Sie mit dem Erstellen der Aurora globalen Datenbank fertig sind, identifiziert dieser Name den primären DB-Cluster.

b. Geben Sie Ihr eigenes Passwort für das Standard-Admin-Konto für den DB-Cluster ein, oder lassen Sie es Aurora für Sie generieren. Wenn Sie „Passwort automatisch generieren“ wählen, erhalten Sie die Option zum Kopieren des Passworts.



4. Wählen Sie für DB instance class (DB-Instance-Klasse) `db.r5.large` oder eine andere arbeitsspeicheroptimierte DB-Instance-Klasse aus. Wir empfehlen, db.r5 oder eine höhere Instance-Klasse zu nutzen.



5. Für Verfügbarkeit und Haltbarkeit empfehlen wir Ihnen, Aurora für die Erstellung einer Aurora-Replica in einer anderen AZ für Sie zu wählen. Wenn Sie jetzt keine Aurora-Replica erstellen, müssen Sie dies später tun.
6. Wählen Sie bei Anbindung die auf Amazon VPC basierende Virtual Private Cloud (VPC) aus, die die virtuelle Netzwerkumgebung für diese DB-Instance definiert. Sie können die Standardwerte auswählen, um diese Aufgabe zu vereinfachen.
7. (Optional) Schließen Sie die Einstellungen für die Datenbankauthentifizierung ab. Die Passwortauthentifizierung ist immer aktiviert. Um den Prozess zu vereinfachen, können Sie diesen Abschnitt überspringen und später die IAM- oder Passwort- und Kerberos-Authentifizierung einrichten.
8. Für Zusätzliche Konfigurationen führen Sie die folgenden Schritte aus:

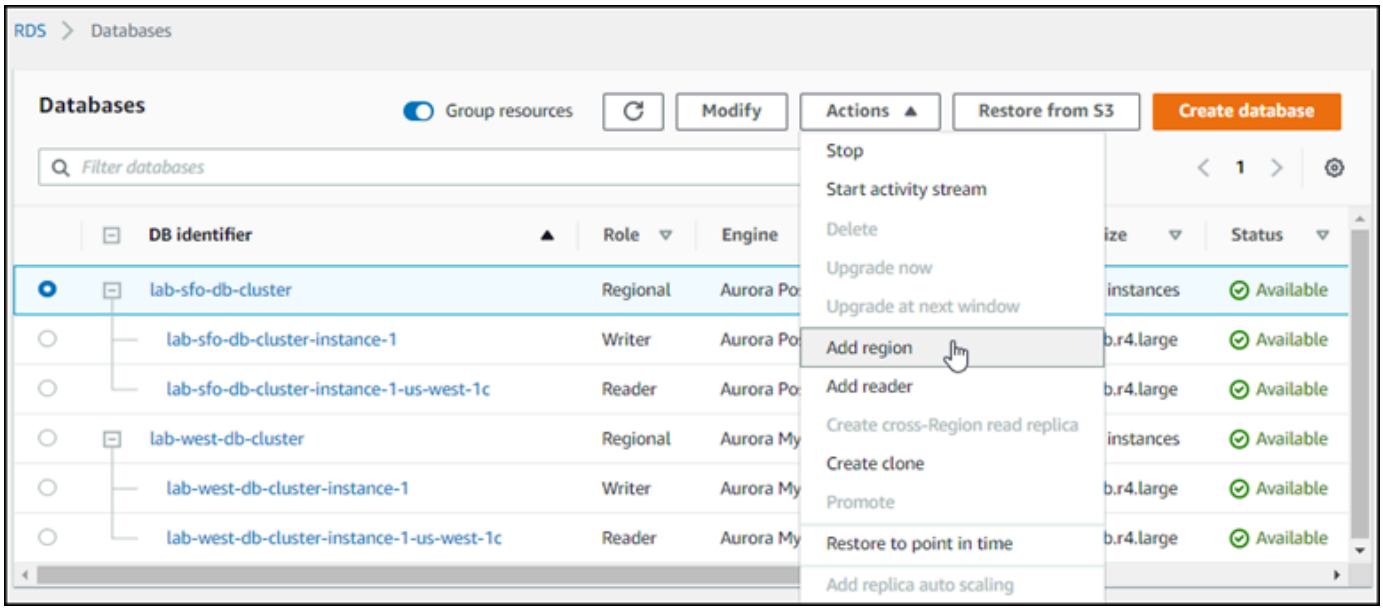
   a. Geben Sie einen Namen für Anfänglicher Datenbankname ein, um die primäre Aurora-DB-Instance für diesen Cluster zu erstellen. Dies ist der Writer-Knoten für den Aurora primären DB-Cluster.

      Belassen Sie die für die DB-Clusterparametergruppe und die DB-Parametergruppe ausgewählten Standardwerte, es sei denn, Sie haben Ihre eigenen benutzerdefinierten Parametergruppen, die Sie verwenden möchten.

   b. Akzeptieren Sie alle anderen Standardeinstellungen für zusätzliche Konfigurationen wie Verschlüsselung, Protokollexporte usw.
9. Wählen Sie Datenbank erstellen aus.

Es kann einige Minuten dauern, bis Aurora den Prozess zum Erstellen der Aurora-DB-Instance, ihrer Aurora Replica und des Aurora-DB-Clusters abgeschlossen hat. Wenn der Cluster einsatzbereit ist, zeigen der Aurora-DB-Cluster und seine Writer- und Replica-Nodes den Status

Verfügbar an. Dies wird der primäre DB-Cluster Ihrer Aurora globalen Datenbank, nachdem Sie einen sekundären Cluster hinzugefügt haben.



Wenn Ihr primäre DB-Cluster verfügbar ist, erstellen Sie einen oder mehrere sekundäre Cluster, indem Sie die Schritte Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank.

AWS CLI

Die AWS CLI-Befehle in den folgenden Prozeduren führen die folgenden Aufgaben aus:

1. Erstellen einer globalen Aurora-Datenbank, Eingabe eines Namens und Spezifizierung des Typs der Aurora-Datenbank-Engine, den Sie verwenden möchten.
2. Erstellen Sie einen Aurora-DB-Cluster für die Aurora globale Datenbank.
3. Erstellen Sie eine Aurora-DB-Instance für den Cluster. Dies ist der primäre Aurora-DB-Cluster der globalen Datenbank.
4. Erstellen Sie eine zweite DB-Instance für den Aurora-DB-Cluster. Dies ist ein Reader zur Vervollständigung des Aurora-DB-Clusters.
5. Erstellen Sie einen zweiten Aurora-DB-Cluster in einer anderen Region und fügen Sie ihn dann Ihrer Aurora globalen Datenbank hinzu, indem Sie die unter beschriebenen Schritte ausführe Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank.

Folgen Sie der Vorgehensweise für Ihre Aurora-Datenbank-Engine.

Erstellen einer globalen Datenbank mit Aurora MySQL

So erstellen Sie eine globale Aurora-Datenbank mit Aurora MySQL:

1. Verwenden Sie den `create-global-cluster`-CLI-Befehl zur Übergabe des Namens der AWS-Region, der Aurora-Datenbank-Engine und der Version.

   Für Linux, macOSoder Unix:

   ```
   aws rds create-global-cluster --region primary_region  \
       --global-cluster-identifier global_database_id \
       --engine aurora-mysql \
       --engine-version version # optional
   ```

   Windows:

   ```
   aws rds create-global-cluster ^
       --global-cluster-identifier global_database_id ^
       --engine aurora-mysql ^
       --engine-version version # optional
   ```

   Dadurch wird eine „leere“ Aurora globale Datenbank mit nur einem Namen (Identifier) und einer Aurora-Datenbank-Engine erstellt. Es kann einige Minuten dauern, bis die Aurora globale Datenbank verfügbar ist. Bevor Sie mit dem nächsten Schritt fortfahren, prüfen Sie mit dem `describe-global-clusters`-CLI-Befehl, ob sie verfügbar ist.

   ```
   aws rds describe-global-clusters --region primary_region --global-cluster-
   identifier global_database_id
   ```

   Wenn die Aurora globale Datenbank verfügbar ist, können Sie ihren primären Aurora-DB-Cluster erstellen.

2. Um einen primären Aurora-DB-Cluster zu erstellen, verwenden Sie den `create-db-cluster`-CLI-Befehl. Fügen Sie den Namen Ihrer Aurora globalen Datenbank mit dem Parameter `--global-cluster-identifier` ein.

   Für Linux, macOSoder Unix:

   ```
   aws rds create-db-cluster \
     --region primary_region \
   ```

```
  --db-cluster-identifier primary_db_cluster_id \
  --master-username userid \
  --master-user-password password \
  --engine aurora-mysql \
  --engine-version version \
  --global-cluster-identifier global_database_id
```

Windows:

```
aws rds create-db-cluster ^
  --region primary_region ^
  --db-cluster-identifier primary_db_cluster_id ^
  --master-username userid ^
  --master-user-password password ^
  --engine aurora-mysql ^
  --engine-version version ^
  --global-cluster-identifier global_database_id
```

Verwenden Sie den `describe-db-clusters` AWS CLI-Befehl, um zu bestätigen, dass der Aurora-DB-Cluster bereit ist. Um einen bestimmten Aurora-DB-Cluster herauszugreifen, verwenden Sie den Parameter `--db-cluster-identifier`. Oder Sie können den Aurora-DB-Cluster-Namen im Befehl weg lassen, um Details zu all Ihren Aurora-DB-Clustern in der angegebenen Region zu erhalten.

```
aws rds describe-db-clusters --region primary_region --db-cluster-
identifier primary_db_cluster_id
```

Wenn die Antwort `"Status": "available"` für den Cluster anzeigt, ist er einsatzbereit.

3. Erstellen Sie die DB-Instance für Ihren primären Aurora-DB-Cluster. Verwenden Sie dazu den `create-db-instance`-CLI-Befehl. Geben Sie den Namen Ihres Aurora-DB-Clusters an und geben Sie die Konfigurationsdetails für die Instance an. Sie müssen die Parameter `--master-username` und `--master-user-password` im Befehl nicht übergeben, da diese vom Aurora-DB-Cluster abgerufen werden.

   Für `--db-instance-class` können Sie nur arbeitsspeicheroptimierte Klassen verwenden, z. B. `db.r5.large`. Wir empfehlen, db.r5 oder eine höhere Instance-Klasse zu nutzen. Weitere Informationen zu diesen Klassen finden Sie unter DB-Instance-Klassen.

   Für Linux, macOSoder Unix:

```
aws rds create-db-instance \
  --db-cluster-identifier primary_db_cluster_id \
  --db-instance-class instance_class \
  --db-instance-identifier db_instance_id \
  --engine aurora-mysql \
  --engine-version version \
  --region primary_region
```

Windows:

```
aws rds create-db-instance ^
  --db-cluster-identifier primary_db_cluster_id ^
  --db-instance-class instance_class ^
  --db-instance-identifier db_instance_id ^
  --engine aurora-mysql ^
  --engine-version version ^
  --region primary_region
```

Die Operation `create-db-instance` kann einige Zeit in Anspruch nehmen. Überprüfen Sie den Status, um festzustellen, ob die Aurora-DB-Instance verfügbar ist, bevor Sie fortfahren.

```
aws rds describe-db-clusters --db-cluster-identifier primary_db_cluster_id
```

Wenn der Befehl den Status „verfügbar“ ausgibt, können Sie eine weitere Aurora-DB-Instance für Ihren primären DB-Cluster erstellen. Dies ist die Reader-Instance (Aurora-Replica) für den Aurora-DB-Cluster.

4. Um eine weitere Aurora-DB-Instance für den Cluster zu erstellen, verwenden Sie den `create-db-instance`-CLI-Befehl.

   Für Linux, macOSoder Unix:

```
aws rds create-db-instance \
  --db-cluster-identifier primary_db_cluster_id \
  --db-instance-class instance_class \
  --db-instance-identifier replica_db_instance_id \
  --engine aurora-mysql
```

   Windows:

```
aws rds create-db-instance ^
  --db-cluster-identifier primary_db_cluster_id ^
  --db-instance-class instance_class ^
  --db-instance-identifier replica_db_instance_id ^
  --engine aurora-mysql
```

Wenn die DB-Instance verfügbar ist, beginnt die Replikation vom Writer-Knoten zum Replica. Bevor Sie fortfahren, überprüfen Sie, ob die DB-Instance mit dem `describe-db-instances`-CLI-Befehl verfügbar ist.

Zu diesem Zeitpunkt verfügen Sie über eine Aurora globale Datenbank mit ihrem primären Aurora-DB-Cluster, der eine Writer-DB-Instance und eine Aurora-Replica enthält. Sie können jetzt einen schreibgeschützten Aurora-DB-Cluster in einer anderen Region hinzufügen, um Ihre Aurora globale Datenbank zu vervollständigen. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank.

Erstellen einer globalen Datenbank mit Aurora PostgreSQL

Wenn Sie mithilfe der folgenden Befehle Aurora-Objekte für eine globale Aurora-Datenbank erstellen, kann es einige Minuten dauern, bis jedes verfügbar ist. Wir empfehlen, dass Sie nach Abschluss eines bestimmten Befehls den Status des jeweiligen Aurora-Objekts überprüfen, um sicherzustellen, dass der Status „Verfügbar“ lautet.

Verwenden Sie dazu den `describe-global-clusters`-CLI-Befehl.

```
aws rds describe-global-clusters --region primary_region
    --global-cluster-identifier global_database_id
```

So erstellen Sie eine globale Aurora-Datenbank mit Aurora PostgreSQL

1. Verwenden Sie den `create-global-cluster`-CLI-Befehl.

   Für Linux, macOSoder Unix:

   ```
   aws rds create-global-cluster --region primary_region  \
       --global-cluster-identifier global_database_id \
       --engine aurora-postgresql \
       --engine-version version # optional
   ```

Windows:

```
aws rds create-global-cluster ^
    --global-cluster-identifier global_database_id ^
    --engine aurora-postgresql ^
    --engine-version version # optional
```

Wenn die Aurora globale Datenbank verfügbar ist, können Sie ihren primären Aurora-DB-Cluster erstellen.

2. Um einen primären Aurora-DB-Cluster zu erstellen, verwenden Sie den `create-db-cluster`-CLI-Befehl. Fügen Sie den Namen Ihrer Aurora globalen Datenbank mit dem Parameter `--global-cluster-identifier` ein.

   Für Linux, macOSoder Unix:

```
aws rds create-db-cluster \
  --region primary_region \
  --db-cluster-identifier primary_db_cluster_id \
  --master-username userid \
  --master-user-password password \
  --engine aurora-postgresql \
  --engine-version version \
  --global-cluster-identifier global_database_id
```

   Windows:

```
aws rds create-db-cluster ^
  --region primary_region ^
  --db-cluster-identifier primary_db_cluster_id ^
  --master-username userid ^
  --master-user-password password ^
  --engine aurora-postgresql ^
  --engine-version version ^
  --global-cluster-identifier global_database_id
```

   Prüfen Sie, ob der Aurora-DB-Cluster bereit ist. Wenn die Antwort des folgenden Befehls `"Status": "available"` für den Aurora-DB-Cluster angezeigt wird, können Sie fortfahren.

```
aws rds describe-db-clusters --region primary_region --db-cluster-
identifier primary_db_cluster_id
```

3. Erstellen Sie die DB-Instance für Ihren primären Aurora-DB-Cluster. Verwenden Sie dazu den `create-db-instance`-CLI-Befehl.

   Übergeben Sie den Namen Ihres Aurora-DB-Clusters mit dem Parameter `--db-cluster-identifier`.

   Sie müssen die Parameter `--master-username` und `--master-user-password` im Befehl nicht übergeben, da diese vom Aurora-DB-Cluster abgerufen werden.

   Für `--db-instance-class` können Sie nur arbeitsspeicheroptimierte Klassen verwenden, z. B. `db.r5.large`. Wir empfehlen, db.r5 oder eine höhere Instance-Klasse zu nutzen. Weitere Informationen zu diesen Klassen finden Sie unter DB-Instance-Klassen.

   Für Linux, macOSoder Unix:

```
aws rds create-db-instance \
  --db-cluster-identifier primary_db_cluster_id \
  --db-instance-class instance_class \
  --db-instance-identifier db_instance_id \
  --engine aurora-postgresql \
  --engine-version version \
  --region primary_region
```

   Windows:

```
aws rds create-db-instance ^
  --db-cluster-identifier primary_db_cluster_id ^
  --db-instance-class instance_class ^
  --db-instance-identifier db_instance_id ^
  --engine aurora-postgresql ^
  --engine-version version ^
  --region primary_region
```

4. Prüfen Sie den Status der Aurora-DB-Instance, bevor Sie fortfahren.

```
aws rds describe-db-clusters --db-cluster-identifier primary_db_cluster_id
```

Wenn die Antwort zeigt, dass der Status der Aurora-DB-Instance- „verfügbar“ ist, können Sie eine weitere Aurora-DB-Instance für Ihren primären DB-Cluster erstellen.

5. Um eine Aurora-Replica für Aurora-DB-Cluster zu erstellen, verwenden Sie den `create-db-instance`CLI-Befehl.

   Für Linux, macOSoder Unix:

   ```
   aws rds create-db-instance \
     --db-cluster-identifier primary_db_cluster_id \
     --db-instance-class instance_class \
     --db-instance-identifier replica_db_instance_id \
     --engine aurora-postgresql
   ```

   Windows:

   ```
   aws rds create-db-instance ^
     --db-cluster-identifier primary_db_cluster_id ^
     --db-instance-class instance_class ^
     --db-instance-identifier replica_db_instance_id ^
     --engine aurora-postgresql
   ```

Wenn die DB-Instance verfügbar ist, beginnt die Replikation vom Writer-Knoten zum Replica. Bevor Sie fortfahren, überprüfen Sie, ob die DB-Instance mit dem `describe-db-instances`-CLI-Befehl verfügbar ist.

Ihre Aurora globale Datenbank existiert nun, verfügt aber nur in ihrer primären Region einen Aurora-DB-Cluster, der aus einer Writer-DB-Instance und einer Aurora-Replica besteht. Sie können jetzt einen schreibgeschützten Aurora-DB-Cluster in einer anderen Region hinzufügen, um Ihre Aurora globale Datenbank zu vervollständigen. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank.

RDS-API

Um eine globale Aurora-Datenbank mit der RDS-API zu erstellen, führen Sie die CreateGlobalCluster Operation aus.

Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank

Eine globale Aurora-Datenbank benötigt mindestens einen sekundären Aurora-DB-Cluster in einer anderen AWS-Region als der primäre Aurora-DB-Cluster. Sie können bis zu fünf sekundäre DB-Cluster an Ihre globale Aurora-Datenbank anschließen. Reduzieren Sie für jeden sekundären DB-Cluster, den Sie Ihrer globalen Aurora-Datenbank hinzufügen, die Anzahl der Aurora-Replicas, die für den primären DB-Cluster zulässig sind, um eins.

Wenn Ihre globale Aurora-Datenbank beispielsweise 5 sekundäre Regionen hat, kann Ihr primärer DB-Cluster nur 10 (statt 15) Aurora-Replikate haben. Weitere Informationen finden Sie unter Anforderungen an die Konfiguration einer Amazon Aurora globalen Datenbank.

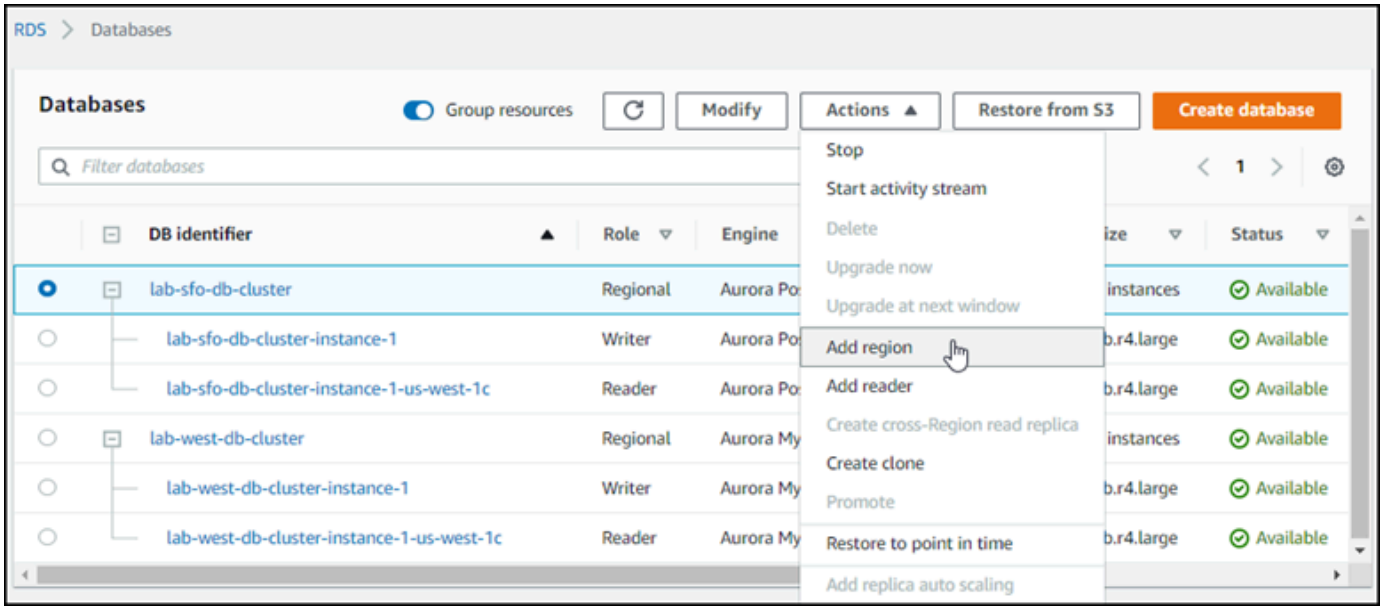
Die Anzahl der Aurora-Replikate (Reader-Instances) im primären DB-Cluster bestimmt die Anzahl der sekundären DB-Cluster, die Sie hinzufügen können. Die Gesamtzahl der Reader-Instances im primären DB-Cluster plus die Anzahl der sekundären Cluster darf nicht mehr als 15 betragen. Wenn Sie zum Beispiel 14 Reader-Instances im primären DB-Cluster und einen sekundären Cluster haben, können Sie der globalen Datenbank keinen weiteren sekundären Cluster hinzufügen.

> **Note**
>
> Wenn Sie für Aurora MySQL Version 3 einen sekundären Cluster erstellen, stellen Sie sicher, dass der Wert von `lower_case_table_names` mit dem Wert im primären Cluster übereinstimmt. Diese Einstellung ist ein Datenbankparameter, der beeinflusst, wie der Server die Groß- und Kleinschreibung von Bezeichnern behandelt. Weitere Informationen zu Datenbankparametern finden Sie unter Arbeiten mit Parametergruppen.
> Es wird empfohlen, beim Erstellen eines sekundären Clusters dieselbe DB-Engine-Version für den primären und den sekundären Cluster zu verwenden. Aktualisieren Sie bei Bedarf den primären Cluster auf die Version des sekundären Clusters. Weitere Informationen finden Sie unter Patch-Level-Kompatibilität für verwaltete regionsübergreifende Umstellungen und Failovers.

Konsole

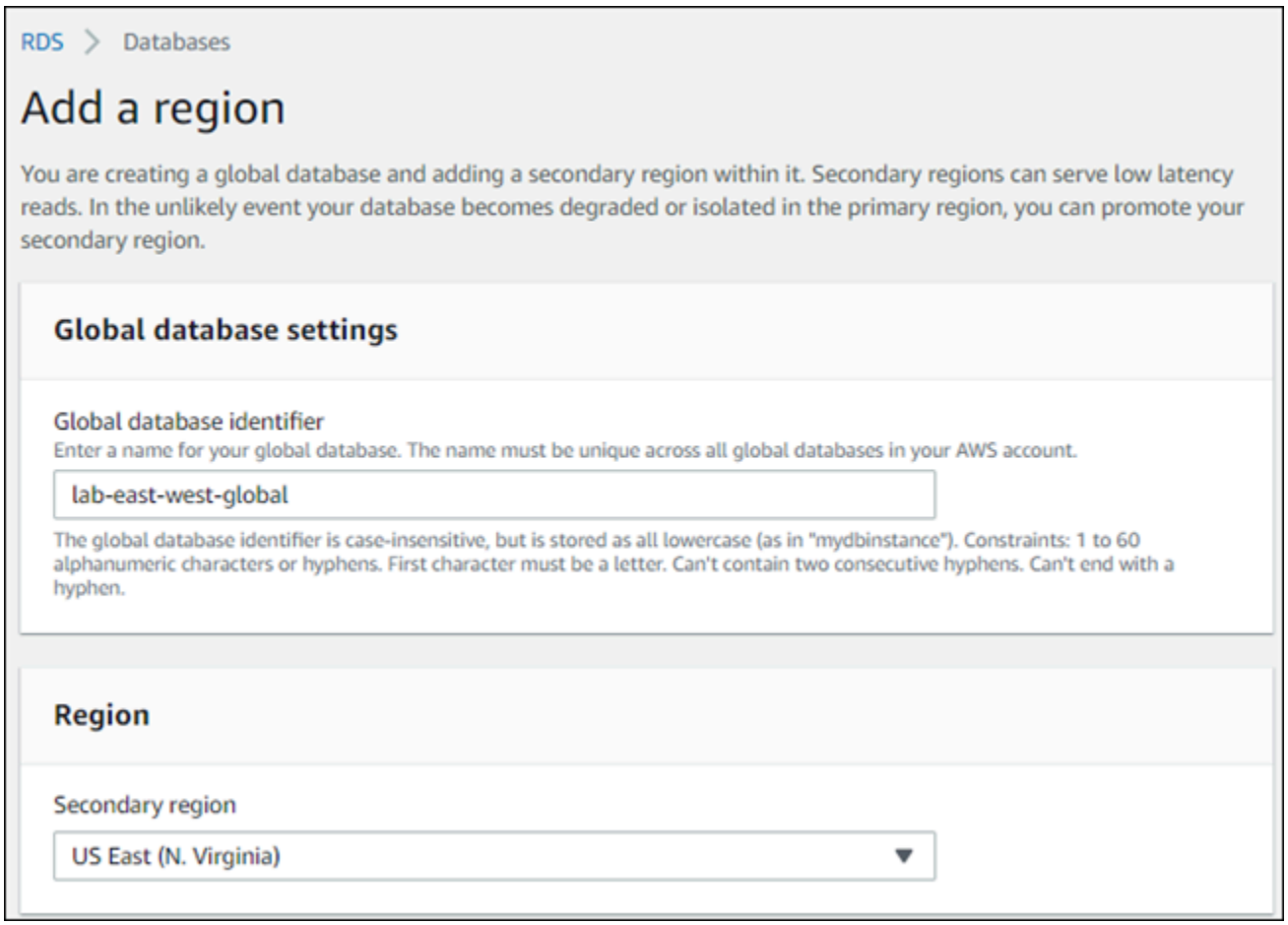
Um ein AWS-Region zu einer globalen Aurora-Datenbank hinzuzufügen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich der AWS Management Console die Option Datenbanken aus.
3. Wählen Sie die Aurora globale Datenbank aus, die einen sekundären Aurora-DB-Cluster benötigt. Stellen Sie sicher, dass der primäre Aurora-DB-Cluster is `Available`.
4. Wählen Sie unter Aktionen die Option Region hinzufügen aus.



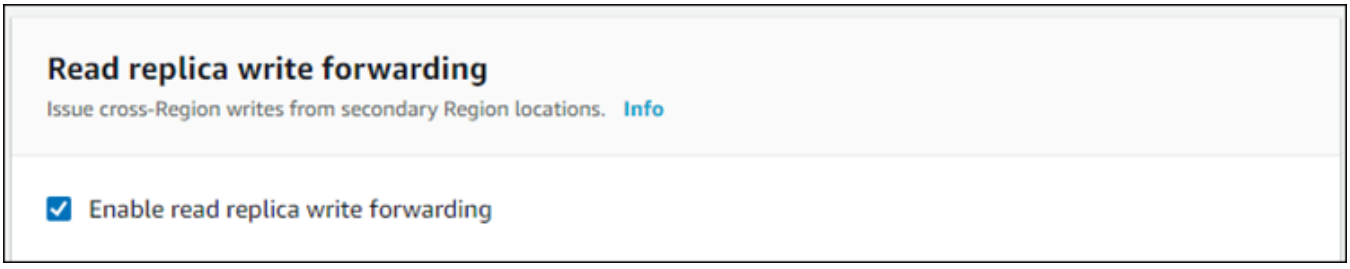
5. Wählen Sie auf der Seite Eine Region hinzufügen die sekundäre AWS-Region aus.

   Sie können keine AWS-Region auswählen, die bereits über einen sekundären Aurora-DB-Cluster für dieselbe globale Aurora-Datenbank verfügt. Außerdem kann dies nicht dieselbe Region sein wie die des primären Aurora-DB-Clusters.



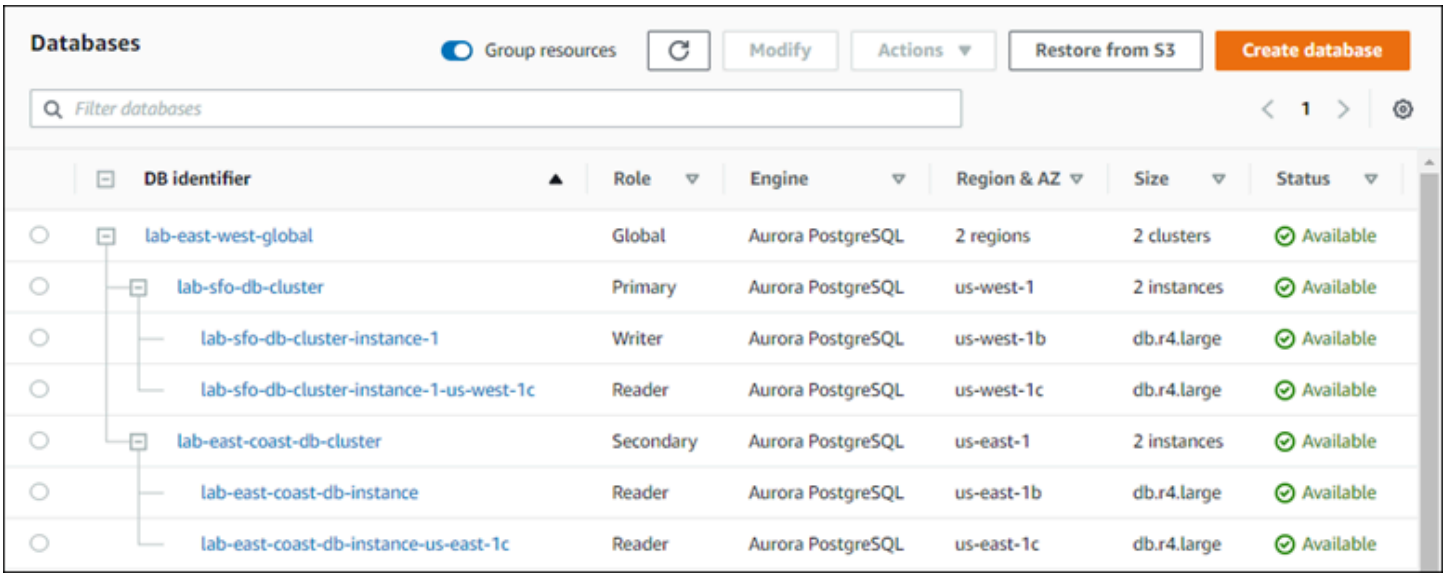
6. Füllen Sie die restlichen Felder für den sekundären Aurora-Cluster in der neuen AWS-Region aus. Dies sind die gleichen Konfigurationsoptionen wie für jede Aurora-DB-Cluster-Instance, mit Ausnahme der folgenden Option nur für Aurora MySQL–basierte globale Aurora-Datenbanken:

   - Read Replica-Schreibweiterleitung aktivieren – Mit dieser optionalen Einstellung leiten die sekundären DB-Cluster Ihrer globalen Aurora-Datenbank Schreibvorgänge an den primären Cluster weiter. Weitere Informationen finden Sie unter Verwenden der Schreibweiterleitung in einer Amazon Aurora globalen Datenbank.



7. Wählen Sie Region hinzufügen aus.

Nachdem Sie die Region zu Ihrer globalen Aurora-Datenbank hinzugefügt haben, können Sie sie in der Liste der Datenbanken in AWS Management Console sehen, wie im Screenshot gezeigt.



AWS CLI

Fügen Sie eine sekundäre AWS-Region zu einer globalen Aurora-Datenbank wie folgt hinzu:

1. Verwenden Sie den `create-db-cluster`-CLI-Befehl mit dem Namen (`--global-cluster-identifier`) Ihrer globalen Aurora-Datenbank. Für andere Parameter, führen Sie die folgenden Schritte aus:
2. Wählen Sie für `--region` eine andere AWS-Region als die Ihrer primären Aurora-Region aus.
3. Wählen Sie bestimmte Werte für die Parameter `--engine-version` und `--engine` aus. Diese Werte entsprechen denen des primären Aurora-DB-Clusters in Ihrer globalen Aurora-Datenbank.
4. Geben Sie für einen verschlüsselten Cluster Ihre primäre AWS-Region als `--source-region` für die Verschlüsselung an.

Im folgenden Beispiel wird ein neuer Aurora-DB-Cluster erstellt und als schreibgeschützter sekundärer Aurora-DB-Cluster an eine globale Aurora-Datenbank angehängt. Im letzten Schritt wird dem neuen Aurora-DB-Cluster eine Aurora-DB-Instance hinzugefügt.

Für Linux, macOSoder Unix:

```
aws rds --region secondary_region \
  create-db-cluster \
    --db-cluster-identifier secondary_cluster_id \
```

```
    --global-cluster-identifier global_database_id \
    --engine aurora-mysql|aurora-postgresql
    --engine-version version

aws rds --region secondary_region \
  create-db-instance \
    --db-instance-class instance_class \
    --db-cluster-identifier secondary_cluster_id \
    --db-instance-identifier db_instance_id \
    --engine aurora-mysql|aurora-postgresql
```

Windows:

```
aws rds --region secondary_region ^
  create-db-cluster ^
    --db-cluster-identifier secondary_cluster_id ^
    --global-cluster-identifier global_database_id_id ^
    --engine aurora-mysql|aurora-postgresql ^
    --engine-version version

aws rds --region secondary_region ^
  create-db-instance ^
    --db-instance-class instance_class ^
    --db-cluster-identifier secondary_cluster_id ^
    --db-instance-identifier db_instance_id ^
    --engine aurora-mysql|aurora-postgresql
```

RDS-API

Um einer globalen Aurora-Datenbank mit der RDS-API eine neue AWS-Region hinzuzufügen, führen Sie die Operation CreateDBCluster aus. Geben Sie die Kennung der vorhandenen globalen Datenbank mithilfe des Parameters `GlobalClusterIdentifier` an.

Erstellen eines Aurora-Headless-DB-Clusters in einer sekundären Region

Obwohl eine globale Aurora-Datenbank mindestens einen sekundären Aurora-DB-Cluster in einer AWS-Region außerhalb der primären Region benötigt, können Sie eine Headless-Konfiguration für den sekundären Cluster verwenden. Ein sekundärer Aurora-Headless-DB-Cluster hat keine DB-Instance. Diese Art der Konfiguration kann die Ausgaben für eine globale Aurora-Datenbank senken. In einem Aurora-DB-Cluster werden die Rechen- und Speicherressourcen entkoppelt. Ohne die DB-Instance wird Ihnen die Rechenleistung nicht in Rechnung gestellt, sondern nur der Speicherplatz.

Richtig eingerichtet, wird das sekundäre Headless-Speichervolume mit dem primären Aurora-DB-Cluster synchonisiert.

Sie fügen den sekundären Cluster wie gewohnt beim Erstellen einer globalen Aurora-Datenbank hinzu. Nachdem der primäre Aurora-DB-Cluster jedoch mit der Replikation zum sekundären Cluster begonnen hat, löschen Sie die Aurora (die schreibgeschützte DB-Instance) aus dem sekundären Aurora-DB-Cluster. Dieser sekundäre Cluster gilt jetzt als „Headless“, da er keine DB-Instance mehr hat. Das Speichervolume wird jedoch mit dem primären Aurora-DB-Cluster synchronisiert.

> **Warning**
>
> Um mit Aurora PostgreSQL einen Headless-Cluster in einer sekundären AWS-Region zu erstellen, verwenden Sie die AWS CLI- oder RDS-API, um die sekundäre AWS-Region hinzuzufügen. Überspringen Sie den Schritt, um die Reader-DB-Instance für den sekundären Cluster zu erstellen. Derzeit wird das Erstellen eines Headless-Clusters in der RDS-Konsole nicht unterstützt. Informationen zur Verwendung der CLI- und API-Prozeduren finden Sie unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank.
> Wenn Ihre globale Datenbank eine niedrigere Engine-Version als 13.4, 12.8 oder 11.13 verwendet, kann das Erstellen einer Reader-DB-Instance in einer sekundären Region und das anschließende Löschen dieser Instance zu einem Aurora-PostgreSQL-Bereinigungsproblem auf der Writer-DB-Instance der primären Region führen. Wenn dieses Problem auftritt, starten Sie die Writer-DB-Instance der primären Region neu, nachdem Sie die Reader-DB-Instance der sekundären Region gelöscht haben.

So fügen Sie Ihrer globalen Aurora-Datenbank einen sekundären Aurora-Headless-DB-Cluster hinzu

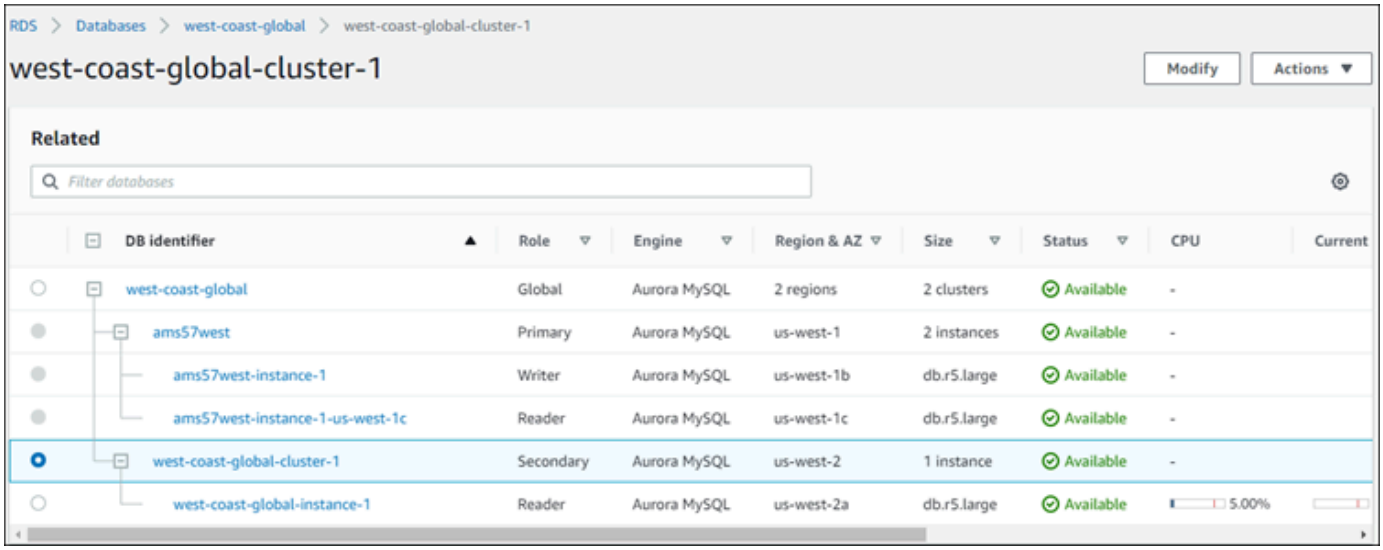
1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich der AWS Management Console die Option Datenbanken aus.
3. Wählen Sie die Aurora globale Datenbank aus, die einen sekundären Aurora-DB-Cluster benötigt. Stellen Sie sicher, dass der primäre Aurora-DB-Cluster is `Available`.
4. Wählen Sie unter Aktionen die Option Region hinzufügen aus.
5. Wählen Sie auf der Seite Eine Region hinzufügen die sekundäre AWS-Region aus.

Sie können keine AWS-Region auswählen, die bereits über einen sekundären Aurora-DB-Cluster für dieselbe globale Aurora-Datenbank verfügt. Außerdem kann dies nicht dieselbe Region sein wie die des primären Aurora-DB-Clusters.

6. Füllen Sie die restlichen Felder für den sekundären Aurora-Cluster in der neuen AWS-Region aus. Dies sind die gleichen Konfigurationsoptionen wie bei jeder Aurora-DB-Cluster-Instance.

   Bei einer Aurora MySQL–basierten globalen Aurora-Datenbank ignorieren Sie die Option Read Replica-Schreibweiterleitung aktivieren. Diese Option hat keine Funktion, nachdem Sie die Reader-Instance gelöscht haben.

7. Wählen Sie Region hinzufügen aus. Nachdem Sie die Region zu Ihrer globalen Aurora-Datenbank hinzugefügt haben, können Sie sie in der Liste der Datenbanken in AWS Management Console sehen, wie im Screenshot gezeigt.

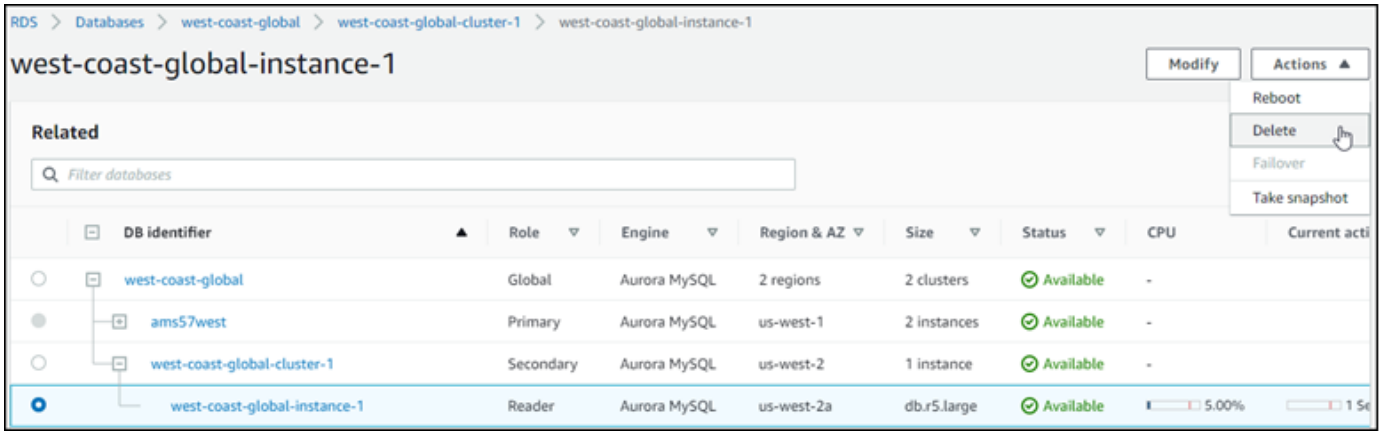


8. Überprüfen Sie den Status des sekundären Aurora-DB-Clusters und seiner Reader-Instance, bevor Sie fortfahren, indem Sie die AWS Management Console oder AWS CLI verwenden. Zum Beispiel:

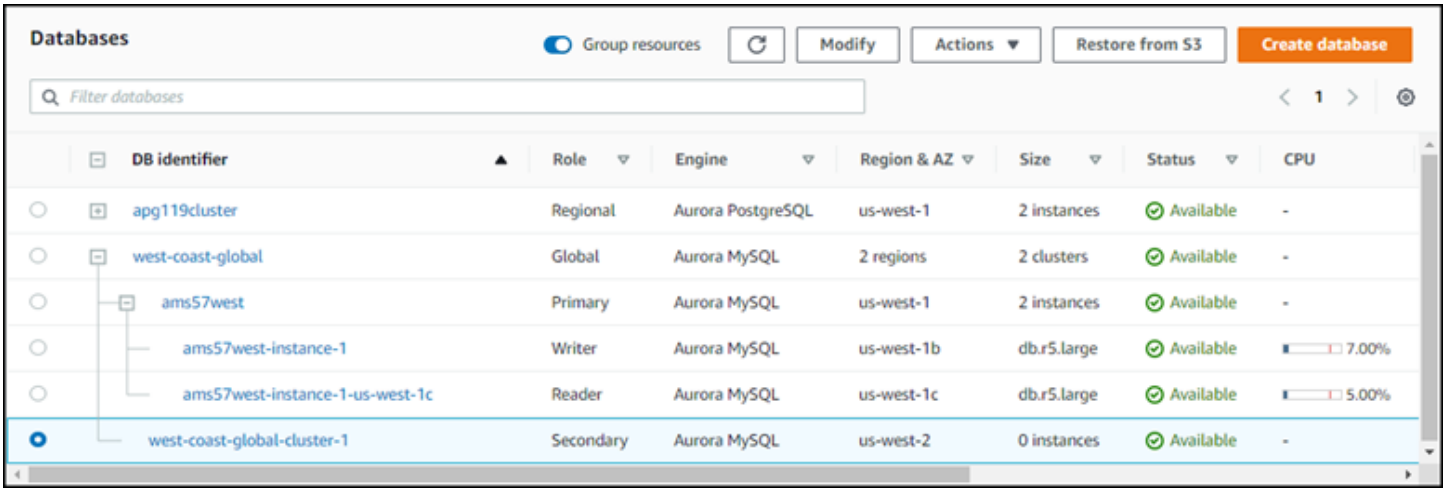
```
$ aws rds describe-db-clusters --db-cluster-identifier secondary-cluster-id --query
 '*[].[Status]' --output text
```

   Es kann mehrere Minuten dauern, bis der Status eines neu hinzugefügten sekundären Aurora-DB-Clusters von `creating` auf `available` wechselt. Wenn der Aurora-DB-Cluster verfügbar ist, können Sie die Reader-Instance löschen.

9. Wählen Sie die Reader-Instance im sekundären Aurora-DB-Cluster aus und klicken Sie dann auf Löschen.



Nach dem Löschen der Reader-Instance bleibt der sekundäre Cluster Teil der globalen Aurora-Datenbank. Ihm ist keine Instance zugeordnet, wie im Folgenden gezeigt.



Sie können diesen sekundären Aurora-Headless-DB-Cluster verwenden, um Ihre globale Amazon-Aurora-Datenbank nach einem ungeplanten Ausfall der primären AWS-Region manuell wiederherzustellen, wenn ein solcher Ausfall auftritt.

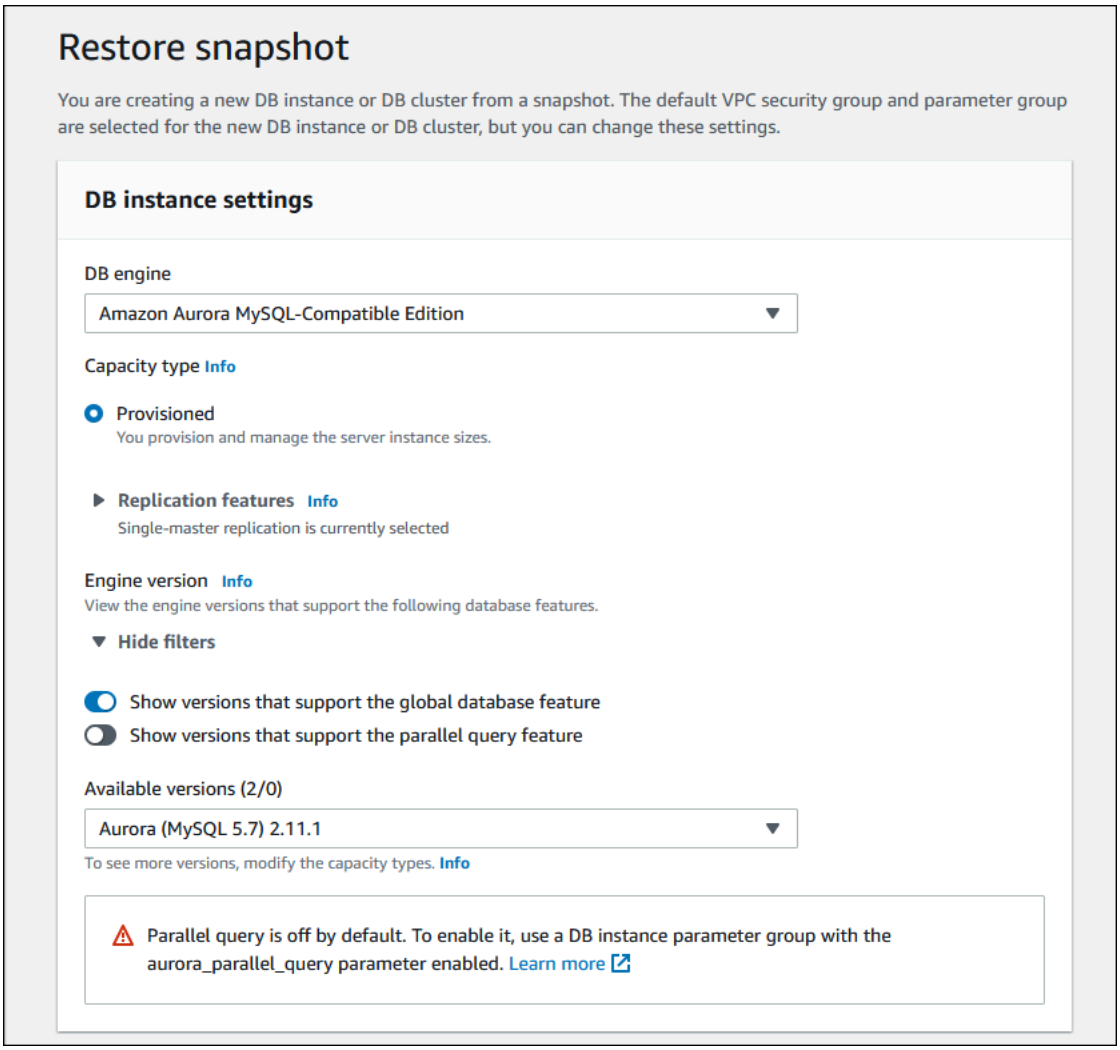
Verwenden eines Snapshot für Ihre globale Amazon-Aurora-Datenbank

Sie können einen Snapshot eines Aurora-DB-Clusters oder von einer Amazon RDS-DB-Instance wiederherstellen, um ihn als Ausgangspunkt für Ihre globale Aurora-Datenbank zu verwenden. Sie stellen den Snapshot wieder her und erstellen gleichzeitig einen neuen von Aurora bereitgestellten DB-Cluster. Sie fügen dann dem wiederhergestellten DB-Cluster eine weitere AWS-Region hinzu und verwandeln sie so in eine globale Aurora-Datenbank. Jeder Aurora-DB-Cluster, den Sie auf diese Weise mit einem Snapshot erstellen, wird zum primären Cluster Ihrer globalen Aurora-Datenbank.

Der Snapshot, den Sie verwenden, kann von einem `provisioned`- oder einem `serverless` Aurora-DB-Cluster stammen.

Wählen Sie während des Wiederherstellungsvorgangs den gleichen DB-Engine-Typ wie den des Snapshots aus. Angenommen, Sie möchten einen Snapshot wiederherstellen, der aus einem Aurora Serverless-DB-Cluster mit Aurora PostgreSQL erstellt wurde. In diesem Fall erstellen Sie einen Aurora PostgreSQL-DB-Cluster mit derselben Aurora-DB-Engine und derselben Version.

Der wiederhergestellte DB-Cluster übernimmt die Rolle des primären Clusters für die globale Aurora-Datenbank, wenn Sie ihm eine AWS-Region hinzufügen. Alle in diesem primären Cluster enthaltenen Daten werden auf alle sekundären Cluster repliziert, die Sie Ihrer globalen Aurora-Datenbank hinzufügen.



Verwalten einer Amazon Aurora Global Database

Die meisten Verwaltungsvorgänge werden auf den einzelnen Clustern ausgeführt, aus denen eine globale Aurora-Datenbank besteht. Wenn Sie Group related resources (Gruppenbezogene Ressourcen) auf der Seite Databases (Datenbanken) in der Konsole auswählen, werden der primäre Cluster und der sekundäre Cluster unter der zugehörigen globalen Datenbank gruppiert. Um die AWS-Regionen zu finden, in denen die DB-Cluster einer globalen Datenbank ausgeführt werden sowie die zugehörige Aurora-DB-Engine, -Version und ihre Kennung, verwenden Sie die Registerkarte Konfiguration.

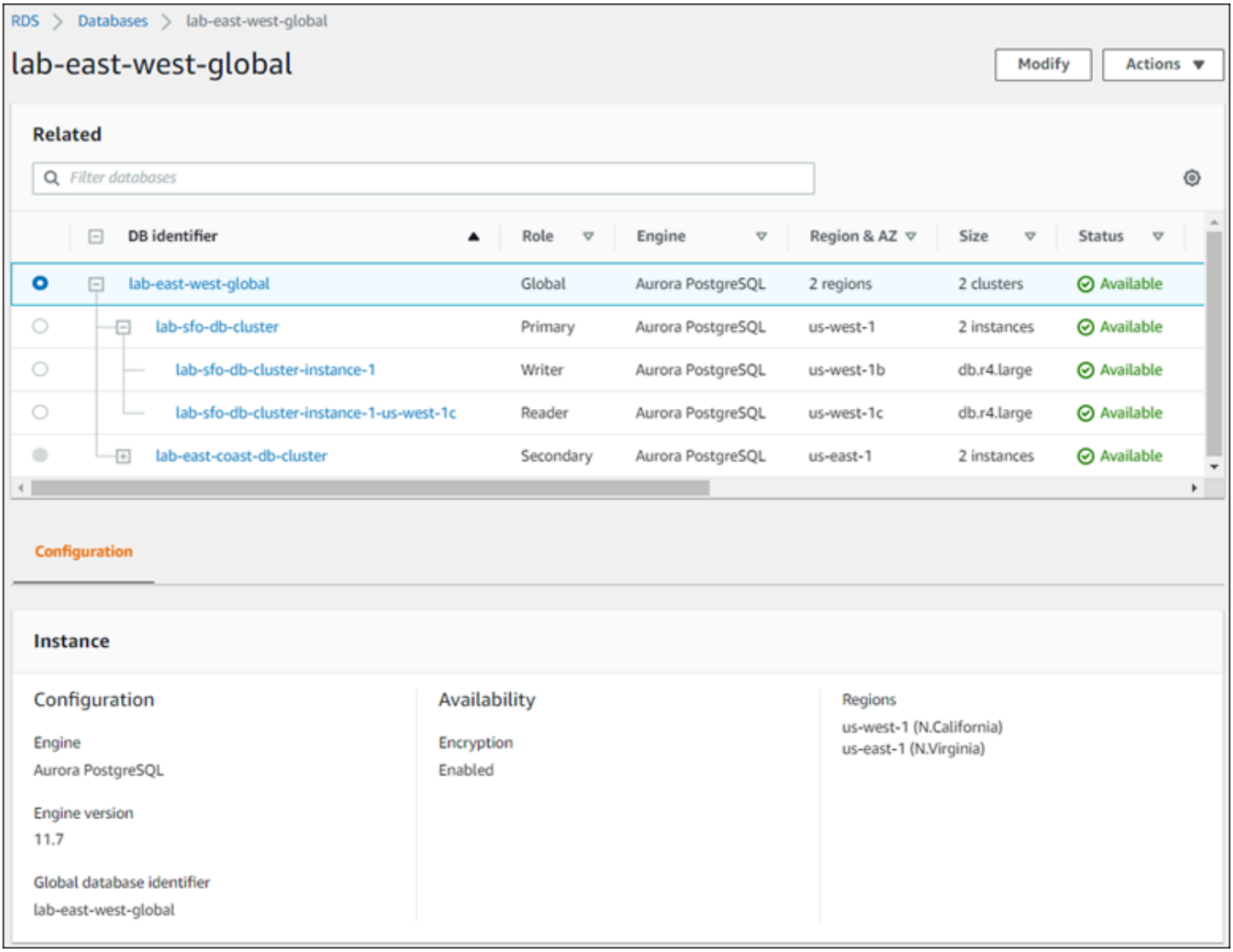
Die regionsübergreifenden Datenbank-Failover-Prozesse stehen nur globalen Aurora-Datenbankobjekten zur Verfügung, nicht einem einzelnen Aurora-DB-Cluster. Weitere Informationen hierzu finden Sie unter Verwenden von Umstellung oder Failover in einer Amazon Aurora Global Database.

Informationen zum Wiederherstellen einer globalen Aurora-Datenbank nach einem ungeplanten Ausfall in ihrer primären Region finden Sie unter Wiederherstellen einer globalen Amazon Aurora-Datenbank nach einem ungeplanten Ausfall.

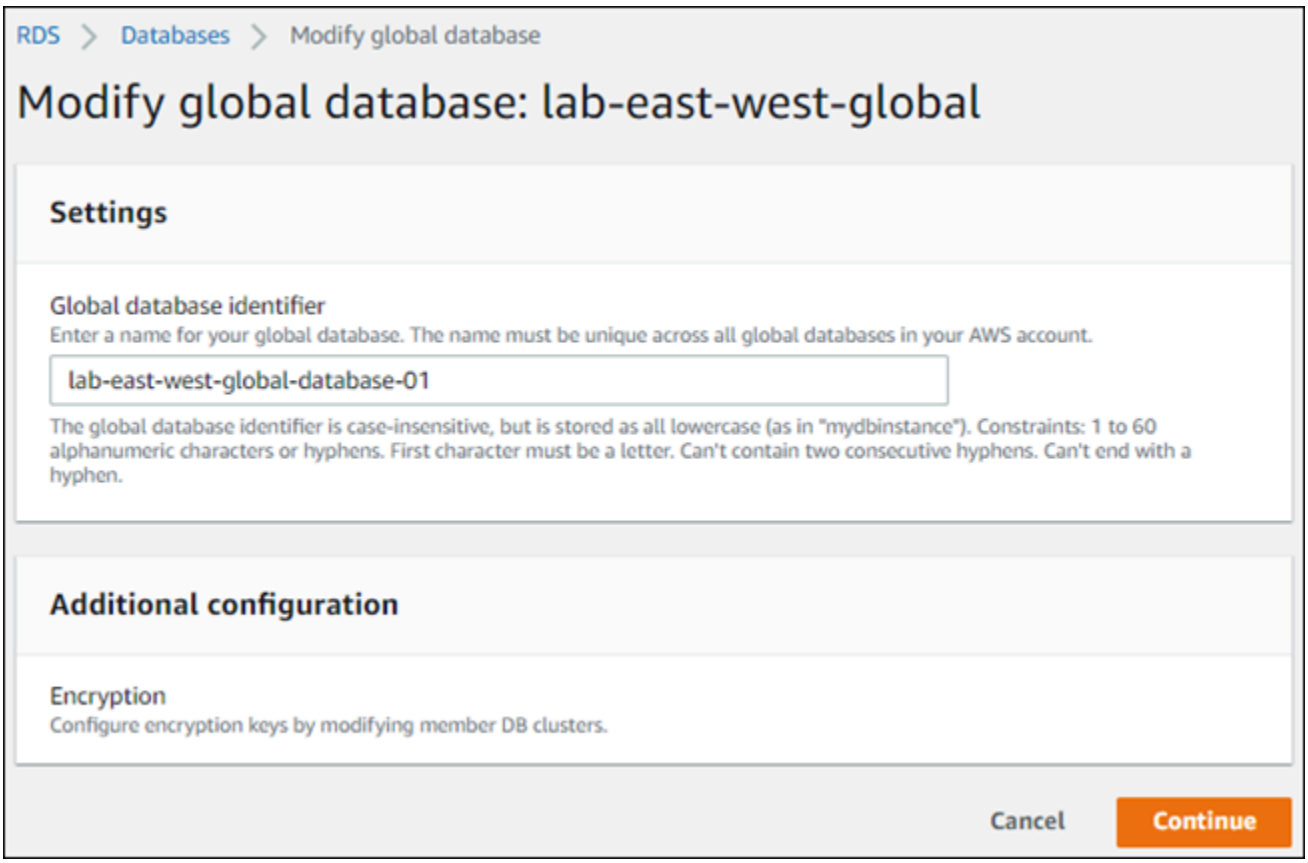
Themen

Verändern einer Amazon Aurora Global Database

In der AWS Management Console werden auf der Seite Datenbanken alle globalen Aurora-Datenbanken mit den jeweiligen primären und sekundären Clustern aufgeführt. Die globale Aurora-Datenbank hat ihre eigenen Konfigurationseinstellungen. Insbesondere verfügt sie über AWS-Regionen, die mit ihren primären und sekundären Clustern verknüpft sind, wie im folgenden Screenshot gezeigt.



Wenn Sie Änderungen an der Aurora globalen Datenbank vornehmen, haben Sie die Möglichkeit, Änderungen abzubrechen, wie im folgenden Screenshot gezeigt.



Wenn Sie Weiter wählen, bestätigen Sie die Änderungen.

Ändern von Parametern für eine Aurora globale Datenbank

Sie können die Parametergruppen jedes Aurora-DB-Cluster für jeden Aurora-Cluster in der globalen Aurora-Datenbank einzeln konfigurieren. Die meisten Parameter funktionieren wie bei anderen Aurora-Clusterarten. Wir empfehlen, dass Sie die Einstellungen zwischen allen Clustern in einer globalen Datenbank konsistent halten. Dies hilft, unerwartete Verhaltensänderungen zu vermeiden, wenn Sie einen sekundären Cluster zum primären Cluster hochstufen.

Sie sollten z. B. die gleichen Einstellungen für Zeitzonen und Zeichensätze verwenden, um inkonsistentes Verhalten zu vermeiden, wenn ein anderer Cluster die Rolle des primären Clusters übernimmt.

Die Konfigurationseinstellungen `aurora_enable_repl_bin_log_filtering` und `aurora_enable_replica_log_compression` haben keine Auswirkungen.

Entfernen eines Clusters aus einer Amazon Aurora Global Database

Sie können Aurora-DB-Cluster aus verschiedenen Gründen aus Ihrer Aurora globalen Datenbank entfernen. Beispielsweise möchten Sie möglicherweise einen Aurora-DB-Cluster aus einer Aurora globalen Datenbank entfernen, wenn der primäre Cluster herabgesetzt oder isoliert wird. Er wird dann zu einem eigenständigen bereitgestellten Aurora-DB-Cluster, der zum Erstellen einer neuen globalen Aurora-Datenbank verwendet werden könnte. Weitere Informationen hierzu finden Sie unter Wiederherstellen einer globalen Amazon Aurora-Datenbank nach einem ungeplanten Ausfall.

Sie können bei Bedarf auch Aurora-DB-Cluster entfernen, wenn Sie eine globale Aurora-Datenbank löschen möchten, die Sie nicht mehr benötigen. Sie können die globale Aurora-Datenbank erst löschen, nachdem Sie alle zugehörigen Aurora-DB-Cluster entfernt haben, wobei der primäre Cluster zuletzt entfernt wird. Weitere Informationen finden Sie unter Löschen einer Amazon Aurora Global Database.

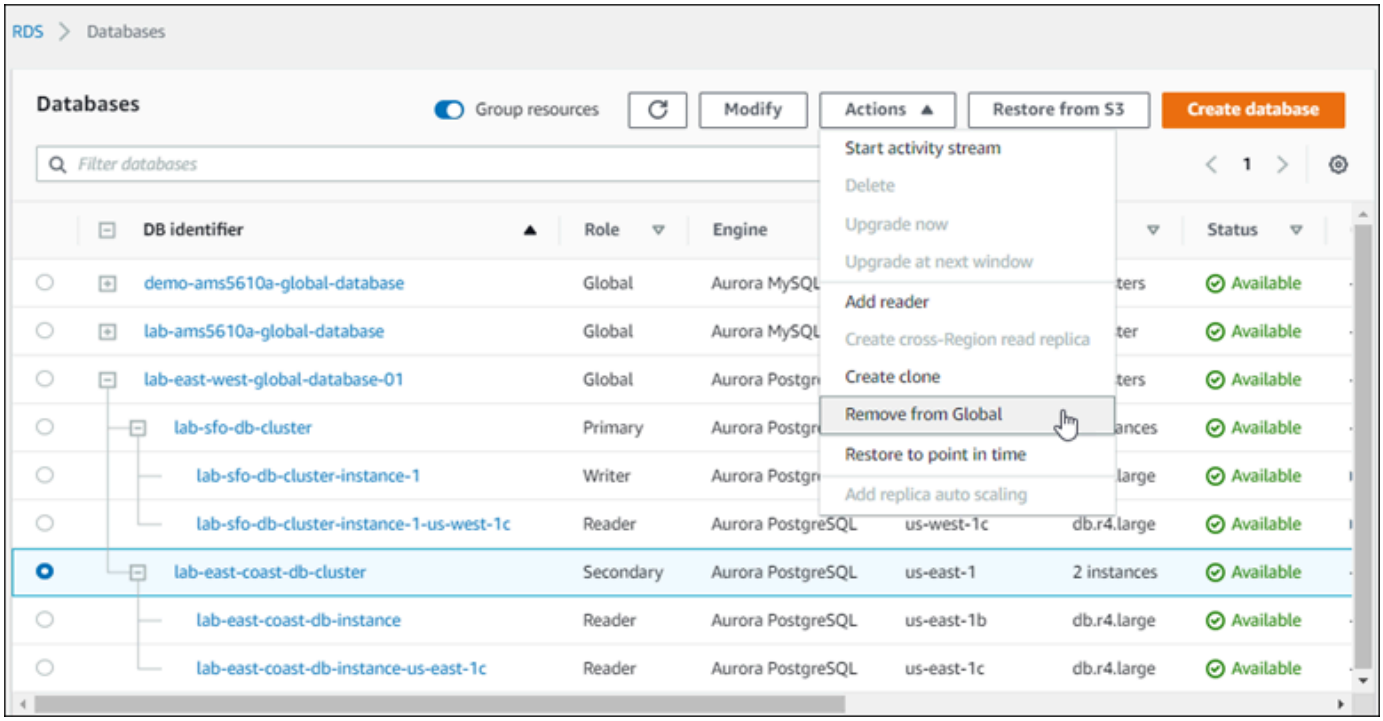
Wenn ein Aurora-DB-Cluster von der globalen Aurora-Datenbank getrennt wird, wird er nicht mehr mit dem primären Cluster synchronisiert. Er wird zu einem eigenständigen bereitgestellten Aurora-DB-Cluster mit vollen Lese-/Schreibfähigkeiten.

Sie können Aurora-DB-Cluster aus Ihrer globalen Aurora-Datenbank mithilfe von AWS Management Console, AWS CLI oder der RDS-API entfernen.

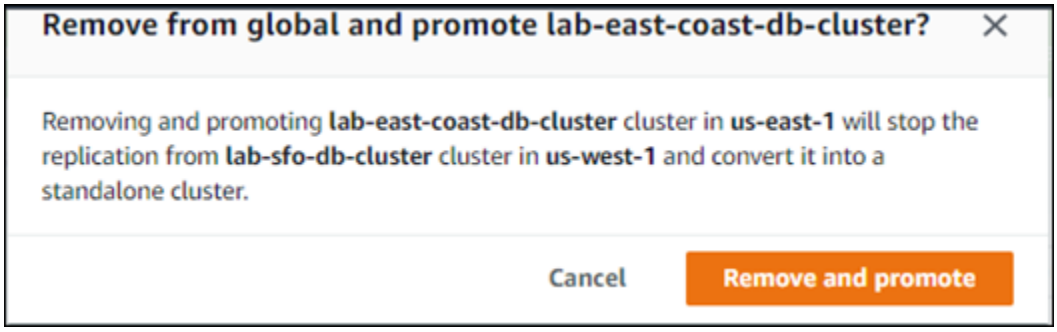
Konsole

So entfernen Sie einen Aurora-Cluster aus einer globalen Aurora-Datenbank:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie den Cluster auf der Seite Databases (Datenbanken) aus.
3. Wählen Sie unter Actions (Aktionen) die Option Remove from Global (Aus 'Global' entfernen) aus.

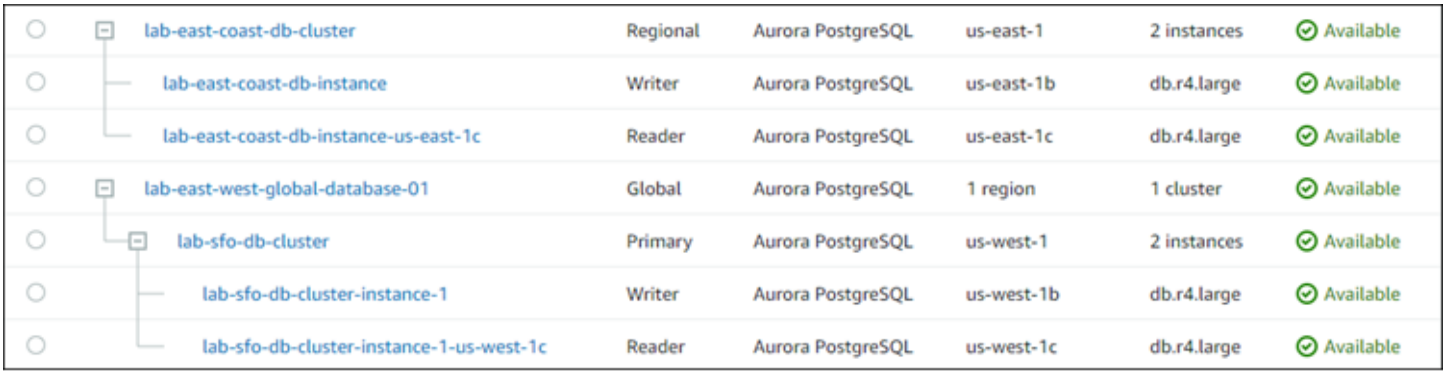


Sie sehen eine Aufforderung, um zu bestätigen, dass Sie den sekundären Cluster von der Aurora globalen Datenbank trennen möchten.



4. Wählen Sie Entfernen und hochstufen , um den Cluster aus der globalen Datenbank zu entfernen.

Der Aurora-DB-Cluster dient nicht mehr als sekundärer Cluster in der Aurora globalen Datenbank und ist nicht mehr mit dem primären DB-Cluster synchronisiert. Er ist ein eigenständiger Aurora-DB-Cluster mit voller Lese-/Schreibfähigkeit.



Nachdem Sie alle sekundären Cluster entfernt oder gelöscht haben, können Sie den primären Cluster auf die gleiche Weise entfernen. Sie können den primären Aurora-DB-Cluster erst von einer Aurora globalen Datenbank trennen (entfernen), nachdem Sie alle sekundären Cluster entfernt haben.

Die globale Aurora-Datenbank kann in der Datenbankliste mit null Regionen und AZs verbleiben. Sie können sie löschen, wenn Sie diese Aurora globale Datenbank nicht mehr verwenden möchten. Weitere Informationen finden Sie unter Löschen einer Amazon Aurora Global Database.

AWS CLI

Um einen Aurora-Cluster aus einer globalen Aurora-Datenbank zu entfernen, führen Sie den remove-from-global-cluster CLI-Befehl mit den folgenden Parametern aus:

- `--global-cluster-identifier` – Der Name (identifier) Ihrer Aurora globalen Datenbank.
- `--db-cluster-identifier` – Der Name jedes Aurora-DB-Clusters, der aus der Aurora globalen Datenbank entfernt werden soll. Entfernen Sie alle sekundären Aurora-DB-Cluster, bevor Sie den primären Cluster entfernen.

Bei den folgenden Beispielen wird zuerst ein sekundärer Cluster und dann der primäre Cluster aus einer globalen Aurora-Datenbank entfernt.

Für Linux, macOSoder Unix:

```
aws rds --region secondary_region \
  remove-from-global-cluster \
    --db-cluster-identifier secondary_cluster_ARN \
    --global-cluster-identifier global_database_id

aws rds --region primary_region \
  remove-from-global-cluster \
```

```
    --db-cluster-identifier primary_cluster_ARN \
    --global-cluster-identifier global_database_id
```

Wiederholen Sie den `remove-from-global-cluster --db-cluster-identifier` *`secondary_cluster_ARN`* -Befehl für jede sekundäre AWS-Region in Ihrer globalen Aurora-Datenbank.

Windows:

```
aws rds --region secondary_region ^
  remove-from-global-cluster ^
    --db-cluster-identifier secondary_cluster_ARN ^
    --global-cluster-identifier global_database_id

aws rds --region primary_region ^
  remove-from-global-cluster ^
    --db-cluster-identifier primary_cluster_ARN ^
    --global-cluster-identifier global_database_id
```

Wiederholen Sie den `remove-from-global-cluster --db-cluster-identifier` *`secondary_cluster_ARN`* -Befehl für jede sekundäre AWS-Region in Ihrer globalen Aurora-Datenbank.

RDS-API

Um einen Aurora-Cluster aus einer globalen Aurora-Datenbank mit der RDS-API zu entfernen, führen Sie die RemoveFromGlobalCluster Aktion aus.

Löschen einer Amazon Aurora Global Database

Da eine Aurora globale Datenbank üblicherweise geschäftskritische Daten enthält, ist es nicht möglich, die globale Datenbank und ihre zugeordneten Cluster in einem einzigen Schritt zu löschen. Um eine globale Aurora-Datenbank zu löschen, führen Sie die folgenden Schritte aus:

- Entfernen Sie alle sekundären DB-Cluster aus der Aurora globalen Datenbank. Jeder Cluster wird zu einem eigenständigen Aurora-DB-Cluster. Um zu erfahren wie, siehe Entfernen eines Clusters aus einer Amazon Aurora Global Database.
- Löschen Sie von jedem eigenständigen Aurora-DB-Cluster alle Aurora-Replicas.
- Entfernen Sie den primären DB-Cluster aus der globalen Aurora-Datenbank. Dieser Cluster wird zu einem eigenständigen Aurora-DB-Cluster.

- Löschen Sie vom primären Aurora-DB-Cluster zuerst alle Aurora-Replicas und löschen Sie dann die Writer-DB-Instance.

Durch das Löschen der Writer-Instance aus dem neu eigenständigen Aurora-DB-Cluster werden normalerweise auch der Aurora-DB-Cluster und die Aurora globale Datenbank entfernt.

Weitere allgemeine Informationen finden Sie unter Löschen einer DB-Instance aus einem Aurora-DB-Cluster.

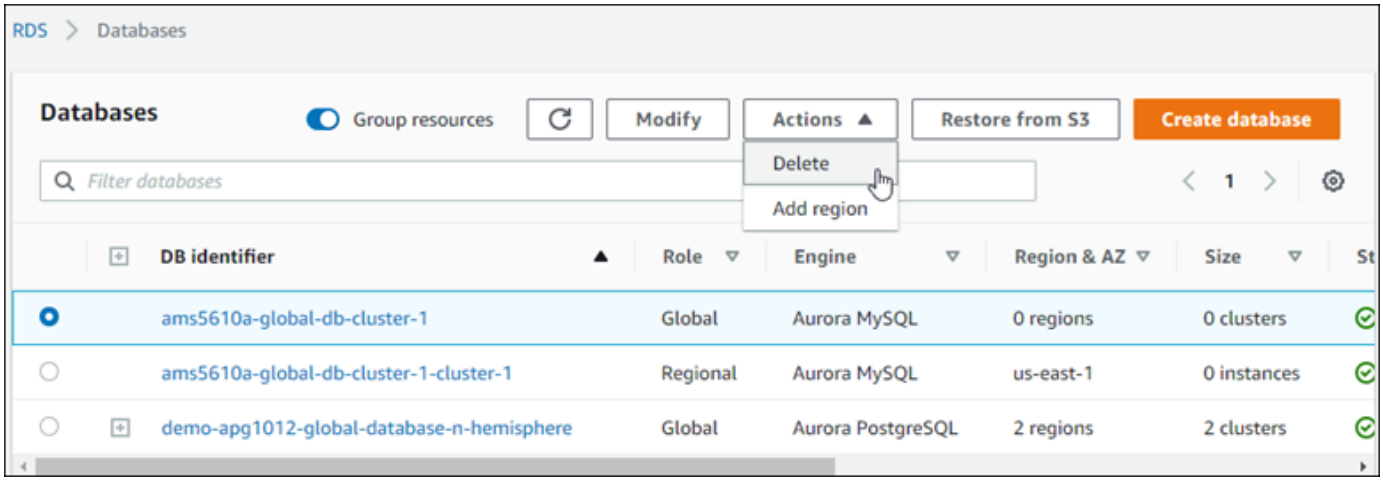
Um eine globale Aurora-Datenbank zu löschen, können Sie AWS Management Console, AWS CLI oder die RDS-API verwenden.

Konsole

So löschen Sie eine globale Aurora-Datenbank

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Datenbanken und suchen Sie die Aurora globale Datenbank, die Sie löschen möchten, in der Liste.
3. Bestätigen Sie, dass alle Cluster aus der globalen Aurora-Datenbank entfernt sind. Die globale Aurora-Datenbank sollte 0 Regionen und AZs sowie eine Größe von 0 Clustern enthalten.

   Wenn die Aurora globale Datenbank Aurora-DB-Cluster enthält, können Sie sie nicht löschen. Trennen Sie bei Bedarf die primären und sekundären Aurora-DB-Cluster von der Aurora globalen Datenbank. Weitere Informationen finden Sie unter Entfernen eines Clusters aus einer Amazon Aurora Global Database.
4. Wählen Sie Ihre globale Aurora-Datenbank in der Liste aus, und wählen Sie dann Löschen im Menü Aktionen aus.



AWS CLI

Um eine globale Aurora-Datenbank zu löschen, führen Sie den delete-global-cluster CLI-Befehl mit dem Namen der AWS-Region und der globalen Aurora-Datenbank-ID aus, wie im folgenden Beispiel gezeigt.

Für Linux, macOSoder Unix:

```
aws rds --region primary_region delete-global-cluster \
   --global-cluster-identifier global_database_id
```

Windows:

```
aws rds --region primary_region delete-global-cluster ^
   --global-cluster-identifier global_database_id
```

RDS-API

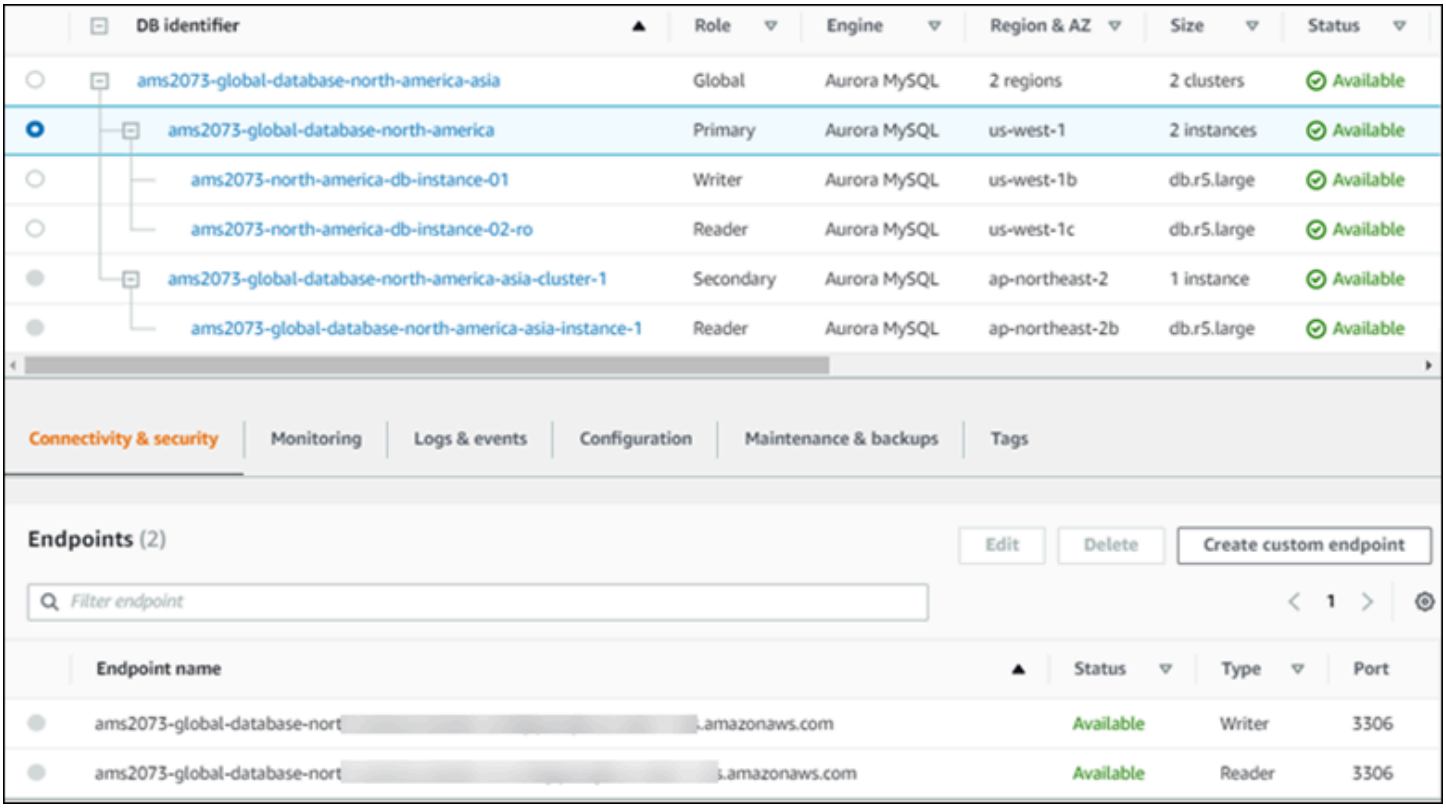
Um einen Cluster zu löschen, der Teil einer globalen Aurora-Datenbank ist, führen Sie die DeleteGlobalCluster -API-Operation aus.

Herstellen einer Verbindung mit einer Amazon Aurora Global Database

Wie Sie eine Verbindung mit einer globalen Aurora-Datenbank herstellen, hängt davon ab, ob Sie in die Datenbank schreiben oder aus der Datenbank lesen müssen:

- Bei schreibgeschütztem Anfragen oder Abfragen stellen Sie eine Verbindung zum Reader-Endpunkt des Aurora-Clusters in Ihrer AWS-Region her.
- Stellen Sie zum Ausführen von Data Manipulation Language (DML)- und Data Definition Language (DDL)-Anweisungen eine Verbindung zum Cluster-Endpunkt des primären Clusters her. Dieser Endpunkt befindet sich möglicherweise in einer anderen AWS-Region als Ihre Anwendung.

Wenn Sie eine globale Aurora-Datenbank in der Konsole anzeigen, können Sie alle für allgemeine Zwecke bestimmten Endpunkte sehen, die mit allen ihren Clustern verknüpft sind. Im folgenden Screenshot wird ein Beispiel gezeigt. Für Schreibvorgänge verwenden Sie einen bestimmten Cluster-Endpunkt, der dem primären Cluster zugeordnet ist. Der primäre Cluster und jeder sekundäre Cluster verfügt über einen Reader-Endpunkt, den Sie für schreibgeschützte Abfragen verwenden. Um die Latenz zu minimieren, wählen Sie den Reader-Endpunkt aus, der sich in Ihrem AWS-Region oder dem Ihnen AWS-Region am nächsten befindet. Im Folgenden wird ein Aurora MySQL-Beispiel gezeigt.



Verwenden der Schreibweiterleitung in einer Amazon Aurora globalen Datenbank

Sie können die Anzahl der Endpunkte reduzieren, die Sie für Anwendungen verwalten müssen, die in Ihrer Aurora globalen Datenbank ausgeführt werden, indem Sie Schreibweiterleitung verwenden. Wenn die Schreibweiterleitung aktiviert ist, leiten sekundäre Cluster in einer Aurora Global Database SQL-Anweisungen, die Schreibvorgänge ausführen, an den primären Cluster weiter. Der primäre Cluster aktualisiert die Quelle und überträgt dann die resultierenden Änderungen an alle sekundären AWS-Regionen zurück.

Die Konfiguration der Schreibweiterleitung erspart Ihnen die Implementierung Ihres eigenen Mechanismus zum Senden von Schreibvorgängen von einer sekundären AWS-Region an die primäre Region. Aurora übernimmt die regionsübergreifende Netzwerk-Einrichtung. Aurora überträgt auch den gesamten erforderlichen Sitzungs- und Transaktionskontext für jede Anweisung. Die Daten werden stets zuerst im primären Cluster geändert und anschließend zu den sekundären Clustern in der Aurora globalen Datenbank repliziert. Daher ist der primäre Cluster die autoritative Quelle und enthält stets die jeweils aktuellen Versionen all Ihrer Daten.

Themen

Verwenden der Schreibweiterleitung in einer globalen Aurora-MySQL-Datenbank

Themen

- Amazon-CloudWatch-Metriken für die Schreibweiterleitung in Aurora MySQL

Verfügbarkeit von Regionen und Versionen der Schreibweiterleitung in Aurora MySQL

Die Schreibweiterleitung wird für Aurora MySQL 2.08.1 und höhere Versionen in jeder Region unterstützt, in der Aurora-MySQL-basierte globale Datenbanken verfügbar sind.

Informationen zur Verfügbarkeit von Versionen und Regionen von globalen Aurora-MySQL-Datenbanken finden Sie unter Globale Aurora-Datenbanken mit Aurora MySQL.

Aktivieren der Schreibweiterleitung in Aurora MySQL

Standardmäßig ist die Schreibweiterleitung nicht aktiviert, wenn Sie einen sekundären Cluster zu einer Aurora Global Database hinzufügen.

Um die Schreibweiterleitung über die AWS Management Console zu aktivieren, wählen Sie das Kontrollkästchen Globale Schreibweiterleitung aktivieren unter Read-Replica-Schreibweiterleitung aus, wenn Sie eine Region für eine globale Datenbank hinzufügen. Ändern Sie den Cluster für einen vorhandenen sekundären Cluster in Globale Schreibweiterleitung aktivieren. Wenn Sie die Schreibweiterleitung ausschalten möchten, deaktivieren Sie beim Hinzufügen der Region oder beim Ändern des sekundären Clusters das Kontrollkästchen Read-Replica-Schreibweiterleitung aktivieren.

Um die Schreibweiterleitung über die AWS CLI zu aktivieren, verwenden Sie die Option `--enable-global-write-forwarding`. Diese Option funktioniert, wenn Sie über den Befehl `create-db-cluster` einen neuen sekundären Cluster erstellen. Sie funktioniert auch, wenn Sie einen vorhandenen sekundären Cluster über den Befehl `modify-db-cluster` ändern. Sie erfordert, dass die globale Datenbank eine Aurora-Version verwendet, die eine Schreibweiterleitung unterstützt. Sie können die Schreibweiterleitung deaktivieren, indem Sie die Option `--no-enable-global-write-forwarding` mit denselben CLI-Befehlen verwenden.

Um die Schreibweiterleitung über die Amazon RDS-API zu aktivieren, legen Sie den Parameter `EnableGlobalWriteForwarding` auf `true` fest. Dieser Parameter funktioniert, wenn Sie über die Operation `CreateDBCluster` einen neuen sekundären Cluster erstellen. Sie funktioniert auch, wenn Sie einen vorhandenen sekundären Cluster über die Operation `ModifyDBCluster` ändern. Sie erfordert, dass die globale Datenbank eine Aurora-Version verwendet, die eine Schreibweiterleitung unterstützt. Sie können die Schreibweiterleitung deaktivieren, indem Sie den Parameter `EnableGlobalWriteForwarding` auf `false` festlegen.

> **Note**
>
> Damit eine Datenbanksitzung die Schreibweiterleitung verwenden kann, geben Sie eine Einstellung für den Konfigurationsparameter `aurora_replica_read_consistency` an. Sie führen dies in jeder Sitzung aus, in der die Schreibweiterleitungsfunktion verwendet wird. Informationen zu diesem Parameter finden Sie unter Isolation und Konsistenz für die Schreibweiterleitung in Aurora MySQL.
>
> Die RDS-Proxy-Funktion unterstützt den `SESSION`-Wert für die Variable `aurora_replica_read_consistency` nicht. Durch das Festlegen dieses Werts kann unerwartetes Verhalten auftreten.

Die folgenden CLI-Beispiele zeigen, wie Sie eine Aurora Global Database mit aktivierter oder deaktivierter Schreibweiterleitung einrichten. Die markierten Elemente stellen die Befehle und Optionen dar, die bei der Einrichtung der Infrastruktur für eine Aurora Global Database Datenbank angegeben werden müssen und konsistent sein müssen.

Im folgenden Beispiel werden eine Aurora Global Database, ein primärer Cluster und ein sekundärer Cluster mit aktivierter Schreibweiterleitung erstellt. Geben Sie Ihre eigenen Daten für Benutzername, Passwort und primäre und sekundäre AWS-Regionen ein.

```
# Create overall global database.
aws rds create-global-cluster --global-cluster-identifier write-forwarding-test \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-east-1

# Create primary cluster, in the same AWS Region as the global database.
aws rds create-db-cluster --global-cluster-identifier write-forwarding-test \
  --db-cluster-identifier write-forwarding-test-cluster-1 \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --master-username user_name --master-user-password password \
  --region us-east-1

aws rds create-db-instance --db-cluster-identifier write-forwarding-test-cluster-1 \
  --db-instance-identifier write-forwarding-test-cluster-1-instance-1 \
  --db-instance-class db.r5.large \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-east-1

aws rds create-db-instance --db-cluster-identifier write-forwarding-test-cluster-1 \
```

```
  --db-instance-identifier write-forwarding-test-cluster-1-instance-2 \
  --db-instance-class db.r5.large \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-east-1

# Create secondary cluster, in a different AWS Region than the global database,
# with write forwarding enabled.
aws rds create-db-cluster --global-cluster-identifier write-forwarding-test \
  --db-cluster-identifier write-forwarding-test-cluster-2 \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-east-2 \
  --enable-global-write-forwarding

aws rds create-db-instance --db-cluster-identifier write-forwarding-test-cluster-2 \
  --db-instance-identifier write-forwarding-test-cluster-2-instance-1 \
  --db-instance-class db.r5.large \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-east-2

aws rds create-db-instance --db-cluster-identifier write-forwarding-test-cluster-2 \
  --db-instance-identifier write-forwarding-test-cluster-2-instance-2 \
  --db-instance-class db.r5.large \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-east-2
```

Das folgende Beispiel setzt das vorherige Beispiel fort. In ihm werden ein sekundärer Cluster ohne aktivierte Schreibweiterleitung erstellt und anschließend die Schreibweiterleitung aktiviert. Nach Abschluss dieses Beispiels ist die Schreibweiterleitung für alle sekundären Cluster in der globalen Datenbank aktiviert.

```
# Create secondary cluster, in a different AWS Region than the global database,
# without write forwarding enabled.
aws rds create-db-cluster --global-cluster-identifier write-forwarding-test \
  --db-cluster-identifier write-forwarding-test-cluster-2 \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-west-1

aws rds create-db-instance --db-cluster-identifier write-forwarding-test-cluster-2 \
  --db-instance-identifier write-forwarding-test-cluster-2-instance-1 \
  --db-instance-class db.r5.large \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-west-1
```

```
aws rds create-db-instance --db-cluster-identifier write-forwarding-test-cluster-2 \
  --db-instance-identifier write-forwarding-test-cluster-2-instance-2 \
  --db-instance-class db.r5.large \
  --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.1 \
  --region us-west-1

aws rds modify-db-cluster --db-cluster-identifier write-forwarding-test-cluster-2 \
  --region us-east-2 \
  --enable-global-write-forwarding
```

Überprüfen, ob die Schreibweiterleitung für einen sekundären Cluster in Aurora MySQL aktiviert ist

Um festzustellen, ob Sie die Schreibweiterleitung aus einem sekundären Cluster verwenden können, können Sie prüfen, ob der Cluster das Attribut besitz `"GlobalWriteForwardingStatus": "enabled"`.

In der AWS Management Console sehen Sie auf der Registerkarte Konfiguration der Detailseite des Clusters den StatusAktiviert für Globale Lesereplikat-Schreibweiterleitung.

Um den Status der globalen Einstellung für die Schreibweiterleitung für alle Cluster anzuzeigen, führen Sie den folgenden AWS CLI-Befehl aus.

Ein sekundärer Cluster zeigt die Werte `"enabled"` oder `"disabled"` an, um anzugeben, ob die Schreibweiterleitung aktiviert oder deaktiviert ist. Der Wert `null` gibt an, dass die Schreibweiterleitung für diesen Cluster nicht verfügbar ist. Entweder ist der Cluster nicht Teil einer globalen Datenbank oder ist der primäre Cluster und nicht kein sekundärer Cluster. Der Wert kann auch `"enabling"` oder `"disabling"` sein, wenn die Schreibweiterleitung gerade aktiviert oder deaktiviert wird.

Example

```
aws rds describe-db-clusters \
--query '*[].
{DBClusterIdentifier:DBClusterIdentifier,GlobalWriteForwardingStatus:GlobalWriteForwardingStatu

[
    {
        "GlobalWriteForwardingStatus": "enabled",
        "DBClusterIdentifier": "aurora-write-forwarding-test-replica-1"
    },
    {
```

```
        "GlobalWriteForwardingStatus": "disabled",
        "DBClusterIdentifier": "aurora-write-forwarding-test-replica-2"
    },
    {
        "GlobalWriteForwardingStatus": null,
        "DBClusterIdentifier": "non-global-cluster"
    }
]
```

Führen Sie den folgenden Befehl aus, um alle sekundären Cluster zu suchen, für die eine globale Schreibweiterleitung aktiviert ist. Dieser Befehl gibt auch den Reader-Endpunkt des Clusters aus. Sie verwenden den Reader-Endpunkt des sekundären Clusters, wenn Sie die Schreibweiterleitung vom sekundären zum primären Cluster in Ihrer globalen Aurora-Datenbank verwenden.

Example

```
aws rds describe-db-clusters --query 'DBClusters[].
{DBClusterIdentifier:DBClusterIdentifier,GlobalWriteForwardingStatus:GlobalWriteForwardingStatu
 | [?GlobalWriteForwardingStatus == `enabled`]'
[
    {
        "GlobalWriteForwardingStatus": "enabled",
        "ReaderEndpoint": "aurora-write-forwarding-test-replica-1.cluster-ro-
cnpexample.us-west-2.rds.amazonaws.com",
        "DBClusterIdentifier": "aurora-write-forwarding-test-replica-1"
    }
]
```

Anwendungs- und SQL-Kompatibilität mit Schreibweiterleitung in Aurora MySQL

Sie können die folgenden Arten von SQL-Anweisungen mit Schreibweiterleitung verwenden:

- Data Manipulation Language (DM)-Anweisungen wie `INSERT`, wie`DELETE` und `UPDATE`. Es gibt einige Einschränkungen für die Eigenschaften dieser Anweisungen, die Sie bei der Schreibweiterleitung verwenden können, wie im Folgenden beschrieben.
- `SELECT ... LOCK IN SHARE MODE`- und `SELECT FOR UPDATE`-Anweisungen.
- `PREPARE`- und `EXECUTE`-Anweisungen.

Bestimmte Anweisungen sind nicht zulässig oder können veraltete Ergebnisse erzeugen, wenn Sie sie in einer globalen Datenbank mit Schreibweiterleitung verwenden. Daher ist die Einstellung

`EnableGlobalWriteForwarding` für sekundäre Cluster standardmäßig deaktiviert. Stellen Sie vor einer Aktivierung sicher, dass der Anwendungscode von keiner dieser Einschränkungen betroffen ist.

Die folgenden Einschränkungen gelten für die SQL-Anweisungen, die Sie für die Schreibweiterleitung verwenden. In einigen Fällen können Sie die Anweisungen auf sekundären Clustern verwenden, bei denen eine Schreibweiterleitung auf Clusterebene aktiviert ist. Dieser Ansatz funktioniert, wenn die Schreibweiterleitung nicht innerhalb der Sitzung durch den Konfigurationsparameter `aurora_replica_read_consistency` aktiviert wird. Der Versuch, eine Anweisung zu verwenden, wenn sie aufgrund der Schreibweiterleitung nicht zulässig ist, verursacht eine Fehlermeldung im folgendem Format.

```
ERROR 1235 (42000): This version of MySQL doesn't yet support 'operation with write
 forwarding'.
```

Data Definition Language (DDL)

Stellen Sie eine Verbindung zum primären Cluster her, um DDL-Anweisungen auszuführen. Sie können sie nicht von Reader-DB-Instances aus ausführen.

Aktualisieren einer permanenten Tabelle mit Daten aus einer temporären Tabelle

Sie können in sekundären Clustern mit aktivierter Schreibweiterleitung temporäre Tabellen verwenden. Sie können jedoch keine DML-Anweisung verwenden, um eine permanente Tabelle zu ändern, wenn sich die Anweisung auf eine temporäre Tabelle bezieht. Beispielsweise können Sie keine `INSERT ... SELECT`-Anweisung verwenden, die die Daten aus einer temporären Tabelle übernimmt. Die temporäre Tabelle ist auf dem sekundären Cluster vorhanden und nicht verfügbar, wenn die Anweisung auf dem primären Cluster ausgeführt wird.

XA-Transaktionen

Sie können die folgenden Anweisungen nicht in einem sekundären Cluster verwenden, wenn die Schreibweiterleitung innerhalb der Sitzung aktiviert wird. Sie können diese Anweisungen in sekundären Clustern verwenden, bei denen die Schreibweiterleitung nicht aktiviert ist, oder innerhalb von Sitzungen mit leerer Einstellung `aurora_replica_read_consistency`. Bevor Sie die Schreibweiterleitung innerhalb einer Sitzung aktivieren, müssen Sie überprüfen, ob Ihr Code diese Anweisungen verwendet.

```
XA {START|BEGIN} xid [JOIN|RESUME]
XA END xid [SUSPEND [FOR MIGRATE]]
XA PREPARE xid
XA COMMIT xid [ONE PHASE]
```

```
XA ROLLBACK xid
XA RECOVER [CONVERT XID]
```

LOAD-Anweisungen für permanente Tabellen

Sie können die folgenden Anweisungen nicht in einem sekundären Cluster mit aktivierter Schreibweiterleitung verwenden.

```
LOAD DATA INFILE 'data.txt' INTO TABLE t1;
        LOAD XML LOCAL INFILE 'test.xml' INTO TABLE t1;
```

Sie können in einem sekundären Cluster Daten in eine temporäre Tabelle laden. Sie dürfen jedoch alle LOAD-Anweisungen, die sich auf permanente Tabellen beziehen, nur im primären Cluster ausführen.

Plugin-Anweisungen

Sie können die folgenden Anweisungen nicht in einem sekundären Cluster mit aktivierter Schreibweiterleitung verwenden.

```
INSTALL PLUGIN example SONAME 'ha_example.so';
UNINSTALL PLUGIN example;
```

SAVEPOINT-Anweisungen

Sie können die folgenden Anweisungen nicht in einem sekundären Cluster verwenden, wenn die Schreibweiterleitung innerhalb der Sitzung aktiviert wird. Sie können diese Anweisungen in sekundären Clustern ohne aktivierte Schreibweiterleitung oder in Sitzungen mit leerer Einstellung `aurora_replica_read_consistency` verwenden. Sie müssen überprüfen, ob Ihr Code diese Anweisungen verwendet, bevor Sie die Schreibweiterleitung innerhalb einer Sitzung aktivieren.

```
SAVEPOINT t1_save;
ROLLBACK TO SAVEPOINT t1_save;
RELEASE SAVEPOINT t1_save;
```

Isolation und Konsistenz für die Schreibweiterleitung in Aurora MySQL

In Sitzungen, die Schreibweiterleitung verwenden, können Sie nur die Isolationsstufe `REPEATABLE READ` verwenden. Obwohl Sie die Isolationsstufe `READ COMMITTED` auch mit schreibgeschützten Clustern in sekundären AWS-Regionen verwenden können, funktioniert diese Isolationsstufe nicht mit

Schreibweiterleitung. Weitere Informationen zu den Isolationsstufen `REPEATABLE READ` und `READ COMMITTED` finden Sie unter Aurora MySQL-Isolierungsstufen.

Sie können den Grad der Lesekonsistenz in einem sekundären Cluster steuern. Die Lesekonsistenzstufe legt fest, wie viel Wartezeit der sekundäre Cluster vor jeder Leseoperation ausführt, um sicherzustellen, dass einige oder alle Änderungen aus dem primären Cluster repliziert werden. Sie können die Lesekonsistenzstufe anpassen, um sicherzustellen, dass alle aus Ihrer Sitzung weitergeleiteten Schreiboperationen im sekundären Cluster vor nachfolgenden Abfragen angezeigt werden. Sie können diese Einstellung auch verwenden, um sicherzustellen, dass Abfragen auf dem sekundären Cluster stets die aktuellsten Updates des primären Clusters angezeigt werden. Dies gilt auch für diejenigen, die von anderen Sitzungen oder anderen Clustern übermittelt wurden. Um diese Art von Verhalten für Ihre Anwendung anzugeben, wählen Sie einen Wert für den Sitzungsebenen-Parameter au `aurora_replica_read_consistency`.

> **Important**
>
> Legen Sie immer den Parameter `aurora_replica_read_consistency` für jede Sitzung fest, für die Sie Schreibvorgänge weiterleiten möchten. Andernfalls aktiviert Aurora die Schreibweiterleitung für diese Sitzung nicht. Dieser Parameter hat standardmäßig einen leeren Wert, wählen Sie daher einen bestimmten Wert, wenn Sie diesen Parameter verwenden. Der Parameter `aurora_replica_read_consistency` wirkt sich nur auf sekundäre Cluster aus, in denen die Schreibweiterleitung aktiviert ist.
> Verwenden Sie für Aurora-MySQL-Version 2 und Version 3 unter 3.04 `aurora_replica_read_consistency` als Sitzungsvariable. Für Aurora-MySQL-Version 3.04 und höher können Sie `aurora_replica_read_consistency` entweder als Sitzungsvariable oder als DB-Cluster-Parameter verwenden.

Für den Parameter `aurora_replica_read_consistency` können Sie die Werte `EVENTUAL`, `SESSION` und `GLOBAL` angeben.

Wenn Sie das Konsistenzniveau erhöhen, verbringt Ihre Anwendung mehr Zeit mit dem Warten auf die Propagierung von Änderungen zwischen AWS-Regionen. Sie können das Verhältnis zwischen schneller Reaktionszeit und der Gewährleistung festlegen, dass vor der Ausführung Ihrer Abfragen Änderungen an anderen Speicherorten vollständig verfügbar sind.

Wenn die Lesekonsistenz auf `EVENTUAL` festgelegt wird, werden Abfragen in einer sekundären AWS-Region, die Schreibweiterleitung verwendet, möglicherweise Daten angezeigt, die aufgrund

von Replikationsverzögerungen leicht veraltet sind. Ergebnisse von Schreiboperationen in derselben Sitzung werden erst angezeigt, wenn die Schreiboperation in der primären Region ausgeführt und zur aktuellen Region repliziert wird. Die Abfrage wartet nicht, bis die aktualisierten Ergebnisse verfügbar sind. Daher könnte sie die älteren Daten oder die aktualisierten Daten abrufen, abhängig vom Zeitpunkt der Anweisungen und der Größe der Replikationsverzögerung.

Wenn die Lesekonsistenz auf `SESSION` festgelegt ist, werden allen Abfragen in einer sekundären AWS-Region, die Schreibweiterleitung verwendet, die Ergebnisse aller in dieser Sitzung ausgeführten Änderungen angezeigt. Die Änderungen werden unabhängig davon angezeigt, ob die Transaktion übergeben wurde. Wenn notwendig, wartet die Abfrage auf die Replikation der Ergebnisse weitergeleiteter Schreiboperationen zur aktuellen Region. Sie wartet nicht auf aktualisierte Ergebnisse aus Schreiboperationen, die in anderen Regionen oder in anderen Sitzungen innerhalb der aktuellen Region ausgeführt werden.

Wenn die Lesekonsistenz auf `GLOBAL` festgelegt ist, werden einer Sitzung in einer sekundären AWS-Region Änderungen angezeigt, die von dieser Sitzung ausgeführt wurden. Außerdem werden ihr alle übergebenen Änderungen sowohl aus der primären AWS-Region als auch aus anderen sekundären AWS-Regionen angezeigt. Jede Abfrage kann für einen bestimmten Zeitraum warten, abhängig von der Sitzungsverzögerung. Die Abfrage wird fortgesetzt, wenn der sekundäre Cluster mit allen übergebenen Daten aus dem primären Cluster mit Stand zu dem Zeitpunkt, an dem die Abfrage gestartet wurde, aktualisiert ist.

Weitere Informationen zu allen mit der Schreibweiterleitung verbundenen Parametern finden Sie unter Konfigurationsparameter für die Schreibweiterleitung in Aurora MySQL.

Beispiele für die Verwendung der Schreibweiterleitung

In diesen Beispielen wird `aurora_replica_read_consistency` als Sitzungsvariable verwendet. Für Aurora-MySQL-Version 3.04 und höher können Sie `aurora_replica_read_consistency` entweder als Sitzungsvariable oder als DB-Cluster-Parameter verwenden.

Im folgenden Beispiel befindet sich der primäre Cluster in der Region US East (N. Virginia). Der sekundäre Cluster befindet sich in der Region USA Ost (Ohio). Das Beispiel zeigt die Auswirkungen ausgeführter `INSERT`-Anweisungen, gefolgt von `SELECT`-Anweisungen. Abhängig vom Wert der Einstellung `aurora_replica_read_consistency` können sich die Ergebnisse abhängig vom Zeitpunkt der Anweisungen unterscheiden. Um eine höhere Konsistenz zu erreichen, können Sie kurz warten, bevor Sie die Anweisung `SELECT` ausführen. Oder Aurora kann automatisch warten, bis die Ergebnisse fertig repliziert sind, bevor mit fortgefahren wir `SELECT`.

In diesem Beispiel gibt es eine Lesekonsistenzeinstellung von `eventual`. Das Ausführen der Anweisung `INSERT` unmittelbar gefolgt von der Anweisung `SELECT` gibt immer noch den Wert von `COUNT(*)` zurück. Dieser Wert gibt die Anzahl der Zeilen an, bevor die neue Zeile eingefügt wird. Wenn Sie kurze Zeit später `SELECT` erneut ausführen, wird die aktualisierte Zeilenzahl zurückgegeben. Die `SELECT`-Anweisungen haben keine Wartezeit.

```
mysql> set aurora_replica_read_consistency = 'eventual';
mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        5 |
+----------+
1 row in set (0.00 sec)
mysql> insert into t1 values (6); select count(*) from t1;
+----------+
| count(*) |
+----------+
|        5 |
+----------+
1 row in set (0.00 sec)
mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        6 |
+----------+
1 row in set (0.00 sec)
```

Bei Festlegung der Lesekonsistenzeinstellung auf `session` wartet eine `SELECT`-Anweisung, die unmittelbar nach einer `INSERT`-Anweisung ausgeführt wird, bis die Änderungen aus der `INSERT`-Anweisung angezeigt werden. Nachfolgende `SELECT`-Anweisungen haben keine Wartezeit.

```
mysql> set aurora_replica_read_consistency = 'session';
mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        6 |
+----------+
1 row in set (0.01 sec)
mysql> insert into t1 values (6); select count(*) from t1; select count(*) from t1;
```

```
Query OK, 1 row affected (0.08 sec)
+----------+
| count(*) |
+----------+
|        7 |
+----------+
1 row in set (0.37 sec)
+----------+
| count(*) |
+----------+
|        7 |
+----------+
1 row in set (0.00 sec)
```

Wenn die Lesekonsistenzeinstellung weiter auf `session` festgelegt ist, wird durch die Einführung einer kurzen Wartezeit nach der Ausführung einer `INSERT`-Anweisung die aktualisierte Zeilenzahl zum Zeitpunkt der nächsten Ausführung der `SELECT`-Anweisung verfügbar.

```
mysql> insert into t1 values (6); select sleep(2); select count(*) from t1;
Query OK, 1 row affected (0.07 sec)
+----------+
| sleep(2) |
+----------+
|        0 |
+----------+
1 row in set (2.01 sec)
+----------+
| count(*) |
+----------+
|        8 |
+----------+
1 row in set (0.00 sec)
```

Wenn die Leseksistenzeinstellung auf `global` festgelegt ist, wartet jede `SELECT`-Anweisung, um sicherzustellen, dass alle Datenänderungen mit Stand zur Startzeit der Anweisung angezeigt werden, bevor die Abfrage ausgeführt wird. Die Wartezeit für die einzelnen `SELECT`-Anweisungen ist von der Replikationsverzögerung zwischen dem primären und den sekundären Clustern abhängig.

```
mysql> set aurora_replica_read_consistency = 'global';
mysql> select count(*) from t1;
+----------+
| count(*) |
```

```
+----------+
|        8 |
+----------+
1 row in set (0.75 sec)
mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        8 |
+----------+
1 row in set (0.37 sec)
mysql> select count(*) from t1;
+----------+
| count(*) |
+----------+
|        8 |
+----------+
1 row in set (0.66 sec)
```

Ausführen von Multipart-Anweisungen mit Schreibweiterleitung in Aurora MySQL

Eine DML-Anweisung kann aus mehreren Teilen bestehen, z. B. einer `INSERT ... SELECT`-Anweisung oder einer `DELETE ... WHERE`-Anweisung. In diesem Fall wird die gesamte Anweisung an den primären Cluster weitergeleitet und dort ausgeführt.

Transaktionen mit Schreibweiterleitung in Aurora MySQL

Ob die Transaktion an den primären Cluster weitergeleitet wird, ist vom Zugriffsmodus der Transaktion abhängig. Sie können den Zugriffsmodus für die Transaktion durch Verwendung der Anweisungen `SET TRANSACTION` oder `START TRANSACTION` angeben. Sie können den Transaktionszugriffsmodus auch angeben, indem Sie den Wert der Aurora MySQL-Sitzungsvariablen änder `tx_read_only`. Sie können diesen Sitzungswert nur ändern, wenn Sie mit einem sekundären Cluster verbunden sind, für den die Schreibweiterleitung aktiviert ist.

Wenn eine Transaktion mit langer Laufzeit für einen beträchtlichen Zeitraum keine Anweisung ausgibt, kann sie Leerlaufzeitüberschreitung überschreiten. Dieser Zeitraum hat einen Standardwert von einer Minute. Sie können den Wert auf bis zu einem Tag erhöhen. Eine Transaktion, die die Leerlaufzeitüberschreitung überschreitet, wird vom primären Cluster abgebrochen. Die nächste nachfolgende Anweisung, die Sie übermitteln, empfängt einen Zeitüberschreitungsfehler. In diesem Fall rollt Aurora die Transaktion zurück.

Diese Art von Fehler kann in anderen Fällen auftreten, wenn die Schreibweiterleitung nicht mehr verfügbar ist. Beispielsweise bricht Aurora alle Transaktionen ab, die Schreibweiterleitung verwenden, wenn Sie den primären Cluster neu starten oder die Konfigurationseinstellung für die Schreibweiterleitung deaktivieren.

Konfigurationsparameter für die Schreibweiterleitung in Aurora MySQL

Die Aurora-Cluster-Parametergruppen enthalten Einstellungen für die Schreibweiterleitung. Da es sich um Cluster-Parameter handelt, haben alle DB-Instances in allen Clustern die gleichen Werte für diese Variablen. Details zu diesen Parametern sind in der folgenden Tabelle zusammengefasst, mit Nutzungshinweisen unterhalb der Tabelle.

Name	Scope	Typ	Standardwert	Zulässige Werte
`aurora_fwd_master_idle_timeout` (Aurora-MySQL-Version 2)	Global	Ganzzahl ohne Vorzeichen	60	1 – 86.400
`aurora_fwd_master_max_connections_pct` (Aurora-MySQL-Version 2)	Global	Lange Ganzzahl ohne Vorzeichen	10	0 – 90
`aurora_fwd_writer_idle_timeout` (Aurora-MySQL-Version 3)	Global	Ganzzahl ohne Vorzeichen	60	1 – 86.400
`aurora_fwd_writer_max_connections_pct` (Aurora-MySQL-Version 3)	Global	Lange Ganzzahl ohne Vorzeichen	10	0 – 90
`aurora_replica_read_consistency`	Sitzung	Enum	" (null)	`EVENTUAL`, `SESSION`, `GLOBAL`

Um eingehende Schreibanforderungen aus sekundären Clustern zu steuern, verwenden Sie die folgenden Einstellungen auf dem primären Cluster:

- `aurora_fwd_master_idle_timeout`, `aurora_fwd_writer_idle_timeout`: Die Anzahl der Sekunden, die der primäre Cluster auf Aktivität für eine Verbindung wartet, die aus einem sekundären Cluster weitergeleitet wird, bevor er sie schließt. Wenn die Sitzung über diesen Zeitraum hinaus im Leerlauf ist, bricht Aurora die Sitzung ab.
- `aurora_fwd_master_max_connections_pct`, `aurora_fwd_writer_max_connections_pct`: Die obere Grenze für Datenbankverbindungen, die in einer Writer-DB-Instance für die Verarbeitung von Abfragen verwendet werden können, die von Lesern weitergeleitet werden. Sie wird als Prozentsatz der Einstellung `max_connections` für die Writer-DB-Instance im primären Cluster ausgedrückt. Wenn beispielsweise `max_connections` 800 ist und `aurora_fwd_master_max_connections_pct` oder `aurora_fwd_writer_max_connections_pct` 10 ist, lässt der Writer maximal 80 weitergeleitete Sitzungen gleichzeitig zu. Diese Verbindungen stammen aus demselben, von der Einstellung `max_connections` verwalteten Verbindungspool.

  Diese Einstellung gilt nur für den primären Cluster, wenn für mindestens einen sekundären Cluster die Schreibweiterleitung aktiviert ist. Wenn Sie den Wert verringern, sind vorhandene Verbindungen nicht betroffen. Aurora berücksichtigt den neuen Wert der Einstellung, wenn versucht wird, eine neue Verbindung aus einem sekundären Cluster zu erstellen. Der Standardwert ist 10, was 10 % des Werts für `max_connections` entspricht. Wenn Sie die Abfrageweiterleitung für einen der sekundären Cluster aktivieren, muss diese Einstellung einen Wert ungleich Null haben, damit Schreiboperationen aus sekundären Clustern erfolgreich ausgeführt werden können. Wenn der Wert null ist, empfangen die Schreiboperationen den Fehlercode `ER_CON_COUNT_ERROR` mit der Meldung `Not enough connections on writer to handle your request`.

Der Parameter `aurora_replica_read_consistency` ist ein Parameter auf Sitzungsebene, der die Schreibweiterleitung ermöglicht. Sie benutzen ihn in jeder Sitzung. Sie können `EVENTUAL`, `SESSION` oder `GLOBAL` als Lesekonsistenzstufe angeben. Weitere Informationen über Konsistenzebenen finden Sie unter Isolation und Konsistenz für die Schreibweiterleitung in Aurora MySQL. Für diesen Parameter gelten die folgenden Regeln:

- Dies ist ein Parameter auf Sitzungsebene. Der Standardwert ist '' (leer).
- Die Schreibweiterleitung ist in einer Sitzung nur verfügbar, wenn `aurora_replica_read_consistency` auf `EVENTUAL`, `SESSION` oder `GLOBAL` festgelegt

ist. Dieser Parameter ist nur in Reader-Instances sekundärer Cluster relevant, für die Schreibweiterleitung aktiviert ist und die sich in einer Aurora Global Database befinden.

- Sie können diese Variable (wenn leer) oder nicht eingestellt (wenn sie bereits festgelegt ist) nicht innerhalb einer Multistatement-Transaktion setzen. Sie können sie jedoch während einer solchen Transaktion von einem gültigen Wert (`EVENTUAL`, `SESSION` oder `GLOBAL`) in einen anderen gültigen Wert (`EVENTUAL`, `SESSION` oder `GLOBAL`) ändern.
- Die Variable darf nicht `SET` sein, wenn die Schreibweiterleitung auf dem sekundären Cluster nicht aktiviert ist.
- Das Festlegen der Sitzungsvariablen auf einem primären Cluster hat keine Auswirkungen. Wenn Sie versuchen, diese Variable in einem primären Cluster zu ändern, wird eine Fehlermeldung angezeigt.

Amazon-CloudWatch-Metriken für die Schreibweiterleitung in Aurora MySQL

Die folgenden Amazon CloudWatch-Metriken und Aurora-MySQL-Statusvariablen gelten für den primären Cluster, wenn Sie die Schreibweiterleitung auf einem oder mehreren sekundären Clustern verwenden. Diese Metriken werden alle auf der Writer-DB-Instance im primären Cluster gemessen.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingMasterDMLLatency`	–	Millisekunden	Durchschnittliche Zeit für die Verarbeitung jeder weitergeleiteten DML-Anweisung auf der Writer-DB-Instance. Nicht enthalten ist die Zeit, die der sekundäre Cluster benötigt, um die Schreibanforderung weiterzuleiten, oder die Zeit, um Änderungen zurück

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
			an den sekundären Cluster zu replizieren. Für Aurora-MySQL-Version 2.
`ForwardingMasterDMLThroughput`	–	Anzahl pro Sekunde	Anzahl der weitergeleiteten DML-Anweisungen, die pro Sekunde von dieser Writer-DB-Instance verarbeitet werden. Für Aurora-MySQL-Version 2.
`ForwardingMasterOpenSessions`	`Aurora_fwd_master_open_sessions`	Anzahl	Anzahl der weitergeleiteten Sitzungen auf der Writer-DB-Instance. Für Aurora-MySQL-Version 2.
–	`Aurora_fwd_master_dml_stmt_count`	Anzahl	Gesamtzahl der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Für Aurora-MySQL-Version 2.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
–	`Aurora_fwd_master_dml_stmt_duration`	Mikrosekunden	Gesamtdauer der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Für Aurora-MySQL-Version 2.
–	`Aurora_fwd_master_select_stmt_count`	Anzahl	Gesamtzahl der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Für Aurora-MySQL-Version 2.
–	`Aurora_fwd_master_select_stmt_duration`	Mikrosekunden	Gesamtdauer der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Für Aurora-MySQL-Version 2.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingWriterDMLLatency`	–	Millisekunden	Durchschnittliche Zeit für die Verarbeitung jeder weitergeleiteten DML-Anweisung auf der Writer-DB-Instance. Nicht enthalten ist die Zeit, die der sekundäre Cluster benötigt, um die Schreibanforderung weiterzuleiten, oder die Zeit, um Änderungen zurück an den sekundären Cluster zu replizieren. Für Aurora-MySQL-Version 3.
`ForwardingWriterDMLThroughput`	–	Anzahl pro Sekunde	Anzahl der weitergeleiteten DML-Anweisungen, die pro Sekunde von dieser Writer-DB-Instance verarbeitet werden. Für Aurora-MySQL-Version 3.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingWriterOpenSessions`	`Aurora_fwd_writer_open_sessions`	Anzahl	Anzahl der weitergeleiteten Sitzungen auf der Writer-DB-Instance. Für Aurora-MySQL-Version 3.
–	`Aurora_fwd_writer_dml_stmt_count`	Anzahl	Gesamtzahl der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Für Aurora-MySQL-Version 3.
–	`Aurora_fwd_writer_dml_stmt_duration`	Mikrosekunden	Gesamtdauer der DML-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden.
–	`Aurora_fwd_writer_select_stmt_count`	Anzahl	Gesamtzahl der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Für Aurora-MySQL-Version 3.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
–	`Aurora_fwd_writer_select_stmt_duration`	Mikrosekunden	Gesamtdauer der `SELECT`-Anweisungen, die an diese Writer-DB-Instance weitergeleitet werden. Für Aurora-MySQL-Version 3.

Die folgenden CloudWatch-Metriken und Aurora-MySQL-Statusvariablen gelten für jeden sekundären Cluster. Diese Metriken werden auf jeder Reader-DB-Instance in einem sekundären Cluster mit aktivierter Schreibweiterleitung gemessen.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingReplicaDMLLatency`	–	Millisekunden	Durchschnittliche Reaktionszeit weitergeleiteter DML-Anweisungen auf Replikaten.
`ForwardingReplicaDMLThroughput`	–	Anzahl pro Sekunde	Anzahl der weitergeleiteten DML-Anweisungen, die pro Sekunde verarbeitet werden.
`ForwardingReplicaOpenSessions`	`Aurora_fwd_replica_open_sessions`	Anzahl	Die Anzahl der Sitzungen, die die Schreibweiterleitung für eine Reader-DB-Instance verwenden.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingReplicaReadWaitLatency`	–	Millisekunden	Durchschnittliche Wartezeit, die eine `SELECT`-Anweisung in einer Reader-DB-Instance darauf wartet, zum primären Cluster aufzuholen. Der Grad, in dem die Reader-DB-Instance vor der Verarbeitung einer Abfrage wartet, ist von der Einstellung `aurora_replica_read_consistency` abhängig.
`ForwardingReplicaReadWaitThroughput`	–	Anzahl pro Sekunde	Gesamtzahl der pro Sekunde in allen Sitzungen verarbeiteten `SELECT`-Anweisungen, die Schreibvorgänge weiterleiten.
`ForwardingReplicaSelectLatency`	(–)	Millisekunden	Weitergeleitete `SELECT`-Latenz, Durchschnitt über alle weitergeleiteten `SELECT`-Anweisungen innerhalb des Überwachungszeitraums.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
`ForwardingReplicaSelectThroughput`	–	Anzahl pro Sekunde	Weitergeleiteter `SELECT`-Durchsatz, pro Sekunde, als Durchschnitt innerhalb des Überwachungszeitraums.
–	`Aurora_fwd_replica_dml_stmt_count`	Anzahl	Gesamtzahl der DML-Anweisungen, die aus dieser Reader-DB-Instance weitergeleitet werden.
–	`Aurora_fwd_replica_dml_stmt_duration`	Mikrosekunden	Gesamtdauer aller DML-Anweisungen, die aus dieser Reader-DB-Instance weitergeleitet werden.
–	`Aurora_fwd_replica_errors_session_limit`	Anzahl	Anzahl der Sitzungen, die vom primären Cluster aufgrund einer der folgenden Fehlerbedingungen zurückgewiesen wurden: • Writer voll • Es sind zu viele weitergeleitete Anweisungen in Bearbeitung.

CloudWatch-Metrik	Aurora-MySQL-Statusvariable	Einheit	Beschreibung
–	`Aurora_fwd_replica_read_wait_count`	Anzahl	Gesamtzahl der Lesen-Nach-Schreiben-Wartezeiten auf dieser Reader-DB-Instance.
–	`Aurora_fwd_replica_read_wait_duration`	Mikrosekunden	Gesamtdauer der Wartezeiten aufgrund der Lesekonsistenzeinstellung auf dieser Reader-DB-Instance.
–	`Aurora_fwd_replica_select_stmt_count`	Anzahl	Gesamtzahl der `SELECT`-Anweisungen, die aus dieser Reader-DB-Instance weitergeleitet werden.
–	`Aurora_fwd_replica_select_stmt_duration`	Mikrosekunden	Gesamtdauer der `SELECT`-Anweisungen, die aus dieser Reader-DB-Instance weitergeleitet werden.

Verwenden der Schreibweiterleitung in einer globalen Aurora-PostgreSQL-Datenbank

Themen

- Region und Versionsverfügbarkeit der Schreibweiterleitung in Aurora PostgreSQL
- Aktivieren der Schreibweiterleitung in Aurora PostgreSQL
- Überprüfen auf die Aktivierung der Schreibweiterleitung für einen sekundären Cluster in Ausrora PostgreSQL

- Anwendungs- und SQL-Kompatibilität mit Schreibweiterleitung in Aurora PostgreSQL
- Isolation und Konsistenz für die Schreibweiterleitung in Aurora PostgreSQL
- Ausführen von Multipart-Anweisungen mit Schreibweiterleitung in Aurora PostgreSQL
- Konfigurationsparameter für die Schreibweiterleitung in Aurora PostgreSQL
- CloudWatch Amazon-Metriken für die Schreibweiterleitung in Aurora PostgreSQL
- Warte-Ereignisse für die Schreibweiterleitung in Aurora PostgreSQL

Region und Versionsverfügbarkeit der Schreibweiterleitung in Aurora PostgreSQL

Die Schreibweiterleitung wird mit Aurora-PostgreSQL-Version 15.4 und höheren Nebenversionen sowie mit Version 14.9 und höheren Nebenversionen unterstützt. Die Schreibweiterleitung ist in jeder Region verfügbar, in der auf Aurora PostgreSQL basierende globale Datenbanken verfügbar sind.

Weitere Informationen zur Verfügbarkeit von Versionen und Regionen im Zusammenhang mit globalen Aurora-PostgreSQL-Datenbanken finden Sie unter Globale Aurora-Datenbanken unterstützen Aurora PostgreSQL.

Aktivieren der Schreibweiterleitung in Aurora PostgreSQL

Standardmäßig ist die Schreibweiterleitung nicht aktiviert, wenn Sie einen sekundären Cluster zu einer Aurora Global Database hinzufügen. Sie können die Schreibweiterleitung für Ihren sekundären DB-Cluster aktivieren, während Sie ihn erstellen oder jederzeit danach. Bei Bedarf können Sie es später deaktivieren. Das Aktivieren oder Deaktivieren der Schreibweiterleitung führt nicht zu Ausfallzeiten oder einem Neustart.

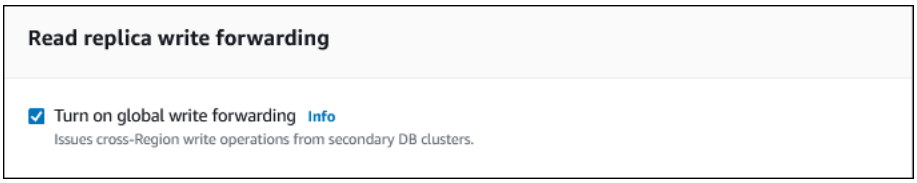
Konsole

In der Konsole können Sie die Schreibweiterleitung aktivieren oder deaktivieren, wenn Sie einen sekundären DB-Cluster erstellen oder ändern.

Aktivierung oder Deaktivierung der Schreibweiterleitung bei der Erstellung eines sekundären DB-Clusters

Wenn Sie einen neuen sekundären DB-Cluster erstellen, aktivieren Sie die Schreibweiterleitung, indem Sie unter Lesereplikat-Schreibweiterleitung das Kontrollkästchen Globale Schreibweiterleitung aktivieren markieren. Oder entfernen Sie die Markierung in dem Kontrollkästchen, um das Feature zu deaktivieren. Befolgen Sie die Anweisungen für Ihre DB-Engine unter Erstellen eines Amazon Aurora-DB Clusters, um einen sekundärem DB-Cluster zu erstellen.

Der folgende Screenshot zeigt den Abschnitt Lesereplikat-Schreibweiterleitung, bei dem das Kontrollkästchen Globale Schreibweiterleitung aktivieren markiert ist.



Aktivierung oder Deaktivierung der Schreibweiterleitung bei der Änderung eines sekundären DB-Clusters

In der Konsole können Sie einen sekundären DB-Cluster ändern, um die Schreibweiterleitung zu aktivieren oder zu deaktivieren.

So aktivieren oder deaktivieren Sie die Schreibweiterleitung für einen vorhandenen sekundären DB-Cluster mit der Konsole

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Datenbanken aus.
3. Wählen Sie den sekundären DB-Cluster aus und klicken Sie dann auf Ändern.
4. Markieren oder löschen Sie im Abschnitt Lesereplikat-Schreibweiterleitung das Kontrollkästchen Globale Schreibweiterleitung aktivieren.
5. Klicken Sie auf Weiter.
6. Wählen Sie für Einplanung von Änderungen die Option Sofort anwenden aus. Wenn Sie Während des nächsten geplanten Wartungszeitfensters anwenden wählen, ignoriert Aurora diese Einstellung und aktiviert die Schreibweiterleitung sofort.
7. Wählen Sie Cluster bearbeiten aus.

AWS CLI

Um die Schreibweiterleitung mithilfe von zu aktivieren AWS CLI, verwenden Sie die `--enable-global-write-forwarding` Option. Diese Option funktioniert, wenn Sie mit dem create-db-clusterBefehl einen neuen sekundären Cluster erstellen. Sie funktioniert auch, wenn Sie einen vorhandenen sekundären Cluster mithilfe des modify-db-clusterBefehls ändern. Sie erfordert, dass die globale Datenbank eine Aurora-Version verwendet, die eine Schreibweiterleitung unterstützt. Sie können die Schreibweiterleitung deaktivieren, indem Sie die Option `--no-enable-global-write-forwarding` mit denselben CLI-Befehlen verwenden.

In den folgenden Verfahren wird beschrieben, wie Sie die Schreibweiterleitung für einen sekundären DB-Cluster in Ihrem globalen Cluster mithilfe von AWS CLI aktivieren oder deaktivieren.

So aktivieren oder deaktivieren Sie die Schreibweiterleitung für einen vorhandenen sekundären DB-Cluster

- Rufen Sie den modify-db-cluster AWS CLI Befehl auf und geben Sie die folgenden Werte ein:
  - `--db-cluster-identifier` – der Name des DB-Clusters.
  - `--enable-global-write-forwarding` zum Aktivieren oder `--no-enable-global-write-forwarding` zum Deaktivieren.

  Das folgende Beispiel aktiviert die Schreibweiterleitung für den DB-Cluster `sample-secondary-db-cluster`.

  Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier sample-secondary-db-cluster \
    --enable-global-write-forwarding
```

  Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier sample-secondary-db-cluster ^
    --enable-global-write-forwarding
```

RDS-API

Um die Schreibweiterleitung über die Amazon RDS-API zu aktivieren, legen Sie den Parameter `EnableGlobalWriteForwarding` auf `true` fest. Dieser Parameter funktioniert, wenn Sie über die Operation CreateDBCluster einen neuen sekundären Cluster erstellen. Er funktioniert auch, wenn Sie einen vorhandenen sekundären Cluster über die Operation ModifyDBCluster ändern. Sie erfordert, dass die globale Datenbank eine Aurora-Version verwendet, die eine Schreibweiterleitung unterstützt. Sie können die Schreibweiterleitung deaktivieren, indem Sie den Parameter `EnableGlobalWriteForwarding` auf `false` festlegen.

Überprüfen auf die Aktivierung der Schreibweiterleitung für einen sekundären Cluster in Ausrora PostgreSQL

Um festzustellen, ob Sie die Schreibweiterleitung aus einem sekundären Cluster verwenden können, können Sie prüfen, ob der Cluster das Attribut besitz `"GlobalWriteForwardingStatus": "enabled"`.

In der AWS Management Console sehen Sie `Read replica write forwarding` auf der Registerkarte Konfiguration die Detailseite für den Cluster. Führen Sie den folgenden AWS CLI Befehl aus, um den Status der Einstellung für die globale Schreibweiterleitung für alle Ihre Cluster zu überprüfen.

Ein sekundärer Cluster zeigt die Werte `"enabled"` oder `"disabled"` an, um anzugeben, ob die Schreibweiterleitung aktiviert oder deaktiviert ist. Der Wert `null` gibt an, dass die Schreibweiterleitung für diesen Cluster nicht verfügbar ist. Entweder ist der Cluster nicht Teil einer globalen Datenbank oder ist der primäre Cluster und nicht kein sekundärer Cluster. Der Wert kann auch `"enabling"` oder `"disabling"` sein, wenn die Schreibweiterleitung gerade aktiviert oder deaktiviert wird.

Example

```
aws rds describe-db-clusters --query '*[].
{DBClusterIdentifier:DBClusterIdentifier,GlobalWriteForwardingStatus:GlobalWriteForwardingStatu
[
    {
        "GlobalWriteForwardingStatus": "enabled",
        "DBClusterIdentifier": "aurora-write-forwarding-test-replica-1"
    },
    {
        "GlobalWriteForwardingStatus": "disabled",
        "DBClusterIdentifier": "aurora-write-forwarding-test-replica-2"
    },
    {
        "GlobalWriteForwardingStatus": null,
        "DBClusterIdentifier": "non-global-cluster"
    }
]
```

Führen Sie den folgenden Befehl aus, um alle sekundären Cluster zu suchen, für die eine globale Schreibweiterleitung aktiviert ist. Dieser Befehl gibt auch den Reader-Endpunkt des Clusters aus. Sie

verwenden den Reader-Endpunkt des sekundären Clusters, wenn Sie die Schreibweiterleitung vom sekundären zum primären Cluster in Ihrer globalen Aurora-Datenbank verwenden.

Example

```
aws rds describe-db-clusters --query 'DBClusters[].
{DBClusterIdentifier:DBClusterIdentifier,GlobalWriteForwardingStatus:GlobalWriteForwardingStatu
 | [?GlobalWriteForwardingStatus == `enabled`]'
[
    {
        "GlobalWriteForwardingStatus": "enabled",
        "ReaderEndpoint": "aurora-write-forwarding-test-replica-1.cluster-ro-
cnpexample.us-west-2.rds.amazonaws.com",
        "DBClusterIdentifier": "aurora-write-forwarding-test-replica-1"
    }
]
```

Anwendungs- und SQL-Kompatibilität mit Schreibweiterleitung in Aurora PostgreSQL

Bestimmte Anweisungen sind nicht zulässig oder können veraltete Ergebnisse erzeugen, wenn Sie sie in einer globalen Datenbank mit Schreibweiterleitung verwenden. Darüber hinaus werden benutzerdefinierte Funktionen und benutzerdefinierte Verfahren nicht unterstützt. Daher ist die Einstellung `EnableGlobalWriteForwarding` für sekundäre Cluster standardmäßig deaktiviert. Stellen Sie vor einer Aktivierung sicher, dass der Anwendungscode von keiner dieser Einschränkungen betroffen ist.

Sie können die folgenden Arten von SQL-Anweisungen mit Schreibweiterleitung verwenden:

- Data Manipulation Language (DML)-Anweisungen wie `INSERT`, `DELETE` und `UPDATE`.
- `SELECT FOR { UPDATE | NO KEY UPDATE | SHARE | KEY SHARE }`-Anweisungen.
- `PREPARE`- und `EXECUTE`-Anweisungen.
- `EXPLAIN`-Anweisungen mit den Anweisungen in dieser Liste

Die folgenden Arten von SQL-Anweisungen werden bei Schreibweiterleitung nicht unterstützt:

- DDL-Anweisungen (Data Definition Language)
- `ANALYZE`
- `CLUSTER`
- `COPY`

- Cursor – Cursors werden nicht unterstützt. Stellen Sie daher sicher, dass Sie sie schließen, bevor Sie die Schreibweiterleitung verwenden.
- `GRANT|REVOKE|REASSIGN OWNED|SECURITY LABEL`
- `LOCK`
- `SAVEPOINT`-Anweisungen.
- `SELECT INTO`
- `SET CONSTRAINTS`
- `TRUNCATE`
- `VACUUM`

Isolation und Konsistenz für die Schreibweiterleitung in Aurora PostgreSQL

In Sitzungen, die Schreibweiterleitung verwenden, können Sie nur die Isolationsstufen `REPEATABLE READ` und `READ COMMITTED` verwenden. Die `SERIALIZABLE`-Isolationsstufe wird jedoch nicht unterstützt.

Sie können den Grad der Lesekonsistenz in einem sekundären Cluster steuern. Die Lesekonsistenzstufe legt fest, wie viel Wartezeit der sekundäre Cluster vor jeder Leseoperation ausführt, um sicherzustellen, dass einige oder alle Änderungen aus dem primären Cluster repliziert werden. Sie können die Lesekonsistenzstufe anpassen, um sicherzustellen, dass alle aus Ihrer Sitzung weitergeleiteten Schreiboperationen im sekundären Cluster vor nachfolgenden Abfragen angezeigt werden. Sie können diese Einstellung auch verwenden, um sicherzustellen, dass Abfragen auf dem sekundären Cluster stets die aktuellsten Updates des primären Clusters angezeigt werden. Dies gilt auch für diejenigen, die von anderen Sitzungen oder anderen Clustern übermittelt wurden. Um diese Art von Verhalten für Ihre Anwendung anzugeben, wählen Sie den entsprechenden Wert für den Sitzungsebenen-Parameter `apg_write_forward.consistency_mode`. Der Parameter `apg_write_forward.consistency_mode` wirkt sich nur auf sekundäre Cluster aus, in denen die Schreibweiterleitung aktiviert ist.

> **Note**
>
> Für den Parameter `apg_write_forward.consistency_mode` können Sie die Werte `SESSION`, `EVENTUAL`, `GLOBAL` oder `OFF` angeben. Standardmäßig ist der Wert auf `SESSION` festgelegt. Wenn Sie den Wert auf `OFF` festlegen, wird die Schreibweiterleitung in der Sitzung deaktiviert.

Wenn Sie das Konsistenzniveau erhöhen, verbringt Ihre Anwendung mehr Zeit damit, darauf zu warten, dass Änderungen zwischen den AWS Regionen übertragen werden. Sie können das Verhältnis zwischen schneller Reaktionszeit und der Gewährleistung festlegen, dass vor der Ausführung Ihrer Abfragen Änderungen an anderen Speicherorten vollständig verfügbar sind.

Bei jeder verfügbaren Konsistenzmodus-Einstellung hat dies folgende Auswirkungen:

- `SESSION`— Bei allen Abfragen in einer sekundären AWS Region, die Schreibweiterleitung verwendet, werden die Ergebnisse aller in dieser Sitzung vorgenommenen Änderungen angezeigt. Die Änderungen werden unabhängig davon angezeigt, ob die Transaktion übergeben wurde. Wenn notwendig, wartet die Abfrage auf die Replikation der Ergebnisse weitergeleiteter Schreiboperationen zur aktuellen Region. Sie wartet nicht auf aktualisierte Ergebnisse aus Schreiboperationen, die in anderen Regionen oder in anderen Sitzungen innerhalb der aktuellen Region ausgeführt werden.
- `EVENTUAL`— Bei Abfragen in einer sekundären AWS Region, die Schreibweiterleitung verwendet, können Daten angezeigt werden, die aufgrund von Replikationsverzögerungen leicht veraltet sind. Ergebnisse von Schreiboperationen in derselben Sitzung werden erst angezeigt, wenn die Schreiboperation in der primären Region ausgeführt und zur aktuellen Region repliziert wird. Die Abfrage wartet nicht, bis die aktualisierten Ergebnisse verfügbar sind. Daher könnte sie die älteren Daten oder die aktualisierten Daten abrufen, abhängig vom Zeitpunkt der Anweisungen und der Größe der Replikationsverzögerung.
- `GLOBAL`— Bei einer Sitzung in einer sekundären AWS Region werden Änderungen vorgenommen, die durch diese Sitzung vorgenommen wurden. Außerdem werden alle vorgenommenen Änderungen sowohl aus der primären AWS Region als auch aus anderen sekundären AWS Regionen angezeigt. Jede Abfrage kann für einen bestimmten Zeitraum warten, abhängig von der Sitzungsverzögerung. Die Abfrage wird fortgesetzt, wenn der sekundäre Cluster zu up-to-date dem Zeitpunkt, zu dem die Abfrage gestartet wurde, alle zugeschriebenen Daten aus dem primären Cluster enthält.
- `OFF` – Die Schreibweiterleitung ist in der Sitzung deaktiviert.

Weitere Informationen zu allen mit der Schreibweiterleitung verbundenen Parametern finden Sie unter Konfigurationsparameter für die Schreibweiterleitung in Aurora PostgreSQL.

Ausführen von Multipart-Anweisungen mit Schreibweiterleitung in Aurora PostgreSQL

Eine DML-Anweisung kann aus mehreren Teilen bestehen, z. B. einer `INSERT ... SELECT`-Anweisung oder einer `DELETE ... WHERE`-Anweisung. In diesem Fall wird die gesamte Anweisung an den primären Cluster weitergeleitet und dort ausgeführt.

Konfigurationsparameter für die Schreibweiterleitung in Aurora PostgreSQL

Die Aurora-Cluster-Parametergruppen enthalten Einstellungen für die Schreibweiterleitung. Da es sich um Cluster-Parameter handelt, haben alle DB-Instances in allen Clustern die gleichen Werte für diese Variablen. Details zu diesen Parametern sind in der folgenden Tabelle zusammengefasst, mit Nutzungshinweisen unterhalb der Tabelle.

Name	Scope	Typ	Standardwert	Zulässige Werte
`apg_write_forward.connect_timeout`	Sitzung	Sekunden	30	0 – 2147483647
`apg_write_forward.consistency_mode`	Sitzung	enum	Sitzung	`SESSION`, `EVENTUAL`, `GLOBAL`, `OFF`
`apg_write_forward.idle_in_transaction_session_timeout`	Sitzung	Millisekunden	86400000	0 – 2147483647
`apg_write_forward.idle_session_timeout`	Sitzung	Millisekunden	300000	0 – 2147483647
`apg_write_forward.max_forwarding_connections_percent`	Global	int	25	1-100

Der `apg_write_forward.max_forwarding_connections_percent`-Parameter definiert die Obergrenze der Datenbankverbindungsslots, die zum Umgang mit von Readern weitergeleiteten

Abfragen verwendet werden können. Er wird als Prozentsatz der Einstellung `max_connections` für die Writer-DB-Instance im primären Cluster ausgedrückt. Wenn beispielsweise `max_connections` `800` und `apg_write_forward.max_forwarding_connections_percent` `10` ist, dann lässt der Writer maximal 80 weitergeleitete Sitzungen gleichzeitig zu. Diese Verbindungen stammen aus demselben, von der Einstellung `max_connections` verwalteten Verbindungspool. Diese Einstellung gilt nur für den primären Cluster, wenn für mindestens einen sekundären Cluster die Schreibweiterleitung aktiviert ist.

Verwenden Sie die folgenden Einstellungen auf dem sekundären Cluster:

- `apg_write_forward.consistency_mode` – Ein Parameter auf Sitzungsebene, der den Grad der Lesekonsistenz auf dem sekundären Cluster steuert. Gültige Werte sind `SESSION`, `EVENTUAL`, `GLOBAL` oder `OFF`. Standardmäßig ist der Wert auf `SESSION` festgelegt. Wenn Sie den Wert auf `OFF` festlegen, wird die Schreibweiterleitung in der Sitzung deaktiviert. Weitere Informationen über Konsistenzebenen finden Sie unter Isolation und Konsistenz für die Schreibweiterleitung in Aurora PostgreSQL. Dieser Parameter ist nur in Reader-Instances sekundärer Cluster relevant, für die Schreibweiterleitung aktiviert ist und die sich in einer Aurora Global Database befinden.
- `apg_write_forward.connect_timeout` – Die maximale Anzahl von Sekunden, die der sekundäre Cluster beim Herstellen einer Verbindung zum primären Cluster wartet, bevor er aufgibt. Ein Wert von `0` bedeutet, dass auf unbestimmte Zeit gewartet werden soll.
- `apg_write_forward.idle_in_transaction_session_timeout` – Die Anzahl der Millisekunden, die der primäre Cluster auf Aktivität für eine Verbindung wartet, die aus einem sekundären Cluster mit einer offenen Transaktion weitergeleitet wird, bevor er sie schließt. Wenn die Sitzung über diesen Zeitraum hinaus inaktiv ist, bricht Aurora die Sitzung ab. Durch einen Wert des Typs `0` wird der Timout deaktiviert.
- `apg_write_forward.idle_session_timeout` – Die Anzahl der Millisekunden, die der primäre Cluster auf Aktivität für eine Verbindung wartet, die aus einem sekundären Cluster weitergeleitet wird, bevor er sie schließt. Wenn die Sitzung über diesen Zeitraum hinaus inaktiv bleibt, beendet Aurora die Sitzung. Durch einen Wert des Typs `0` wird der Timout deaktiviert.

CloudWatch Amazon-Metriken für die Schreibweiterleitung in Aurora PostgreSQL

Die folgenden CloudWatch Amazon-Metriken gelten für den primären Cluster, wenn Sie die Schreibweiterleitung auf einem oder mehreren sekundären Clustern verwenden. Diese Metriken werden alle auf der Writer-DB-Instance im primären Cluster gemessen.

CloudWatch Metrik	Einheiten und Beschreibung
`AuroraForwardingWriterDMLThroughput`	Anzahl pro Sekunde Anzahl der weitergeleiteten DML-Anweisungen, die pro Sekunde von dieser Writer-DB-Instance verarbeitet werden.
`AuroraForwardingWriterOpenSessions`	Anzahl Anzahl der offenen Sitzungen auf dieser Writer-DB-Instance, die weitergeleitete Anfragen verarbeiten.
`AuroraForwardingWriterTotalSessions`	Anzahl Anzahl der weitergeleiteten Sitzungen auf dieser Writer-DB-Instance.

Die folgenden CloudWatch Metriken gelten für jeden sekundären Cluster. Diese Metriken werden auf jeder Reader-DB-Instance in einem sekundären Cluster mit aktivierter Schreibweiterleitung gemessen.

CloudWatch Metrik	Einheit und Beschreibung
`AuroraForwardingReplicaCommitThroughput`	Anzahl pro Sekunde Anzahl der Commits in Sitzungen, die von diesem Replikat pro Sekunde weitergeleitet werden.
`AuroraForwardingReplicaDMLLatency`	Millisekunden Durchschnittliche Reaktionszeit weitergeleiteter DML-Anweisungen in Millisekunden auf Replikaten.
`AuroraForwardingReplicaDMLThroughput`	Anzahl pro Sekunde Anzahl der weitergeleiteten DML-Anweisungen, die in diesem Replikat pro Sekunde verarbeitet werden.
`AuroraForwardingReplicaErrorSessionsLimit`	Anzahl Anzahl der Sitzungen, die vom primären Cluster zurückgewiesen wurden, weil das Limit für die maximale Zahl von Verbindungen oder die maximale Schreibweiterleitung erreicht wurde.

CloudWatch Metrik	Einheit und Beschreibung
`AuroraForwardingReplicaOpenSessions`	Anzahl Die Anzahl der Sitzungen, die die Schreibweiterleitung für eine Replikat-Instance verwenden.
`AuroraForwardingReplicaReadWaitLatency`	Millisekunden Durchschnittliche Wartezeit in Millisekunden, die das Replikat darauf wartet, mit der LSN des primären Clusters konsistent zu sein. Das Ausmaß, in dem die Reader-DB-Instance vor der Verarbeitung einer Abfrage wartet, ist von der Einstellung `apg_write_forward.consistency_mode` abhängig. Weitere Informationen zu dieser Einstellung finden Sie unter the section called “Konfigurationsparameter für die Schreibweiterleitung in Aurora PostgreSQL”.

Warte-Ereignisse für die Schreibweiterleitung in Aurora PostgreSQL

Amazon Aurora generiert die folgenden Warteereignisse, wenn Sie die Schreibweiterleitung mit Aurora PostgreSQL verwenden.

Themen

- IPC: AuroraWriteForwardConnect
- IPC: AuroraWriteForwardConsistencyPoint
- IPC: AuroraWriteForwardExecute
- IPC: AuroraWriteForwardGetGlobalConsistencyPoint
- IPC: AuroraWriteForwardXactAbort
- IPC: AuroraWriteForwardXactCommit
- IPC: AuroraWriteForwardXactStart

IPC: AuroraWriteForwardConnect

Das `IPC:AuroraWriteForwardConnect`-Ereignis tritt ein, wenn ein Backend-Prozess auf dem sekundären DB-Cluster darauf wartet, dass eine Verbindung zum Writer-Knoten des primären DB-Clusters geöffnet wird.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Dieses Ereignis nimmt zu, wenn die Anzahl der Verbindungsversuche vom Leseknoten einer sekundären Region zum Writer-Knoten des primären DB-Clusters zunimmt.

Aktionen

Reduzieren Sie die Anzahl gleichzeitiger Verbindungen von einem sekundären Knoten zum Writer-Knoten der primären Region.

IPC: AuroraWriteForwardConsistencyPoint

Das `IPC:AuroraWriteForwardConsistencyPoint`-Ereignis beschreibt, wie lange eine Abfrage von einem Knoten im sekundären-DB-Cluster darauf wartet, dass die Ergebnisse weitergeleiteter Schreiboperationen in die aktuelle Region repliziert werden. Dieses Ereignis wird nur generiert, wenn der Parameter `apg_write_forward.consistency_mode` auf Sitzungsebene auf einen der folgenden Werte gesetzt ist:

- `SESSION` – Abfragen auf einem sekundären Knoten warten auf die Ergebnisse aller in dieser Sitzung ausgeführten Änderungen.
- `GLOBAL` – Abfragen auf einem sekundären Knoten warten auf die Ergebnisse der in dieser Sitzung vorgenommenen Änderungen sowie auf alle festgeschriebenen Änderungen sowohl aus der primären Region als auch aus anderen sekundären Regionen im globalen Cluster.

Informationen zum Einstellen des Parameters `apg_write_forward.consistency_mode` finden Sie unter the section called “Konfigurationsparameter für die Schreibweiterleitung in Aurora PostgreSQL”.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Zu den häufigsten Ursachen für längere Wartezeiten gehören:

- Erhöhte Replikatverzögerung, gemessen anhand der CloudWatch `ReplicaLag` Amazon-Metrik. Weitere Informationen zu dieser Metrik finden Sie unter Überwachung einer Aurora PostgreSQL-Replikation.

- Erhöhte Last auf dem Writer-Knoten der primären Region oder auf dem sekundären Knoten.

Aktionen

Ändern Sie Ihren Konsistenzmodus je nach den Anforderungen Ihrer Anwendung.

IPC: AuroraWriteForwardExecute

Das `IPC:AuroraWriteForwardExecute`-Ereignis tritt ein, wenn ein Backend-Prozess auf dem sekundären DB-Cluster darauf wartet, dass eine weitergeleitete Abfrage abgeschlossen wird und Ergebnisse vom Writer-Knoten des primären DB-Clusters abgerufen werden.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Zu den häufigsten Ursachen für längere Wartezeiten zählen auch die Folgenden:

- Abrufen einer großen Zahl von Zeilen aus dem Writer-Knoten der primären Region.
- Eine erhöhte Netzwerklatenz zwischen dem sekundären Knoten und dem Writer-Knoten der primären Region erhöht die Zeit, die der sekundäre Knoten benötigt, um Daten vom Writer-Knoten zu empfangen.
- Eine erhöhte Belastung des sekundären Knotens kann die Übertragung der Abfrageanforderung vom sekundären Knoten zum Writer-Knoten der primären Region verzögern.
- Eine erhöhte Belastung des Writer-Knotens der primären Region kann die Übertragung der Daten vom Writer-Knoten zum sekundären Knoten verzögern.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

- Optimieren Sie Abfragen, um nur die erforderlichen Daten abzurufen.
- Optimieren Sie DML-Operationen (Data Manipulation Language), um nur die erforderlichen Daten zu ändern.
- Wenn der sekundäre Knoten oder der Writer-Knoten der primären Region durch die CPU- oder Netzwerkbandbreite eingeschränkt ist, sollten Sie erwägen, ihn auf einen Instance-Typ mit mehr CPU-Kapazität oder mehr Netzwerkbandbreite umzustellen.

IPC: AuroraWriteForwardGetGlobalConsistencyPoint

Das `IPC:AuroraWriteForwardGetGlobalConsistencyPoint`-Ereignis tritt ein, wenn ein Backend-Prozess auf dem sekundären DB-Cluster, der den Konsistenzmodus GLOBAL verwendet, darauf wartet, den globalen Konsistenzpunkt vom Writer-Knoten zu erhalten, bevor er eine Abfrage ausführt.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Zu den häufigsten Ursachen für längere Wartezeiten zählen auch die Folgenden:

- Eine erhöhte Netzwerklatenz zwischen dem sekundären Knoten und dem Writer-Knoten der primären Region erhöht die Zeit, die der sekundäre Knoten benötigt, um Daten vom Writer-Knoten zu empfangen.
- Eine erhöhte Belastung des sekundären Knotens kann die Übertragung der Abfrageanforderung vom sekundären Knoten zum Writer-Knoten der primären Region verzögern.
- Eine erhöhte Belastung des Writer-Knotens der primären Region kann die Übertragung der Daten vom Writer-Knoten zum sekundären Knoten verzögern.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

- Ändern Sie Ihren Konsistenzmodus je nach den Anforderungen Ihrer Anwendung.
- Wenn der sekundäre Knoten oder der Writer-Knoten der primären Region durch die CPU- oder Netzwerkbandbreite eingeschränkt ist, sollten Sie erwägen, ihn auf einen Instance-Typ mit mehr CPU-Kapazität oder mehr Netzwerkbandbreite umzustellen.

IPC: AuroraWriteForwardXactAbort

Das `IPC:AuroraWriteForwardXactAbort`-Ereignis tritt ein, wenn ein Back-End-Prozess auf dem sekundären DB-Cluster auf das Ergebnis einer Remote-Bereinigungsabfrage wartet. Bereinigungsabfragen werden ausgegeben, um den Prozess nach dem Abbruch einer per Schreibweiterleitung weitergeleiteten Transaktion wieder in den entsprechenden Zustand zu versetzen. Amazon Aurora führt diese entweder aus, weil ein Fehler gefunden wurde oder weil ein Benutzer einen expliziten `ABORT`-Befehl ausgegeben oder eine laufende Abfrage abgebrochen hat.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Zu den häufigsten Ursachen für längere Wartezeiten zählen auch die Folgenden:

- Eine erhöhte Netzwerklatenz zwischen dem sekundären Knoten und dem Writer-Knoten der primären Region erhöht die Zeit, die der sekundäre Knoten benötigt, um Daten vom Writer-Knoten zu empfangen.
- Eine erhöhte Belastung des sekundären Knotens kann die Übertragung der Bereinigungsabfrage-Anforderung vom sekundären Knoten zum Writer-Knoten der primären Region verzögern.
- Eine erhöhte Belastung des Writer-Knotens der primären Region kann die Übertragung der Daten vom Writer-Knoten zum sekundären Knoten verzögern.

Aktionen

Abhängig von den Ursachen Ihres Warteereignisses empfehlen wir verschiedene Aktionen.

- Untersuchen Sie die Ursache für die abgebrochene Transaktion.
- Wenn der sekundäre Knoten oder der Writer-Knoten der primären Region durch die CPU- oder Netzwerkbandbreite eingeschränkt ist, sollten Sie erwägen, ihn auf einen Instance-Typ mit mehr CPU-Kapazität oder mehr Netzwerkbandbreite umzustellen.

IPC: AuroraWriteForwardXactCommit

Das `IPC:AuroraWriteForwardXactCommit`-Ereignis tritt ein, wenn ein Backend-Prozess auf dem sekundären DB-Cluster auf das Ergebnis eines weitergeleiteten Commit-Transaktionsbefehls wartet.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Zu den häufigsten Ursachen für längere Wartezeiten zählen auch die Folgenden:

- Eine erhöhte Netzwerklatenz zwischen dem sekundären Knoten und dem Writer-Knoten der primären Region erhöht die Zeit, die der sekundäre Knoten benötigt, um Daten vom Writer-Knoten zu empfangen.
- Eine erhöhte Belastung des sekundären Knotens kann die Übertragung der Abfrageanforderung vom sekundären Knoten zum Writer-Knoten der primären Region verzögern.
- Eine erhöhte Belastung des Writer-Knotens der primären Region kann die Übertragung der Daten vom Writer-Knoten zum sekundären Knoten verzögern.

Aktionen

Wenn der sekundäre Knoten oder der Writer-Knoten der primären Region durch die CPU- oder Netzwerkbandbreite eingeschränkt ist, sollten Sie erwägen, ihn auf einen Instance-Typ mit mehr CPU-Kapazität oder mehr Netzwerkbandbreite umzustellen.

IPC: AuroraWriteForwardXactStart

Das `IPC:AuroraWriteForwardXactStart`-Ereignis tritt ein, wenn ein Backend-Prozess auf dem sekundären DB-Cluster auf das Ergebnis eines weitergeleiteten Transaktionsstartbefehls wartet.

Wahrscheinliche Ursachen für erhöhte Wartezeiten

Zu den häufigsten Ursachen für längere Wartezeiten zählen auch die Folgenden:

- Eine erhöhte Netzwerklatenz zwischen dem sekundären Knoten und dem Writer-Knoten der primären Region erhöht die Zeit, die der sekundäre Knoten benötigt, um Daten vom Writer-Knoten zu empfangen.
- Eine erhöhte Belastung des sekundären Knotens kann die Übertragung der Abfrageanforderung vom sekundären Knoten zum Writer-Knoten der primären Region verzögern.
- Eine erhöhte Belastung des Writer-Knotens der primären Region kann die Übertragung der Daten vom Writer-Knoten zum sekundären Knoten verzögern.

Aktionen

Wenn der sekundäre Knoten oder der Writer-Knoten der primären Region durch die CPU- oder Netzwerkbandbreite eingeschränkt ist, sollten Sie erwägen, ihn auf einen Instance-Typ mit mehr CPU-Kapazität oder mehr Netzwerkbandbreite umzustellen.

Verwenden von Umstellung oder Failover in einer Amazon Aurora Global Database

Eine globale Aurora-Datenbank bietet mehr Schutz für Business Continuity und Disaster Recovery (BCDR) als die Standard-Hochverfügbarkeit, die von einem Aurora-DB-Cluster in einer einzigen AWS-Region Region bereitgestellt wird. Mithilfe einer globalen Aurora-Datenbank können Sie für echte regionale Katastrophen oder vollständige Service-Level-Ausfälle planen und diese schnell beheben. Die Wiederherstellung nach einem Notfall wird in der Regel von den folgenden beiden Geschäftszielen bestimmt:

- Recovery Time Objective (RTO) – Die Zeit, die ein System benötigt, um nach einem Notfall in einen arbeitsfähigen Zustand zurückzukehren. Mit anderen Worten: RTO misst die Ausfallzeit. Für eine globale Aurora-Datenbank kann sich die RTO in einer Größenordnung von Minuten bewegen.
- Recovery Point Objective (RPO) – Die Datenmenge, die nach einer Katastrophe oder einem Serviceausfall verloren gehen kann (gemessen in Zeit). Dieser Datenverlust ist in der Regel auf asynchrone Replikationsverzögerungen zurückzuführen. Für eine globale Aurora-Datenbank wird die RPO in der Regel in Sekunden gemessen. Mit einer Aurora PostgreSQL–basierten globalen Datenbank können Sie den Parameter `rds.global_db_rpo` verwenden, um die RPO-Obergrenze festzulegen und zu überwachen, dies könnte jedoch die Transaktionsverarbeitung auf dem Writer-Knoten des primären Clusters beeinträchtigen. Weitere Informationen finden Sie unter Verwalten von RPOs für Aurora PostgreSQL–basierte globale Datenbanken.

Beim Umschalten oder einem Failover einer globalen Aurora-Datenbank muss ein DB-Cluster in einer der sekundären Regionen Ihrer globalen Datenbank zum primären DB-Cluster heraufgestuft werden. Der Begriff „regionaler Ausfall“ wird häufig verwendet, um eine Vielzahl von Ausfallszenarien zu beschreiben. Ein schlimmstmögliches Szenario könnte ein großflächiger Ausfall aufgrund eines katastrophalen Ereignisses sein, das Hunderte von Quadratkilometern betrifft. Die meisten Ausfälle sind jedoch viel stärker lokal begrenzt und betreffen nur einen kleinen Teil der Cloud-Dienste oder Kundensysteme. Berücksichtigen Sie den gesamten Umfang des Ausfalls, um sicherzustellen, dass regionsübergreifendes Failover die richtige Lösung ist, und wählen Sie die für die jeweilige Situation geeignete Failover-Methode aus. Ob Sie den Failover- oder den Umstellungs-Ansatz verwenden sollten, hängt vom jeweiligen Ausfallszenario ab:

- Failover – Verwenden Sie diesen Ansatz, um die Daten nach einem ungeplanten Ausfall wiederherzustellen. Damit führen Sie ein regionsübergreifendes Failover auf einen der sekundären DB-Cluster in Ihrer globalen Aurora-Datenbank durch. Das RPO für diesen Ansatz ist in der Regel ein Wert ungleich Null, der in Sekunden gemessen wird. Das Ausmaß des Datenverlusts hängt von der Verzögerung der globalen Aurora-Datenbankreplikation zum AWS-Regionen Zeitpunkt des Ausfalls ab. Weitere Informationen hierzu finden Sie unter Wiederherstellen einer globalen Amazon Aurora-Datenbank nach einem ungeplanten Ausfall.
- Umstellung – Dieser Vorgang wurde zuvor als „verwaltetes geplantes Failover“ bezeichnet. Dieser Ansatz ist für kontrollierte Umgebungen gedacht, z. B. für betriebliche Wartung und andere geplante Betriebsverfahren. Da diese Funktion die sekundären DB-Cluster mit dem primären synchronisiert, bevor andere Änderungen vorgenommen werden, ist der RPO 0 (kein Datenverlust). Weitere Informationen hierzu finden Sie unter Durchführen von Umstellungen für Amazon Aurora Global Databases.

> **Note**
>
> Wenn Sie zu einem kopflosen sekundären Aurora-DB-Cluster umstellen oder ein Failover durchführen möchten, müssen Sie diesem zunächst eine DB-Instance hinzufügen. Weitere Informationen zu kopflosen DB-Clustern finden Sie unter Erstellen eines Aurora-Headless-DB-Clusters in einer sekundären Region.

Themen

Wiederherstellen einer globalen Amazon Aurora-Datenbank nach einem ungeplanten Ausfall

In sehr seltenen Fällen kann es in Ihrer globalen Aurora-Datenbank zu einem unerwarteten Ausfall in der primären AWS-Region kommen. In einem solchen Fall sind der primäre Aurora-DB-Cluster und sein Writer-Knoten nicht verfügbar, und die Replikation zwischen dem primären Cluster und den sekundären Clustern wird angehalten. Um Ausfallzeiten (RTO) und Datenverlust (RPO) zu minimieren, können Sie schnell ein regionsübergreifendes Failover durchführen.

Es gibt zwei Methoden für ein Failover in einer Notfallwiederherstellungssituation:

- Verwaltetes Failover — Diese Methode wird für die Notfallwiederherstellung empfohlen. Wenn Sie diese Methode verwenden, fügt Aurora die alte primäre Region automatisch wieder als sekundäre Region zur globalen Datenbank hinzu, sobald sie wieder verfügbar ist. Somit wird die ursprüngliche Topologie Ihres globalen Clusters beibehalten. Um zu erfahren, wie Sie diese Methode verwenden, vgl. Ausführen von verwalteten geplanten Failovers für globale Aurora-Datenbanken.
- Manuelles Failover – Diese alternative Methode kann verwendet werden, wenn ein verwaltetes Failover nicht in Frage kommt, z. B. wenn in Ihren primären und sekundären Regionen inkompatible Engine-Versionen ausgeführt werden. Um zu erfahren, wie Sie diese Methode verwenden, vgl. Ausführen von manuellen geplanten Failovers für globale Aurora-Datenbanken.

> **Important**
>
> Beide Failover-Methoden können zum Verlust von Schreibtransaktionsdaten führen, die vor dem Eintreten des Failover-Ereignisses nicht zur gewählten sekundären Region repliziert wurden. Der Wiederherstellungsprozess, der eine DB-Instance auf dem ausgewählten sekundären DB-Cluster zur primären Writer-DB-Instance hochstuft, garantiert jedoch, dass sich die Daten in einem transaktionskonsistenten Zustand befinden.

Ausführen von verwalteten geplanten Failovers für globale Aurora-Datenbanken

Dieser Ansatz dient der Geschäftskontinuität im Falle einer echten regionalen Katastrophe oder eines kompletten Service-Level-Ausfalls.

Während eines verwalteten geplanten Failovers erfolgt ein Failover Ihres primären Clusters auf eine von Ihnen gewählte sekundäre Region, während die vorhandene Replikationstopologie Ihrer globalen Aurora-Datenbank beibehalten wird. Der gewählte sekundäre Cluster stuft einen seiner schreibgeschützten Knoten auf vollen Writer-Status herauf. In diesem Schritt kann der Cluster die Rolle des primären Clusters übernehmen. Ihre Datenbank ist für kurze Zeit nicht verfügbar, während dieser Cluster seine neue Rolle annimmt. Daten, die nicht vom alten primären auf den ausgewählten sekundären Cluster repliziert wurden, fehlen, wenn dieser sekundäre zum neuen primären Cluster wird.

> **Note**
>
> Sie können ein verwaltetes regionsübergreifendes Datenbank-Failover für eine globale Aurora-Datenbank nur durchführen, wenn die primären und sekundären DB-Cluster dieselben Engine-Haupt- und Nebenversionen sowie dasselbe Patch-Level haben. Die Patch-Level können je nach Nebenversion der Engine unterschiedlich sein. Weitere Informationen finden Sie unter Patch-Level-Kompatibilität für verwaltete regionsübergreifende Umstellungen und Failovers. Wenn Ihre Engine-Versionen nicht kompatibel sind, können Sie das Failover manuell durchführen, indem Sie die Schritte unter Ausführen von manuellen geplanten Failovers für globale Aurora-Datenbanken ausführen.

Um Datenverlust zu minimieren, empfehlen wir Ihnen, vor der Verwendung dieser Funktion Folgendes zu tun:

- Schalten Sie Anwendungen offline, um zu verhindern, dass Schreibvorgänge an den primären Cluster der globalen Aurora-Datenbank gesendet werden.
- Überprüfen Sie die Verzögerungszeiten für alle sekundären Aurora-DB-Cluster in der globalen Aurora-Datenbank. Durch die Auswahl der sekundären Region mit der geringsten Replikationsverzögerung kann der Datenverlust in der aktuell ausgefallenen primären Region minimiert werden. Verwenden Sie Amazon CloudWatch für alle Aurora PostgreSQL-basierten globalen Datenbanken und für Aurora MySQL-basierte globale Datenbanken ab Engine-Versionen 3.04.0 und höher oder 2.12.0 und höher, um die Metrik für alle sekundären DB-Cluster anzuzeigen. `AuroraGlobalDBRPOLag` Zeigen Sie für niedrigere Nebenversionen von Aurora MySQL-basierten globalen Datenbanken stattdessen die `AuroraGlobalDBReplicationLag`-Metrik an. Diese Metriken geben an, wie weit (in Millisekunden) ein sekundärer Cluster gegenüber dem primären DB-Cluster verzögert ist.

  Weitere Informationen zu CloudWatch Metriken für Aurora finden Sie unterMetriken auf Clusterebene für Amazon Aurora.

Während eines verwalteten Failovers wird der ausgewählte sekundäre DB-Cluster in seine neue Rolle als primärer Cluster hochgestuft. Er übernimmt jedoch nicht die verschiedenen Konfigurationsoptionen des primären DB-Clusters. Wenn die Konfiguration nicht übereinstimmt, kann dies Leistungsprobleme, Workload-Inkompatibilitäten und anderes anomales Verhalten zur Folge haben. Um solche Probleme zu vermeiden, empfehlen wir Ihnen, die Unterschiede zwischen den Clustern Ihrer globalen Aurora-Datenbank wie folgt aufzulösen:

- Konfigurieren Sie die Aurora-DB-Cluster-Parametergruppe für den neuen primären Cluster, falls erforderlich – Sie können Ihre Aurora-DB-Cluster-Parametergruppen für jeden Aurora-Cluster in Ihrer globalen Aurora-Datenbank unabhängig konfigurieren. Wenn Sie also einen sekundären DB-Cluster zur Übernahme der primären Rolle hochstufen, kann die Parametergruppe des sekundären Clusters im Vergleich zum primären Cluster möglicherweise anders konfiguriert sein. Ist dies der Fall, ändern Sie die Parametergruppe des hochgestuften sekundären DB-Clusters so, dass sie den Einstellungen des primären Clusters entspricht. Um zu erfahren wie, siehe Ändern von Parametern für eine Aurora globale Datenbank.
- Überwachungstools und -optionen wie Amazon CloudWatch Events und Alarme konfigurieren — Konfigurieren Sie den beworbenen DB-Cluster mit den gleichen Protokollierungsfunktionen, Alarmen usw., wie es für die globale Datenbank erforderlich ist. Wie bei Parametergruppen wird die Konfiguration für diese Funktionen während des Failover-Prozesses nicht vom primären Cluster übernommen. Einige CloudWatch Metriken, wie z. B. die Verzögerung bei der Replikation, sind

nur für sekundäre Regionen verfügbar. Daher ändert ein Failover die Art und Weise, wie diese Metriken angezeigt und Alarme für sie eingerichtet werden, und es können Änderungen an allen vordefinierten Dashboards erforderlich sein. Weitere Informationen zu Aurora-DB-Clustern und zur Überwachung finden Sie unter Übersicht über die Überwachung von Amazon Aurora.

- Integrationen mit anderen AWS Diensten konfigurieren — Wenn Ihre globale Aurora-Datenbank in AWS Dienste wie, AWS Secrets Manager AWS Identity and Access Management, Amazon S3 und integriert ist AWS Lambda, müssen Sie sicherstellen, dass diese nach Bedarf konfiguriert sind. Weitere Informationen zur Integration globaler Aurora-Datenbanken in IAM, Amazon S3 und Lambda finden Sie unter Verwenden von globalen Amazon-Aurora-Datenbanken mit anderen AWS-Services. Weitere Informationen zu Secrets Manager finden Sie unter So automatisieren Sie die Replikation von Geheimnissen in AWS Secrets Manager Across AWS-Regionen.

In der Regel übernimmt der gewählte sekundäre Cluster innerhalb weniger Minuten die primäre Rolle. Sobald der Writer-Knoten der neuen primären Region verfügbar ist, können Sie Ihre Anwendungen mit diesem verbinden und Ihre Workloads fortsetzen. Nachdem Aurora den neuen primären Cluster hochgestuft hat, werden automatisch alle zusätzlichen Cluster der sekundären Region neu erstellt.

Da die globalen Aurora-Datenbanken die asynchrone Replikation verwenden, kann die Replikationsverzögerung in jeder sekundären Region variieren. Aurora baut diese sekundären Regionen neu auf, sodass sie genau dieselben point-in-time Daten wie der neue Cluster der primären Region haben. Die Dauer der vollständigen Neuerstellungsaufgabe kann je nach Größe des Speichervolumens und der Entfernung zwischen den Regionen einige Minuten bis mehrere Stunden dauern. Wenn der Wiederaufbau der Cluster der sekundären Region aus der neuen primären Region abgeschlossen ist, stehen sie für den Lesezugriff zur Verfügung.

Sobald der neue primäre Writer hochgestuft und verfügbar ist, kann der Cluster der neuen primären Region Lese- und Schreibvorgänge für die globale Aurora-Datenbank abwickeln. Stellen Sie sicher, dass Sie den Endpunkt für Ihre Anwendung ändern, um den neuen Endpunkt zu verwenden. Wenn Sie die angegebenen Namen beim Erstellen der globalen Aurora-Datenbank akzeptiert haben, können Sie den Endpunkt ändern, indem Sie `-ro` aus der Endpunkt-Zeichenfolge des hochgestuften Clusters in Ihrer Anwendung entfernen.

Beispielsweise wird der Endpunkt des sekundären Clusters `my-global.cluster-ro-aaaaaabbbbbb.us-west-1.rds.amazonaws.com` zu `my-global.cluster-aaaaaabbbbbb.us-west-1.rds.amazonaws.com`, wenn dieser Cluster zum primären Cluster hochgestuft wird.

Wenn Sie RDS-Proxy verwenden, stellen Sie sicher, dass Sie die Schreibvorgänge Ihrer Anwendung an den entsprechenden Lese-/Schreibendpunkt des Proxys umleiten, der dem neuen primären Cluster zugeordnet ist. Dieser Proxy-Endpunkt kann der Standardendpunkt oder ein benutzerdefinierter Lese-/Schreibendpunkt sein. Weitere Informationen finden Sie unter So funktionieren RDS-Proxy-Endpunkte mit globalen Datenbanken.

Um die ursprüngliche Topologie des globalen Datenbank-Clusters wiederherzustellen, überwacht Aurora die Verfügbarkeit der alten primären Region. Sobald diese Region fehlerfrei und wieder verfügbar ist, fügt Aurora sie automatisch wieder als sekundäre Region zum globalen Cluster hinzu. Bevor das neue Speichervolume in der alten Primärregion erstellt wird, versucht Aurora, zum Zeitpunkt des Fehlers einen Snapshot des alten Speichervolumes zu erstellen. Auf diese Weise können Sie alle fehlenden Daten wiederherstellen. Wenn dieser Vorgang erfolgreich ist, platziert Aurora diesen Snapshot mit dem Namen „rds: unplanned-global-failover - *`name-of-old-primary-DB-Cluster`* - *`timestamp`*" im Snapshot-Abschnitt von. AWS Management ConsoleSie können diesen Snapshot auch in den Informationen sehen, die von der DescribeDB-API-Operation zurückgegeben werden. ClusterSnapshots

> **Note**
>
> Der Snapshot des alten Speichervolumes ist ein System-Snapshot, der der auf dem alten primären Cluster konfigurierten Aufbewahrungsfrist für Backups unterliegt. Um diesen Snapshot außerhalb des Aufbewahrungszeitraums zu speichern, können Sie ihn kopieren, um ihn als manuellen Snapshot zu speichern. Weitere Informationen zum Kopieren von Snapshots, einschließlich der Preise, finden Sie unter Kopieren eines DB-Cluster-Snapshots.

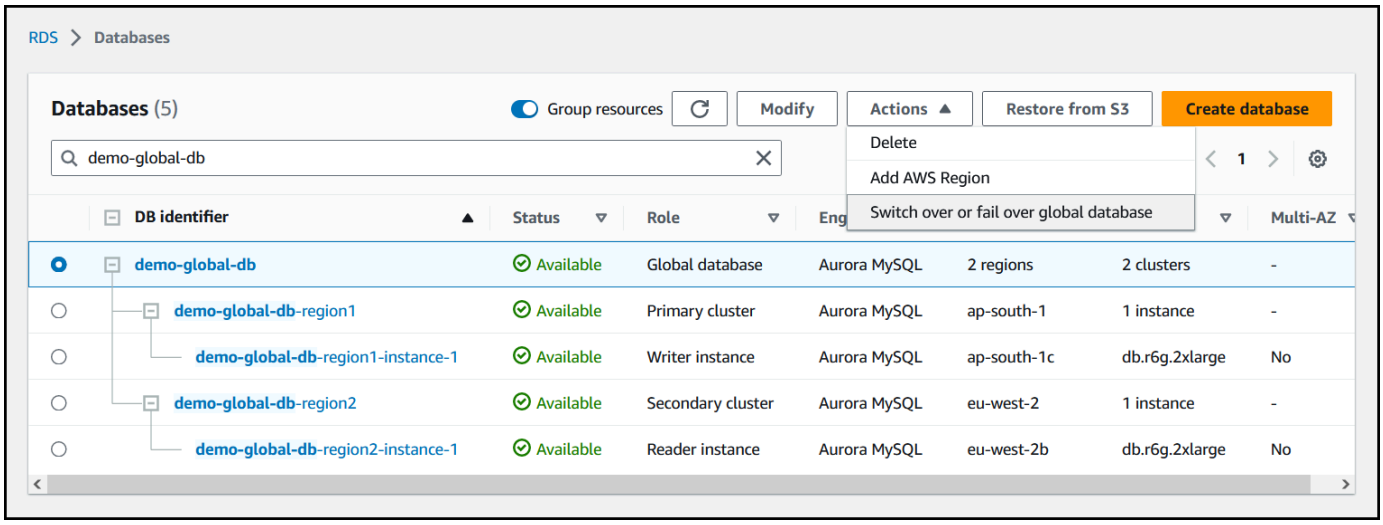
Nachdem die ursprüngliche Topologie wiederhergestellt ist, können Sie ein Failback Ihrer globalen Datenbank auf die ursprüngliche primäre Region durchführen, indem Sie eine Umstellung durchführen, wenn dies für Ihr Unternehmen und Ihren Workload am sinnvollsten ist. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Durchführen von Umstellungen für Amazon Aurora Global Databases.

Sie können ein Failover für Ihre globale Aurora-Datenbank mithilfe der AWS Management Console AWS CLI, der oder der RDS-API durchführen.

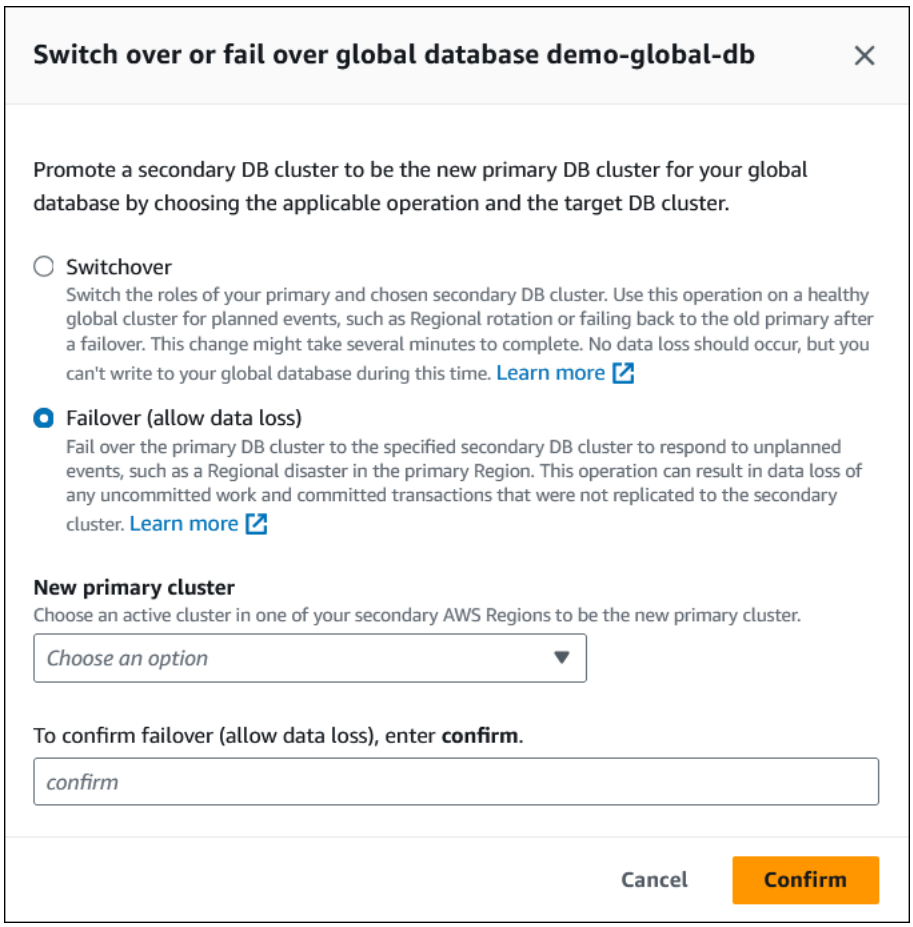
Konsole

So starten Sie den verwalteten Failover-Prozess in Ihrer globalen Aurora-Datenbank

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Datenbanken und suchen Sie die globale Aurora-Datenbank, für die Sie ein Failover ausführen möchten.
3. Wählen Sie im Menü Aktionen die Option Failover für globale Datenbank aus.

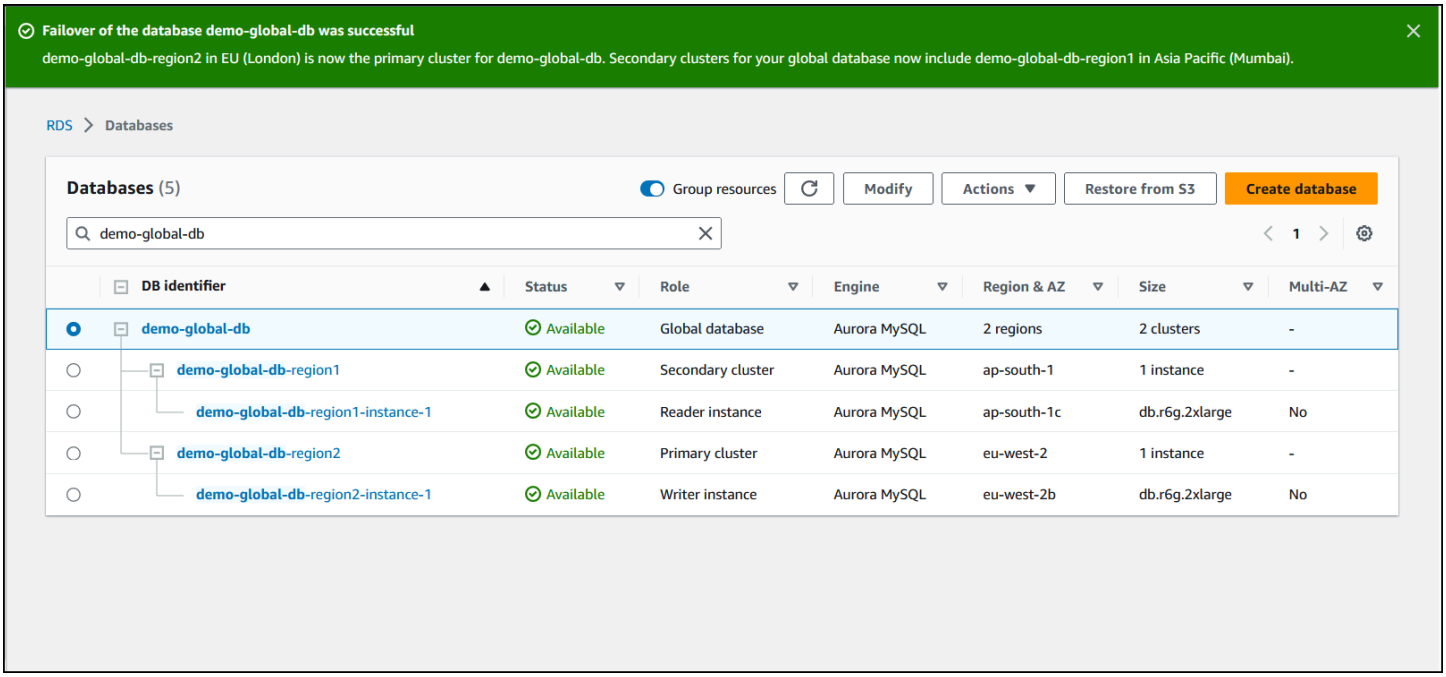


4. Wählen Sie Failover (Datenverlust zulassen).



5. Wählen Sie für Neuer primärer Cluster einen aktiven Cluster in einem Ihrer sekundären AWS-Regionen Cluster als neuen primären Cluster aus.
6. Geben Sie **`confirm`** ein, und wählen Sie dann Bestätigen.

Wenn das Failover abgeschlossen ist, werden die Aurora-DB-Cluster und ihr aktueller Status wie im Folgenden in der Liste Datenbanken dargestellt angezeigt.



AWS CLI

So führen Sie das verwaltete Failover für eine globale Aurora-Datenbank durch

Verwenden Sie den `failover-global-cluster`-CLI-Befehl, um ein Failover für Ihre globale Aurora-Datenbank auszuführen. Mit dem Befehl können Sie Werte für die folgenden Parameter übertragen.

- `--region`— Geben Sie an AWS-Region , wo der sekundäre DB-Cluster, den Sie als neuen primären DB-Cluster für die globale Aurora-Datenbank verwenden möchten, ausgeführt wird.
- `--global-cluster-identifier` – Geben Sie den Namen Ihrer globalen Aurora-Datenbank an.
- `--target-db-cluster-identifier` – Geben Sie den Amazon-Ressourcennamen (ARN) des Aurora-DB-Clusters an, den Sie als neuen primären Cluster für die globale Aurora-Datenbank hochstufen möchten.
- `--allow-data-loss` – Machen Sie dies ausdrücklich zu einer Failover- und nicht zu einer Umstellungs-Operation. Ein Failover-Vorgang kann zu Datenverlusten führen, wenn die asynchronen Replikationskomponenten das Senden aller replizierten Daten an die sekundäre Region nicht abgeschlossen haben.

Für LinuxmacOS, oderUnix:

```
aws rds --region region_of_selected_secondary \
```

```
    failover-global-cluster --global-cluster-identifier global_database_id \
    --target-db-cluster-identifier arn_of_secondary_to_promote \
    --allow-data-loss
```

Windows:

```
aws rds --region region_of_selected_secondary ^
    failover-global-cluster --global-cluster-identifier global_database_id ^
    --target-db-cluster-identifier arn_of_secondary_to_promote ^
    --allow-data-loss
```

RDS-API

Um ein Failover für eine globale Aurora-Datenbank durchzuführen, führen Sie den FailoverGlobalClusterAPI-Vorgang aus.

Ausführen von manuellen geplanten Failovers für globale Aurora-Datenbanken

In einigen Szenarien können Sie den verwalteten Failover-Prozess möglicherweise nicht verwenden. Ein Beispiel ist etwa, wenn auf Ihrem primären und sekundären DB-Cluster keine kompatiblen Engine-Versionen ausgeführt werden. In diesem Fall können Sie diesem manuellen Prozess folgen, um ein Failover Ihrer globalen Datenbank in Ihre sekundäre Zielregion durchzuführen.

> **Tip**
>
> Bevor Sie diesen Prozess verwenden, sollten Sie sich damit vertraut machen. Halten Sie einen Plan bereit, um bei den ersten Anzeichen eines regionsweiten Problems schnell handeln zu können. Sie können bereit sein, die sekundäre Region mit der geringsten Replikationsverzögerung zu identifizieren, indem Sie Amazon CloudWatch regelmäßig verwenden, um die Verzögerungszeiten für die sekundären Cluster zu verfolgen. Testen Sie Ihren Plan, um zu überprüfen, ob Ihre Verfahren vollständig und genau sind, und stellen Sie sicher, dass die Mitarbeiter darin geschult sind, ein Failover für die Notfallwiederherstellung durchzuführen, bevor es wirklich erforderlich ist.

Führen Sie nach einem ungeplanten Ausfall in der primären Region ein Failover auf einen sekundären Cluster wie folgt manuell durch:

1. Beenden Sie die Ausgabe von DML-Anweisungen und anderen Schreibvorgängen an den primären Aurora-DB-Cluster während des AWS-Region Ausfalls.

2. Identifizieren Sie einen Aurora-DB-Cluster von einem sekundären AWS-Region , der als neuer primärer DB-Cluster verwendet werden soll. Wenn Sie zwei oder mehr sekundäre Cluster AWS-Regionen in Ihrer globalen Aurora-Datenbank haben, wählen Sie den sekundären Cluster mit der geringsten Replikationsverzögerung.
3. Trennen Sie Ihren ausgewählten sekundären DB-Cluster von der globalen Aurora-Datenbank.

   Das Entfernen eines sekundären DB-Clusters aus einer globalen Aurora-Datenbank stoppt sofort die Replikation vom primären zu diesem sekundären Cluster und stuft ihn als ein eigenständiges bereitgestelltes Aurora-DB-Cluster mit uneingeschränkter Lese-/Schreibfunktion ein. Alle anderen sekundären Aurora-DB-Cluster, die mit dem primären Cluster in der Region mit dem Ausfall verknüpft sind, sind weiterhin verfügbar und können Aufrufe von Ihrer Anwendung annehmen. Sie verbrauchen auch Ressourcen. Da Sie die globale Aurora-Datenbank neu erstellen, entfernen Sie die anderen sekundären DB-Cluster, bevor Sie die neue globale Aurora-Datenbank in den folgenden Schritten erstellen. Dadurch werden Dateninkonsistenzen zwischen den DB-Clustern in der globalen Aurora-Datenbank vermieden (split-brain-Probleme).

   Ausführliche Schritte zum Trennen finden Sie unter Entfernen eines Clusters aus einer Amazon Aurora Global Database.
4. Konfigurieren Sie Ihre Anwendung neu, um alle Schreibvorgänge mit ihrem neuen Endpunkt an diesen eigenständigen Aurora-DB-Cluster zu senden. Wenn Sie die angegebenen Namen beim Erstellen der globalen Aurora-Datenbank akzeptiert haben, können Sie den Endpunkt ändern, indem Sie `-ro` aus der Endpunkt-Zeichenfolge des Clusters in Ihrer Anwendung entfernen.

   Beispielsweise wird der Endpunkt `my-global.cluster-ro-aaaaaabbbbbb.us-west-1.rds.amazonaws.com` des sekundären Clusters zu `my-global.cluster-aaaaaabbbbbb.us-west-1.rds.amazonaws.com`, wenn dieser Cluster von der globalen Aurora-Datenbank getrennt wird.

   Dieser Aurora-DB-Cluster wird zum primären Cluster einer neuen globalen Aurora-Datenbank, wenn Sie im nächsten Schritt beginnen Regionen hinzuzufügen.

   Wenn Sie RDS-Proxy verwenden, stellen Sie sicher, dass Sie die Schreibvorgänge Ihrer Anwendung an den entsprechenden Lese-/Schreibendpunkt des Proxys umleiten, der dem neuen primären Cluster zugeordnet ist. Dieser Proxy-Endpunkt kann der Standardendpunkt oder ein benutzerdefinierter Lese-/Schreibendpunkt sein. Weitere Informationen finden Sie unter So funktionieren RDS-Proxy-Endpunkte mit globalen Datenbanken.
5. Fügen Sie AWS-Region dem DB-Cluster einen hinzu. Wenn Sie dies tun, beginnt der Replikationsprozess vom primären zum sekundären Cluster. Ausführliche Schritte zum

Hinzufügen einer Region finden Sie unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank.

6. Fügen Sie nach AWS-Regionen Bedarf weitere hinzu, um die Topologie wiederherzustellen, die zur Unterstützung Ihrer Anwendung erforderlich ist.

Stellen Sie sicher, dass Schreibvorgänge der Anwendung vor, während und nach diesen Änderungen an den richtigen Aurora-DB-Cluster gesendet werden. Dadurch werden Dateninkonsistenzen zwischen den DB-Clustern in der globalen Aurora-Datenbank vermieden (split-brain-Probleme).

Wenn Sie als Reaktion auf einen Ausfall in einem neu konfiguriert haben AWS-Region, können Sie diesen nach Behebung AWS-Region des Ausfalls wieder zum primären Server machen. Dazu fügen Sie die alte AWS-Region Ihrer neuen globalen Datenbank hinzu und verwenden dann den Umstellungs-Prozess, um die Rolle zu wechseln. Ihre Aurora Global Database muss eine Version von Aurora PostgreSQL oder Aurora MySQL verwenden, die Umstellungen unterstützt. Weitere Informationen finden Sie unter Durchführen von Umstellungen für Amazon Aurora Global Databases.

Durchführen von Umstellungen für Amazon Aurora Global Databases

> **Note**
>
> Umstellungen wurden früher als „verwaltete geplante Failovers“ bezeichnet.

Mithilfe von Switchovers können Sie die Region Ihres primären Clusters routinemäßig ändern. Dieser Ansatz ist für kontrollierte Szenarien gedacht, z. B. für betriebliche Wartung und andere geplante Betriebsverfahren.

Es gibt drei gängige Anwendungsfälle für die Verwendung von Umstellungen.

- Für Anforderungen an die „regionale Rotation“, die in bestimmten Branchen gelten. Beispielsweise könnten die Vorschriften für Finanzdienstleistungen vorschreiben, dass Tier-0-Systeme für mehrere Monate in eine andere Region wechseln müssen, um sicherzustellen, dass die Notfallwiederherstellungsverfahren regelmäßig geübt werden.
- Für "follow-the-sun" -Anwendungen mit mehreren Regionen. Beispielsweise möchte ein Unternehmen möglicherweise Schreibvorgänge mit niedrigerer Latenz in verschiedenen Regionen bereitstellen, basierend auf den Geschäftszeiten in verschiedenen Zeitzonen.
- Als zero-data-loss Methode, um nach einem Failover zur ursprünglichen primären Region zurückzukehren.

> **Note**
>
> Umstellungen sind so konzipiert, dass sie auf einer funktionierenden Aurora Global Database verwendet werden können. Folgen Sie zur Wiederherstellung nach einem ungeplanten Ausfall dem entsprechenden Verfahren unter Wiederherstellen einer globalen Amazon Aurora-Datenbank nach einem ungeplanten Ausfall.
> Um eine Umstellung durchführen zu können, muss Ihr sekundärer DB-Cluster genau dieselbe Engine-Version ausführen, einschließlich des Patch-Levels, je nach Engine-Version. Weitere Informationen finden Sie unter Patch-Level-Kompatibilität für verwaltete regionsübergreifende Umstellungen und Failovers. Bevor Sie mit der Umstellung beginnen, überprüfen Sie die Engine-Versionen in Ihrem globalen Cluster, um sicherzustellen, dass diese verwaltete regionsübergreifende Umstellungen unterstützen, und aktualisieren Sie sie bei Bedarf.

Während einer Umstellung wechselt Aurora Ihren primären Cluster zu der von Ihnen gewählten sekundären Region, während die vorhandene Replikationstopologie Ihrer Aurora Global Database beibehalten wird. Bevor die Umstellung gestartet wird, wartet Aurora, bis alle Cluster der sekundären Region vollständig mit dem Cluster der primären Region synchronisiert sind. Dann wird der DB-Cluster in der primären Region schreibgeschützt, und der ausgewählte sekundäre Cluster stuft einen seiner schreibgeschützten Knoten auf vollen Writer-Status hoch. Durch die Heraufstufung dieses Knotens zu einem Writer kann dieser sekundäre Cluster die Rolle des primären Clusters übernehmen. Da alle sekundären Cluster zu Beginn des Prozesses mit dem primären Cluster synchronisiert wurden, setzt die neue primäre Version den Betrieb für die globale Aurora-Datenbank fort, ohne dass Daten verloren gehen. Ihre Datenbank ist für kurze Zeit nicht verfügbar, während der primäre und der ausgewählte sekundäre Cluster ihre neuen Rollen übernehmen.

Um die Anwendungsverfügbarkeit zu optimieren, empfehlen wir Ihnen, vor der Verwendung dieser Funktion Folgendes zu tun:

- Führen Sie diesen Vorgang außerhalb der Spitzenzeiten oder zu einem anderen Zeitpunkt durch, wenn die Schreibvorgänge auf den primären DB-Clustern minimal sind.
- Schalten Sie Anwendungen offline, um zu verhindern, dass Schreibvorgänge an den primären Cluster der globalen Aurora-Datenbank gesendet werden.
- Überprüfen Sie die Verzögerungszeiten für alle sekundären Aurora-DB-Cluster in der globalen Aurora-Datenbank. Verwenden Sie Amazon CloudWatch für alle Aurora PostgreSQL-basierten globalen Datenbanken und für Aurora MySQL-basierte globale Datenbanken ab Engine-Versionen 3.04.0 und höher oder 2.12.0 und höher, um die Metrik für alle sekundären DB-Cluster anzuzeigen.

`AuroraGlobalDBRPOLag` Zeigen Sie für niedrigere Nebenversionen von Aurora MySQL-basierten globalen Datenbanken stattdessen die `AuroraGlobalDBReplicationLag`-Metrik an. Diese Metriken geben an, wie weit (in Millisekunden) ein sekundärer Cluster gegenüber dem primären DB-Cluster verzögert ist. Der Wert verhält sich direkt proportional zu der Zeit, die Aurora zum Abschließen der Umstellung benötigt. Je größer der Verzögerungswert, desto länger dauert die Umstellung.

Weitere Informationen zu CloudWatch Metriken für Aurora finden Sie unterMetriken auf Clusterebene für Amazon Aurora.

Während einer Umstellung wird der ausgewählte sekundäre DB-Cluster in seine neue Rolle als primärer Cluster hochgestuft. Er übernimmt jedoch nicht die verschiedenen Konfigurationsoptionen des primären DB-Clusters. Wenn die Konfiguration nicht übereinstimmt, kann dies Leistungsprobleme, Workload-Inkompatibilitäten und anderes anomales Verhalten zur Folge haben. Um solche Probleme zu vermeiden, empfehlen wir Ihnen, die Unterschiede zwischen den Clustern Ihrer globalen Aurora-Datenbank wie folgt aufzulösen:

- Konfigurieren Sie die Aurora-DB-Cluster-Parametergruppe für den neuen primären Cluster, falls erforderlich – Sie können Ihre Aurora-DB-Cluster-Parametergruppen für jeden Aurora-Cluster in Ihrer globalen Aurora-Datenbank unabhängig konfigurieren. Wenn Sie also einen sekundären DB-Cluster zur Übernahme der primären Rolle hochstufen, kann die Parametergruppe des sekundären Clusters im Vergleich zum primären Cluster möglicherweise anders konfiguriert werden. Ist dies der Fall, ändern Sie die Parametergruppe des hochgestuften sekundären DB-Clusters so, dass sie den Einstellungen des primären Clusters entspricht. Um zu erfahren wie, siehe Ändern von Parametern für eine Aurora globale Datenbank.
- Überwachungstools und -optionen wie Amazon CloudWatch Events und Alarme konfigurieren — Konfigurieren Sie den beworbenen DB-Cluster mit den gleichen Protokollierungsfunktionen, Alarmen usw., wie es für die globale Datenbank erforderlich ist. Wie bei Parametergruppen wird die Konfiguration für diese Funktionen während der Umstellung nicht vom primären Cluster übernommen. Einige CloudWatch Metriken, wie z. B. die Verzögerung bei der Replikation, sind nur für sekundäre Regionen verfügbar. Daher ändert sich bei einer Umstellung die Art und Weise, wie diese Metriken angezeigt und Alarme für sie eingerichtet werden, und es können Änderungen an allen vordefinierten Dashboards erforderlich sein. Weitere Informationen zu Aurora-DB-Clustern und zur Überwachung finden Sie unter Übersicht über die Überwachung von Amazon Aurora.
- Integrationen mit anderen AWS Diensten konfigurieren — Wenn Ihre globale Aurora-Datenbank in AWS Dienste wie Amazon S3 integriert ist AWS Secrets Manager AWS Identity and Access

Management, stellen Sie sicher AWS Lambda, dass Sie Ihre Integrationen mit diesen Diensten nach Bedarf konfigurieren. Weitere Informationen zur Integration globaler Aurora-Datenbanken in IAM, Amazon S3 und Lambda finden Sie unter Verwenden von globalen Amazon-Aurora-Datenbanken mit anderen AWS-Services. Weitere Informationen zu Secrets Manager finden Sie unter So automatisieren Sie die Replikation von Geheimnissen in AWS Secrets Manager Across AWS-Regionen.

> **Note**
>
> In der Regel kann der Rollenwechsel bis zu mehreren Minuten dauern. Das Erstellen zusätzlicher sekundärer Cluster kann jedoch je nach Größe Ihrer Datenbank und der physischen Entfernung zwischen den Regionen einige Minuten bis mehrere Stunden dauern.

Wenn der Umstellungs-Prozess abgeschlossen ist, kann der hochgestufte Aurora-DB-Cluster Schreibvorgänge für die Aurora Global Database verarbeiten. Stellen Sie sicher, dass Sie den Endpunkt für Ihre Anwendung ändern, um den neuen Endpunkt zu verwenden. Wenn Sie die angegebenen Namen beim Erstellen der globalen Aurora-Datenbank akzeptiert haben, können Sie den Endpunkt ändern, indem Sie `-ro` aus der Endpunkt-Zeichenfolge des hochgestuften Clusters in Ihrer Anwendung entfernen.

Beispielsweise wird der Endpunkt des sekundären Clusters `my-global.cluster-ro-aaaaaabbbbbb.us-west-1.rds.amazonaws.com` zu `my-global.cluster-aaaaaabbbbbb.us-west-1.rds.amazonaws.com`, wenn dieser Cluster zum primären Cluster hochgestuft wird.

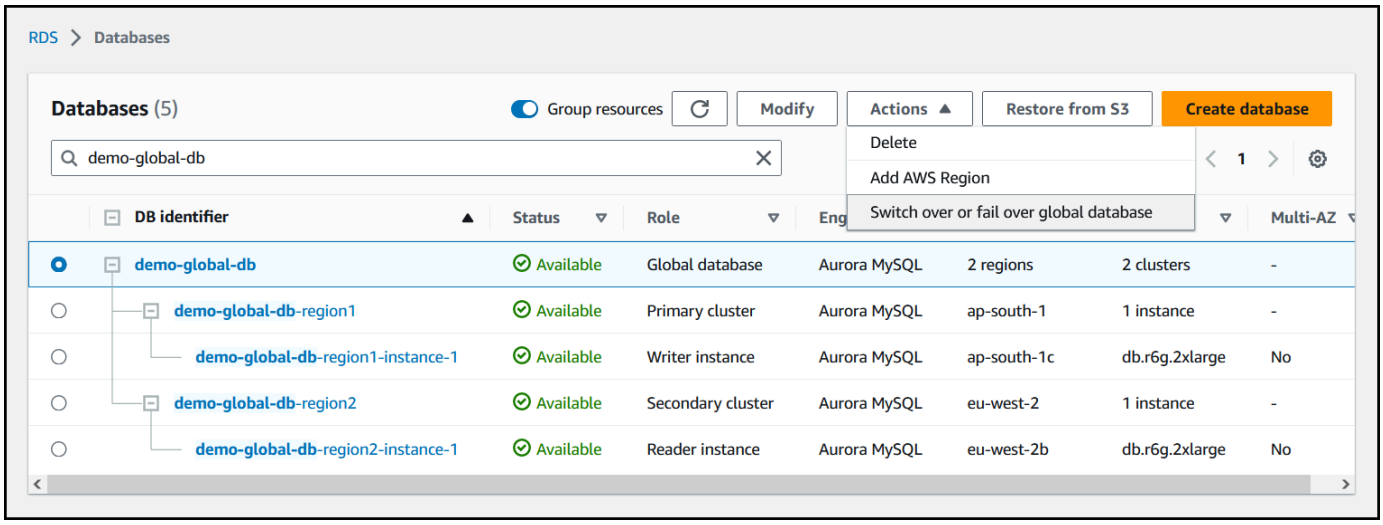
Wenn Sie RDS-Proxy verwenden, stellen Sie sicher, dass Sie die Schreibvorgänge Ihrer Anwendung an den entsprechenden Lese-/Schreibendpunkt des Proxys umleiten, der dem neuen primären Cluster zugeordnet ist. Dieser Proxy-Endpunkt kann der Standardendpunkt oder ein benutzerdefinierter Lese-/Schreibendpunkt sein. Weitere Informationen finden Sie unter So funktionieren RDS-Proxy-Endpunkte mit globalen Datenbanken.

Sie können Ihre globale Aurora-Datenbank mithilfe der AWS Management Console, der oder der AWS CLI RDS-API umschalten.

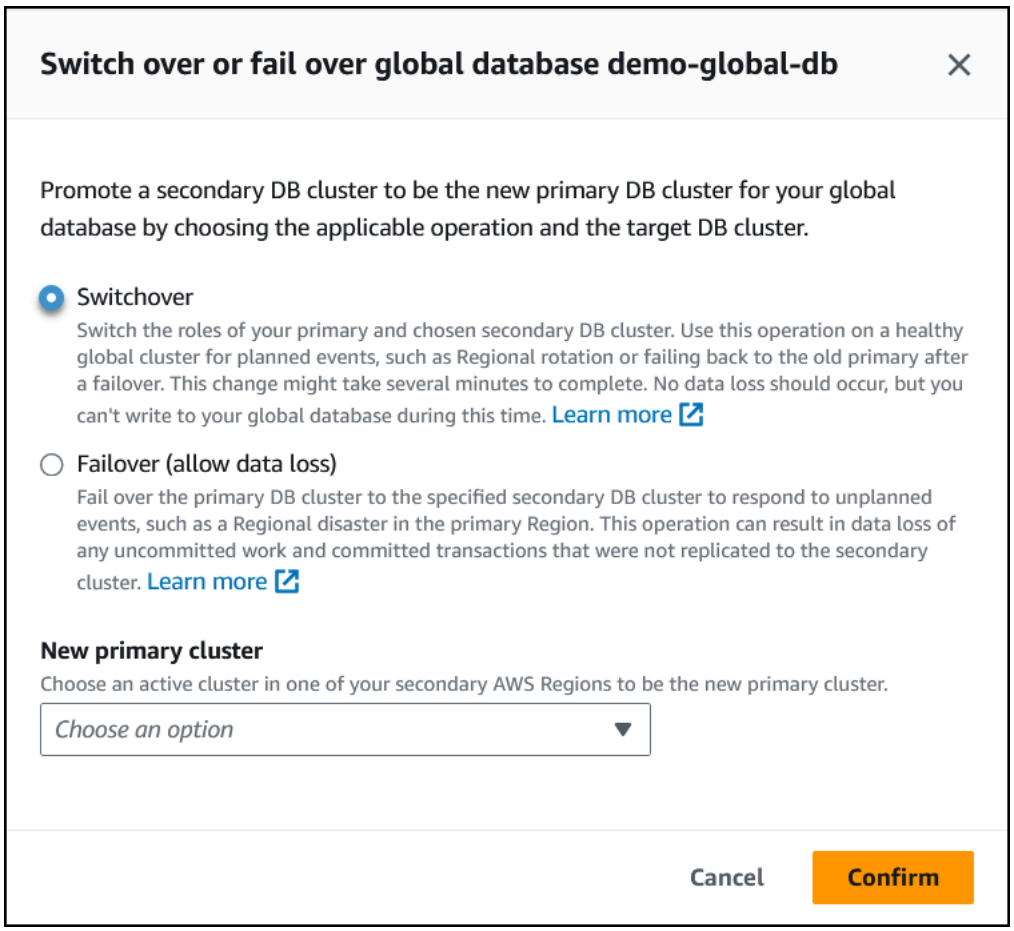
Konsole

So führen Sie eine Umstellung in Ihrer Aurora Global Database durch

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Datenbanken aus und suchen Sie die Aurora Global Database, für die Sie eine Umstellung ausführen möchten.
3. Wählen Sie im Menü Aktionen die Option Failover für globale Datenbank ausführen aus.

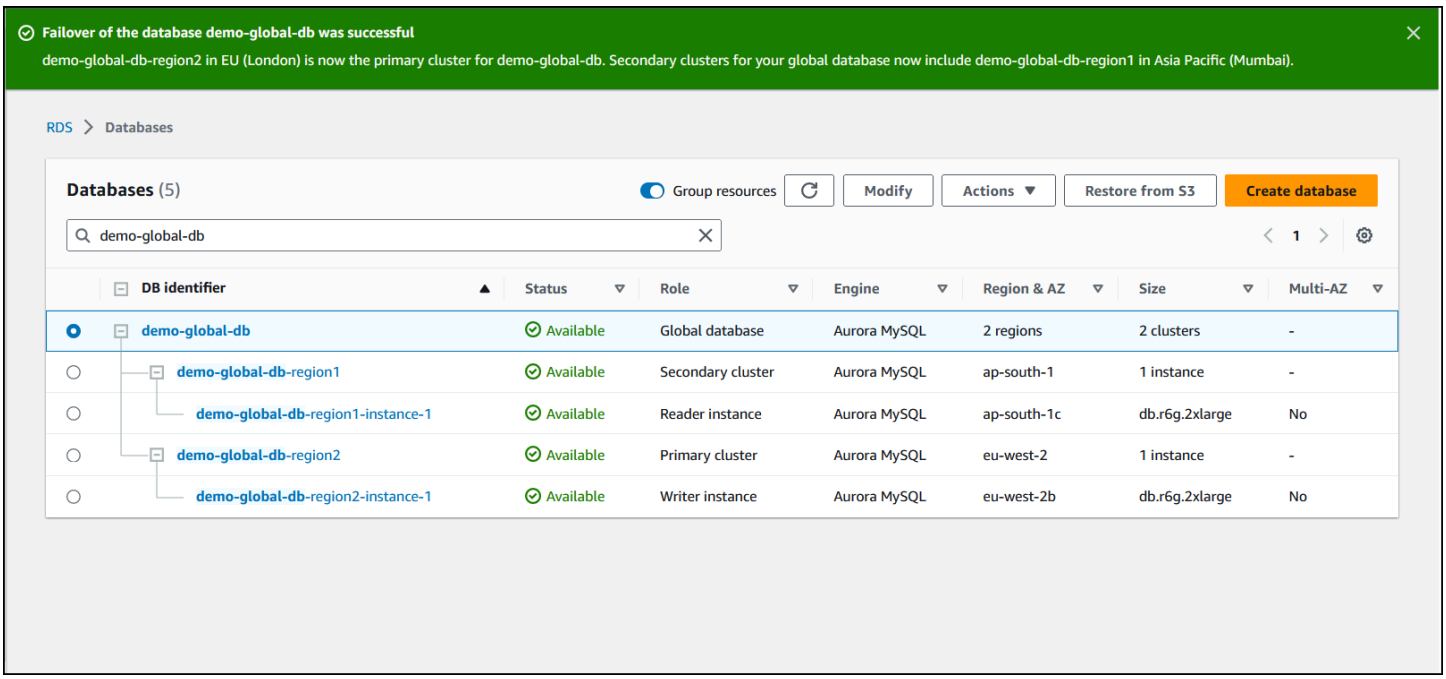


4. Wählen Sie Umschaltung.



5. Wählen Sie für Neuer primärer Cluster einen aktiven Cluster in einem Ihrer sekundären AWS-Regionen Cluster als neuen primären Cluster aus.
6. Wählen Sie Bestätigen aus.

Wenn die Umstellung abgeschlossen ist, werden die Aurora-DB-Cluster und ihr aktueller Status wie im Folgenden dargestellt in der Liste Datenbanken angezeigt.



AWS CLI

So führen Sie eine Umstellung auf einer Aurora Global Database durch

Verwenden Sie den `switchover-global-cluster`-CLI-Befehl, um eine Umstellung für Ihre Aurora Global Database auszuführen. Mit dem Befehl können Sie Werte für die folgenden Parameter übertragen.

- `--region`— Geben Sie an AWS-Region , wo der primäre DB-Cluster der globalen Aurora-Datenbank läuft.
- `--global-cluster-identifier` – Geben Sie den Namen Ihrer globalen Aurora-Datenbank an.
- `--target-db-cluster-identifier` – Geben Sie den Amazon-Ressourcennamen (ARN) des Aurora-DB-Clusters an, den Sie als primäres Cluster für die globale Aurora-Datenbank hochstufen möchten.

Für LinuxmacOS, oderUnix:

```
aws rds --region region_of_primary \
   switchover-global-cluster --global-cluster-identifier global_database_id \
  --target-db-cluster-identifier arn_of_secondary_to_promote
```

Windows:

```
aws rds --region region_of_primary ^
   switchover-global-cluster --global-cluster-identifier global_database_id ^
  --target-db-cluster-identifier arn_of_secondary_to_promote
```

RDS-API

Um zu einer globalen Aurora-Datenbank zu wechseln, führen Sie den SwitchoverGlobalClusterAPI-Vorgang aus.

Verwalten von RPOs für Aurora PostgreSQL–basierte globale Datenbanken

Mit einer Aurora PostgreSQL–basierten globalen Datenbank können Sie den Recovery Point Objective (RPO)-Wert für Ihre globale Aurora-Datenbank mithilfe des Parameters `rds.global_db_rpo` verwalten. RPO gibt die maximale Datenmenge an, die im Falle eines Ausfalls verloren gehen kann.

Wenn Sie eine RPO für Ihre Aurora PostgreSQL–basierte globale Datenbank festlegen, überwacht Aurora die RPO-Verzögerungszeit aller sekundären Cluster, um sicherzustellen, dass mindestens ein sekundärer Cluster innerhalb des angestrebten RPO-Bereichs liegt. Die RPO-Verzögerungszeit ist eine weitere zeitbasierte Metrik.

Das RPO wird verwendet, wenn Ihre Datenbank AWS-Region nach einem Failover den Betrieb in einer neuen Datenbank wieder aufnimmt. Aurora bewertet RPO- und RPO-Verzögerungszeiten, um Transaktionen auf dem primären Netzwerk wie folgt zu übertragen (oder zu blockieren):

- Die Transaktion wird durchgeführt, wenn mindestens ein sekundärer DB-Cluster eine RPO-Verzögerungszeit hat, die kleiner ist als die RPO.
- Die Transaktion wird blockiert, wenn alle sekundären DB-Cluster RPO-Verzögerungszeiten haben, die größer sind als die RPO. Außerdem wird das Ereignis in der PostgreSQL-Protokolldatei erfasst und es werden Warteereignisse ausgegeben, die die blockierten Sessions anzeigen.

Wenn sich also alle sekundären Cluster hinter der Ziel-RPO befinden, pausiert Aurora die Transaktionen im primären Cluster, bis mindestens einer der sekundären Cluster den Rückstand aufholt. Pausierte Transaktionen werden fortgesetzt und übergeben, sobald die Verzögerungszeit mindestens eines sekundären DB-Clusters geringer ist als die RPO. Das Ergebnis ist, dass keine Transaktionen übertragen werden können, bis die RPO erreicht ist.

Der `rds.global_db_rpo`-Parameter ist dynamisch. Wenn Sie nicht möchten, dass alle Schreibtransaktionen angehalten werden, bis die Verzögerung ausreichend abnimmt, können Sie ihn

schnell zurücksetzen. In diesem Fall erkennt Aurora die Änderung und implementiert sie nach einer kurzen Verzögerung.

> **Important**
>
> In einer globalen Datenbank mit nur zwei Regionen empfehlen wir, den Standardwert des Parameters `rds.global_db_rpo` in der Parametergruppe der sekundären Region beizubehalten. Andernfalls könnte ein Failover zu dieser Region aufgrund eines Verlusts der primären Region dazu führen, dass Aurora Transaktionen unterbricht. Warten Sie stattdessen, bis Aurora den Neuaufbau des Clusters in der alten ausgefallenen Region abgeschlossen hat, bevor Sie diesen Parameter ändern, um ein maximales RPO zu erzwingen.

Wenn Sie diesen Parameter wie folgt festlegen, können Sie auch die von ihm generierten Metriken überwachen. Sie können dies tun, indem Sie `psql` oder ein anderes Tool verwenden, um den primären DB-Cluster der globalen Aurora-Datenbank abzufragen und detaillierte Informationen über den Betrieb Ihrer Aurora PostgreSQL–basierten globalen Datenbank zu erhalten. Um zu erfahren wie, siehe Überwachen von Aurora-PostgreSQL-basierten globalen Datenbanken.

Themen

- Festlegen des Recovery Point Objective
- Anzeigen des Recovery Point Objective (Zeitraums zwischen zwei Datensicherungen)
- Deaktivieren des Recovery Point Objective

Festlegen des Recovery Point Objective

Der Parameter `rds.global_db_rpo` steuert die RPO-Einstellung für eine PostgreSQL-Datenbank. Dieser Parameter wird von Aurora PostgreSQL unterstützt. Gültige Werte für `rds.global_db_rpo` liegen zwischen 20 und 2.147.483.647 Sekunden (68 Jahre). Wählen Sie einen realistischen Wert, der Ihren Geschäftsanforderungen und Ihrem Anwendungsfall entspricht. Wenn Sie beispielsweise bis zu 10 Minuten für Ihre RPO festlegen möchten, dann setzen Sie den Wert auf 600.

Sie können diesen Wert für Ihre Aurora-PostgreSQL-basierte globale Datenbank festlegen, indem Sie die AWS Management Console, die AWS CLI oder die RDS-API verwenden.

Konsole

So legen Sie den RPO fest:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie den primären Cluster Ihrer globalen Aurora-Datenbank und öffnen Sie die Registerkarte Konfiguration, um die DB-Cluster-Parametergruppe zu suchen. Die Standardparametergruppe für ein primäres DB-Cluster mit Aurora PostgreSQL 11.7 ist beispielsweise `default.aurora-postgresql11`.

   Parametergruppen können nicht direkt bearbeitet werden. Stattdessen führen Sie die folgenden Schritte aus:

   - Erstellen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe, wobei Sie die entsprechende Standardparametergruppe als Ausgangspunkt verwenden. So erstellen Sie beispielsweise eine benutzerdefinierte DB-Cluster-Parametergruppe basierend au `default.aurora-postgresql11`.
   - Legen Sie in Ihrer benutzerdefinierten DB-Parametergruppe den Wert des Parameters rds.global_db_rpo fest, der Ihrem Anwendungsfall entspricht. Gültige Werte liegen zwischen 20 Sekunden und dem maximalen ganzzahligen Wert von 2.147.483.647 (68 Jahre).
   - Wenden Sie die geänderte DB-Cluster-Parametergruppe auf Ihr Aurora-DB-Cluster an.

Weitere Informationen finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe.

AWS CLI

Verwenden Sie den CLI-Befehl modify-db-cluster-parameter-group, um den `rds.global_db_rpo` Parameter festzulegen. Geben Sie im Befehl den Namen der Parametergruppe Ihres primären Clusters und die Werte für den RPO-Parameter an.

Im folgenden Beispiel wird die RPO für die primäre DB-Cluster-Parametergruppe namens auf 600 Sekunden (10 Minuten) festgeleg `my_custom_global_parameter_group`.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name my_custom_global_parameter_group \
```

```
    --parameters
 "ParameterName=rds.global_db_rpo,ParameterValue=600,ApplyMethod=immediate"
```

Windows:

```
aws rds modify-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name my_custom_global_parameter_group ^
    --parameters
 "ParameterName=rds.global_db_rpo,ParameterValue=600,ApplyMethod=immediate"
```

RDS-API

Verwenden Sie den Amazon RDS ClusterParameterGroupModifyDB-API-Vorgang, um den `rds.global_db_rpo` Parameter zu ändern.

Anzeigen des Recovery Point Objective (Zeitraums zwischen zwei Datensicherungen)

Die Recovery Point Objective (RPO) einer globalen Datenbank wird im `rds.global_db_rpo`-Parameter für jeden DB-Cluster gespeichert. Sie können eine Verbindung zum Endpunkt für den sekundären Cluster herstellen, den Sie anzeigen möchten, und mit `psql` die Instance nach diesem Wert abfragen.

```
db-name=>show rds.global_db_rpo;
```

Wenn dieser Parameter nicht festgelegt ist, gibt die Abfrage Folgendes zurück:

```
rds.global_db_rpo
-------------------
 -1
(1 row)
```

Diese nächste Antwort stammt von einem sekundären DB-Cluster mit einer RPO-Einstellung von einer Minute.

```
rds.global_db_rpo
-------------------
 60
(1 row)
```

Sie können auch die CLI verwenden, um herauszufinden, ob in einem der Aurora-DB-Cluster `rds.global_db_rpo` aktiviert ist, indem Sie die CLI verwenden, um die Werte aller `user`-Parameter für den Cluster zu erhalten.

FürLinux, odermacOS: Unix

```
aws rds describe-db-cluster-parameters \
 --db-cluster-parameter-group-name lab-test-apg-global \
 --source user
```

Windows:

```
aws rds describe-db-cluster-parameters ^
 --db-cluster-parameter-group-name lab-test-apg-global *
 --source user
```

Der Befehl gibt für alle `user`-Parameter, die keine `default-engine`- oder `system`-DB-Cluster-Parameter sind, eine Ausgabe zurück, die der folgenden Ausgabe ähnelt.

```
{
    "Parameters": [
        {
            "ParameterName": "rds.global_db_rpo",
            "ParameterValue": "60",
            "Description": "(s) Recovery point objective threshold, in seconds, that
 blocks user commits when it is violated.",
            "Source": "user",
            "ApplyType": "dynamic",
            "DataType": "integer",
            "AllowedValues": "20-2147483647",
            "IsModifiable": true,
            "ApplyMethod": "immediate",
            "SupportedEngineModes": [
                "provisioned"
            ]
        }
    ]
}
```

Weitere Informationen zum Anzeigen von Parametern der Clusterparametergruppe finden Sie unter Anzeigen der Parameterwerte für eine DB-Cluster-Parametergruppe.

Deaktivieren des Recovery Point Objective

Um den RPO zu deaktivieren, setzen Sie den `rds.global_db_rpo`-Parameter zurück. Sie können Parameter mithilfe der AWS Management Console AWS CLI, der oder der RDS-API zurücksetzen.

Konsole

So deaktivieren Sie den RPO:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Parameter groups (Parametergruppen) aus.
3. Wählen Sie in der Liste Ihre primäre DB-Cluster-Parametergruppe aus.
4. Wählen Sie Parameter bearbeiten aus.
5. Wählen Sie das Feld neben dem Parameter rds.global_db_rpo aus.
6. Klicken Sie auf Reset (Zurücksetzen).
7. Wenn auf dem Bildschirm Reset parameters in DB parameter group (Parameter in DB-Parametergruppe zurücksetzen) angezeigt wird, wählen Sie Reset parameters (Parameter zurücksetzen) aus.

Weitere Informationen zum Zurücksetzen eines Parameters mit der Konsole finden Sie unter Ändern von Parametern in einer DB-Cluster-Parametergruppe.

AWS CLI

Verwenden Sie den Befehl reset-db-cluster-parameter-group, um den `rds.global_db_rpo` Parameter zurückzusetzen.

Für LinuxmacOS, oderUnix:

```
aws rds reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name global_db_cluster_parameter_group \
    --parameters "ParameterName=rds.global_db_rpo,ApplyMethod=immediate"
```

Windows:

```
aws rds reset-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name global_db_cluster_parameter_group ^
```

```
    --parameters "ParameterName=rds.global_db_rpo,ApplyMethod=immediate"
```

RDS-API

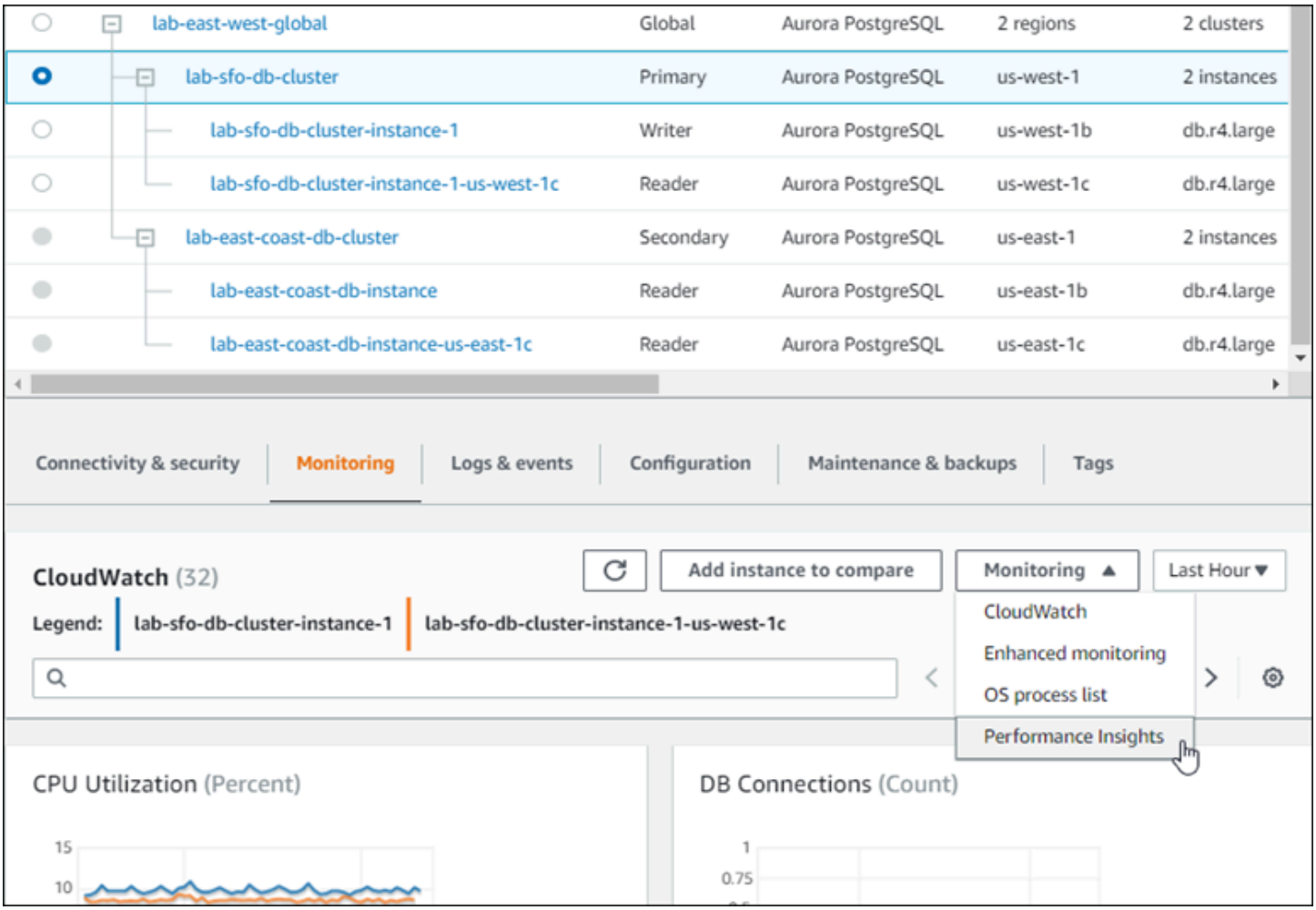
Verwenden Sie den Amazon RDS-API-Vorgang ResetDB ClusterParameterGroup, um den `rds.global_db_rpo` Parameter zurückzusetzen.

Überwachung einer Amazon Aurora Global Database

Wenn Sie die Aurora-DB-Cluster erstellen, aus denen Ihre Aurora globale Datenbank besteht, können Sie viele Optionen auswählen, mit denen Sie die Leistung Ihres DB-Clusters überwachen können. Diese Optionen umfassen Folgendes:

- Amazon RDS Performance Insights – Es ermöglicht Performance-Schema in der zugrunde liegenden Aurora-Datenbank-Engine. Weitere Informationen über Performance Insights und Aurora globale Datenbanken finden Sie unter Überwachung einer Amazon Aurora globalen Datenbank mit Amazon RDS Performance Insights.
- „Enhanced Monitoring“ (Erweiterte Überwachung) – Es generiert Metriken für die Prozess- oder Thread-Nutzung auf der CPU. Weitere Informationen zur erweiterten Überwachung finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).
- Amazon CloudWatch Logs – Es publiziert festgelegte Protokolltypen nach CloudWatch Logs. Fehlerprotokolle werden standardmäßig veröffentlicht. Sie können jedoch andere für Ihre Aurora-Datenbank-Engine spezifische Protokolle auswählen.
  - Für Aurora MySQL–basierte Aurora-DB-Cluster können Sie das Audit-Log, das allgemeine Protokoll und das langsame Abfrage-Log exportieren.
  - Für Aurora PostgreSQL–basierte Aurora-DB-Cluster können Sie das PostgreSQL-Protokoll exportieren.
- Für Aurora-MySQL-basierte globale Datenbanken können Sie bestimmte `information_schema`-Tabellen verwenden, um den Status Ihrer globalen Aurora-Datenbank und deren Instances zu überprüfen. Um zu erfahren wie dies geht, vgl. Überwachung der Aurora-MySQL-basierten globalen Datenbanken.
- Für Aurora-PostgreSQL-basierte globale Datenbanken können Sie bestimmte Funktionen verwenden, um den Status Ihrer Aurora globalen Datenbank und ihrer Instances zu überprüfen. Um zu erfahren wie dies geht, vgl. Überwachen von Aurora-PostgreSQL-basierten globalen Datenbanken.

Der folgende Screenshot zeigt einige der Optionen, die auf der Registerkarte Überwachung eines primären Aurora-DB-Clusters in einer Aurora globalen Datenbank verfügbar sind.



Weitere Informationen finden Sie unter Überwachung von Metriken in einem Amazon-Aurora-Cluster.

Überwachung einer Amazon Aurora globalen Datenbank mit Amazon RDS Performance Insights

Sie können Amazon RDS Performance Insights für Ihre globalen Aurora-Datenbanken verwenden. Sie aktivieren diese Funktion einzeln für jeden Aurora-DB-Cluster in Ihrer Aurora globalen Datenbank. Dazu wählen Sie Performance Insights aktivieren im Abschnitt Zusätzliche Konfiguration der Seite „Datenbank erstellen“. Oder Sie können Ihre Aurora-DB-Cluster ändern, um diese Funktion zu verwenden, nachdem sie in Betrieb sind. Sie können Performance Insights für jeden Cluster, der zur Aurora globalen Datenbank gehört, aktivieren bzw. deaktivieren.

Die von Performance Insights erstellten Berichte gelten für jeden Cluster in der globalen Datenbank. Wenn Sie einer globalen Aurora-Datenbank, die Performance Insights bereits verwendet, eine neue

sekundäre AWS-Region hinzufügen, müssen Sie Performance Insights im neu hinzugefügten Cluster aktivieren. Die Performance Insights-Einstellung wird nicht von der vorhandenen globalen Datenbank übernommen.

Sie können beim Anzeigen der Performance Insights-Seite für eine DB-Instance, die einer globalen Datenank angefügt ist, zwischen AWS-Regionen wechseln. Möglicherweise werden unmittelbar nach dem Wechsel der AWS-Regionen allerdings keine Leistungsdaten angezeigt. Auch wenn die DB-Instances in jeder AWS-Region identische Namen tragen, weicht die zugeordnete Performance Insights-URL für jede DB-Instance ab. Wählen Sie nach dem Wechsel der AWS-Regionen den Namen der DB-Instance erneut im Performance Insights-Navigationsbereich aus.

Für DB-Instances, die einer globalen Datenbank zugeordnet sind, können sich in jeder AWS-Region andere Faktoren auf die Leistung auswirken. Die DB-Instances können in jeder AWS-Region z. B. eine andere Kapazität aufweisen.

Weitere Informationen zum Verwenden von Performance Insights finden Sie unter Überwachung mit Performance Insights auf .

Überwachung von globalen Aurora-Datenbanken mithilfe von Datenbank-Aktivitätsstreams

Durch die Verwendung von Datenbank-Aktivitätsstreams können Sie Alarme für die Prüfung von Aktivitäten in den DB-Clustern Ihrer globalen Datenbank überwachen und einstellen. Sie starten einen Datenbank-Aktivitätsstream separat auf jedem DB-Cluster. Jeder Cluster liefert Auditdaten innerhalb seiner eigenen AWS-Region an seinen eigenen Kinesis-Stream. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.

Überwachung der Aurora-MySQL-basierten globalen Datenbanken

Um den Status einer auf Aurora MySQL basierenden globalen Datenbank abzurufen, fragen Sie die Tabellen information_schema.aurora_global_db_status und information_schema.aurora_global_db_instance_

> **Note**
>
> Die Tabellen `information_schema.aurora_global_db_status` und `information_schema.aurora_global_db_instance_status` sind nur mit globalen Aurora-MySQL-Datenbanken ab Version 3.04.0 verfügbar.

So überwachen Sie eine Aurora-MySQL-basierte globale Datenbank

1. Stellen Sie mithilfe eines MySQL-Clients eine Verbindung zum primären Cluster-Endpunkt der globalen Datenbank her. Weitere Informationen zum Herstellen einer Verbindung finden Sie unter Herstellen einer Verbindung mit einer Amazon Aurora Global Database.
2. Fragen Sie die Tabelle `information_schema.aurora_global_db_status` in einem mysql-Befehl ab, um die primären und sekundären Volumes aufzulisten. Diese Abfrage gibt die Verzögerungszeiten der sekundären DB-Cluster der globalen Datenbank zurück, wie im folgenden Beispiel dargestellt.

```
mysql> select * from information_schema.aurora_global_db_status;
```

```
AWS_REGION | HIGHEST_LSN_WRITTEN | DURABILITY_LAG_IN_MILLISECONDS |
 RPO_LAG_IN_MILLISECONDS | LAST_LAG_CALCULATION_TIMESTAMP | OLDEST_READ_VIEW_TRX_ID
-----------+---------------------+--------------------------------
+------------------------+---------------------------------
+------------------------
us-east-1  |           183537946 |                              0   |
      0 |  1970-01-01 00:00:00.000000     |               0
us-west-2  |           183537944 |                              428 |
      0 |  2023-02-18 01:26:41.925000     |               20806982
(2 rows)
```

   Die Ausgabe enthält eine Zeile für jeden DB-Cluster der globalen Datenbank, die die folgenden Spalten enthält:

   - AWS_REGION – die AWS-Region, in der sich dieser DB-Cluster befindet. Tabellen, in denen die AWS-Regionen nach Engine aufgelistet sind, finden Sie unter Regionen und Availability Zones.
   - HIGHEST_LSN_WRITTEN – die höchste Log-Sequenznummer (LSN), die derzeit auf diesem DB-Cluster geschrieben wird.

     Eine Log-Sequenznummer (LSN) ist eine eindeutige fortlaufende Nummer, die einen Datensatz im Datenbank-Transaktionsprotokoll identifiziert. LSNs werden so angeordnet, dass eine größere LSN eine spätere Transaktion darstellt.
   - DURABILITY_LAG_IN_MILLISECONDS – die Differenz der Zeitstempelwerte zwischen `HIGHEST_LSN_WRITTEN` in einem sekundären DB-Cluster

und HIGHEST_LSN_WRITTEN im primären DB-Cluster. Der Wert ist immer 0 im primären DB-Cluster der globalen Aurora-Datenbank.

- RPO_LAG_IN_MILLISECONDS – die Verzögerung des Zeitraums im Hinblick auf Recovery Point Objective (RPO). Die RPO-Verzögerung ist die Zeit, die benötigt wird, bis die letzte Benutzertransaktion COMMIT auf einem sekundären DB-Cluster gespeichert wird, nachdem sie auf dem primären DB-Cluster einer globalen Aurora-Datenbank abgelegt wurde. Der Wert ist immer 0 im primären DB-Cluster der globalen Aurora-Datenbank.

  Einfach ausgedrückt berechnet diese Metrik das Recovery Point Objective für jeden DB-Cluster voon Aurora MySQL in der globalen Aurora-Datenbank, d. h., wie viele Daten bei einem Ausfall verloren gehen könnten. Wie die Verzögerung wird auch RPO zeitlich gemessen.
- LAST_LAG_CALCULATION_TIMESTAMP – der Zeitstempel mit Angabe des Zeitpunkts, zu dem die Werte für DURABILITY_LAG_IN_MILLISECONDS und RPO_LAG_IN_MILLISECONDS zuletzt berechnet wurden. Ein Zeitwert wie 1970-01-01 00:00:00+00 bedeutet, dass dies der primäre DB-Cluster ist.
- OLDEST_READ_VIEW_TRX_ID – die ID der ältesten Transaktion, bis zu der die Writer-DB-Instance Daten löschen kann.

3. Fragen Sie die Tabelle information_schema.aurora_global_db_instance_status ab, um alle sekundären DB-Instances sowohl für den primären DB-Cluster als auch für sekundäre DB-Cluster aufzulisten.

```
mysql> select * from information_schema.aurora_global_db_instance_status;
```

```
SERVER_ID            |              SESSION_ID              | AWS_REGION
 | DURABLE_LSN | HIGHEST_LSN_RECEIVED | OLDEST_READ_VIEW_TRX_ID |
 OLDEST_READ_VIEW_LSN | VISIBILITY_LAG_IN_MSEC
---------------------+--------------------------------------+------------
+-------------+----------------------+------------------------
+----------------------+------------------------
ams-gdb-primary-i2   | MASTER_SESSION_ID                    | us-east-1  |
 183537698   |                    0 |                      0 |
 0 |                      0
ams-gdb-secondary-i1 | cc43165b-bdc6-4651-abbf-4f74f08bf931 | us-west-2  |
 183537689   |            183537692 |                20806928 |
 183537682 |                      0
```

```
ams-gdb-secondary-i2 | 53303ff0-70b5-411f-bc86-28d7a53f8c19 | us-west-2  |
 183537689   |            183537692 |                20806928 |
 183537682 |                   677
ams-gdb-primary-i1   | 5af1e20f-43db-421f-9f0d-2b92774c7d02 | us-east-1  |
 183537697   |            183537698 |                20806930 |
 183537691 |                    21
(4 rows)
```

Die Ausgabe enthält eine Zeile für jede DB-Instance der globalen Datenbank, die die folgenden Spalten enthält:

- SERVER_ID – die Server-ID für die DB-Instance.
- SESSION_ID – eine eindeutige ID für die aktuelle Sitzung. Der Wert `MASTER_SESSION_ID` bezeichnet die (primäre) Writer-DB-Instance.
- AWS_REGION – die AWS-Region, in der sich diese DB-Instance befindet. Tabellen, in denen die AWS-Regionen nach Engine aufgelistet sind, finden Sie unter Regionen und Availability Zones.
- DURABLE_LSN – die LSN, die im Speicher als dauerhaft definiert wurde.
- HIGHEST_LSN_RECEIVED – die höchste LSN, die die DB-Instance von der DB-Writer-Instance empfangen hat.
- OLDEST_READ_VIEW_TRX_ID – die ID der ältesten Transaktion, bis zu der die Writer-DB-Instance Daten löschen kann.
- OLDEST_READ_VIEW_LSN – die älteste LSN, die von der DB-Instance zum Lesen aus dem Speicher verwendet wird.
- VISIBILITY_LAG_IN_MSEC – für Reader im primären DB-Cluster, wie weit diese DB-Instance der Writer-DB-Instance in Millisekunden hinterherhinkt. Für Reader in einem sekundären DB-Cluster, wie weit diese DB-Instance dem sekundären Volume in Millisekunden hinterherhinkt.

Um zu sehen, wie sich diese Werte im Laufe der Zeit verändern, betrachten Sie den folgenden Transaktionsblock, in dem eine Tabelleneinfügung eine Stunde dauert.

```
mysql> BEGIN;
mysql> INSERT INTO table1 SELECT Large_Data_That_Takes_1_Hr_To_Insert;
mysql> COMMIT;
```

In einigen Fällen kann es nach der `BEGIN`-Anweisung zu einer Netzwerktrennung zwischen dem primären DB-Cluster und dem sekundären DB-Cluster kommen. In diesem Fall beginnt der

Wert DURABILITY_LAG_IN_MILLISECONDS des sekundäre DB-Clusters zu steigen. Am Ende der `INSERT`-Anweisung beträgt der Wert DURABILITY_LAG_IN_MILLISECONDS 1 Stunde. Der Wert RPO_LAG_IN_MILLISECOND ist jedoch 0, da alle Benutzerdaten, die zwischen dem primären DB-Cluster und dem sekundären DB-Cluster übertragen werden, immer noch dieselben sind. Sobald die `COMMIT`-Anweisung abgeschlossen ist, steigt der Wert RPO_LAG_IN_MILLISECONDSWert steigt.

Überwachen von Aurora-PostgreSQL-basierten globalen Datenbanken

Verwenden Sie die Funktionen `aurora_global_db_status` und `aurora_global_db_instance_status`, um den Status einer Aurora-PostgreSQL-basierten globalen Datenbank anzuzeigen.

> **Note**
>
> Die Funktionen `aurora_global_db_status` und `aurora_global_db_instance_status` werden nur von Aurora PostgreSQL unterstützt.

So überwachen Sie eine Aurora PostgreSQL-basierte globale Datenbank

1. Stellen Sie mithilfe eines PostgreSQL-Dienstprogramms wie psql eine Verbindung zum primären Cluster-Endpunkt der globalen Datenbank her. Weitere Informationen zum Herstellen einer Verbindung finden Sie unter Herstellen einer Verbindung mit einer Amazon Aurora Global Database.
2. Sie verwenden die Funktion `aurora_global_db_status` in einem psql-Befehl, um die primären und sekundären Volumes aufzulisten. Dadurch werden die Verzögerungszeiten der sekundären DB-Cluster der globalen Datenbank angezeigt.

```
postgres=> select * from aurora_global_db_status();
```

```
aws_region | highest_lsn_written | durability_lag_in_msec | rpo_lag_in_msec |
 last_lag_calculation_time  | feedback_epoch | feedback_xmin
------------+---------------------+------------------------+-----------------
+----------------------------+----------------+--------------
us-east-1  |         93763984222 |                     -1 |              -1 |
 1970-01-01 00:00:00+00     |              0 |              0
us-west-2  |         93763984222 |                    900 |            1090 |
 2020-05-12 22:49:14.328+00 |              2 |    3315479243
```

```
(2 rows)
```

Die Ausgabe enthält eine Zeile für jeden DB-Cluster der globalen Datenbank, die die folgenden Spalten enthält:

- aws_region Die AWS-Region, in der sich dieser DB-Cluster befindet. Tabellen, in denen die AWS-Regionen nach Engine aufgelistet sind, finden Sie unter Regionen und Availability Zones.
- highest_lsn_written – Die höchste Log-Sequenznummer (LSN), die derzeit auf diesem DB-Cluster geschrieben wird.

  Eine Log-Sequenznummer (LSN) ist eine eindeutige fortlaufende Nummer, die einen Datensatz im Datenbank-Transaktionsprotokoll identifiziert. LSNs werden so angeordnet, dass eine größere LSN eine spätere Transaktion darstellt.
- durability_lag_in_msec – Die Zeitstempeldifferenz zwischen der höchsten Log-Sequenznummer, die auf einem sekundären DB-Cluster (`highest_lsn_written`) geschrieben wurde, und der `highest_lsn_written` auf dem primären DB-Cluster.
- rpo_lag_in_msec – Die Verzögerung des Zeitraums zwischen zwei Datensicherungen (RPO). Diese Verzögerung ist die Zeitdifferenz zwischen dem letzten Benutzertransaktions-Commit, der auf einem sekundären DB-Cluster gespeichert ist, und dem letzten Benutzertransaktions-Commit, der auf dem primären DB-Cluster gespeichert ist.
- last_lag_calculation_time – Der Zeitstempel mit Angabe des Zeitpunkts, zu dem die Werte für `durability_lag_in_msec` und `rpo_lag_in_msec` zuletzt berechnet wurden.
- feedback_epoch – Die Epoche, die ein sekundärer DB-Cluster beim Erzeugen von Hot-Standby-Informationen verwendet.

  Hot-Standby bedeutet, dass ein DB-Cluster eine Verbindung herstellen und Abfragen durchführen kann, während sich der Server im Wiederherstellungs- oder Standby-Modus befindet. Hot-Standby-Feedbacks sind Informationen über den DB-Cluster, wenn dieser sich im Hot-Standby-Modus befindet. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation zu Hot Standby.
- feedback_xmin – Die minimale (älteste) aktive Transaktions-ID, die von einem sekundären DB-Cluster verwendet wird.

3. Verwenden Sie die Funktion `aurora_global_db_instance_status`, um alle sekundären DB-Instances sowohl für den primären DB-Cluster als auch für sekundäre DB-Cluster aufzulisten.

```
postgres=> select * from aurora_global_db_instance_status();
```

```
server_id                                    |              session_id
  | aws_region | durable_lsn | highest_lsn_rcvd | feedback_epoch | feedback_xmin |
 oldest_read_view_lsn | visibility_lag_in_msec
----------------------------------------------+--------------------------------------
+------------+-------------+------------------+----------------+--------------
+----------------------+-----------------------
apg-global-db-rpo-mammothrw-elephantro-1-n1 | MASTER_SESSION_ID
 | us-east-1  | 93763985102 |                  |                |              |
                    |
apg-global-db-rpo-mammothrw-elephantro-1-n2 | f38430cf-6576-479a-b296-dc06b1b1964a
 | us-east-1  | 93763985099 |      93763985102 |              2 |    3315479243 |
       93763985095 |                    10
apg-global-db-rpo-elephantro-mammothrw-n1   | 0d9f1d98-04ad-4aa4-8fdd-e08674cbbbfe
 | us-west-2  | 93763985095 |      93763985099 |              2 |    3315479243 |
       93763985089 |                  1017
(3 rows)
```

Die Ausgabe enthält eine Zeile für jede DB-Instance der globalen Datenbank, die die folgenden Spalten enthält:

- server_id – Die Server-ID für die DB-Instance.
- session_id – Eine eindeutige ID für die aktuelle Sitzung.
- aws_region Die AWS-Region, in der sich diese DB-Instance befindet. Tabellen, in denen die AWS-Regionen nach Engine aufgelistet sind, finden Sie unter Regionen und Availability Zones.
- durable_lsn – Der LSN wurde im Speicher dauerhaft gemacht.
- highest_lsn_rcvd – Die höchste LSN, die die DB-Instance von der DB-Writer-Instance empfangen hat.
- feedback_epoch – Die Epoche, die die DB-Instance beim Erzeugen der Hot-Standby-Informationen verwendet.

  Hot standby bedeutet, dass eine DB-Instance eine Verbindung herstellen und Abfragen durchführen kann, während sich der Server im Wiederherstellungs- oder Standby-Modus befindet. Hot-Standby-Feedbacks sind Informationen über die DB-Instance, wenn diese

sich im Hot-Standby-Modus befindet. Weitere Informationen finden Sie in der PostgreSQL-Dokumentation zu Hot Standby.

- feedback_xmin – Die minimale (älteste) aktive Transaktions-ID, die von der DB-Instance verwendet wird.
- oldest_read_view_lsn – Die älteste LSN, die von der DB-Instance zum Lesen aus dem Speicher verwendet wird.
- visibility_lag_in_msec – Wie stark diese DB-Instance gegenüber der DB-Schreiber-Instance zeitlich verzögert ist.

Um zu sehen, wie sich diese Werte im Laufe der Zeit verändern, betrachten Sie den folgenden Transaktionsblock, in dem eine Tabelleneinfügung eine Stunde dauert.

```
psql> BEGIN;
psql> INSERT INTO table1 SELECT Large_Data_That_Takes_1_Hr_To_Insert;
psql> COMMIT;
```

In einigen Fällen kann es nach der `BEGIN`-Anweisung zu einer Netzwerktrennung zwischen dem primären DB-Cluster und dem sekundären DB-Cluster kommen. Wenn dies der Fall ist, beginnt sich der `durability_lag_in_msec`-Wert des sekundären DB-Clusters zu erhöhen. Am Ende der `INSERT`-Anweisung beträgt der `durability_lag_in_msec`-Wert 1 Stunde. Der Wert `rpo_lag_in_msec` ist jedoch 0, da alle Benutzerdaten, die zwischen dem primären DB-Cluster und dem sekundären DB-Cluster übertragen werden, immer noch dieselben sind. Sobald die `COMMIT`-Anweisung abgeschlossen ist, erhöht sich der `rpo_lag_in_msec`-Wert.

Verwenden von globalen Amazon-Aurora-Datenbanken mit anderen AWS-Services

Sie können Ihre globalen Aurora-Datenbanken mit anderen AWS-Services wie Amazon S3 und AWS Lambda verwenden. Dies erfordert, dass alle Aurora-DB-Cluster in Ihrer globalen Datenbank die gleichen Privilegien, externen Funktionen usw. in den jeweiligen AWS-Regionen aufweisen. Da ein schreibgeschützter sekundärer Aurora-DB-Cluster in einer Aurora globalen Datenbank zur Rolle des primären Clusters hochgestuft werden kann, empfehlen wir, dass Sie im Voraus Schreibrechte für alle Aurora-DB-Cluster für alle Dienste einrichten, die Sie mit Ihrer Aurora globalen Datenbank verwenden möchten.

Die folgenden Verfahren fassen die für jeden AWS-Service zu ergreifenden Maßnahmen zusammen.

So rufen Sie AWS Lambda-Funktionen aus einer globalen Aurora-Datenbank auf

1. Führen Sie für alle Aurora-Cluster, aus denen die globale Aurora-Datenbank besteht, die unter beschriebenen Schritte au Aufrufen einer Lambda-Funktion aus einem Amazon Aurora MySQL-DB-Cluster.
2. Legen Sie für jeden Cluster in der Aurora globalen Datenbank den (ARN) der neuen IAM (IAM) - Rolle fest.
3. Verknüpfen Sie die in Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben erstellte Rolle mit allen Clustern in der globalen Aurora-Datenbank, um Datenbankbenutzern in einer globalen Aurora-Datenbank das Aufrufen von Lambda-Funktionen zu erlauben.
4. Konfigurieren Sie jeden Cluster in der globalen Aurora-Datenbank so, dass ausgehende Verbindungen zu Lambda zugelassen werden. Detaillierte Anweisungen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.

So laden Sie Daten aus Amazon S3

1. Führen Sie für alle Aurora-Cluster, aus denen die globale Aurora-Datenbank besteht, die unter beschriebenen Schritte au Laden von Daten in einen Amazon Aurora MySQL-DB-Cluster aus Textdateien in einem Amazon S3-Bucket.
2. Legen Sie bei jedem Aurora-Cluster in der globalen Datenbank für den Amazon-Ressourcennamen (ARN) der neuen IAM-Rolle entweder den Cluster-Parameter `aurora_load_from_s3_role` oder `aws_default_s3_role` fest Wenn für `aurora_load_from_s3_role` keine IAM-Rolle angegeben wird, verwendet Aurora die unter `aws_default_s3_role` angegebene IAM-Rolle.
3. Um Datenbankbenutzern in einer globalen Aurora-Datenbank den Zugriff auf Amazon S3 zu gewähren, verknüpfen Sie die in Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben erstellte Rolle mit jedem Aurora-Cluster in der globalen Datenbank.
4. Konfigurieren Sie jeden Aurora-Cluster in der globalen Datenbank so, dass ausgehende Verbindungen zu S3 zugelassen werden. Detaillierte Anweisungen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.

So speichern Sie abgefragte Daten auf Amazon S3

1. Führen Sie für alle Aurora-Cluster, aus denen die globale Aurora-Datenbank besteht, die unter beschriebenen Schritte au Speichern von Daten aus einem Amazon Aurora MySQL-DB-Cluster in Textdateien in einem Amazon S3-Bucket.
2. Legen Sie bei jedem Aurora-Cluster in der globalen Datenbank für den Amazon-Ressourcennamen (ARN) der neuen IAM-Rolle entweder den Cluster-Parameter `aurora_select_into_s3_role` oder `aws_default_s3_role` fest Wenn für `aurora_select_into_s3_role` keine IAM-Rolle angegeben wird, verwendet Aurora die unter `aws_default_s3_role` angegebene IAM-Rolle.
3. Um Datenbankbenutzern in einer globalen Aurora-Datenbank den Zugriff auf Amazon S3 zu gewähren, verknüpfen Sie die in Erstellen einer IAM-Rolle, um Amazon Aurora den Zugriff auf AWS-Services zu erlauben erstellte Rolle mit jedem Aurora-Cluster in der globalen Datenbank.
4. Konfigurieren Sie jeden Aurora-Cluster in der globalen Datenbank so, dass ausgehende Verbindungen zu S3 zugelassen werden. Detaillierte Anweisungen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.

Aktualisieren einer Amazon Aurora Global Database

Das Upgrade einer globalen Aurora-Datenbank folgt den gleichen Verfahren wie das Upgrade von Aurora-DB-Clustern. Im Folgenden sind jedoch einige wichtige Unterschiede aufgeführt, die Sie beachten müssen, bevor Sie den Prozess starten.

Wir empfehlen, den primären und den sekundären DB-Cluster auf dieselbe Version zu aktualisieren. Sie können ein verwaltetes regionsübergreifendes Datenbank-Failover für eine globale Aurora-Datenbank nur durchführen, wenn die primären und sekundären DB-Cluster dieselben Engine-Haupt- und Nebenversionen sowie dasselbe Patch-Level haben. Die Patch-Level können je nach Nebenversion der Engine unterschiedlich sein. Weitere Informationen finden Sie unter Patch-Level-Kompatibilität für verwaltete regionsübergreifende Umstellungen und Failovers.

Hauptversions-Upgrades

Wenn Sie ein Hauptversions-Upgrade einer Amazon Aurora Global Database durchführen, aktualisieren Sie den globalen Datenbank-Cluster statt der einzelnen darin enthaltenen Cluster.

Informationen zum Aktualisieren einer globalen Aurora-PostgreSQL-Datenbank auf eine höhere Hauptversion finden Sie unter Hauptversions-Upgrades für globale Datenbanken.

> **Note**
>
> Mit einer globalen Aurora-Datenbank, die auf Aurora PostgreSQL basiert, können Sie kein Hauptversions-Upgrade der Aurora-DB-Engine durchführen, wenn die Recovery Point Objective (RPO)-Funktion aktiviert ist. Weitere Informationen über RPO-Funktion finden Sie unter Verwalten von RPOs für Aurora PostgreSQL–basierte globale Datenbanken.

Informationen zum Aktualisieren einer globalen Aurora-MySQL-Datenbank auf eine höhere Hauptversion finden Sie unter In-Situ-Hauptversions-Upgrades für globale Datenbanken.

> **Note**
>
> Mit einer globalen Aurora-Datenbank, die auf Aurora MySQL basiert, können Sie kein direktes Upgrade von Aurora MySQL Version 2 auf Version 3 durchführen, wenn der `lower_case_table_names`-Parameter aktiviert ist.
> Um ein Hauptversions-Upgrade auf Aurora MySQL Version 3 bei Verwendung von `lower_case_table_names` durchzuführen, gehen Sie wie folgt vor:
>
> 1. Entfernen Sie alle sekundären Regionen aus dem globalen Cluster. Führen Sie die Schritte unter Entfernen eines Clusters aus einer Amazon Aurora Global Database aus.
> 2. Aktualisieren Sie die Engine-Version der primären Region zu Aurora-MySQL-Version 3. Führen Sie die Schritte unter Erläuterung der Durchführung eines direkten Upgrades aus.
> 3. Fügen Sie dem globalen Cluster sekundäre Regionen hinzu. Führen Sie die Schritte unter Hinzufügen einer AWS-Region zu einer globalen Amazon-Aurora-Datenbank aus.
>
> Sie können stattdessen auch die Snapshot-Wiederherstellungsmethode verwenden. Weitere Informationen finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.

Unterversion-Upgrades

Bei einem Unterversion-Upgrade auf einer globalen Aurora-Datenbank aktualisieren Sie alle sekundären Cluster, bevor Sie den primären Cluster aktualisieren.

Informationen zum Aktualisieren einer globalen Aurora-PostgreSQL-Datenbank auf eine kleinere Hauptversion finden Sie unter So führen Sie Upgrades von Nebenversionen durch und wenden

Patches an. Informationen zum Aktualisieren einer globalen Aurora-MySQL-Datenbank auf eine Unterversion finden Sie unter Upgrade von Aurora MySQL durch Ändern der Engine-Version.

Bevor Sie die Aktualisierung durchführen, lesen Sie die folgenden Hinweise:

- Eine Aktualisierung der Unterversion eines sekundären Clusters hat keinerlei Auswirkungen auf die Verfügbarkeit oder Nutzung des primären Clusters.
- Ein sekundärer Cluster muss über mindestens eine DB-Instance verfügen, um ein Unterversions-Upgrade durchzuführen.
- Wenn Sie eine globale Aurora-MySQL-Datenbank auf Version 2.11.* aktualisieren, müssen Sie Ihre primären und sekundären DB-Cluster auf exakt dieselbe Version aktualisieren, einschließlich des Patch-Levels.
- Um verwaltete regionsübergreifende Datenbankumstellungen oder -Failovers zu unterstützen, müssen Sie Ihre primären und sekundären DB-Cluster auf genau dieselbe Version aktualisieren, einschließlich des Patch-Levels, je nach Engine-Version. Weitere Informationen finden Sie unter Patch-Level-Kompatibilität für verwaltete regionsübergreifende Umstellungen und Failovers.

Patch-Level-Kompatibilität für verwaltete regionsübergreifende Umstellungen und Failovers

Wenn Sie Ihre Aurora Global Database auf eine der folgenden Engine-Nebenversionen aktualisieren, können Sie verwaltete regionsübergreifende Datenbankumstellungen oder -Failovers durchführen, auch wenn die Patch-Level Ihrer primären und sekundären DB-Cluster nicht übereinstimmen. Für Engine-Nebenversionen, die niedriger sind als die in dieser Liste aufgeführten, müssen Sie Ihre primären und sekundären DB-Cluster auf dieselben Haupt-, Neben- und Patch-Level aktualisieren, um verwaltete regionsübergreifende Datenbankumstellungen oder -Failovers durchzuführen. Sehen Sie sich unbedingt die Versionsinformationen und die Hinweise in der folgenden Tabelle an.

> **Note**
>
> Bei manuellen regionsübergreifenden Failovern können Sie den Failover-Vorgang ausführen, solange auf dem sekundären Ziel-DB-Cluster dieselbe Engine-Haupt- und -Nebenversion wie auf dem primären DB-Cluster ausgeführt wird. In diesem Fall müssen die Patch-Level nicht übereinstimmen.

Datenbank-Engine	Engine-Nebenversionen	Hinweise
Aurora MySQL	Keine Nebenversionen	Bei allen Nebenversionen können Sie verwaltete regionsübergreifende Umstellungen oder Failovers nur durchführen, wenn die Patch-Level der primären und sekundären DB-Cluster übereinstimmen.
Aurora PostgreSQL	• Version 14.5 und höhere Unterversionen • Version 13.8 und höhere Unterversionen • Version 12.12 und höhere Unterversionen • Version 11.17 und höhere Unterversionen	Mit den in der vorherigen Spalte aufgeführten Nebenversionen der Engine können Sie verwaltete regionsübergreifende Datenbank umstellungen oder -Failovers von einem primären DB-Cluster mit einem Patch-Level auf einen sekundären DB-Cluster mit einem anderen Patch-Level durchführen. Bei niedrigeren Nebenversionen können Sie verwaltete regionsübergreifende Umstellungen oder Failovers nur durchführen, wenn die Patch-Level der primären und sekundären DB-Cluster übereinstimmen.

Verwenden von Amazon RDS Proxy für Aurora

Durch die Verwendung von Amazon RDS Proxy können Sie Ihren Anwendungen erlauben, Datenbankverbindungen zu bündeln und gemeinsam zu nutzen, um ihre Skalierbarkeit zu verbessern. RDS Proxy macht Anwendungen widerstandsfähiger gegenüber Datenbankfehlern, indem er automatisch eine Verbindung zu einer Standby-DB-Instance herstellt, während Anwendungsverbindungen erhalten bleiben. Mithilfe von RDS Proxy können Sie auch die AWS Identity and Access Management (IAM-) Authentifizierung für Datenbanken erzwingen und Anmeldeinformationen sicher in AWS Secrets Manager speichern.

Mit RDS-Proxy können Sie unvorhersehbare Spitzen des Datenbankverkehrs bewältigen. Andernfalls können diese Überlastungen zu Problemen führen, da Verbindungen zu viele Abonnenten haben oder neue Verbindungen schnell hergestellt werden. RDS-Proxy richtet einen Datenbankverbindungspool ein und verwendet Verbindungen in diesem Pool wieder. Dieser Ansatz vermeidet den Speicher- und CPU-Overhead, der jedes Mal beim Öffnen einer neuen Datenbankverbindung erforderlich wäre. Um eine Datenbank vor Überbelegung zu schützen, können Sie die Anzahl der erstellten Datenbankverbindungen kontrollieren.

RDS Proxy stellt Anwendungsverbindungen, die nicht sofort vom Verbindungspool aus bedient werden können, in die Warteschlange oder drosselt sie. Obwohl Latenzen zunehmen können, kann Ihre Anwendung weiter skalieren, ohne dass die Datenbank abrupt ausfällt oder überfordert wird. Wenn Verbindungsanforderungen die von Ihnen angegebenen Grenzwerte überschreiten, lehnt RDS Proxy Anwendungsverbindungen ab (d. h. die Last wird abgeworfen). Gleichzeitig wird eine vorhersehbare Leistung für die Last aufrechterhalten, die RDS mit der verfügbaren Kapazität bewältigen kann.

Sie können den Overhead für die Verarbeitung von Anmeldeinformationen reduzieren und für jede neue Verbindung eine sichere Verbindung herstellen. Einige dieser Arbeiten kann RDS Proxy im Auftrag der Datenbank verarbeiten.

RDS Proxy ist mit den Engine-Versionen, die es unterstützt, vollständig kompatibel. Sie können RDS-Proxy für die meisten Anwendungen ohne Codeänderungen aktivieren. Eine Liste der unterstützten Engine-Versionen finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Amazon RDS Proxy.

Themen

- Planen des Verwendungsortes von RDS-Proxy
- Konzepte und Terminologie zu RDS Proxy
- Erste Schritte mit RDS Proxy
- Verwalten eines RDS-Proxy
- Arbeiten mit Amazon RDS Proxy-Endpunkten
- Überwachen von RDS-Proxy-Metriken mit Amazon CloudWatch
- Arbeiten mit RDS-Proxy-Ereignissen
- Befehlszeilenbeispiele für RDS Proxy
- Fehlersuche für RDS Proxy
- Verwenden von RDS Proxy mit AWS CloudFormation
- Verwenden von RDS Proxy mit globalen Aurora-Datenbanken

Verfügbarkeit von Regionen und Versionen

Hinweise zur Versionsunterstützung der Datenbank-Engine und zur Verfügbarkeit von RDS-Proxy in einem bestimmten AWS-Region Fall finden Sie unterUnterstützte Regionen und Aurora-DB-Engines für Amazon RDS Proxy.

Kontingente und Einschränkungen für RDS Proxy

Die folgenden Einschränkungen gelten für RDS Proxy:

- Jede AWS-Konto ID ist auf 20 Proxys begrenzt. Wenn für Ihre Anwendung mehr Proxys erforderlich sind, fordern Sie eine Erhöhung über die Seite Servicekontingente in der an. AWS Management Console Wählen Sie auf der Seite Service Quotas Amazon Relational Database Service (Amazon RDS) aus und suchen Sie nach Proxys, um eine Kontingenterhöhung zu beantragen. AWS kann Ihr Kontingent oder die ausstehende Prüfung Ihrer Anfrage automatisch um erhöhen. AWS Support
- Jeder Proxy kann bis zu 200 zugehörige Secrets Manager-Secrets haben. Somit kann jeder Proxy jederzeit eine Verbindung mit bis zu 200 verschiedenen Benutzerkonten herstellen.
- Jeder Proxy hat einen Standardendpunkt. Sie können auch bis zu 20 Proxy-Endpunkte für jeden Proxy hinzufügen. Sie können diese Endpoints erstellen, anzeigen, ändern und löschen.
- In einem Aurora-Cluster, werden alle Verbindungen, die den Standard-Proxy-Endpunkt verwenden, von der Aurora-Writer-Instance verarbeitet. Um einen Lastenausgleich für leseintensive Workloads

durchzuführen, können Sie einen schreibgeschützten Endpunkt für einen Proxy erstellen. Dieser Endpunkt übergibt Verbindungen an den Reader-Endpunkt des Clusters. Auf diese Weise können Ihre Proxy-Verbindungen die Vorteile von Aurora-Leseskalierbarkeit nutzen. Weitere Informationen finden Sie unter Überblick über Proxy-Endpunkte.

- Sie können RDS-Proxy mit Clustern von Aurora Serverless v2 verwenden, jedoch nicht mit Clustern von Aurora Serverless v1.
- Ihr RDS Proxy muss sich in derselben VPC wie die Datenbank befinden. Obwohl die Datenbank öffentlich zugänglich sein kann, kann der Proxy dies nicht sein. Wenn Sie beispielsweise Prototypen für Ihre Datenbank auf einem lokalen Host erstellen, können Sie keine Verbindung zu Ihrem Proxy herstellen, es sei denn, Sie haben die erforderlichen Netzwerkanforderungen für die Verbindung zum Proxy eingerichtet. Dies liegt daran, dass sich Ihr lokaler Host außerhalb der VPC des Proxys befindet.

  > **Note**
  >
  > Für Aurora-DB-Cluster können Sie den VPC-übergreifenden Zugriff aktivieren. Erstellen Sie dazu einen zusätzlichen Endpunkt für einen Proxy und geben Sie eine andere VPC, Subnetze und Sicherheitsgruppen mit diesem Endpunkt an. Weitere Informationen finden Sie unter Zugreifen auf Aurora-Datenbanken über VPCs hinweg.

- Sie können RDS Proxy nicht mit einer VPC verwenden, für deren Tenancy `dedicated` festgelegt wurde.
- Wenn Sie den RDS-Proxy mit einem Aurora-DB-Cluster der verwenden, für den die IAM-Authentifizierung aktiviert ist, überprüfen Sie die Benutzerauthentifizierung. Benutzer, die eine Verbindung über einen Proxy herstellen, müssen sich mit ihren Anmeldedaten authentifizieren. Details zu Secrets Manager und zur IAM-Unterstützung in RDS Proxy finden Sie unter Datenbankanmeldedaten einrichten in AWS Secrets Manager und AWS Identity and Access Management (IAM-) Richtlinien einrichten.
- Sie können RDS Proxy nicht mit benutzerdefiniertem DNS verwenden, wenn Sie die SSL-Hostnamenvalidierung nutzen.
- Jeder Proxy kann einem einzelnen Ziel-DB-Cluster zugeordnet werden. Sie können jedoch mehrere Proxys demselben DB-Cluster zuordnen.
- Jede Anweisung mit einer Textgröße über 16 KB bewirkt, dass der Proxy die Sitzung in der aktuellen Verbindung fixiert.
- In bestimmten Regionen gelten Einschränkungen für Availability-Zones (AZ), die Sie bei der Erstellung des Proxys berücksichtigen müssen. Die Region USA Ost (Nord-Virginia) unterstützt

RDS-Proxy nicht in der Availability Zone `use1-az3`. Die Region USA West (Nordkalifornien) unterstützt RDS-Proxy nicht in der Availability Zone `usw1-az2`. Achten Sie beim Auswählen von Subnetzen während der Proxy-Erstellung darauf, dass Sie keine Subnetze in den oben genannten Availability Zones auswählen.

- Derzeit unterstützt RDS Proxy keine globalen Bedingungskontextschlüssel.

  Weitere Informationen über globale Bedingungskontextschlüssel finden Sie unter Globale AWS - Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Weitere Informationen zu den Einschränkungen für jede DB-Engine finden Sie in den folgenden Abschnitten:

- Weitere Einschränkungen für Aurora MySQL
- Weitere Einschränkungen für Aurora PostgreSQL

Weitere Einschränkungen für Aurora MySQL

Die folgenden zusätzlichen Einschränkungen gelten für RDS Proxy mit Datenbanken von RDS für MySQL:

- Der RDS Proxy unterstützt MySQL `sha256_password` und `caching_sha2_password` Authentifizierungs-Plug-Ins nicht. Diese Plug-Ins implementieren SHA-256-Hashing für Benutzerkontenpasswörter.
- Derzeit führen alle Proxys Listening auf Port 3306 für MySQL durch. Die Proxys stellen weiterhin eine Verbindung mit Ihrer Datenbank her, indem Sie den Port verwenden, den Sie in den Datenbankeinstellungen angegeben haben.
- Sie können RDS Proxy nicht mit selbst verwalteten MySQL-Datenbanken in EC2-Instances verwenden.
- Sie können RDS Proxy nicht mit einer RDS-for-MySQL-DB-Instance verwenden, bei welcher der Parameter `read_only` in der DB-Parametergruppe auf 1 gesetzt wurde.
- RDS Proxy unterstützt den komprimierten MySQL-Modus nicht. Es unterstützt z. B. nicht die Komprimierung, die von den Optionen `--compress` oder `-C` des `mysql`-Befehls verwendet wird.
- Datenbankverbindungen, die einen Befehl `GET DIAGNOSTIC` verarbeiten, geben möglicherweise ungenaue Informationen zurück, wenn der RDS-Proxy dieselbe Datenbankverbindung

für eine weitere Abfrage wiederverwendet. Dies kann passieren, wenn der RDS-Proxy Datenbankverbindungen multiplexiert.

- Einige SQL-Anweisungen und Funktionen `SET LOCAL` können z. B. den Verbindungsstatus ändern, ohne dass es zu einer Fixierung kommt. Informationen zum aktuellen Fixierungsverhalten finden Sie unter Vermeiden des Fixierens.
- Die Verwendung der `ROW_COUNT()` Funktion in einer Abfrage mit mehreren Anweisungen wird nicht unterstützt.
- RDS Proxy unterstützt keine Client-Anwendungen, die nicht mehrere Antwortnachrichten in einem TLS-Datensatz verarbeiten können.

> **Important**
>
> Setzen Sie in der Initialisierungsabfrage bei Proxys, die mit MySQL-Datenbanken verknüpft sind, den Konfigurationsparameter `sql_auto_is_null` nicht auf `true` oder einen Wert ungleich Null. Dies kann zu einem falschen Anwendungsverhalten führen.

Weitere Einschränkungen für Aurora PostgreSQL

Die folgenden zusätzlichen Einschränkungen gelten für RDS Proxy mit Datenbanken von Aurora PostgreSQL:

- RDS Proxy unterstützt keine Sitzungs-Pinning-Filter für PostgreSQL.
- Derzeit führen alle Proxys Listening auf Port 5432 für PostgreSQL durch.
- Für PostgreSQL unterstützt RDS Proxy derzeit nicht das Abbrechen einer Abfrage von einem Client durch Ausgeben von `CancelRequest`. Dies ist beispielsweise der Fall, wenn Sie eine lange andauernde Abfrage in einer interaktiven psql-Sitzung mithilfe von Strg+C abbrechen.
- Die Ergebnisse der PostgreSQL-Funktion lastval sind nicht immer genau. Verwenden Sie zur Umgehung die INSERT-Anweisung mit der Klausel `RETURNING`.
- RDS Proxy unterstützt derzeit den Streaming-Replikationsmodus nicht.

> **Important**
>
> Wenn Sie bei vorhandenen Proxys mit PostgreSQL-Datenbanken die Datenbankauthentifizierung so ändern, dass nur `SCRAM` verwendet wird, ist der Proxy für

bis zu 60 Sekunden nicht verfügbar. Um das Problem zu vermeiden, führen Sie einen der folgenden Schritte aus:

- Stellen Sie sicher, dass die Datenbank sowohl die `SCRAM`- als auch die `MD5`-Authentifizierung zulässt.
- Wenn Sie nur die `SCRAM`-Authentifizierung verwenden möchten, erstellen Sie einen neuen Proxy, migrieren Sie Ihren Anwendungsdatenverkehr auf den neuen Proxy und löschen Sie dann den zuvor mit der Datenbank verknüpften Proxy.

Planen des Verwendungsortes von RDS-Proxy

Sie können ermitteln, welche Ihrer DB-Instances, Cluster und Anwendungen möglicherweise am meisten von der Verwendung von RDS Proxy profitieren. Berücksichtigen Sie dazu folgende Faktoren:

- Alle DB-Cluster, auf denen gelegentlich der Fehler „zu viele Verbindungen“ auftritt, sind gut geeignet für die Zuordnung zu einem Proxy. Dies ist oft durch einen hohen Wert der `-ConnectionAttempts` CloudWatch Metrik gekennzeichnet. Der Proxy ermöglicht es Anwendungen, viele Clientverbindungen zu öffnen, während der Proxy eine geringere Anzahl langlebiger Verbindungen mit dem DB-Cluster verwaltet.
- Bei DBances können Cluster, die kleinere AWS Instance-Klassen wie T2 oder T3 verwenden, die Verwendung eines Proxys dazu beitragen, out-of-memory Bedingungen zu vermeiden. Sie kann auch dazu beitragen, den CPU-Overhead für das Herstellen von Verbindungen zu reduzieren. Diese Bedingungen können auftreten, wenn es um eine große Anzahl von Verbindungen geht.
- Sie können bestimmte Amazon- CloudWatch Metriken überwachen, um festzustellen, ob sich eine DB DB-Cluster bestimmten Arten von Grenzwerten nähert. Diese Grenzwerte gelten für die Anzahl der Verbindungen und den Arbeitsspeicher, der mit der Verbindungsverwaltung verbunden ist. Sie können auch bestimmte CloudWatch Metriken überwachen, um festzustellen, ob eine DB- ein DB-Cluster viele kurzlebige Verbindungen verarbeitet. Das Öffnen und Beenden solcher Verbindungen kann einen Leistungs-Overhead für Ihre Datenbank verursachen. Informationen zu den zu überwachenden Metriken finden Sie unter Überwachen von RDS-Proxy-Metriken mit Amazon CloudWatch.
- AWS Lambda-Funktionen können auch gute Kandidaten für die Verwendung eines Proxys sein. Diese Funktionen stellen häufig kurze Datenbankverbindungen her, die von dem von RDS Proxy angebotenen Verbindungspooling profitieren. Sie können alle IAM-Authentifizierungen nutzen, die

Sie bereits für Lambda-Funktionen haben, anstatt Datenbankanmeldeinformationen im Lambda-Anwendungscode zu verwalten.

- Anwendungen, die in der Regel eine große Anzahl von Datenbankverbindungen öffnen und schließen und über keine integrierten Mechanismen für das Verbindungspooling verfügen, bieten sich für die Verwendung eines Proxys an.
- Anwendungen, die eine große Anzahl von Verbindungen über lange Zeiträume offen halten, sind in der Regel gute Kandidaten für die Verwendung eines Proxys. Anwendungen in Branchen wie Software as a Service (SaaS) oder E-Commerce minimieren häufig die Latenz für Datenbankanfragen, da sie Verbindungen offen lassen. Mit RDS Proxy kann eine Anwendung mehr Verbindungen offen halten als möglich, wenn eine direkte Verbindung mit der DB- DB-Cluster hergestellt wird.
- Möglicherweise haben Sie die IAM-Authentifizierung und Secrets Manager aufgrund der Komplexität der Einrichtung einer solchen Authentifizierung für alle DB-Cluster nicht übernommen. Wenn dies der Fall ist, können Sie die vorhandenen Authentifizierungsmethoden beibehalten und die Authentifizierung an einen Proxy delegieren. Der Proxy kann die Authentifizierungsrichtlinien für Clientverbindungen für bestimmte Anwendungen erzwingen. Sie können alle IAM-Authentifizierungen nutzen, die Sie bereits für Lambda-Funktionen haben, anstatt Datenbankanmeldeinformationen im Lambda-Anwendungscode zu verwalten.
- RDS-Proxy kann dazu beitragen, Anwendungen widerstandsfähiger und transparenter gegenüber Datenbankausfällen zu machen. RDS-Proxy umgeht Domain Name System (DNS)-Caches, um die Failover-Zeiten für Multi-AZ-Datenbanken von Aurora um bis zu 66 % zu reduzieren. RDS-Proxy leitet den Datenverkehr außerdem automatisch an eine neue Datenbank-Instance weiter, wobei Anwendungsverbindungen erhalten bleiben. Dadurch werden Failovers für Anwendungen transparenter.

Konzepte und Terminologie zu RDS Proxy

Sie können die Verbindungsverwaltung für Ihre Amazon-Aurora-DB-Cluster vereinfachen, indem Sie RDS-Proxy verwenden.

RDS Proxy verarbeitet den Netzwerkverkehr zwischen der Clientanwendung und der Datenbank. Es tut dies auf aktive Weise, indem es das Datenbankprotokoll erfasst Anschließend passt er sein Verhalten basierend auf den SQL-Operationen aus Ihrer Anwendung und den Ergebnismengen aus der Datenbank an.

RDS Proxy reduziert den Arbeitsspeicher- und CPU-Overhead für die Verbindungsverwaltung in Ihrer Datenbank. Die Datenbank benötigt weniger Arbeitsspeicher und CPU-Ressourcen, wenn Anwendungen viele gleichzeitige Verbindungen öffnen. Es erfordert auch keine Logik in Ihren Anwendungen, um Verbindungen zu schließen und wieder zu öffnen, die für eine lange Zeit inaktiv bleiben. Ebenso erfordert es weniger Anwendungslogik, um Verbindungen im Falle eines Datenbankproblems wiederherzustellen.

Die Infrastruktur für RDS Proxy ist hochverfügbar und wird über mehrere Availability Zones (AZs) bereitgestellt. Die Berechnung, der Arbeitsspeicher und der Speicher für RDS Proxy sind unabhängig vom Aurora DB-Cluster Ihrer . Diese Trennung hilft, den Overhead auf Ihren Datenbankservern zu senken, sodass sie ihre Ressourcen für die Bereitstellung von Datenbank-Workloads einsetzen können. Die RDS Proxy-Rechenressourcen sind serverless und werden automatisch basierend auf der Datenbank-Workload skaliert.

Themen

Überblick über RDS Proxy-Konzepte

RDS Proxy verbreitet die Infrastruktur zum Ausführen des Verbindungspoolings und die anderen Funktionen, die in den folgenden Abschnitten beschrieben werden. Die in der RDS-Konsole dargestellten Proxys werden auf der Seite Proxys angezeigt.

Jeder Proxy verarbeitet Verbindungen zu einer einzelnen , einem Aurora-DB-Cluster. Bei von Aurora bereitgestellten Clustern bestimmt der Proxy die aktuelle Writer-Instance automatisch.

Die Verbindungen, die ein Proxy offen hält und für Ihre Datenbankanwendungen verfügbar hält, bilden den Verbindungspool.

Standardmäßig kann RDS Proxy eine Verbindung nach jeder Transaktion in Ihrer Sitzung wiederverwenden. Diese Wiederverwendung auf Transaktionsebene wird als Multiplexing bezeichnet. Wenn RDS Proxy vorübergehend eine Verbindung aus dem Verbindungspool entfernt wird, um sie

wiederzuverwenden, wird dieser Vorgang als Ausleihen der Verbindung bezeichnet. Wenn dies sicher ist, wird diese Verbindung an den Verbindungspool RDS Proxy zurückgegeben.

In einigen Fällen kann RDS Proxy nicht gewährleisten, dass eine Datenbankverbindung außerhalb der aktuellen Sitzung sicher wiederzuverwenden ist. In diesen Fällen bleibt die Sitzung auf derselben Verbindung erhalten, bis die Sitzung beendet ist. Dieses Fallback-Verhalten wird als Fixierung (Pinning) bezeichnet.

Ein Proxy hat einen Standard-Endpunkt. Sie stellen eine Verbindung mit diesem Endpunkt her, wenn Sie mit einem Amazon-Aurora-DB-Cluster arbeiten. Sie tun dies, anstatt eine Verbindung mit dem Lese-/Schreib-Endpunkt herzustellen, der direkt mit dem Cluster verbunden wird. Die speziellen Endpunkte für einen Aurora-Cluster stehen Ihnen weiterhin zur Verfügung. Für Aurora-DB-Cluster können Sie auch zusätzliche Lese-/Schreib- und schreibgeschützte Endpunkte erstellen. Weitere Informationen finden Sie unter Überblick über Proxy-Endpunkte.

Sie können beispielsweise weiterhin eine Verbindung zum Clusterendpunkt für Verbindungen mit Lese-/Schreibzugriff ohne Verbindungspooling herstellen. Sie können weiterhin eine Verbindung zum Leser-Endpunkt für schreibgeschützte Verbindungen mit Lastenausgleich herstellen. Sie können weiterhin eine Verbindung zu den Instance-Endpunkten für die Diagnose und Behebung von Fehlern in bestimmten DB-Instances innerhalb eines Clusters herstellen. Wenn Sie andere AWS Dienste verwenden, z. B. AWS Lambda um eine Verbindung zu RDS-Datenbanken herzustellen, ändern Sie deren Verbindungseinstellungen, sodass der Proxy-Endpunkt verwendet wird. Beispielsweise geben Sie den Proxy-Endpunkt an, damit Lambda-Funktionen auf Ihre Datenbank zugreifen und gleichzeitig die RDS Proxy-Funktionalität nutzen können.

Jeder Proxy enthält eine Zielgruppe. Diese Zielgruppe verkörpert den Aurora DB-Cluster der , zu dem der Proxy eine Verbindung herstellen kann. Bei einem Aurora-Cluster ist die Zielgruppe standardmäßig allen DB-Instances in diesem Cluster zugeordnet. Auf diese Weise kann sich der Proxy mit jeder Aurora-DB-Instance verbinden, die zur Writer-Instance im Cluster hochgestuft wird. Der Aurora DB-Cluster der , der einem Proxy zugeordnet ist, werden als Ziele dieses Proxys bezeichnet. Wenn Sie einen Proxy über die Konsole erstellen, erstellt RDS Proxy auch die entsprechende Zielgruppe und registriert die zugeordneten Ziele automatisch.

Eine Engine-Familie ist eine verwandte Gruppe von Datenbank-Engines, die dasselbe DB-Protokoll verwenden. Sie wählen die Engine-Familie für jeden Proxy, den Sie erstellen.

Verbindungspooling

Jeder Proxy führt ein Verbindungspooling für die Writer-Instance der zugehörigen Aurora-DB aus. Das Verbindungspooling ist eine Optimierung, die den Overhead reduziert, der mit dem Öffnen und Beenden von Verbindungen und dem Vorhandensein vieler aktiver Verbindungen gleichzeitig verbunden ist. Dieser Overhead umfasst den Arbeitsspeicher, der für die Verarbeitung jeder neuen Verbindung erforderlich ist. Es ist außerdem CPU-Overhead erforderlich, um jede Verbindung zu schließen und eine neue zu öffnen. Beispiele hierfür sind TLS-/SSL-Handshaking, Authentifizierung, Aushandlungsfunktionen usw. Das Verbindungspooling vereinfacht Ihre Anwendungslogik. Sie müssen keinen Anwendungscode schreiben, um die Anzahl gleichzeitig geöffneter Verbindungen zu minimieren.

Jeder Proxy führt darüber hinaus Multiplexing von Verbindungen aus, auch bekannt als Wiederverwendung von Verbindungen. Beim Multiplexing führt RDS-Proxy alle Operationen für eine Transaktion mit einer zugrunde liegenden Datenbankverbindung aus. RDS kann dann eine andere Verbindung für die nächste Transaktion verwenden. Sie können viele gleichzeitige Verbindungen zum Proxy öffnen und der Proxy hält eine geringere Anzahl von Verbindungen zur DB-Instance oder zum Cluster offen. Dadurch wird der Speicher-Overhead für Verbindungen auf dem Datenbankserver weiter minimiert. Diese Technik reduziert auch die Wahrscheinlichkeit des Fehlers "zu viele Verbindungen".

RDS Proxy-Sicherheit

RDS Proxy verwendet die vorhandenen RDS-Sicherheitsmechanismen wie TLS/SSL und AWS Identity and Access Management (IAM). Allgemeine Informationen zu diesen Sicherheitsfunktionen finden Sie unter Sicherheit in Amazon Aurora. Sie sollten sich außerdem unbedingt damit vertraut machen, wie Aurora mit Authentifizierung, Autorisierung und anderen Sicherheitsbereichen arbeitet.

RDS Proxy kann als zusätzliche Sicherheitsebene zwischen Clientanwendungen und der zugrunde liegenden Datenbank fungieren. Sie können beispielsweise mithilfe von TLS 1.3 eine Verbindung zum Proxy herstellen, auch wenn die zugrunde liegende DB-Instance eine ältere Version von TLS unterstützt. Sie können mithilfe einer IAM-Rolle eine Verbindung mit dem Proxy herstellen. Dies gilt auch dann, wenn der Proxy mithilfe der nativen Benutzer- und Passwortauthentifizierungsmethode eine Verbindung mit der Datenbank herstellt. Mit dieser Technik können Sie hohe Authentifizierungsanforderungen für Datenbankanwendungen ohne einen kostspieligen Migrationsaufwand für die DB-Instances selbst erzwingen.

Sie speichern die von RDS Proxy verwendeten Datenbankanmeldeinformationen in AWS Secrets Manager. Jeder Datenbankbenutzer für den Aurora DB-Cluster der , auf den ein Proxy zugreift,

muss über ein entsprechendes Geheimnis in Secrets Manager verfügen. Sie können auch die IAM-Authentifizierung für Benutzer von RDS Proxy einrichten. Auf diese Weise können Sie die IAM-Authentifizierung für den Datenbankzugriff erzwingen, selbst wenn die Datenbanken weiterhin die native Passwortauthentifizierung verwenden. Es wird empfohlen, diese Sicherheitsfunktionen zu verwenden, anstatt Datenbankanmeldeinformationen in Ihren Anwendungscode einzubetten.

Verwenden von TLS/SSL mit RDS Proxy

Sie können eine Verbindung zu RDS Proxy über das TLS/SSL-Protokoll herstellen.

> **Note**
>
> RDS Proxy verwendet Zertifikate von AWS Certificate Manager (ACM). Wenn Sie RDS Proxy verwenden, müssen Sie keine Amazon RDS-Zertifikate herunterladen oder Anwendungen aktualisieren, die RDS Proxy-Verbindungen verwenden.

Um TLS für alle Verbindungen zwischen dem Proxy und Ihrer Datenbank zu erzwingen, können Sie beim Erstellen oder Ändern eines Proxys in der die AWS Management Console Einstellung Transport Layer Security erforderlich angeben.

Mit RDS Proxy können Sie auch sicherstellen, dass Ihre Sitzung TLS/SSL zwischen Ihrem Client und dem RDS Proxy-Endpunkt verwendet. Damit RDS Proxy so verfährt, müssen Sie die clientseitige Anforderung festlegen. Für SSL-Verbindungen mit einer Datenbank unter Verwendung von RDS Proxy werden keine SSL-Sitzungsvariablen festgelegt.

- Geben Sie für Aurora MySQL die clientseitige Anforderung mit dem Parameter `--ssl-mode` an, wenn Sie den Befehl `mysql` ausführen.
- Geben Sie für Aurora PostgreSQL `sslmode=require` als Teil der `conninfo`-Zeichenfolge an, wenn Sie den Befehl `psql` ausführen.

RDS Proxy unterstützt die TLS-Protokollversionen 1.0, 1.1, 1.2 und 1.3. Sie können eine Verbindung mit dem Proxy herstellen, indem Sie eine höhere TLS-Version verwenden, als Sie in der zugrunde liegenden Datenbank verwenden.

Standardmäßig richten Client-Programme eine verschlüsselte Verbindung mit RDS Proxy ein, wobei weitere Kontrolle über die Option `--ssl-mode` verfügbar ist. Clientseitig unterstützt RDS Proxy alle SSL-Modi.

Für den Client sind die SSL-Modi die folgenden:

PREFERRED

SSL ist die erste Wahl, aber nicht erforderlich.

DISABLED

SSL ist nicht zulässig.

REQUIRED

SSL erzwingen.

VERIFY_CA

SSL erzwingen und die Zertifizierungsstelle (CA) überprüfen.

VERIFY_IDENTITY

SSL erzwingen und die CA sowie den CA-Hostname überprüfen.

Bei Verwendung eines Clients mit `--ssl-mode VERIFY_CA` oder `VERIFY_IDENTITY`, geben Sie die Option `--ssl-ca` an, die auf eine CA im `.pem`-Format verweist. Für die zu verwendende `.pem`-Datei laden Sie alle Root-CA-PEMs von Amazon Trust Services herunter und speichern sie in einer einzelnen `.pem`-Datei.

RDS Proxy verwendet Platzhalterzertifikate, die sowohl für eine Domain als auch für ihre Subdomänen gelten. Wenn Sie den `mysql`-Client für die Verbindung mit dem SSL-Modus `VERIFY_IDENTITY` verwenden, müssen Sie derzeit den MySQL 8.0-kompatiblen Befehl `mysql` verwenden.

Failover

Failover ist eine Funktion mit hoher Verfügbarkeit, die eine Datenbank-Instance durch eine andere ersetzt, wenn die ursprüngliche Instance nicht verfügbar ist. Ein Failover kann aufgrund eines Problems mit einer Datenbank-Instance auftreten. Er kann aber auch Teil normaler Wartungsverfahren sein, z. B. während eines Datenbank-Upgrades. Failover gilt für Aurora-DB-Cluster mit einer oder mehreren Reader-Instances zusätzlich zur Writer-Instance.

Durch die Verbindung über einen Proxy sind Ihre Anwendungen widerstandsfähiger gegenüber Datenbank-Failovers. Wenn die ursprüngliche DB-Instance nicht verfügbar ist, stellt RDS Proxy eine Verbindung mit der Standby-Datenbank her, ohne dass die inaktiven Anwendungsverbindungen

verworfen werden. Dies trägt dazu bei, den Failover-Prozess zu beschleunigen und zu vereinfachen. Dadurch wird Ihre Anwendung weniger beeinträchtigt als ein typischer Neustart oder ein Datenbankproblem.

Ohne RDS Proxy ist ein Failover mit einem kurzen Ausfall verbunden. Während des Ausfalls können Sie im Failover keine Schreibvorgänge an der Datenbank ausführen. Alle vorhandenen Datenbankverbindungen werden unterbrochen und Ihre Anwendung muss sie erneut öffnen. Die Datenbank wird für neue Verbindungen und Schreiboperationen verfügbar, wenn eine schreibgeschützte DB-Instance anstelle einer nicht verfügbaren Instance hochgestuft wird.

Während DB-Failovers akzeptiert RDS Proxy weiterhin Verbindungen mit derselben IP-Adresse und leitet Verbindungen automatisch an die neue primäre DB-Instance weiter. Clients, die eine Verbindung über RDS Proxy herstellen, sind nicht anfällig für Folgendes:

- DNS (Domain Name System)-Ausbreitungsverzögerungen beim Failover.
- Lokale DNS-Zwischenspeicherung.
- Verbindungszeitüberschreitungen.
- Unsicherheit darüber, welche DB-Instance der aktuelle Writer ist.
- Warten auf eine Abfrageantwort eines früheren Writers, die nicht verfügbar wurde, ohne Verbindungen zu schließen.

Bei Anwendungen, die über eigene Verbindungspools verfügen, sorgt RDS Proxy dafür, dass die meisten Verbindungen bei Failovers oder anderen Unterbrechungen aktiv bleiben. Nur Verbindungen, die sich mitten in einer Transaktion oder SQL-Anweisung befinden, werden unterbrochen. RDS Proxy akzeptiert sofort neue Verbindungen. Wenn der Datenbank-Schreiber nicht verfügbar ist, werden eingehende Anfragen in RDS Proxy in die Warteschlange gesetzt.

Für Anwendungen, die nicht über eigene Verbindungspools verfügen, bietet RDS Proxy schnellere Verbindungsraten und mehr offene Verbindungen. Es reduziert den teuren Overhead, der mit dem häufigen Herstellen neuer Verbindungen über die Datenbank verbunden ist. Hierfür werden Datenbankverbindungen wiederverwendet, die im RDS Proxy-Verbindungspool verwaltet werden. Dieser Ansatz ist besonders wichtig für TLS-Verbindungen, die mit erheblichen Setupkosten verbunden sind.

Transaktionen

Alle Anweisungen innerhalb einer einzelnen Transaktion verwenden immer dieselbe zugrunde liegende Datenbankverbindung. Die Verbindung wird für eine andere Sitzung verfügbar, wenn die

Transaktion beendet wird. Die Verwendung der Transaktion als Granularitätseinheit hat folgende Auswirkungen:

- Die Wiederverwendung von Verbindungen kann nach jeder einzelnen Anweisung erfolgen, wenn die Einstellung `autocommit` von Aurora MySQL aktiviert ist.
- Ist die Einstellung `autocommit` deaktiviert, beginnt im Gegensatz dazu die erste Anweisung, die Sie in einer Sitzung ausgeben, eine neue Transaktion. Angenommen, Sie geben die Sequenz `SELECT`, `INSERT`, `UPDATE` und andere Data Manipulation Language (DML)-Anweisungen ein. In diesem Fall wird die Wiederverwendung von Verbindungen erst vorgenommen, wenn Sie einen `COMMIT`, `ROLLBACK` ausgeben oder die Transaktion anderweitig beenden.
- Die Eingabe einer DDL-Anweisung (Data Definition Language) bewirkt, dass die Transaktion beendet wird, nachdem diese Anweisung abgeschlossen wurde.

RDS Proxy erkennt über das Netzwerkprotokoll, das von der Datenbank-Clientanwendung verwendet wird, wenn eine Transaktion beendet wird. Die Transaktionserkennung beruht nicht auf Schlüsselwörtern wie beispielsweise `COMMIT` oder `ROLLBACK`, die im Text der SQL-Anweisung angezeigt werden.

In einigen Fällen kann RDS Proxy eine Datenbankanforderung erkennen, die es unpraktisch macht, Ihre Sitzung auf eine andere Verbindung zu verschieben. In diesen Fällen wird das Multiplexing für diese Verbindung während der verbleibenden Sitzung deaktiviert. Die gleiche Regel gilt, wenn RDS Proxy nicht sicher sein kann, dass das Multiplexing für die Sitzung praktikabel ist. Diese Operation wird als Fixierung (Pinning) bezeichnet. Hinweise zum Erkennen und Minimieren von Fixierungen finden Sie unter Vermeiden des Fixierens.

Erste Schritte mit RDS Proxy

In den folgenden Abschnitten erfahren Sie, wie Sie den RDS-Proxy einrichten und verwalten. Sie erfahren auch, wie Sie verwandte Sicherheitsoptionen festlegen. Diese Optionen steuern, wer auf jeden Proxy zugreifen kann und wie jeder Proxy eine Verbindung zu DB-Instances herstellt.

Themen

- Einrichten der Netzwerkvoraussetzungen
- Datenbankanmeldedaten einrichten in AWS Secrets Manager
- AWS Identity and Access Management (IAM-) Richtlinien einrichten
- Erstellen eines RDS Proxy

- Anzeigen eines RDS Proxy
- Verbinden mit einer Datenbank über RDS Proxy

Einrichten der Netzwerkvoraussetzungen

Für die Verwendung von RDS Proxy benötigen Sie eine gemeinsame Virtual Private Cloud (VPC) zwischen Ihrer , dem Aurora-DB-Cluster und dem RDS-Proxy. Diese VPC sollte über mindestens zwei Subnetze verfügen, die sich in verschiedenen Availability Zones befinden. Ihr Konto kann entweder der Eigentümer dieser Subnetze sein oder sie mit anderen Konten teilen. Weitere Informationen zur VPC-Freigabe finden Sie unter Arbeiten mit freigegebenen VPCs.

Ihre Client-Anwendungsressourcen wie Amazon EC2, Lambda oder Amazon ECS können sich in derselben VPC wie der Proxy befinden. Sie können sich auch in einer vom Proxy getrennten VPC befinden. Wenn Sie eine Verbindung mit Aurora-DB-Clustern hergestellt haben, verfügen Sie bereits über die erforderlichen Netzwerkressourcen.

Themen

- Abrufen von Informationen zu Ihren Subnetzen
- Planen der Kapazität von IP-Adressen

Abrufen von Informationen zu Ihren Subnetzen

Wenn Sie gerade erst mit Aurora beginnen, können Sie sich mit den Grundlagen der Verbindung zu einer Datenbank vertraut machen, indem Sie die Verfahren unter befolgenEinrichten Ihrer Umgebung für Amazon Aurora. Sie können auch das Tutorial in ansehe Erste Schritte mit Amazon Aurora.

Um einen Proxy zu erstellen, müssen Sie die Subnetze und die VPC angeben, in denen der Proxy betrieben wird. Das folgende Linux-Beispiel zeigt AWS CLI Befehle, die die VPCs und Subnetze untersuchen, die Ihrem gehören. AWS-Konto Insbesondere übergeben Sie Subnetz-IDs als Parameter, wenn Sie ein Proxy mit der CLI erstellen.

```
aws ec2 describe-vpcs
aws ec2 describe-internet-gateways
aws ec2 describe-subnets --query '*[].[VpcId,SubnetId]' --output text | sort
```

Das folgende Linux-Beispiel zeigt AWS CLI Befehle zum Ermitteln der Subnetz-IDs, die einem bestimmten Aurora DB-Cluster einer bestimmten entsprechen.

Bei einem Aurora-Cluster finden Sie zuerst die ID für eine der zugehörigen DB-Instances. Sie können die von dieser DB-Instance verwendeten Subnetz-IDs extrahieren. Untersuchen Sie dazu die verschachtelten Felder innerhalb der Attribute `DBSubnetGroup` und `Subnets` in der Describe-Ausgabe für die DB-Instance. Sie geben einige oder alle dieser Subnetz-IDs an, wenn Sie einen Proxy für diesen Datenbankserver einrichten.

```
$ # Find the ID of any DB instance in the cluster.
$  aws rds describe-db-clusters --db-cluster-identifier my_cluster_id --query '*[].
[DBClusterMembers]||[0]||[0][*].DBInstanceIdentifier' --output text
```

```
my_instance_id
instance_id_2
instance_id_3
```

Nachdem Sie die ID der DB-Instance gefunden haben, untersuchen Sie die zugehörige VPC, um ihre Subnetze zu finden. Das folgende Linux-Beispiel zeigt wie es geht.

```
$ #From the DB instance, trace through the DBSubnetGroup and Subnets to find the subnet
 IDs.
$ aws rds describe-db-instances --db-instance-identifier my_instance_id --query '*[].
[DBSubnetGroup]||[0]||[0]||[Subnets]||[0]||[*].SubnetIdentifier' --output text
```

```
subnet_id_1
subnet_id_2
subnet_id_3
...
```

```
$ #From the DB instance, find the VPC.
$ aws rds describe-db-instances --db-instance-identifier my_instance_id --query '*[].
[DBSubnetGroup]||[0]||[0].VpcId' --output text
```

```
my_vpc_id
```

```
$ aws ec2 describe-subnets --filters Name=vpc-id,Values=my_vpc_id --query '*[].
[SubnetId]' --output text
```

```
subnet_id_1
subnet_id_2
```

```
subnet_id_3
subnet_id_4
subnet_id_5
subnet_id_6
```

Planen der Kapazität von IP-Adressen

Ein RDS-Proxy passt seine Kapazität basierend auf der Größe und Anzahl der bei ihm registrierten DB-Instances automatisch nach Bedarf an. Bestimmte Operationen erfordern möglicherweise auch zusätzliche Proxykapazität, z. B. die Erhöhung der Größe einer registrierten Datenbank oder interne Wartungsvorgänge für den RDS-Proxy. Bei diesen Vorgängen benötigt Ihr Proxy möglicherweise mehr IP-Adressen, um die zusätzliche Kapazität bereitzustellen. Mit diesen zusätzlichen Adressen kann Ihr Proxy skaliert werden, ohne Ihre Workload zu beeinträchtigen. Ein Mangel an freien IP-Adressen in Ihren Subnetzen verhindert, dass ein Proxy hochskaliert wird. Dies kann zu höheren Abfragelatenzen oder Verbindungsfehlern bei Clients führen. RDS benachrichtigt Sie durch das Ereignis `RDS-EVENT-0243`, wenn in Ihren Subnetzen nicht genügend freie IP-Adressen vorhanden sind. Weitere Informationen zu diesem Ereignis finden Sie unter Arbeiten mit RDS-Proxy-Ereignissen.

Im Folgenden finden Sie die empfohlene Mindestanzahl an IP-Adressen, die Sie in Ihren Subnetzen für Ihren Proxy frei lassen sollten, basierend auf der Größe der DB-Instance-Klassen.

DB-Instance-Klasse	Mindestanzahl freier IP-Adressen
db.*.xlarge oder kleiner	10
db.*.2xlarge	15
db.*.4xlarge	25
db.*.8xlarge	45
db.*.12xlarge	60
db.*.16xlarge	75
db.*.24xlarge	110

Bei dieser empfohlenen Anzahl von IP-Adressen handelt es sich um Schätzungen für einen Proxy, der nur den Standardendpunkt verwendet. Ein Proxy mit zusätzlichen Endpunkten oder Read

Replicas benötigt möglicherweise mehr freie IP-Adressen. Wir empfehlen, für jeden weiteren Endpunkt drei weitere IP-Adressen zu reservieren. Es wird empfohlen, für jede Read Replica zusätzliche IP-Adressen zu reservieren, wie in der Tabelle angegeben, basierend auf der Größe der Read Replica.

> **Note**
>
> RDS Proxy unterstützt nicht mehr als 215 IP-Adressen in einer VPC.

Angenommen, Sie möchten die erforderlichen IP-Adressen für einen Proxy schätzen, der einem Aurora-DB-Cluster zugeordnet ist.

Gehen Sie in diesem Fall von folgenden Annahmen aus:

- Ihr Aurora DB-Cluster verfügt über 1 Writer-Instance der Größe db.r5.8xlarge und 1 Reader-Instance der Größe db.r5.2xlarge.
- Der Proxy, der mit diesem DB-Cluster verbunden ist, verfügt über den Standardendpunkt und 1 benutzerdefinierten Endpunkt mit der schreibgeschützten Rolle.

In diesem Fall benötigt der Proxy ungefähr 63 freie IP-Adressen (45 für die Writer-Instance, 15 für die Reader-Instance und 3 für den zusätzlichen benutzerdefinierten Endpunkt).

Datenbankanmeldedaten einrichten in AWS Secrets Manager

Für jeden von Ihnen erstellten Proxy verwenden Sie zunächst den Service Secrets Manager, um Gruppen von Anmeldeinformationen aus Benutzername und Passwort zu speichern. Sie erstellen ein separates Secrets Manager Manager-Geheimnis für jedes Datenbankbenutzerkonto, mit dem sich der Proxy auf dem Aurora DB-Cluster der verbindet.

In der Secrets Manager Manager-Konsole erstellen Sie diese Geheimnisse mit Werten für die `password` Felder `username` und. Auf diese Weise kann der Proxy eine Verbindung zu den entsprechenden Datenbankbenutzern auf einem Aurora-DB-Cluster der herstellen, den Sie dem Proxy zuordnen. Hierfür können Sie die Einstellung Credentials for other database (Anmeldeinformationen für andere Datenbank), Credentials for RDS database (Anmeldeinformationen für die RDS-Datenbank) oder Other type of secrets (Andere Art von Secret) verwenden. Geben Sie die entsprechenden Werte für die Felder Benutzername und Passwort sowie

Werte für alle anderen Pflichtfelder ein. Der Proxy ignoriert andere Felder wie Host und Port, wenn sie im Secret vorhanden sind. Diese Details werden automatisch vom Proxy bereitgestellt.

Sie können auch Andere Arten von Geheimnissen wählen. In diesem Fall erstellen Sie das Secret mit den Schlüsseln namens `username` und `password`.

Um eine Verbindung über den Proxy als bestimmter Datenbankbenutzer herzustellen, stellen Sie sicher, dass das mit einem geheimen Schlüssel verknüpfte Passwort mit dem Datenbankkennwort für diesen Benutzer übereinstimmt. Wenn eine Unstimmigkeit vorliegt, können Sie das zugehörige Geheimnis in Secrets Manager aktualisieren. In diesem Fall können Sie weiterhin eine Verbindung zu anderen Konten herstellen, bei denen die geheimen Anmeldeinformationen und die Datenbankpasswörter übereinstimmen.

Wenn Sie einen Proxy über die AWS CLI oder RDS-API erstellen, geben Sie die Amazon-Ressourcennamen (ARNs) der entsprechenden Geheimnisse an. Diesen Vorgang führen Sie für alle DB-Benutzerkonten aus, auf die der Proxy zugreifen kann. In der AWS Management Console wählen Sie die Geheimnisse anhand ihrer aussagekräftigen Namen aus.

Anweisungen zum Erstellen von Secrets in Secrets Manager finden Sie auf der Seite Erstellen eines Secrets in der Secrets Manager-Dokumentation. Verwenden Sie eine der folgenden Techniken:

- Verwenden Sie Secrets Manager in der Konsole.
- Wenn Sie die CLI zum Erstellen eines Secrets Manager-Secrets für die Verwendung mit RDS Proxy verwenden möchten, verwenden Sie einen Befehl wie den folgenden.

```
aws secretsmanager create-secret
  --name "secret_name"
  --description "secret_description"
  --region region_name
  --secret-string '{"username":"db_user","password":"db_user_password"}'
```

- Sie können auch einen benutzerdefinierten Schlüssel erstellen, um Ihr Secrets Manager Manager-Geheimnis zu verschlüsseln. Der folgende Befehl erstellt einen Beispielschlüssel.

```
PREFIX=my_identifier
aws kms create-key --description "$PREFIX-test-key" --policy '{
  "Id":"$PREFIX-kms-policy",
  "Version":"2012-10-17",
  "Statement":
    [
      {
```

```
        "Sid":"Enable IAM User Permissions",
        "Effect":"Allow",
        "Principal":{"AWS":"arn:aws:iam::account_id:root"},
        "Action":"kms:*","Resource":"*"
      },
      {
        "Sid":"Allow access for Key Administrators",
        "Effect":"Allow",
        "Principal":
          {
            "AWS":
              ["$USER_ARN","arn:aws:iam:account_id::role/Admin"]
          },
        "Action":
          [
            "kms:Create*",
            "kms:Describe*",
            "kms:Enable*",
            "kms:List*",
            "kms:Put*",
            "kms:Update*",
            "kms:Revoke*",
            "kms:Disable*",
            "kms:Get*",
            "kms:Delete*",
            "kms:TagResource",
            "kms:UntagResource",
            "kms:ScheduleKeyDeletion",
            "kms:CancelKeyDeletion"
          ],
        "Resource":"*"
      },
      {
        "Sid":"Allow use of the key",
        "Effect":"Allow",
        "Principal":{"AWS":"$ROLE_ARN"},
        "Action":["kms:Decrypt","kms:DescribeKey"],
        "Resource":"*"
      }
    ]
}'
```

Mit den folgenden Befehlen werden beispielsweise Secrets Manager Manager-Geheimnisse für zwei Datenbankbenutzer erstellt:

```
aws secretsmanager create-secret \
  --name secret_name_1 --description "db admin user" \
  --secret-string '{"username":"admin","password":"choose_your_own_password"}'

aws secretsmanager create-secret \
  --name secret_name_2 --description "application user" \
  --secret-string '{"username":"app-user","password":"choose_your_own_password"}'
```

Verwenden Sie die folgenden Befehle, um diese mit Ihrem benutzerdefinierten AWS KMS Schlüssel verschlüsselten Geheimnisse zu erstellen:

```
aws secretsmanager create-secret \
  --name secret_name_1 --description "db admin user" \
  --secret-string '{"username":"admin","password":"choose_your_own_password"}'
  --kms-key-id arn:aws:kms:us-east-2:account_id:key/key_id

aws secretsmanager create-secret \
  --name secret_name_2 --description "application user" \
  --secret-string '{"username":"app-user","password":"choose_your_own_password"}'
  --kms-key-id arn:aws:kms:us-east-2:account_id:key/key_id
```

Verwenden Sie einen Befehl wie den folgenden, um die Geheimnisse zu sehen, die Ihrem AWS Konto gehören.

```
aws secretsmanager list-secrets
```

Wenn Sie einen Proxy mit der CLI erstellen, übergeben Sie die Amazon-Ressourcennamen (ARNs) von einem oder mehreren Secrets an den `--auth`-Parameter. Das folgende Linux-Beispiel zeigt, wie Sie einen Bericht erstellen, der nur den Namen und den ARN jedes Geheimnisses enthält, das Ihrem AWS Konto gehört. In diesem Beispiel wird der Parameter `--output table` verwendet, der in AWS CLI Version 2 verfügbar ist. Wenn Sie AWS CLI Version 1 verwenden, verwenden Sie `--output text` stattdessen.

```
aws secretsmanager list-secrets --query '*[].[Name,ARN]' --output table
```

Verwenden Sie einen Befehl wie den folgenden, um zu überprüfen, ob Sie die richtigen Anmeldeinformationen im richtigen Format im Secret gespeichert haben. Ersetzen Sie den Kurznamen oder den ARN des Secrets für *your_secret_name*.

```
aws secretsmanager get-secret-value --secret-id your_secret_name
```

Die Ausgabe sollte eine Zeile enthalten, die einen JSON-codierten Wert wie den folgenden anzeigt.

```
"SecretString": "{\"username\":\"your_username\",\"password\":\"your_password\"}",
```

AWS Identity and Access Management (IAM-) Richtlinien einrichten

Nachdem Sie die Secrets in Secrets Manager erstellt haben, erstellen Sie eine IAM-Richtlinie, die auf diese Secrets zugreifen kann. Allgemeine Informationen zur Verwendung von IAM finden Sie unter Identity and Access Management für Amazon Aurora.

> **Tip**
>
> Das folgende Verfahren gilt, wenn Sie die IAM-Konsole verwenden. Wenn Sie die AWS Management Console für RDS verwenden, kann RDS die IAM-Richtlinie automatisch für Sie erstellen. In diesem Fall können Sie das folgende Verfahren überspringen.

So erstellen Sie eine IAM-Richtlinie, die auf Ihre Secrets Manager-Geheimnisse für die Verwendung mit Ihrem Proxy zugreift

1. Melden Sie sich an der IAM-Konsole an. Folgen Sie dem Prozess „Rolle erstellen“, wie unter IAM-Rollen erstellen beschrieben, und wählen Sie „Rolle erstellen, um Berechtigungen an einen Dienst zu delegieren“ aus. AWS

   Wählen Sie als Typ vertrauenswürdiger Entitäten die Option AWS -Service aus. Wählen Sie unter Anwendungsfall die Option RDS aus der Dropdownliste Anwendungsfälle für andere AWS -Services aus. Wählen Sie RDS – Rolle zu Datenbank hinzufügen aus.
2. Führen Sie für die neue Rolle den Schritt Add inline policy (Inline-Richtlinie hinzufügen) aus. Verwenden Sie die gleichen allgemeinen Verfahren wie unter Bearbeiten von IAM-Richtlinien. Fügen Sie den folgenden JSON-Text in das JSON-Textfeld ein. Ersetzen Sie die Vorgabe durch Ihre eigene Konto-ID. Ersetzen Sie Ihre AWS Region durch. `us-east-2` Ersetzen Sie die

Amazon-Ressourcennamen (ARNs) durch die von Ihnen erstellten Secrets, vgl. Angeben von KMS-Schlüsseln in IAM-Richtlinienanweisungen. Ersetzen Sie für die `kms:Decrypt` Aktion den ARN des Standard-Schlüssels AWS KMS key oder Ihren eigenen KMS-Schlüssel. Welchen ARN Sie verwenden, hängt davon ab, welchen Sie zum Verschlüsseln der Secrets von Secrets Manager verwendet haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": [
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_1",
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_2"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "kms:Decrypt",
            "Resource": "arn:aws:kms:us-east-2:account_id:key/key_id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
                }
            }
        }
    ]
}
```

3. Bearbeiten Sie die Vertrauensrichtlinie für diese IAM-Rolle. Fügen Sie den folgenden JSON-Text in das JSON-Textfeld ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "rds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Die folgenden Befehle führen dieselbe Operation über die durc AWS CLI.

```
PREFIX=my_identifier
USER_ARN=$(aws sts get-caller-identity --query "Arn" --output text)

aws iam create-role --role-name my_role_name \
  --assume-role-policy-document '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"Service":
["rds.amazonaws.com"]},"Action":"sts:AssumeRole"}]}'

ROLE_ARN=arn:aws:iam::account_id:role/my_role_name

aws iam put-role-policy --role-name my_role_name \
  --policy-name $PREFIX-secret-reader-policy --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": [
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_1",
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_2"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "kms:Decrypt",
            "Resource": "arn:aws:kms:us-east-2:account_id:key/key_id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
                }
            }
```

```
        }
    ]
}
```

Erstellen eines RDS Proxy

Um Verbindungen für einen DB-Cluster zu verwalten, erstellen Sie einen Proxy. Sie können einen Proxy einem DB-Cluster von Aurora MySQL oder einem Aurora PostgreSQL zuordnen.

AWS Management Console

So erstellen Sie einen Proxy

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Proxies (Proxys).
3. Wählen Sie Create proxy (Proxy erstellen).
4. Wählen Sie alle Einstellungen für Ihren Proxy.

   Geben Sie für die Proxy-Konfiguration folgende Informationen an:

   - Engine family (Engine-Familie). Diese Einstellung legt fest, welches Datenbanknetzwerkprotokoll der Proxy erkennt, wenn er den Netzwerkverkehr zu und von der Datenbank interpretiert. Wählen Sie für Aurora MySQL MariaDB und MySQL aus. Für Aurora PostgreSQL wählen Sie PostgreSQL aus.
   - Proxy identifier (Proxy-ID. Geben Sie einen Namen an, der innerhalb Ihrer AWS Konto-ID und Ihrer aktuellen AWS Region eindeutig ist.
   - Idle client connection timeout (Zeitüberschreitung bei Client-Leerlauf. Wählen Sie einen Zeitraum, in dem eine Client-Verbindung inaktiv sein kann, bevor der Proxy sie schließt. Der Standardwert ist 1.800 Sekunden (30 Minuten). Eine Client-Verbindung gilt als inaktiv, wenn die Anwendung innerhalb der angegebenen Zeit nach Abschluss der vorherigen Anforderung keine neue Anforderung absendet. Die zugrunde liegende Datenbankverbindung bleibt offen und wird an den Verbindungspool zurückgegeben. Somit ist sie für neue Clientverbindungen verfügbar.

     Damit der Proxy proaktiv veraltete Verbindungen entfernt, verringern Sie den Timeout für inaktive Client-Verbindungen. Wenn die Arbeitslast stark ansteigt, erhöhen Sie das Timeout für inaktive Client-Verbindungen, um die Kosten für den Verbindungsaufbau zu sparen.“

Machen Sie für Zielgruppenkonfiguration folgende Angaben:

- Database (Datenbank. Wählen Sie eine , den Aurora-DB-Cluster, auf die Sie über diesen Proxy zugreifen möchten. Die Liste enthält nur DB-Instances und Cluster mit kompatiblen Datenbank-Engines, Engine-Versionen und anderen Einstellungen. Wenn die Liste leer ist, erstellen Sie eine neue DB-Instance oder einen neuen Cluster, mit der/dem RDS Proxy kompatibel ist. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Erstellen eines Amazon Aurora-DB Clusters. Versuchen Sie dann erneut, den Proxy zu erstellen.
- Connection pool maximum connections (Max. Verbindungen Verbindungspool. Geben Sie einen Wert zwischen 1 und 100 an. Diese Einstellung stellt den Prozentsatz des `max_connections`-Wertes dar, den RDS Proxy für Verbindungen verwenden kann. Wenn Sie nur einen Proxy mit dieser DB-Instance oder diesem DB-Cluster verwenden möchten, können Sie den Wert auf 100 setzen. Weitere Informationen dazu, wie RDS Proxy diese Einstellung verwendet, finden Sie unter MaxConnectionsProzent.
- Session pinning filters (Filter zum Anheften von Sitzungen. (Optional) Mit dieser Option können Sie den RDS-Proxy zwingen, Sitzungen bei bestimmten Status nicht zu fixieren. Dadurch werden die standardmäßigen Sicherheitsmaßnahmen für das Multiplexing von Datenbankverbindungen über Client-Verbindungen hinweg umgangen. Derzeit wird die Einstellung für PostgreSQL nicht unterstützt. Die einzige Wahl ist. `EXCLUDE_VARIABLE_SETS`

  Die Aktivierung dieser Einstellung kann dazu führen, dass sich Sitzungsvariablen einer Verbindung auf andere Verbindungen auswirken. Dies kann zu Fehlern oder Problemen mit der Korrektheit führen, wenn Ihre Abfragen von Sitzungsvariablenwerten abhängen, die außerhalb der aktuellen Transaktion festgelegt wurden. Erwägen Sie, diese Option zu verwenden, nachdem Sie sich vergewissert haben, dass Ihre Anwendungen Datenbankverbindungen über mehrere Client-Verbindungen gemeinsam nutzen können.

  Die folgenden Muster können als sicher angesehen werden:

  - `SET`-Anweisungen, bei denen der effektive Wert der Sitzungsvariablen nicht geändert wird, d. h. dass keine Änderung an der Sitzungsvariablen vorgenommen wird.
  - Sie ändern den Wert der Sitzungsvariablen und führen eine Anweisung in derselben Transaktion aus.

  Weitere Informationen finden Sie unter Vermeiden des Fixierens.

- Connection borrow timeout (Zeitüberschreitung für die Verbindung. In einigen Fällen erwarten Sie möglicherweise, dass der Proxy manchmal alle verfügbaren Verbindungen nutzt. In solchen Fällen können Sie angeben, wie lange der Proxy wartet, bis eine Datenbankverbindung verfügbar ist, bevor ein Timeout-Fehler zurückgegeben wird. Sie können einen Zeitraum von maximal fünf Minuten angeben. Diese Einstellung gilt nur, wenn der Proxy die maximale Anzahl von Verbindungen geöffnet hat und alle Verbindungen bereits verwendet werden.
- Initialisierungsabfrage. (Optional) Sie können eine oder mehrere SQL-Anweisungen für die Ausführung durch den Proxy beim Öffnen jeder neuen Datenbankverbindung festlegen. Diese Einstellung wird in der Regel zusammen mit `SET` Anweisungen verwendet, um sicherzustellen, dass jede Verbindung identische Einstellungen wie Zeitzone und Zeichensätze hat. Verwenden Sie für mehrere Anweisungen Semikola als Trennzeichen. Sie können auch mehrere Variablen in eine einzelne `SET`-Anweisung einschließen, z. B. `SET x=1, y=2`.

Geben Sie unter Authentication (Authentifizierung) Informationen für Folgendes an:

- IAM role (IAM-Rolle. Wählen Sie eine IAM-Rolle aus, die berechtigt ist, auf die zuvor ausgewählten Secrets Manager-Geheimnisse zuzugreifen. Oder Sie können eine neue IAM-Rolle aus dem AWS Management Console erstellen.
- Secrets Manager Geheimnisse. Wählen Sie mindestens ein Secrets Manager Manager-Geheimnis, das Datenbank-Benutzeranmeldedaten enthält, die es dem Proxy ermöglichen, auf den Aurora DB-Cluster der zuzugreifen.
- Client authentication type (Client-Authentifizierungstyp). Wählen Sie den Authentifizierungstyp, den der Proxy für Verbindungen von Clients verwendet. Die ausgewählte Option gilt für alle Secrets-Manager-Secrets, die Sie diesem Proxy zuordnen. Wenn Sie für jedes Geheimnis einen anderen Client-Authentifizierungstyp angeben müssen, erstellen Sie Ihren Proxy stattdessen mithilfe der AWS CLI oder der API.
- IAM Authentication (IAM-Authentifizierung. Wählen Sie aus, ob die IAM-Authentifizierung für Verbindungen mit Ihrem Proxy erforderlich ist oder nicht zugelassen werden soll. Die ausgewählte Option gilt für alle Secrets-Manager-Secrets, die Sie diesem Proxy zuordnen. Wenn Sie für jedes Geheimnis eine andere IAM-Authentifizierung angeben müssen, erstellen Sie Ihren Proxy stattdessen mithilfe der AWS CLI oder der API.

Geben Sie für Anbindung folgende Informationen an:

- Require Transport Layer Security (Transport Layer Security erfordern). Wählen Sie diese Einstellung, wenn der Proxy TLS/SSL für alle Clientverbindungen erzwingen soll. Bei einer verschlüsselten oder unverschlüsselten Verbindung mit einem Proxy verwendet der Proxy dieselbe Verschlüsselungseinstellung, wenn er eine Verbindung mit der zugrunde liegenden Datenbank herstellt.
- Subnets (Subnetze. Dieses Feld ist mit allen Subnetzen gefüllt, die mit Ihrer VPC verknüpft sind. Sie können alle Subnetze entfernen, die Sie für diesen Proxy nicht benötigen. Sie müssen mindestens zwei Subnetze übrig lassen.

Stellen Sie eine zusätzliche Anbindungskonfiguration bereit:

- VPC Security Group (VPC-Sicherheitsgruppe. Wählen Sie eine vorhandene VPC-Sicherheitsgruppe aus. Oder Sie können eine neue Sicherheitsgruppe aus dem AWS Management Console erstellen. Sie müssen die Regeln für eingehenden Datenverkehr so konfigurieren, dass Ihre Anwendungen auf den Proxy zugreifen können. Außerdem müssen Sie die Regeln für ausgehenden Datenverkehr so konfigurieren, das Datenverkehr von Ihren DB-Zielen zugelassen wird.

  > **Note**
  >
  > Diese Sicherheitsgruppe muss Verbindungen vom Proxy mit der Datenbank zulassen. Dieselbe Sicherheitsgruppe wird für eingehenden Datenverkehr von Ihren Anwendungen zum Proxy und für ausgehenden Datenverkehr vom Proxy zur Datenbank verwendet. Angenommen, Sie verwenden dieselbe Sicherheitsgruppe für Ihre Datenbank und Ihren Proxy. Stellen Sie in diesem Fall sicher, dass Sie angeben, dass Ressourcen in dieser Sicherheitsgruppe mit anderen Ressourcen in derselben Sicherheitsgruppe kommunizieren können.
  > Wenn Sie eine freigegebene VPC verwenden, können Sie die Standardsicherheitsgruppe für die VPC oder eine zu einem anderen Konto gehörende Gruppe nicht verwenden. Wählen Sie eine Sicherheitsgruppe aus, die zu Ihrem Konto gehört. Wenn keine vorhanden ist, erstellen Sie eine. Weitere Informationen zu dieser Einschränkung finden Sie unter Arbeiten mit freigegebenen VPCs.

RDS stellt einen Proxy über mehrere Availability Zones hinweg bereit, um eine hohe Verfügbarkeit zu gewährleisten. Um die AZ-übergreifende Kommunikation für einen solchen

Proxy zu ermöglichen, muss die Zugriffssteuerungsliste (ACL) für Ihr Proxy-Subnetz den Engine-Port-spezifischen Ausgang und den Eingang aller Ports zulassen. Weitere Informationen zu Netzwerk-ACLs finden Sie unter Datenverkehr in Subnetzen mit Netzwerk-ACLs steuern. Wenn die Netzwerk-ACL für Ihren Proxy und Ihr Ziel identisch sind, müssen Sie eine TCP-Protokoll-Ingress-Regel hinzufügen, bei der die Quelle auf die VPC-CIDR festgelegt ist. Sie müssen auch eine Engine-Port-spezifische TCP-Protokollausgangsregel hinzufügen, bei der das Ziel auf die VPC-CIDR festgelegt ist.

(Optional) Stellen Sie eine erweiterte Konfiguration bereit:

- Enable enhanced logging (Erweiterte Protokollierung aktivieren. Sie können diese Einstellung aktivieren, um Proxy-Kompatibilitäts- oder Leistungsprobleme zu beheben.

  Wenn diese Einstellung aktiviert ist, nimmt der RDS-Proxy detaillierte Informationen zur Proxyleistung in seine Protokolle auf. Diese Informationen helfen Ihnen beim Debugging von Problemen mit dem SQL-Verhalten oder der Leistung und Skalierbarkeit der Proxy-Verbindungen. Aktivieren Sie diese Einstellung daher nur zum Debuggen und wenn Sie Sicherheitsmaßnahmen getroffen haben, um vertrauliche Informationen zu schützen, die in den Protokollen erscheinen.

  Um den mit Ihrem Proxy verbundenen Overhead zu minimieren, wird diese Einstellung von RDS Proxy automatisch 24 Stunden nach der Aktivierung deaktiviert. Aktivieren Sie sie vorübergehend, um ein bestimmtes Problem zu beheben.

5. Wählen Sie Create Proxy (Proxy erstellen).

AWS CLI

Um einen Proxy mit dem zu erstellen AWS CLI, rufen Sie den Befehl create-db-proxy mit den folgenden erforderlichen Parametern auf:

- `--db-proxy-name`
- `--engine-family`
- `--role-arn`
- `--auth`
- `--vpc-subnet-ids`

Bei `--engine-family`-Wert ist die Groß- und Kleinschreibung zu beachten.

Example

FürLinux, oder: macOS Unix

```
aws rds create-db-proxy \
    --db-proxy-name proxy_name \
    --engine-family { MYSQL | POSTGRESQL | SQLSERVER } \
    --auth ProxyAuthenticationConfig_JSON_string \
    --role-arn iam_role \
    --vpc-subnet-ids space_separated_list \
    [--vpc-security-group-ids space_separated_list] \
    [--require-tls | --no-require-tls] \
    [--idle-client-timeout value] \
    [--debug-logging | --no-debug-logging] \
    [--tags comma_separated_list]
```

Windows:

```
aws rds create-db-proxy ^
    --db-proxy-name proxy_name ^
    --engine-family { MYSQL | POSTGRESQL | SQLSERVER } ^
    --auth ProxyAuthenticationConfig_JSON_string ^
    --role-arn iam_role ^
    --vpc-subnet-ids space_separated_list ^
    [--vpc-security-group-ids space_separated_list] ^
    [--require-tls | --no-require-tls] ^
    [--idle-client-timeout value] ^
    [--debug-logging | --no-debug-logging] ^
    [--tags comma_separated_list]
```

Nachstehend finden Sie ein Beispiel für den JSON-Wert der `--auth`-Option. Dieses Beispiel wendet auf jedes Secret einen anderen Client-Authentifizierungstyp an.

```
[
  {
    "Description": "proxy description 1",
    "AuthScheme": "SECRETS",
    "SecretArn": "arn:aws:secretsmanager:us-
west-2:123456789123:secret/1234abcd-12ab-34cd-56ef-1234567890ab",
    "IAMAuth": "DISABLED",
    "ClientPasswordAuthType": "POSTGRES_SCRAM_SHA_256"
```

```
  },

  {
    "Description": "proxy description 2",
    "AuthScheme": "SECRETS",
    "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:seret/1234abcd-12ab-34cd-56ef-1234567890cd",
    "IAMAuth": "DISABLED",
    "ClientPasswordAuthType": "POSTGRES_MD5"

  },

  {
    "Description": "proxy description 3",
    "AuthScheme": "SECRETS",
    "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122221111:secret/1234abcd-12ab-34cd-56ef-1234567890ef",
    "IAMAuth": "REQUIRED"
  }

]
```

Tip

Wenn Sie die Subnetz-IDs nicht bereits kennen, die für den Parameter `--vpc-subnet-ids` verwendet werden sollen, finden Sie unter Einrichten der Netzwerkvoraussetzungen Beispiele, wie Sie diese finden können.

Note

Diese Sicherheitsgruppe muss den Zugriff auf die Datenbank zulassen, mit welcher der Proxy eine Verbindung herstellt. Dieselbe Sicherheitsgruppe wird für eingehenden Datenverkehr von Ihren Anwendungen zum Proxy und für ausgehenden Datenverkehr vom Proxy zur Datenbank verwendet. Angenommen, Sie verwenden dieselbe Sicherheitsgruppe für Ihre Datenbank und Ihren Proxy. Stellen Sie in diesem Fall sicher, dass Sie angeben, dass Ressourcen in dieser Sicherheitsgruppe mit anderen Ressourcen in derselben Sicherheitsgruppe kommunizieren können.
Wenn Sie eine freigegebene VPC verwenden, können Sie die Standardsicherheitsgruppe für die VPC oder eine zu einem anderen Konto gehörende Gruppe nicht verwenden. Wählen

Sie eine Sicherheitsgruppe aus, die zu Ihrem Konto gehört. Wenn keine vorhanden ist, erstellen Sie eine. Weitere Informationen zu dieser Einschränkung finden Sie unter Arbeiten mit freigegebenen VPCs.

Um die richtigen Verknüpfungen für den Proxy zu erstellen, verwenden Sie auch den Befehl register-db-proxy-targets. Angabe des `default`-Zielgruppennamens. RDS Proxy erstellt automatisch eine Zielgruppe mit diesem Namen, wenn Sie jeden Proxy erstellen.

```
aws rds register-db-proxy-targets
    --db-proxy-name value
    [--target-group-name target_group_name]
    [--db-instance-identifiers space_separated_list]  # rds db instances, or
    [--db-cluster-identifiers cluster_id]        # rds db cluster (all instances)
```

RDS-API

Um einen RDS Proxy zu erstellen, rufen Sie die Amazon RDS-API-Operation CreateDBProxy auf. Sie übergeben einen Parameter mit der Datenstruktur. AuthConfig

RDS Proxy erstellt automatisch eine Zielgruppe mit dem Namen `default`, wenn Sie die einzelnen Proxys erstellen. Sie ordnen der Zielgruppe einen zu, indem Sie die Funktion RegisterDB ProxyTargets aufrufen.

Anzeigen eines RDS Proxy

Nachdem Sie einen oder mehrere RDS-Proxys erstellt haben, können Sie alle anzeigen. Dies ermöglicht es, ihre Konfigurationsdetails zu überprüfen und auszuwählen, welche geändert, gelöscht usw. werden sollen.

Damit Datenbankanwendungen einen Proxy verwenden können, müssen Sie den Proxy-Endpunkt in der Verbindungszeichenfolge angeben.

AWS Management Console

So zeigen Sie Ihren Proxy an

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie in der oberen rechten Ecke von die AWS Region aus AWS Management Console, in der Sie den RDS-Proxy erstellt haben.
3. Wählen Sie im Navigationsbereich Proxies (Proxys).
4. Wählen Sie den Namen eines RDS-Proxys, um dessen Details anzuzeigen.
5. Auf der Detailseite zeigt der Abschnitt Zielgruppen, wie der Proxy mit einem bestimmten Aurora DB-Cluster einer bestimmten verknüpft ist. Sie können dem Link zur Standard-Zielgruppenseite folgen, um weitere Details zur Zuordnung zwischen dem Proxy und der Datenbank anzuzeigen. Auf dieser Seite werden Einstellungen angezeigt, die Sie beim Erstellen des Proxys angegeben haben. Dazu gehören maximaler Verbindungsprozentsatz, Zeitüberschreitung für die Verbindung, Engine-Familie und Sitzungs-Pinning-Filter.

CLI

Um Ihren Proxy mit der CLI anzuzeigen, verwenden Sie den Befehl describe-db-proxies. Standardmäßig werden alle Proxys angezeigt, die Ihrem AWS Konto gehören. Um Details für einen einzelnen Proxy anzuzeigen, geben Sie seinen Namen mit dem Parameter `--db-proxy-name` an.

```
aws rds describe-db-proxies [--db-proxy-name proxy_name]
```

Verwenden Sie die folgenden Befehle, um die anderen Informationen anzuzeigen, die mit dem Proxy verknüpft sind.

```
aws rds describe-db-proxy-target-groups  --db-proxy-name proxy_name

aws rds describe-db-proxy-targets --db-proxy-name proxy_name
```

Verwenden Sie die folgende Befehlsfolge, um weitere Details zu den Elementen anzuzeigen, die mit dem Proxy verknüpft sind:

1. Um eine Liste von Proxys anzufordern, führen Sie describe-db-proxies aus.
2. Führen Sie describe-db-proxy-target-groups `--db-proxy-name` aus, um Verbindungsparameter anzuzeigen, wie den maximalen Prozentsatz der Verbindungen, die der Proxy verwenden kann. Verwenden Sie den Namen des Proxys als Parameterwert.
3. Um die Details des Aurora-DB-Clusters der anzuzeigen, der mit der zurückgegebenen Zielgruppe verknüpft ist, führen Sie describe-db-proxy-targets aus.

RDS-API

Verwenden Sie den Vorgang DescribeDBProxies, um Ihre Proxys mit der RDS-API anzuzeigen. Er gibt Werte des Datentyps DBProxy zurück.

Um Details zu den Verbindungseinstellungen für den Proxy zu sehen, verwenden Sie die Proxybezeichner aus diesem Rückgabewert mit dem Vorgang DescribeDB Groups. ProxyTarget Es gibt Werte des ProxyTargetDB-Gruppen-Datentyps zurück.

Verwenden Sie den Vorgang DescribeDB, um die mit dem Proxy verknüpfte RDS-Instance oder den Aurora-DB-Cluster zu ProxyTargets sehen. Sie gibt Werte des ProxyTargetDB-Datentyps zurück.

Verbinden mit einer Datenbank über RDS Proxy

Sie stellen eine Verbindung mit einem Aurora-DB-Cluster oder einem Cluster, der Aurora Serverless v2 verwendet, über einen Proxy in der Regel auf die gleiche Weise her, wie Sie eine direkte Verbindung mit der Datenbank herstellen. Der Hauptunterschied besteht darin, dass Sie anstelle des Cluster-Endpunkts den Proxy-Endpunkt angeben. Standardmäßig verfügen alle Proxy-Verbindungen über Lese-/Schreibfunktionen und verwenden die Writer-Instance. Wenn Sie den Reader-Endpunkt normalerweise für schreibgeschützte Verbindungen verwenden, können Sie einen zusätzlichen schreibgeschützten Endpunkt für den Proxy erstellen. Diesen Endpunkt können Sie auf die gleiche Weise verwenden. Weitere Informationen finden Sie unter Überblick über Proxy-Endpunkte.

Themen

- Herstellen einer Verbindung mit einem Proxy mithilfe der systemeigenen Authentifizierung
- Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung
- Überlegungen zum Herstellen einer Verbindung mit einem Proxy mit PostgreSQL

Herstellen einer Verbindung mit einem Proxy mithilfe der systemeigenen Authentifizierung

Gehen Sie wie folgt vor, um mithilfe der systemeigenen Authentifizierung eine Verbindung zu einem Proxy herzustellen:

1. Suchen Sie den Proxy-Endpunkt. Im finden Sie den AWS Management Console Endpunkt auf der Detailseite für den entsprechenden Proxy. Mit dem AWS CLI können Sie den Befehl describe-db-proxies verwenden. Im folgenden Beispiel wird gezeigt, wie dies geschieht.

```
# Add --output text to get output as a simple tab-separated list.
$ aws rds describe-db-proxies --query '*[*].
{DBProxyName:DBProxyName,Endpoint:Endpoint}'
[
    [
        {
            "Endpoint": "the-proxy.proxy-demo.us-east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy"
        },
        {
            "Endpoint": "the-proxy-other-secret.proxy-demo.us-
east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-other-secret"
        },
        {
            "Endpoint": "the-proxy-rds-secret.proxy-demo.us-
east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-rds-secret"
        },
        {
            "Endpoint": "the-proxy-t3.proxy-demo.us-east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-t3"
        }
    ]
]
```

2. Geben Sie den Endpunkt als Hostparameter in der Verbindungszeichenfolge für Ihre Client-Anwendung an. Geben Sie beispielsweise den Proxy-Endpunkt als Wert für die Option `mysql -h` oder `psql -h` an.
3. Geben Sie denselben Datenbankbenutzernamen und dasselbe Passwort an, die Sie normalerweise verwenden.

Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung

Wenn Sie die IAM-Authentifizierung für RDS Proxy verwenden, müssen Sie die Benutzer Ihrer Datenbank auf die Authentifizierung mit ihrem regulären Benutzernamen und Passwort festlegen. Die IAM-Authentifizierung gilt für den Abruf von Benutzername und Passwort aus Secrets Manager durch RDS Proxy. Die Verbindung von RDS Proxy zur zugrunde liegenden Datenbank erfolgt nicht über IAM.

Um mithilfe der IAM-Authentifizierung eine Verbindung zum RDS-Proxy herzustellen, verwenden Sie dasselbe allgemeine Verbindungsverfahren wie für die IAM-Authentifizierung mit einem Aurora DB-Cluster einer . Allgemeine Informationen zur Verwendung von IAM finden Sie unter Sicherheit in Amazon Aurora.

Zu den Hauptunterschieden bei der IAM-Nutzung für RDS Proxy gehören die folgenden:

- Sie konfigurieren nicht jeden einzelnen Datenbankbenutzer mit einem Autorisierungs-Plugin. Die Datenbankbenutzer haben weiterhin normale Benutzernamen und Passwörter innerhalb der Datenbank. Sie richten Secrets Manager-Geheimnisse ein, die diese Benutzernamen und Passwörter enthalten, und autorisieren RDS Proxy, die Anmeldeinformationen von Secrets Manager abzurufen.

  Die IAM-Authentifizierung gilt für die Verbindung zwischen Ihrem Clientprogramm und dem Proxy. Der Proxy authentifiziert sich dann bei der Datenbank mit den Anmeldeinformationen aus Benutzername und Passwort, die von Secrets Manager abgerufen wurden.
- Anstelle des Instance-, Cluster- oder Leser-Endpunkts geben Sie den Proxy-Endpunkt an. Weitere Informationen zum Proxy-Endpunkt finden Sie unter Herstellen einer Verbindung zu Ihrem DB--Cluster mithilfe der IAM-Authentifizierung.
- Im Anwendungsfall mit direkter Datenbank-IAM-Authentifizierung wählen Sie Datenbankbenutzer selektiv aus und konfigurieren sie so, dass sie mit einem speziellen Authentifizierungs-Plug-In identifiziert werden. Sie können dann mit IAM-Authentifizierung eine Verbindung zu diesen Benutzern herstellen.

  Im Proxy-Anwendungsfall müssen Sie dem Proxy die Geheimnisse bereitstellen, die den Benutzernamen und das Passwort eines Benutzers enthalten (native Authentifizierung). Anschließend stellen Sie mithilfe der IAM-Authentifizierung eine Verbindung mit dem Proxy her. Hierzu generieren Sie ein Authentifizierungstoken mit dem Proxy-Endpunkt und nicht mit dem Datenbankendpunkt. Sie verwenden auch einen Benutzernamen, der mit einem der Benutzernamen für die von Ihnen angegebenen Geheimnisse übereinstimmt.
- Sie müssen Transport Layer Security (TLS)/Secure Sockets Layer (SSL) verwenden, wenn Sie mit IAM-Authentifizierung eine Verbindung zu einem Proxy herstellen.

Sie können einem bestimmten Benutzer Zugriff auf den Proxy gewähren, indem Sie die IAM-Richtlinie ändern. Ein Beispiel folgt.

```
"Resource": "arn:aws:rds-db:us-east-2:1234567890:dbuser:prx-ABCDEFGHIJKL01234/db_user"
```

Überlegungen zum Herstellen einer Verbindung mit einem Proxy mit PostgreSQL

Wenn ein Client in PostgreSQL eine Verbindung mit einer PostgreSQL-Datenbank startet, sendet er eine Startup-Meldung. Diese Nachricht enthält Paare von Parameternamen und Wertzeichenfolgen. Weitere Informationen finden Sie unter `StartupMessage` in den PostgreSQL-Nachrichtenformaten in der PostgreSQL-Dokumentation.

Wenn Sie eine Verbindung über einen RDS Proxy herstellen, kann die Startmeldung die folgenden aktuell erkannten Parameter enthalten:

- `user`
- `database`

Die Startmeldung kann auch die folgenden zusätzlichen Laufzeitparameter enthalten:

- `application_name`
- `client_encoding`
- `DateStyle`
- `TimeZone`
- `extra_float_digits`
- `search_path`

Weitere Informationen zum PostgreSQL-Messaging finden Sie im Frontend/Backend-Protokoll in der PostgreSQL-Dokumentation.

Wenn Sie für PostgreSQL JDBC verwenden, empfehlen wir Folgendes, um Pinning zu vermeiden:

- Stellen Sie den JDBC-Verbindungsparameter `assumeMinServerVersion` mindestens auf `9.0` ein, um Pinning zu vermeiden. Dadurch wird verhindert, dass der JDBC-Treiber beim Verbindungsstart, wenn er ausgeführt wird, einen zusätzlichen Roundtrip durchführt. `SET extra_float_digits = 3`
- Setzen Sie den JDBC-Verbindungsparameter `ApplicationName` auf *`any/your-application-name`*, um Pinning zu vermeiden. Dadurch wird verhindert, dass der JDBC-Treiber beim Starten der Verbindung einen zusätzlichen Roundtrip ausführt, wenn er ausführ `SET application_name = "PostgreSQL JDBC Driver"`. Beachten Sie, dass der JDBC-Parameter `ApplicationName`, der PostgreSQL-`StartupMessage`-Parameter aber `application_name` ist.

Weitere Informationen finden Sie unter Vermeiden des Fixierens. Weitere Informationen zum Herstellen einer Verbindung mit JDBC finden Sie unter Verbinden mit der Datenbank in der PostgreSQL-Dokumentation.

Verwalten eines RDS-Proxy

Dieser Abschnitt enthält Informationen zur Verwaltung des Betriebs und der Konfiguration des RDS-Proxys. Diese Verfahren helfen Ihrer Anwendung, Datenbankverbindungen möglichst effizient zu nutzen und eine maximale Wiederverwendung der Verbindung zu erzielen. Je mehr Sie die Wiederverwendung der Verbindung nutzen können, desto mehr CPU- und Arbeitsspeicher-Overhead können Sie sparen. Dies reduziert wiederum die Latenz für Ihre Anwendung und ermöglicht es der Datenbank, mehr Ressourcen für die Verarbeitung von Anwendungsanforderungen zu verwenden.

Themen

Ändern eines RDS Proxy

Sie können bestimmte Einstellungen ändern, die einem Proxy zugeordnet sind, nachdem Sie den Proxy erstellt haben. Dazu ändern Sie den Proxy selbst, die zugehörige Zielgruppe oder beides. Jedem Proxy ist eine Zielgruppe zugeordnet.

AWS Management Console

> **Important**
>
> Die Werte in den Feldern Client authentication type (Client-Authentifizierungstyp) und IAM authentication (IAM-Authentifizierung) gelten für alle Secrets-Manager-Secrets, die diesem Proxy zugeordnet sind. Um für jedes Geheimnis unterschiedliche Werte anzugeben, ändern Sie Ihren Proxy, indem Sie stattdessen die AWS CLI oder die API verwenden.

So ändern Sie die Einstellungen für einen Proxy:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Proxies (Proxys).
3. Wählen Sie in der Liste der Proxys den Proxy aus, dessen Einstellungen Sie ändern möchten, oder gehen Sie zur Detailseite.
4. Wählen Sie für Actions (Aktionen) die Option Modify (Ändern) aus.
5. Geben Sie die zu ändernden Eigenschaften ein, oder wählen Sie sie aus. Sie können folgende Formen angeben:
   - Proxy-Identifikator - Benennen Sie den Proxy um, indem Sie einen neuen Identifikator eingeben.
   - Zeitüberschreitung für Client-Verbindungsleerlauf— Geben Sie einen Zeitraum für das Timeout für die Clientleerlauf ein.
   - IAM-Rolle - Ändern Sie die IAM-Rolle, die zum Abrufen der Geheimnisse von Secrets Manager verwendet wird.
   - Secrets Manager-Secrets— Hinzufügen oder entfernen Sie Secrets Manager Geheimnisse. Diese Secrets entsprechen Datenbankbenutzernamen und Passwörtern.
   - Client authentication type (Client-Authentifizierungstyp) – (nur PostgreSQL) Ändern Sie den Authentifizierungstyp für Client-Verbindungen zum Proxy.
   - IAM authentication (IAM-Authentifizierung) – Verlangen oder unterbinden Sie die IAM-Authentifizierung für Verbindungen mit dem Proxy.
   - Require Transport Layer Security— Aktivieren oder deaktivieren Sie die Anforderung für Transport Layer Security (TLS).
   - VPC-Sicherheitsgruppe - Fügen Sie VPC-Sicherheitsgruppen hinzu oder entfernen Sie sie, damit der Proxy sie verwenden kann.
   - Aktivieren der erweiterten Protokollierung— Aktivieren oder deaktivieren Sie die erweiterte Protokollierung.
6. Wählen Sie Ändern aus.

Wenn Sie die Einstellungen, die Sie ändern möchten, in der Liste nicht gefunden haben, verwenden Sie das folgende Verfahren, um die Zielgruppe für den Proxy zu aktualisieren. Die Zielgruppe, die einem Proxy zugeordnet ist, steuert die Einstellungen für die physischen Datenbankverbindungen.

Jedem Proxy ist eine Zielgruppe mit dem Namen `default` zugeordnet, die automatisch zusammen mit dem Proxy erstellt wird.

Sie können die Zielgruppe nur über die Proxy-Detailseite ändern, nicht über die Liste auf der Seite Proxies (Proxys).

So ändern Sie die Einstellungen für eine Proxy-Zielgruppe:

1. Gehen Sie auf der Seite Proxys zur Detailseite für einen Proxy.
2. Wählen Sie für Target groups (Zielgruppen) den `default`-Link aus. Derzeit haben alle Proxys eine einzelne Zielgruppe mit dem Namen `default`.
3. Wählen Sie auf der Detailseite für die Standard-Zielgruppe die Option Modify (Ändern).
4. Wählen Sie neue Einstellungen für die Eigenschaften aus, die Sie ändern können:

   - Datenbank – Wählen Sie einen anderen Aurora-Cluster aus.
   - Maximale Verbindungen des Verbindungspools - Legen Sie fest, wie viel Prozent der maximal verfügbaren Verbindungen der Proxy nutzen kann.
   - Vortrags-Anheftungsfilter – Wählen Sie optional einen Vortrags-Anheftungsfilter aus. Dadurch werden die standardmäßigen Sicherheitsmaßnahmen für das Multiplexing von Datenbankverbindungen über Client-Verbindungen hinweg umgangen. Derzeit wird die Einstellung für PostgreSQL nicht unterstützt. Die einzige Wahl ist. `EXCLUDE_VARIABLE_SETS`

     Die Aktivierung dieser Einstellung kann dazu führen, dass sich Sitzungsvariablen einer Verbindung auf andere Verbindungen auswirken. Dies kann zu Fehlern oder Problemen mit der Korrektheit führen, wenn Ihre Abfragen von Sitzungsvariablenwerten abhängen, die außerhalb der aktuellen Transaktion festgelegt wurden. Erwägen Sie, diese Option zu verwenden, nachdem Sie sich vergewissert haben, dass Ihre Anwendungen Datenbankverbindungen über mehrere Client-Verbindungen gemeinsam nutzen können.

     Die folgenden Muster können als sicher angesehen werden:

     - `SET`-Anweisungen, bei denen der effektive Wert der Sitzungsvariablen nicht geändert wird, d. h. dass keine Änderung an der Sitzungsvariablen vorgenommen wird.
     - Sie ändern den Wert der Sitzungsvariablen und führen eine Anweisung in derselben Transaktion aus.

     Weitere Informationen finden Sie unter Vermeiden des Fixierens.

- Connection borrow timeout— Passen Sie das Timeout-Intervall der Verbindung an. Diese Einstellung gilt, wenn für den Proxy bereits die maximale Anzahl von Verbindungen verwendet wird. Diese Einstellung legt fest, wie lange der Proxy wartet, bis eine Verbindung verfügbar ist, bevor ein Timeout-Fehler zurückgegeben wird.
- Initialisierungsabfrage— (Optional) Fügen Sie eine Initialisierungsabfrage hinzu oder ändern Sie die aktuelle. Sie können eine oder mehrere SQL-Anweisungen für die Ausführung durch den Proxy beim Öffnen jeder neuen Datenbankverbindung festlegen. Diese Einstellung wird normalerweise mit `SET`-Anweisungen verwendet, um sicherzustellen, dass jede Verbindung identische Einstellungen wie Zeitzone und Zeichensatz hat. Verwenden Sie für mehrere Anweisungen Semikola als Trennzeichen. Sie können auch mehrere Variablen in eine einzelne `SET`-Anweisung einschließen, z. B. `SET x=1, y=2`.

  Sie können bestimmte Eigenschaften, z. B. die Zielgruppenkennung und die Datenbank-Engine, nicht ändern.

5. Wählen Sie Modify target group (Zielgruppe ändern).

AWS CLI

Um einen Proxy mithilfe von zu ändern, verwenden Sie die Befehle modify-db-proxy AWS CLI, modify-db-proxy-target-group, deregister-db-proxy-targets und register-db-proxy-targets.

Mit dem Befehl `modify-db-proxy` können Sie Eigenschaften wie die folgenden ändern:

- Der Satz von Secrets Manager-Secrets, die vom Proxy verwendet werden.
- Ob TLS erforderlich ist.
- Das Timeout für Client-Leerlauf.
- Ob zusätzliche Informationen aus SQL-Anweisungen zum Debuggen protokolliert werden sollen.
- Die IAM-Rolle, die zum Abrufen von Secrets Manager-Secrets verwendet wird.
- Die vom Proxy verwendeten Sicherheitsgruppen.

Das folgende Beispiel zeigt, wie ein vorhandener Proxy umbenannt wird.

```
aws rds modify-db-proxy --db-proxy-name the-proxy --new-db-proxy-name the_new_name
```

Um verbindungsbezogene Einstellungen zu ändern oder die Zielgruppe umzubenennen, verwenden Sie den Befehl `modify-db-proxy-target-group`. Derzeit haben alle Proxys eine einzelne Zielgruppe mit dem Namen `default`. Bei der Arbeit mit dieser Zielgruppe geben Sie den Namen des Proxys und `default` für den Namen der Zielgruppe an.

Das folgende Beispiel zeigt, wie Sie zuerst die `MaxIdleConnectionsPercent`-Einstellung für einen Proxy überprüfen und dann mithilfe der Zielgruppe ändern.

```
aws rds describe-db-proxy-target-groups --db-proxy-name the-proxy

{
    "TargetGroups": [
        {
            "Status": "available",
            "UpdatedDate": "2019-11-30T16:49:30.342Z",
            "ConnectionPoolConfig": {
                "MaxIdleConnectionsPercent": 50,
                "ConnectionBorrowTimeout": 120,
                "MaxConnectionsPercent": 100,
                "SessionPinningFilters": []
            },
            "TargetGroupName": "default",
            "CreatedDate": "2019-11-30T16:49:27.940Z",
            "DBProxyName": "the-proxy",
            "IsDefault": true
        }
    ]
}

aws rds modify-db-proxy-target-group --db-proxy-name the-proxy --target-group-name
 default --connection-pool-config '
{ "MaxIdleConnectionsPercent": 75 }'

{
    "DBProxyTargetGroup": {
        "Status": "available",
        "UpdatedDate": "2019-12-02T04:09:50.420Z",
        "ConnectionPoolConfig": {
            "MaxIdleConnectionsPercent": 75,
            "ConnectionBorrowTimeout": 120,
            "MaxConnectionsPercent": 100,
            "SessionPinningFilters": []
        },
```

```
        "TargetGroupName": "default",
        "CreatedDate": "2019-11-30T16:49:27.940Z",
        "DBProxyName": "the-proxy",
        "IsDefault": true
    }
}
```

Mit den Befehlen `deregister-db-proxy-targets` und `register-db-proxy-targets` ändern Sie, welchen Aurora-DB-Clustern der Proxy über die Zielgruppe zugeordnet ist. Derzeit kann jeder Proxy eine Verbindung zu einem Aurora-DB-Cluster der herstellen. Die Zielgruppe verfolgt die Verbindungsdetails für alle , alle DB-Instances in einem Aurora-Cluster.

Das folgende Beispiel beginnt mit einem Proxy, der einem Aurora MySQL-Cluster mit dem Namen zugeordnet is `cluster-56-2020-02-25-1399`. Das Beispiel zeigt, wie der Proxy so geändert wird, dass er eine Verbindung zu einem anderen Cluster namens herstellen kan `provisioned-cluster`.

Wenn Sie mit einem Aurora-DB-Cluster arbeiten, geben Sie die Option `--db-cluster-identifier` an.

Im folgenden Beispiel wird ein Aurora MySQL-Proxy geändert. Ein Aurora PostgreSQL-Proxy hat Port 5432.

```
aws rds describe-db-proxy-targets --db-proxy-name the-proxy

{
    "Targets": [
        {
            "Endpoint": "instance-9814.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "instance-9814"
        },
        {
            "Endpoint": "instance-8898.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "instance-8898"
        },
        {
            "Endpoint": "instance-1018.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
```

```
            "RdsResourceId": "instance-1018"
        },
        {
            "Type": "TRACKED_CLUSTER",
            "Port": 0,
            "RdsResourceId": "cluster-56-2020-02-25-1399"
        },
        {
            "Endpoint": "instance-4330.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "instance-4330"
        }
    ]
}

aws rds deregister-db-proxy-targets --db-proxy-name the-proxy --db-cluster-identifier
 cluster-56-2020-02-25-1399

aws rds describe-db-proxy-targets --db-proxy-name the-proxy

{
    "Targets": []
}

aws rds register-db-proxy-targets --db-proxy-name the-proxy --db-cluster-identifier
 provisioned-cluster

{
    "DBProxyTargets": [
        {
            "Type": "TRACKED_CLUSTER",
            "Port": 0,
            "RdsResourceId": "provisioned-cluster"
        },
        {
            "Endpoint": "gkldje.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "gkldje"
        },
        {
            "Endpoint": "provisioned-1.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
```

```
            "Port": 3306,
            "RdsResourceId": "provisioned-1"
        }
    ]
}
```

RDS-API

Um einen Proxy mithilfe der RDS-API zu ändern, verwenden Sie die Operationen ModifyDBProxy, ModifyDB ProxyTargetGroup, ProxyTargetsDeregisterDB und RegisterDB. ProxyTargets

Mit `ModifyDBProxy` können Sie Eigenschaften wie die folgenden ändern:

- Der Satz von Secrets Manager-Secrets, die vom Proxy verwendet werden.
- Ob TLS erforderlich ist.
- Das Timeout für Client-Leerlauf.
- Ob zusätzliche Informationen aus SQL-Anweisungen zum Debuggen protokolliert werden sollen.
- Die IAM-Rolle, die zum Abrufen von Secrets Manager-Secrets verwendet wird.
- Die vom Proxy verwendeten Sicherheitsgruppen.

Mit `ModifyDBProxyTargetGroup` können Sie verbindungsbezogene Einstellungen ändern oder die Zielgruppe umbenennen. Derzeit haben alle Proxys eine einzelne Zielgruppe mit dem Namen `default`. Bei der Arbeit mit dieser Zielgruppe geben Sie den Namen des Proxys und `default` für den Namen der Zielgruppe an.

Mit `DeregisterDBProxyTargets` und ändern Sie`RegisterDBProxyTargets`, mit welchem Aurora-Cluster der der Proxy über seine Zielgruppe verknüpft ist. Derzeit kann jeder Proxy eine Verbindung mit einem Aurora-DB-Cluster herstellen. Die Zielgruppe verfolgt die Verbindungsdetails für die DB-Instances in einem Aurora-Cluster.

Hinzufügen eines neuen Datenbankbenutzers

In einigen Fällen können Sie einen neuen Datenbankbenutzer zu einem Aurora-Cluster mit Proxy-Zuordnung hinzufügen. Fügen Sie dazu ein Secrets Manager-Secret hinzu, um die Anmeldeinformationen für diesen Benutzer zu speichern, oder verwenden Sie ein Secret neu. Wählen Sie dazu eine der folgenden Optionen:

1. Erstellen Sie ein neues Secrets-Manager-Secret, indem Sie das unter beschriebene Verfahren verwende Datenbankanmeldedaten einrichten in AWS Secrets Manager.

2. Aktualisieren Sie die IAM-Rolle, um RDS Proxy Zugriff auf das neue Secrets Manager-Geheimnis zu gewähren. Aktualisieren Sie dazu den Ressourcenabschnitt der IAM-Rollenrichtlinie.
3. Ändern Sie den RDS-Proxy, um das neue Secret von Secrets Manager unter Secrets Manager Secrets hinzuzufügen.
4. Wenn der neue Benutzer an die Stelle eines vorhandenen Benutzers tritt, aktualisieren Sie die Anmeldeinformationen, die im Secrets Manager-Secret des Proxys für den vorhandenen Benutzer gespeichert sind.

Hinzufügen eines neuen Datenbankbenutzers zu einer PostgreSQL-Datenbank

Wenn Sie Ihrer PostgreSQL-Datenbank einen neuen Benutzer hinzufügen, wenn Sie den folgenden Befehl ausgeführt haben:

```
REVOKE CONNECT ON DATABASE postgres FROM PUBLIC;
```

Gewähren Sie dem Benutzer `rdsproxyadmin` die `CONNECT`-Berechtigung, damit der Benutzer Verbindungen in der Zieldatenbank überwachen kann.

```
GRANT CONNECT ON DATABASE postgres TO rdsproxyadmin;
```

Sie können auch anderen Zieldatenbankbenutzern die Durchführung von Zustandsprüfungen ermöglichen, indem Sie im obigen Befehl `rdsproxyadmin` auf den Datenbankbenutzer ändern.

Ändern des Passworts für einen Datenbankbenutzer

In einigen Fällen können Sie das Passwort für einen Datenbankbenutzer in einem Aurora-Cluster mit Proxy-Zuordnung ändern. Aktualisieren Sie dazu das entsprechende Secrets Manager-Secret mit dem neuen Passwort.

Client- und Datenbankverbindungen

Verbindungen von Ihrer Anwendung zum RDS-Proxy werden als Client-Verbindungen bezeichnet. Verbindungen von einem Proxy zur Datenbank sind Datenbankverbindungen. Bei Verwendung von RDS-Proxy werden Client-Verbindungen am Proxy beendet, während Datenbankverbindungen innerhalb des RDS-Proxys verwaltet werden.

Anwendungsseitiges Verbindungspooling kann den Vorteil bieten, dass der wiederkehrende Verbindungsaufbau zwischen Ihrer Anwendung und dem RDS-Proxy reduziert wird.

Berücksichtigen Sie die folgenden Konfigurationsaspekte, bevor Sie einen anwendungsseitigen Verbindungspool implementieren:

- Maximale Lebensdauer der Client-Verbindung: RDS Proxy erzwingt eine maximale Lebensdauer von Client-Verbindungen von 24 Stunden. Dieser Wert kann nicht konfiguriert werden. Konfigurieren Sie Ihren Pool mit einer maximalen Verbindungsdauer von weniger als 24 Stunden, um unerwartete Verbindungsabbrüche beim Client zu vermeiden.
- Timeout im Leerlauf der Client-Verbindung: Der RDS-Proxy erzwingt eine maximale Leerlaufzeit für Client-Verbindungen. Konfigurieren Sie Ihren Pool mit einem Timeout für inaktive Verbindungen, der niedriger ist als die Einstellung für das Leerlaufzeitlimit für Client-Verbindungen für den RDS-Proxy, um unerwartete Verbindungsabbrüche zu vermeiden.

Die maximale Anzahl von Client-Verbindungen, die in Ihrem anwendungsseitigen Verbindungspool konfiguriert sind, muss nicht auf die Einstellung max_connections für den RDS-Proxy beschränkt sein.

Das Pooling von Client-Verbindungen führt zu einer längeren Lebensdauer der Client-Verbindung. Wenn es bei Ihren Verbindungen zum Pinning kommt, kann das Pooling von Client-Verbindungen die Effizienz des Multiplexings verringern. Clientverbindungen, die im anwendungsseitigen Verbindungspool angeheftet, aber inaktiv sind, behalten weiterhin eine Datenbankverbindung bei und verhindern, dass die Datenbankverbindung von anderen Clientverbindungen wiederverwendet wird. Überprüfen Sie Ihre Proxyprotokolle, um zu überprüfen, ob es bei Ihren Verbindungen zu Pinning kommt.

> **Note**
>
> RDS-Proxy schließt Datenbankverbindungen nach 24 Stunden, wenn sie nicht mehr verwendet werden. Der Proxy führt diese Aktion unabhängig vom Wert der Einstellung für maximale Leerlaufverbindungen aus.

Konfigurieren der Verbindungseinstellungen

Um das Verbindungs-Pooling von RDS Proxy anzupassen, können Sie die folgenden Einstellungen ändern:

- IdleClientTimeout
- MaxConnectionsProzent

- MaxIdleConnectionsPercent
- ConnectionBorrowTimeout

IdleClientTimeout

Sie können angeben, wie lange eine Client-Verbindung inaktiv sein kann, bevor der Proxy sie schließt. Der Standardwert ist 1.800 Sekunden (30 Minuten).

Eine Client-Verbindung gilt als inaktiv, wenn die Anwendung innerhalb der angegebenen Zeit nach Abschluss der vorherigen Anforderung keine neue Anforderung absendet. Die zugrunde liegende Datenbankverbindung bleibt offen und wird an den Verbindungspool zurückgegeben. Somit ist sie für neue Clientverbindungen verfügbar. Wenn Sie möchten, dass der Proxy proaktiv veraltete Verbindungen entfernt und so das Timeout für inaktive Client-Verbindungen verringert. Wenn Ihr Workload häufig Verbindungen mit dem Proxy herstellt, erhöhen Sie das Timeout für inaktive Client-Verbindungen, um die Kosten für den Verbindungsaufbau zu sparen.

Diese Einstellung wird durch das Feld Timeout für die Verbindung bei inaktiven Clients in der RDS-Konsole und durch die `IdleClientTimeout` Einstellung in der AWS CLI und der API dargestellt. Informationen dazu, wie Sie den Wert des Felds Idle client connection timeout (Zeitüberschreitung bei Client-Verbindungsinaktivität) in der RDS-Konsole ändern, finden Sie unter AWS Management Console. Informationen dazu, wie Sie den Wert der Einstellung `IdleClientTimeout` ändern, finden Sie unter dem CLI-Befehl modify-db-proxy oder der API-Operation ModifyDBProxy.

MaxConnectionsProzent

Sie können die Anzahl der Verbindungen beschränken, die ein RDS Proxy mit der Zieldatenbank herstellen kann. Sie geben das Limit als Prozentsatz der maximal für Ihre Datenbank verfügbaren Verbindungen an. Diese Einstellung wird durch das Feld Maximale Anzahl an Verbindungen für den Verbindungspool in der RDS-Konsole und durch die `MaxConnectionsPercent` Einstellung in der AWS CLI und der API dargestellt.

Der Wert `MaxConnectionsPercent` wird als Prozentsatz der Einstellung `max_connections` für den Aurora-DB-Cluster ausgedrückt, die von der Zielgruppe verwendet wird. Der Proxy erstellt nicht alle diese Verbindungen im Voraus. Diese Einstellung ermöglicht es dem Proxy, diese Verbindungen so einzurichten, wie es der Workload benötigt.

Beispielsweise legt RDS Proxy für ein registriertes Datenbankziel, für das `max_connections` auf 1000 und `MaxConnectionsPercent` auf 95 festgelegt ist, 950 Verbindungen als Obergrenze für gleichzeitige Verbindungen mit diesem Datenbankziel fest.

Ein häufiger Nebeneffekt, der auftritt, wenn Ihre Workload die maximale Anzahl zulässiger Datenbankverbindungen erreicht, ist ein Anstieg der allgemeinen Abfragelatenz in Verbindung mit einer Erhöhung der Metrik `DatabaseConnectionsBorrowLatency`. Sie können die aktuell verwendeten Datenbankverbindungen und die Gesamtzahl der zulässigen Datenbankverbindungen überwachen, indem Sie die Metriken `DatabaseConnections` und `MaxDatabaseConnectionsAllowed` vergleichen.

Beachten Sie für das Festlegen dieses Parameters die folgenden bewährten Methoden:

- Sorgen Sie für ausreichend Verbindungsspielraum für Änderungen des Workload-Musters. Es wird empfohlen, den Parameter mindestens 30 % über Ihrer zuletzt überwachten maximalen Nutzung einzustellen. Da RDS Proxy die Kontingente für Datenbankverbindungen auf mehrere Knoten neu verteilt, können interne Kapazitätsänderungen mindestens 30 % Spielraum für zusätzliche Verbindungen erfordern, um erhöhte Ausleihlatenzen zu vermeiden.
- RDS Proxy reserviert eine bestimmte Anzahl von Verbindungen für die aktive Überwachung, um schnelles Failover, Weiterleitung von Datenverkehr und interne Operationen zu unterstützen. Die Metrik `MaxDatabaseConnectionsAllowed` umfasst diese reservierten Verbindungen nicht. Sie stellt die Anzahl der Verbindungen dar, die für den Workload verfügbar sind, und kann niedriger sein als der aus der Einstellung `MaxConnectionsPercent` abgeleitete Wert.

  Die empfohlenen `MaxConnectionsPercent` Mindestwerte lauten wie folgt:

  - db.t3.small: 100
  - db.t3.medium: 55
  - db.t3.large: 35
  - db.r3.large oder höher: 20

  Wenn mehrere Ziel-Instances bei RDS Proxy registriert sind, z. B. ein Aurora-Cluster mit Leserknoten, legen Sie den Mindestwert auf der Grundlage der kleinsten registrierten Instance fest.

Informationen dazu, wie Sie den Wert des Felds Connection pool maximum connections (Max. Verbindungen Verbindungspool) in der RDS-Konsole ändern, finden Sie unter AWS Management Console. Informationen zum Ändern des Werts der `MaxConnectionsPercent` Einstellung finden Sie im CLI-Befehl modify-db-proxy-target-group oder in der API-Operation ModifyDB Group. ProxyTarget

> **Important**
>
> Wenn der DB-Cluster Teil einer globalen Datenbank mit aktivierter Schreibweiterleitung ist, reduzieren Sie den `MaxConnectionsPercent`-Wert Ihres Proxys um das Kontingent, das der Schreibweiterleitung zugewiesen ist. Das Kontingent für die Schreibweiterleitung ist im DB-Cluster-Parameter `aurora_fwd_writer_max_connections_pct` festgelegt. Informationen zur Schreibweiterleitung finden Sie unter Verwenden der Schreibweiterleitung in einer Amazon Aurora globalen Datenbank.

Informationen zu Datenbankverbindungslimits finden Sie unter Maximale Verbindungen zu einer Aurora-MySQL-DB-Instance und Maximale Verbindungen zu einer Aurora-PostgreSQL-DB-Instance.

MaxIdleConnectionsPercent

Sie können die Anzahl inaktiver Datenbankverbindungen festlegen, die RDS Proxy im Verbindungspool behalten kann. Standardmäßig betrachtet RDS Proxy eine Datenbankverbindung in seinem Pool als inaktiv, wenn fünf Minuten lang keine Aktivität auf der Verbindung stattgefunden hat.

Der `MaxIdleConnectionsPercent` Wert wird als Prozentsatz der `max_connections` Einstellung für die Zielgruppe der RDS-DB-Instance ausgedrückt. Der Standardwert ist 50 Prozent von `MaxConnectionsPercent` und die Obergrenze ist der Wert `MaxConnectionsPercent`. Wenn beispielsweise 80 ist`MaxConnectionsPercent`, dann `MaxIdleConnectionsPercent` ist der Standardwert 40.

Bei einem hohen Wert lässt der Proxy einen hohen Prozentsatz an ungenutzten Datenbankverbindungen offen. Bei einem niedrigen Wert schließt der Proxy einen hohen Prozentsatz von inaktiven Datenbankverbindungen. Wenn Ihre Workloads unvorhersehbar sind, sollten Sie erwägen, einen hohen Wert für `MaxIdleConnectionsPercent` festzulegen. Dies bedeutet, dass RDS-Proxy Aktivitätsspitzen verarbeiten kann, ohne viele neue Datenbankverbindungen zu öffnen.

Diese Einstellung wird durch die `MaxIdleConnectionsPercent` Einstellung von `DBProxyTargetGroup` in der AWS CLI und der API dargestellt. Informationen zum Ändern des Werts der `MaxIdleConnectionsPercent` Einstellung finden Sie im CLI-Befehl modify-db-proxy-target-group oder in der API-Operation ModifyDB Group. ProxyTarget

Informationen zu Datenbankverbindungslimits finden Sie unter Maximale Verbindungen zu einer Aurora-MySQL-DB-Instance und Maximale Verbindungen zu einer Aurora-PostgreSQL-DB-Instance.

ConnectionBorrowTimeout

Sie können angeben, wie lange RDS Proxy warten soll, bis eine Datenbankverbindung im Verbindungspool verfügbar ist, bevor ein Timeout-Fehler zurückgegeben wird. Standardmäßig sind 120 Sekunden festgelegt. Diese Einstellung greift, wenn die maximale Anzahl von Verbindungen erreicht ist und daher keine Verbindungen im Verbindungspool verfügbar sind. Es gilt auch, wenn keine geeignete Datenbankinstanz für die Bearbeitung der Anfrage verfügbar ist, z. B. wenn ein Failover-Vorgang ausgeführt wird. Mit dieser Einstellung können Sie die beste Wartezeit für Ihre Anwendung festlegen, ohne das Abfragetimeout in Ihrem Anwendungscode zu ändern.

Diese Einstellung wird durch das Feld Timeout für die Verbindungsausleihe in der RDS-Konsole oder durch die `ConnectionBorrowTimeout` Einstellung `DBProxyTargetGroup` in der AWS CLI OR-API dargestellt. Informationen dazu, wie Sie den Wert des Felds Connection borrow timeout (Zeitüberschreitung für die Verbindung) in der RDS-Konsole ändern, finden Sie unter AWS Management Console. Informationen zum Ändern des Werts der `ConnectionBorrowTimeout` Einstellung finden Sie im CLI-Befehl modify-db-proxy-target-group oder in der API-Operation ModifyDB Group. ProxyTarget

Vermeiden des Fixierens

Multiplexing ist effizienter, wenn Datenbankanforderungen nicht auf Statusinformationen aus früheren Anforderungen angewiesen sind. In diesem Fall kann RDS Proxy eine Verbindung zum Abschluss jeder Transaktion wiederverwenden. Beispiele für solche Zustandsinformationen sind die meisten Variablen und Konfigurationsparameter, die Sie durch `SET`-oder `SELECT`-Anweisungen ändern können. SQL-Transaktionen auf einer Clientverbindung können standardmäßig zwischen zugrunde liegenden Datenbankverbindungen Multiplexing durchführen.

Ihre Verbindungen zum Proxy können einen Status eingeben, der als Pinning (Fixieren) bezeichnet wird. Wenn eine Verbindung angeheftet wird, verwendet jede spätere Transaktion dieselbe zugrunde liegende Datenbankverbindung, bis die Sitzung beendet ist. Andere Clientverbindungen können diese Datenbankverbindung auch erst dann wieder verwenden, wenn die Sitzung beendet ist. Die Sitzung wird beendet, wenn die Clientverbindung unterbrochen wird.

RDS Proxy heftet automatisch eine Clientverbindung an eine bestimmte DB-Verbindung an, wenn eine Sitzungsstatusänderung erkannt wird, die für andere Sitzungen nicht geeignet ist. Das Fixieren verringert die Effektivität der Wiederverwendung der Verbindung. Wenn alle oder fast alle Verbindungen fixiert sind, können Sie Ihren Anwendungscode oder Ihre Workload ändern, um dafür zu sorgen, dass Fixierungen weniger erforderlich sind.

Ihre Anwendung ändert beispielsweise eine Sitzungsvariable oder einen Konfigurationsparameter. In diesem Fall können sich spätere Anweisungen darauf verlassen, dass die neue Variable oder der neue Parameter wirksam ist. Wenn also RDS Proxy Anforderungen verarbeitet, um Sitzungsvariablen oder Konfigurationseinstellungen zu ändern, wird diese Sitzung an die DB-Verbindung fixiert. Auf diese Weise bleibt der Sitzungsstatus für alle späteren Transaktionen in derselben Sitzung gültig.

Bei Datenbank-Engines gilt diese Regel nicht für alle Parameter, die Sie festlegen können. RDS Proxy verfolgt bestimmte Anweisungen und Variablen. Daher fixiert RDS Proxy die Sitzung nicht, wenn Sie sie ändern. In diesem Fall verwendet RDS Proxy nur die Verbindung für andere Sitzungen erneut, die dieselben Werte für diese Einstellungen haben. Die Listen der verfolgten Anweisungen und Variablen für Aurora MySQL finden Sie unter Welche Daten RDS-Proxy für Aurora-MySQL-Datenbanken verfolgt.

Welche Daten RDS-Proxy für Aurora-MySQL-Datenbanken verfolgt

Im Folgenden sind die MySQL-Anweisungen aufgeführt, die RDS Proxy verfolgt:

- DROP DATABASE
- DROP SCHEMA
- USE

Im Folgenden sind die MySQL-Variablen aufgeführt, die RDS Proxy verfolgt:

- `AUTOCOMMIT`
- `AUTO_INCREMENT_INCREMENT`
- `CHARACTER SET (or CHAR SET)`
- `CHARACTER_SET_CLIENT`
- `CHARACTER_SET_DATABASE`
- `CHARACTER_SET_FILESYSTEM`
- `CHARACTER_SET_CONNECTION`
- `CHARACTER_SET_RESULTS`
- `CHARACTER_SET_SERVER`
- `COLLATION_CONNECTION`
- `COLLATION_DATABASE`
- `COLLATION_SERVER`

- `INTERACTIVE_TIMEOUT`
- `NAMES`
- `NET_WRITE_TIMEOUT`
- `QUERY_CACHE_TYPE`
- `SESSION_TRACK_SCHEMA`
- `SQL_MODE`
- `TIME_ZONE`
- `TRANSACTION_ISOLATION (or TX_ISOLATION)`
- `TRANSACTION_READ_ONLY (or TX_READ_ONLY)`
- `WAIT_TIMEOUT`

Minimieren des Fixierens

Die Leistungsoptimierung für RDS Proxy beinhaltet den Versuch, die Wiederverwendung von Verbindungen auf Transaktionsebene (Multiplexing) zu maximieren, indem das Fixieren minimiert wird.

Sie können das Fixieren wie folgt minimieren:

- Vermeiden Sie unnötige Datenbankanforderungen, die Anheften (Pinning) verursachen könnten.
- Legen Sie Variablen und Konfigurationseinstellungen konsistent über alle Verbindungen hinweg fest. Auf diese Weise verwenden spätere Sitzungen häufiger Verbindungen, die über diese speziellen Einstellungen verfügen.

  Wenn für PostgreSQL jedoch eine Variable festgelegt wird, wird die Sitzung durch Pinning fixiert.
- Wenden Sie bei einer MySQL-Engine-Familiendatenbank einen Sitzungs-Pinning-Filter auf den Proxy an. Sie können bestimmte Arten von Operationen vom Fixieren der Sitzung ausnehmen, wenn Sie wissen, dass dies den korrekten Betrieb Ihrer Anwendung nicht beeinträchtigt.
- Sehen Sie sich anhand der CloudWatch Amazon-Metrik `DatabaseConnectionsCurrentlySessionPinned` an, wie häufig das Anheften erfolgt. Informationen zu dieser und anderen CloudWatch Kennzahlen finden Sie unterÜberwachen von RDS-Proxy-Metriken mit Amazon CloudWatch.
- Wenn Sie `SET`-Anweisungen verwenden, um eine identische Initialisierung für jede Clientverbindung durchzuführen, können Sie dies tun, während Sie das Multiplexing auf

Transaktionsebene beibehalten. In diesem Fall verschieben Sie die Anweisungen, die den ursprünglichen Sitzungsstatus einrichten, in die Initialisierungsabfrage, die von einem Proxy verwendet wird. Diese Eigenschaft ist eine Zeichenfolge, die eine oder mehrere SQL-Anweisungen enthält, die durch Semikola getrennt sind.

Beispielsweise können Sie eine Initialisierungsabfrage für einen Proxy definieren, der bestimmte Konfigurationsparameter festlegt. RDS Proxy wendet dann diese Einstellungen an, wenn eine neue Verbindung für diesen Proxy eingerichtet wird. Sie können die entsprechenden `SET`-Anweisungen aus Ihrem Anwendungscode entfernen, damit sie das Multiplexing auf Transaktionsebene nicht beeinträchtigen.

Metriken zur Häufigkeit des Pinnings für einen Proxy finden Sie unter Überwachen von RDS-Proxy-Metriken mit Amazon CloudWatch.

Bedingungen, die für alle Engine-Familien zum Pinning führen

Der Proxy fixiert die Sitzung an der aktuellen Verbindung in den folgenden Situationen an, in denen Multiplexing unerwartetes Verhalten verursachen kann:

- Jede Anweisung mit einer Textgröße über 16 KB bewirkt, dass der Proxy die Sitzung fixiert.

Bedingungen, die das Fixieren für Aurora MySQL verursachen

Bei MySQL verursachen die folgenden Interaktionen ein Pinning:

- Die expliziten MySQL-Anweisungen `LOCK TABLE`, `LOCK TABLES` oder `FLUSH TABLES WITH READ LOCK` bewirken, dass der Proxy ein Pinning der Sitzung vornimmt.
- Durch Erstellen benannter Sperren mit `GET_LOCK` wird bewirkt, dass der Proxy ein Pinning der Sitzung vornimmt.
- Wenn Sie eine Benutzervariable oder eine Systemvariable festlegen (mit einigen Ausnahmen), wird der Proxy die Sitzung fixieren. Wenn diese Situation die Wiederverwendung Ihrer Verbindung zu stark einschränkt, wählen Sie `SET` Operationen aus, die kein Pinning verursachen. Weitere Informationen dazu, wie Sie dies tun, indem Sie die Eigenschaft „Session pinning filters“ festlegen, finden Sie unter Erstellen eines RDS Proxy und Ändern eines RDS Proxy.
- Beim Erstellen einer temporären Tabelle fixiert der Proxy die Sitzung. Auf diese Weise wird der Inhalt der temporären Tabelle während der gesamten Sitzung beibehalten, unabhängig von den Transaktionsgrenzen.

- Der Aufruf der Funktionen `ROW_COUNT`, `FOUND_ROWS` und `LAST_INSERT_ID` verursacht manchmal Pinning.

  Die genauen Umstände, unter denen diese Funktionen Pinning verursachen, können sich zwischen Aurora-MySQL-Versionen unterscheiden, die mit MySQL 5.7 kompatibel sind.
- Vorbereitete Anweisungen bewirken, dass der Proxy die Sitzung fixiert. Diese Regel bestimmt, ob die vorbereitete Anweisung SQL-Text oder das Binärprotokoll verwendet.
- RDS Proxy pingt keine Verbindungen an, wenn Sie SET LOCAL verwenden.
- Das Aufrufen von gespeicherten Prozeduren und gespeicherten Funktionen verursacht kein Pinning. RDS Proxy erkennt keine Änderungen des Sitzungsstatus, die aus solchen Aufrufen resultieren. Stellen Sie sicher, dass Ihre Anwendung den Sitzungsstatus in gespeicherten Routinen nicht ändert, wenn Sie darauf angewiesen sind, dass dieser Sitzungsstatus transaktionsübergreifend beibehalten wird. Beispielsweise ist RDS Proxy derzeit nicht mit einer gespeicherten Prozedur kompatibel, die eine temporäre Tabelle erstellt, die für alle Transaktionen beibehalten wird.

Wenn Sie über eingehende Kenntnisse über das Verhalten Ihrer Anwendung verfügen, können Sie das Pinning-Verhalten für bestimmte Anwendungsanweisungen überspringen. Dazu wählen Sie beim Erstellen des Proxys die Option Sitzungs-Pinning-Filter. Derzeit können Sie das Sitzungs-Pinning für das Festlegen von Sitzungsvariablen und Konfigurationseinstellungen deaktivieren.

Bedingungen, die das Fixieren für Aurora PostgreSQL verursachen

Für PostgreSQL verursachen die folgenden Interaktionen eine Fixierung:

- `SET`Befehle verwenden.
- Verwendung von `EXECUTE` Befehlen `PREPARE` `DISCARDDEALLOCATE`,, oder zur Verwaltung von vorbereiteten Anweisungen.
- Temporäre Sequenzen, Tabellen oder Ansichten erstellen
- Cursor deklarieren.
- Der Sitzungsstatus wird verworfen.
- Abhören auf einem Benachrichtigungskanal.
- Laden eines Bibliotheksmoduls wie`auto_explain`.
- Manipulieren von Sequenzen mit Funktionen wie `nextval` und`setval`.

- Interaktion mit Sperren mithilfe von Funktionen wie `pg_advisory_lock` und`pg_try_advisory_lock`.

  > **Note**
  >
  > RDS Proxy legt keine Sicherheitssperren auf Transaktionsebene fest`pg_advisory_xact_lock`, insbesondere nicht auf `pg_advisory_xact_lock_shared`, `pg_try_advisory_xact_lock`, und`pg_try_advisory_xact_lock_shared`.

- Einstellung eines Parameters oder Zurücksetzen eines Parameters auf seine Standardwerte Insbesondere die Verwendung von `set_config` Befehlen `SET` und zum Zuweisen von Standardwerten zu Sitzungsvariablen.
- Das Aufrufen von gespeicherten Prozeduren und gespeicherten Funktionen verursacht kein Pinning. RDS Proxy erkennt keine Änderungen des Sitzungsstatus, die aus solchen Aufrufen resultieren. Stellen Sie sicher, dass Ihre Anwendung den Sitzungsstatus in gespeicherten Routinen nicht ändert, wenn Sie darauf angewiesen sind, dass dieser Sitzungsstatus transaktionsübergreifend beibehalten wird. Beispielsweise ist RDS Proxy derzeit nicht mit einer gespeicherten Prozedur kompatibel, die eine temporäre Tabelle erstellt, die für alle Transaktionen beibehalten wird.

Löschen eines RDS Proxy

Sie können einen Proxy löschen, wenn Sie ihn nicht mehr benötigen. Oder Sie können einen Proxy löschen, wenn Sie die zugehörige DB-Instance oder den zugehörigen Cluster außer Betrieb nehmen.

AWS Management Console

So löschen Sie einen Proxy:

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Proxies (Proxys).
3. Wählen Sie den zu löschenden Proxy aus der Liste aus.
4. Wählen Sie Delete Proxy (Proxy löschen).

AWS CLI

Um einen DB-Proxy zu löschen, verwenden Sie den AWS CLI Befehl delete-db-proxy. Um zugehörige Zuordnungen zu entfernen, verwenden Sie auch den Befehl deregister-db-proxy-targets .

```
aws rds delete-db-proxy --name proxy_name
```

```
aws rds deregister-db-proxy-targets
    --db-proxy-name proxy_name
    [--target-group-name target_group_name]
    [--target-ids comma_separated_list]       # or
    [--db-instance-identifiers instance_id]       # or
    [--db-cluster-identifiers cluster_id]
```

RDS-API

Um einen DB-Proxy zu löschen, rufen Sie die Amazon RDS-API-Funktion DeleteDBProxy auf. Um verwandte Elemente und Verknüpfungen zu löschen, rufen Sie auch die Funktionen DeleteDB Group und DeregisterDB auf. ProxyTarget ProxyTargets

Arbeiten mit Amazon RDS Proxy-Endpunkten

Im Folgenden können Sie mehr über Endpunkte für RDS-Proxy erfahren und wie man sie benutzt. Durch die Verwendung von Proxy-Endpunkten können Sie die folgenden Funktionen nutzen:

- Sie können mehrere Endpunkte mit einem Proxy verwenden, um Verbindungen von verschiedenen Anwendungen unabhängig voneinander zu überwachen und zu beheben.
- Sie können Reader-Endpunkte mit Aurora-DB-Cluster zur Verbesserung der Leseskalierbarkeit und Hochverfügbarkeit für Ihre abfrageintensiven Anwendungen verwenden.
- Sie können einen VPC-übergreifenden Endpunkt verwenden, um den Zugriff auf Datenbanken in einer VPC aus Ressourcen wie Amazon EC2-Instances in einer anderen VPC zu erlauben.

Themen

- Überblick über Proxy-Endpunkte
- Verwenden von Reader-Endpunkten mit Aurora-Clustern
- Zugreifen auf Aurora-Datenbanken über VPCs hinweg

- Erstellen eines Proxy-Endpunktes
- Anzeigen von Proxy-Endpunkten
- Ändern eines Proxy-Endpunkts
- Löschen eines Proxy-Endpunkts
- Limits für Proxy-Endpunkte

Überblick über Proxy-Endpunkte

Arbeiten mit RDS-Proxy-Endpunkten umfassen die gleichen Arten von Verfahren wie bei Aurora-DB-Cluster- und Reader-Endpunkten. Wenn Sie nicht mit Aurora-Endpunkten vertraut sind finden Sie weitere Informationen unter Amazon Aurora-Verbindungsverwaltung.

Standardmäßig hat der Endpunkt, mit dem Sie eine Verbindung herstellen, wenn Sie RDS Proxy mit einem Aurora-Cluster verwenden, Lese-/Schreibfähigkeit. Infolgedessen sendet dieser Endpunkt alle Anforderungen an die Writer-Instance des Clusters. Alle diese Verbindungen werden auf den `max_connections`-Wert für die Writer-Instance angerechnet. Wenn Ihr Proxy mit einem Aurora-DB-Cluster verbunden ist, können Sie zusätzliche Lese-/Schreib- oder schreibgeschützte Endpunkte für diesen Proxy erstellen.

Sie können einen schreibgeschützten Endpunkt mit Ihrem Proxy für schreibgeschützte Abfragen verwenden. Sie verwenden diesen, wie Sie den Reader-Endpunkt für einen von Aurora bereitgestellten Cluster nutzen. Auf diese Weise können Sie die Leseskalierbarkeit eines Aurora-Cluster mit einer oder mehreren Reader-DB-Instances nutzen. Sie können mehr gleichzeitige Abfragen ausführen und mehr gleichzeitige Verbindungen herstellen, indem Sie einen schreibgeschützten Endpunkt verwenden und Ihrem Aurora--Cluster nach Bedarf mehr Reader-DB-Instances hinzufügen.

> **Tip**
>
> Wenn Sie einen Proxy für einen Aurora-Cluster mit der AWS Management Console erstellen, können Sie RDS-Proxy einen Reader-Endpunkt automatisch erstellen lassen. Informationen zu den Vorteilen eines Reader-Endpunkts finden Sie unter Verwenden von Reader-Endpunkten mit Aurora-Clustern.

Für einen Proxy-Endpunkt, den Sie erstellen, können Sie den Endpunkt auch einer anderen Virtual Private Cloud (VPC) zuordnen, als der Proxy selbst verwendet. Auf diese Weise können Sie sich

von einer anderen VPC aus mit dem Proxy verbinden, z. B. von einer VPC, die von einer anderen Anwendung in Ihrem Unternehmen verwendet wird.

Informationen zu Limits im Zusammenhang mit Proxy-Endpunkten finden Sie unter Limits für Proxy-Endpunkte.

In den RDS Proxy-Protokollen wird jedem Eintrag der Name des zugehörigen Proxy-Endpunkts vorangestellt. Dieser Name kann derjenige sein, den Sie für einen benutzerdefinierten Endpunkt angegeben haben. Oder es kann der spezielle Name `default` für den Standardendpunkt eines Proxys sein, der Lese-/Schreibanforderungen ausführt.

Jeder Proxy-Endpunkt hat seinen eigenen Satz von CloudWatch Metriken. Sie können die Metriken für alle Endpunkte eines Proxys überwachen. Sie können auch Metriken für einen bestimmten Endpunkt oder für alle Lese-/Schreib- oder schreibgeschützten Endpunkte eines Proxys überwachen. Weitere Informationen finden Sie unter Überwachen von RDS-Proxy-Metriken mit Amazon CloudWatch.

Ein Proxy-Endpunkt verwendet denselben Authentifizierungsmechanismus wie der zugehörige Proxy. Für RDS Proxy richtet automatisch Berechtigungen und Autorisierungen für den benutzerdefinierten Endpunkt ein, die mit den Eigenschaften des zugehörigen Proxys übereinstimmen.

Informationen zur Funktionsweise von Proxy-Endpunkten für DB-Cluster in einer globalen Aurora-Datenbank finden Sie unter So funktionieren RDS-Proxy-Endpunkte mit globalen Datenbanken.

Verwenden von Reader-Endpunkten mit Aurora-Clustern

Sie können schreibgeschützte Endpunkte namens Reader-Endpunkte erstellen und eine Verbindung herstellen, wenn Sie RDS Proxy mit Aurora-Clustern verwenden. Diese Reader-Endpunkte tragen dazu bei, die Leseskalierbarkeit Ihrer abfrageintensiven Anwendungen zu verbessern. Reader-Endpunkte helfen auch, die Verfügbarkeit Ihrer Verbindungen zu verbessern, wenn eine Reader-DB-Instance in Ihrem Cluster nicht verfügbar ist.

> **Note**
>
> Wenn Sie angeben, dass ein neuer Endpunkt schreibgeschützt ist, verlangt RDS Proxy, dass der Aurora-Cluster eine oder mehrere Reader-DB-Instances hat. In einigen Fällen ändern Sie ggf. das Ziel des Proxys in einen Aurora-Cluster, der einen Aurora-Cluster mit nur einem Writer oder mit mehreren Writern enthält. In diesem Fall schlagen alle Anfragen an den Reader-Endpunkt mit einem Fehler fehl. Anfragen schlagen auch fehl, wenn das Ziel des Proxys eine RDS-Instance anstelle eines Aurora-Clusters ist.

Wenn ein Aurora-Cluster Reader-Instances hat, aber diese Instances nicht verfügbar sind, wartet RDS Proxy darauf, die Anfrage zu senden, anstatt sofort einen Fehler zu zurückzugeben. Wenn innerhalb des Zeitraums der Zeitüberschreitung für die Verbindung keine Reader-Instance verfügbar wird, schlägt die Anfrage mit einem Fehler fehl.

Wie Reader-Endpunkte die Verfügbarkeit von Anwendungen unterstützen

In einigen Fällen sind möglicherweise eine oder mehrere Reader-Instances in Ihrem Cluster nicht verfügbar. In diesem Fall können Verbindungen, die einen Reader-Endpunkt eines DB-Proxys verwenden, schneller wiederhergestellt werden als solche, die den Aurora-Reader-Endpunkt verwenden. RDS Proxy leitet Verbindungen nur an die verfügbaren Reader-Instances im Cluster weiter. Es gibt keine Verzögerung aufgrund von DNS-Caching, wenn eine Instance nicht verfügbar ist.

Wenn die Verbindung Multiplexing durchführt, leitet RDS Proxy nachfolgende Abfragen ohne Unterbrechung Ihrer Anwendung an eine andere Reader-DB-Instance weiter. Bei der automatischen Umstellung auf eine neue Reader-Instance prüft RDS Proxy die Replikationsverzögerung der alten und neuen Reader-Instance. RDS Proxy stellt sicher, dass die neue Reader-Instance mit den gleichen Änderungen wie die vorherige Reader-Instance auf dem neuesten Stand ist. Auf diese Weise hat Ihre Anwendung niemals veraltete Daten, wenn RDS Proxy von einer Reader-DB-Instance zu einer anderen wechselt.

Wenn die Verbindung fixiert ist, gibt die nächste Abfrage der Verbindung einen Fehler zurück. Ihre Anwendung kann sich jedoch sofort wieder mit demselben Endpunkt verbinden. RDS Proxy leitet die Verbindung zu einer anderen Reader-DB-Instance weiter, die sich im Status `available` befindet. Wenn Sie die Verbindung manuell wiederherstellen, überprüft RDS Proxy nicht die Replikationsverzögerung zwischen den alten und neuen Reader-Instances.

Wenn Ihr Aurora-Cluster keine Reader-Instances verfügbar hat, prüft RDS Proxy, ob diese Bedingung vorübergehend oder dauerhaft ist. Das Verhalten ist in jedem Fall wie folgt:

- Angenommen, Ihr Cluster hat eine oder mehrere Reader-DB-Instances, aber keine von ihnen befindet sich im Status `Available`. Zum Beispiel könnten alle Reader-Instances neu gestartet werden oder Probleme aufweisen. In diesem Fall warten Versuche, eine Verbindung zu einem Reader-Endpunkt herzustellen, darauf, dass eine Reader-Instance verfügbar wird. Wenn innerhalb des Zeitraums der Zeitüberschreitung für die Verbindung keine Reader-Instance verfügbar wird, schlägt der Verbindungsversuch fehl. Wenn eine Reader-Instance verfügbar wird, ist der Verbindungsversuch erfolgreich.

- Angenommen, Ihr Cluster hat keine Reader-DB-Instances. In diesem Fall gibt RDS Proxy sofort einen Fehler zurück, wenn Sie versuchen, eine Verbindung zu einem Reader-Endpunkt herzustellen. Um dieses Problem zu beheben, fügen Sie Ihrem Cluster eine oder mehrere Reader-Instances hinzu, bevor Sie eine Verbindung zum Reader-Endpunkt herstellen.

Wie Reader-Endpunkte bei der Skalierbarkeit von Abfragen unterstützen

Reader-Endpunkte für einen Proxy unterstützen mit einer Aurora-Abfrage die Skalierbarkeit auf folgende Weise:

- Wenn Sie Reader-Instances zu Ihrem Aurora-Cluster hinzufügen, kann RDS Proxy neue Verbindungen zu beliebigen Reader-Endpunkten an die verschiedenen Reader-Instances weiterleiten. Auf diese Weise verlangsamen Abfragen, die mit einer Reader-Endpunktverbindung durchgeführt werden, keine Abfragen, die über eine andere Reader-Endpunktverbindung durchgeführt werden. Die Abfragen laufen auf separaten DB-Instances. Jede DB-Instance verfügt über eigene Rechenressourcen, Puffer-Cache usw.
- Wo praktisch, verwendet RDS Proxy dieselbe Reader-DB-Instance für alle Abfragen unter Verwendung einer bestimmten Reader-Endpunktverbindung. Auf diese Weise kann eine Reihe von verwandten Abfragen in denselben Tabellen das Caching, die Planoptimierung usw. für eine bestimmte DB-Instance nutzen.
- Wenn eine Reader-DB-Instance nicht verfügbar ist, hängt die Auswirkung auf Ihre Anwendung davon ab, ob die Sitzung Multiplexing durchführt oder fixiert ist. Wenn die Sitzung Multiplexing durchführt, leitet RDS Proxy leitet alle nachfolgenden Abfragen an eine andere Reader-DB-Instance weiter, ohne dass Sie etwas unternehmen müssen. Wenn die Sitzung fixiert ist, bekommt Ihre Anwendung einen Fehler und muss sich erneut verbinden. Sie können sich sofort wieder mit dem Reader-Endpunkt verbinden und RDS Proxy leitet die Verbindung zu einer verfügbaren Reader-DB-Instance. Weitere Informationen zum Multiplexing und Pinning für Proxy-Sitzungen finden Sie unter Überblick über RDS Proxy-Konzepte.
- Je mehr Reader-DB-Instances Sie in dem Cluster haben, desto mehr gleichzeitige Verbindungen können Sie mithilfe von Reader-Endpunkten herstellen. Angenommen, Ihr Cluster verfügt über vier Reader-DB-Instances, die jeweils so konfiguriert sind, dass sie 200 gleichzeitige Verbindungen unterstützen. Nehmen wir außerdem an, Ihr Proxy ist so konfiguriert, dass er 50 % der maximalen Verbindungen verwendet. Hier beträgt die maximale Anzahl von Verbindungen, die Sie über die Reader-Endpunkte im Proxy herstellen können, 100 (50% von 200) für Reader 1. Es sind auch 100 für Reader 2 usw. bei insgesamt 400. Wenn Sie die Anzahl der Reader-DB-Instances im Cluster

auf acht verdoppeln, verdoppelt sich die maximale Anzahl von Verbindungen über die Reader-Endpunkte ebenfalls, und zwar auf 800.

Beispiele für die Verwendung von Reader-Endpunkten

Das folgende Linux-Beispiel zeigt, wie Sie bestätigen können, dass Sie mit einem Aurora MySQL-Cluster durch einen Reader-Endpunkt verbunden sind. Die `innodb_read_only`-Konfigurationseinstellung ist aktiviert. Versuche Schreibvorgänge wie `CREATE DATABASE`-Anweisungen durchzuführen, schlagen mit einem Fehler fehl. Und Sie können bestätigen, dass Sie mit einer Reader-DB-Instance verbunden sind, indem Sie den Namen der DB-Instance mit der `aurora_server_id`-Variable prüfen.

> **Tip**
>
> Verlassen Sie sich nicht nur darauf, den Namen der DB-Instance zu überprüfen, um festzustellen, ob die Verbindung lesen/schreibgeschützt oder schreibgeschützt ist. Denken Sie daran, dass DB-Instances in Aurora-Clustern die Rollen zwischen Writer und Reader ändern können, wenn Failovers auftreten.

```
$ mysql -h endpoint-demo-reader.endpoint.proxy-demo.us-east-1.rds.amazonaws.com -u
 admin -p
...
mysql> select @@innodb_read_only;
+--------------------+
| @@innodb_read_only |
+--------------------+
|                  1 |
+--------------------+
mysql> create database shouldnt_work;
ERROR 1290 (HY000): The MySQL server is running with the --read-only option so it
 cannot execute this statement

mysql> select @@aurora_server_id;
+---------------------------------------+
| @@aurora_server_id                    |
+---------------------------------------+
| proxy-reader-endpoint-demo-instance-3 |
+---------------------------------------+
```

Das folgende Beispiel zeigt, wie Ihre Verbindung zu einem Proxy-Reader-Endpunkt auch dann weiterfunktioniert, wenn die Reader-DB-Instance gelöscht wird. In diesem Beispiel hat der Aurora-Cluster zwei Reader-Instances, `instance-5507` und `instance-7448`. Die Verbindung zum Reader-Endpunkt beginnt mit der Verwendung einer der Reader-Instances. Im Beispiel wird diese Reader-Instance durch einen Befehl `delete-db-instance` gelöscht. Für nachfolgende Abfragen wechselt RDS Proxy zu einer anderen Reader-Instance.

```
$ mysql -h reader-demo.endpoint.proxy-demo.us-east-1.rds.amazonaws.com
  -u my_user -p
...
mysql> select @@aurora_server_id;
+--------------------+
| @@aurora_server_id |
+--------------------+
| instance-5507      |
+--------------------+

mysql> select @@innodb_read_only;
+--------------------+
| @@innodb_read_only |
+--------------------+
|                  1 |
+--------------------+

mysql> select count(*) from information_schema.tables;
+----------+
| count(*) |
+----------+
|      328 |
+----------+
```

Während die `mysql`-Sitzung noch ausgeführt wird, löscht der folgende Befehl die Reader-Instance, mit der der Reader-Endpunkt verbunden ist.

```
aws rds delete-db-instance --db-instance-identifier instance-5507 --skip-final-snapshot
```

Abfragen in der `mysql`-Sitzung funktionieren weiterhin, ohne dass eine erneute Verbindung erforderlich ist. RDS Proxy wechselt automatisch zu einer anderen Reader-DB-Instance.

```
mysql> select @@aurora_server_id;
+--------------------+
```

```
| @@aurora_server_id |
+--------------------+
| instance-7448      |
+--------------------+

mysql> select count(*) from information_schema.TABLES;
+----------+
| count(*) |
+----------+
|      328 |
+----------+
```

Zugreifen auf Aurora-Datenbanken über VPCs hinweg

Standardmäßig befinden sich die Komponenten Ihres Aurora--Technologie-Stacks alle in derselben Amazon-VPC. Nehmen wir zum Beispiel an, dass eine Anwendung in einer Amazon-EC2-Instance eine Verbindung mit einem Aurora-DB-Cluster herstellt. In diesem Fall müssen sich der Anwendungsserver und die Datenbank beide innerhalb derselben VPC befinden.

Mit RDS Proxy können Sie den Zugriff auf einen Aurora-DB-Clustereine in einer VPC von Ressourcen in einer anderen VPC aus einrichten, z. B. EC2-Instances. Zum Beispiel könnte Ihre Organisation mehrere Anwendungen haben, die auf dieselben Datenbankressourcen zugreifen. Jede Anwendung könnte sich in einer eigenen VPC befinden.

Um den VPC-übergreifenden Zugriff zu aktivieren, erstellen Sie einen neuen Endpunkt für den Proxy. Der Proxy selbst befindet sich in derselben VPC wie der Aurora-DB-Cluster. Der VPC-übergreifenden Endpunkt befindet sich jedoch in der anderen VPC bei den anderen Ressourcen wie den EC2-Instances. Der VPC-übergreifende Endpunkt ist mit Subnetzen und Sicherheitsgruppen aus derselben VPC wie der EC2 und anderen Ressourcen verknüpft. Mit diesen Zuordnungen können Sie von den Anwendungen aus eine Verbindung zum Endpunkt herstellen, die aufgrund der VPC-Einschränkungen sonst nicht auf die Datenbank zugreifen können.

In den folgenden Schritten wird erläutert, wie Sie einen VPC-übergreifenden Endpunkt erstellen und darauf über RDS Proxy zugreifen:

1. Erstellen Sie zwei VPCs oder wählen Sie zwei VPCs, die Sie bereits für Aurora -Aufgaben verwenden. Jede VPC sollte über eigene Netzwerkressourcen wie ein Internet-Gateway, Routing-Tabellen, Subnetze und Sicherheitsgruppen verfügen. Wenn Sie nur eine VPC haben, können Sie Erste Schritte mit Amazon Aurora für die Schritte zum Einrichten einer anderen VPC zur erfolgreichen Verwendung von Aurora konsultieren. . Sie können Ihre vorhandene VPC auch in

der Amazon EC2-Konsole untersuchen, um die Arten von Ressourcen zu sehen, die miteinander verbunden werden sollen.

2. Erstellen Sie einen DB-Proxy, der mit dem Aurora-DB-Cluster verknüpft ist, mit dem/der Sie eine Verbindung herstellen möchten. Folgen Sie dem Verfahren unter Erstellen eines RDS Proxy.
3. Auf der Seite Einzelheiten für Ihren Proxy in der RDS-Konsole unter dem Abschnitt Proxy-Endpunkte wählen Sie Endpunkt erstellen. Folgen Sie dem Verfahren unter Erstellen eines Proxy-Endpunktes.
4. Wählen Sie aus, ob der VPC-übergreifende Endpunkt zum Lesen/Schreiben oder schreibgeschützt sein soll.
5. Anstatt den Standard der gleichen VPC wie für den Aurora-DB-Cluster zu akzeptieren, wählen Sie eine andere VPC. Diese VPC muss sich in derselben AWS-Region befinden wie die VPC, in der sich der Proxy befindet.
6. Anstatt nun die Standardeinstellungen für Subnetze und Sicherheitsgruppen von derselben VPC wie für den Aurora-DB-Cluster zu akzeptieren, treffen Sie eine neue Auswahl. Wählen Sie diese basierend auf den Subnetzen und Sicherheitsgruppen aus der von Ihnen ausgewählten VPC.
7. Sie müssen keine der Einstellungen für die Secrets Manager-Secrets ändern. Dieselben Anmeldeinformationen funktionieren für alle Endpunkte für Ihren Proxy, unabhängig davon, in welcher VPC sich jeder Endpunkt befindet.
8. Warten Sie, bis der neue Endpunkt den Status verfügbar erreicht.
9. Notieren Sie sich den vollständigen Endpunktnamen. Dies ist der Wert, der auf *`Region_name`*`.rds.amazonaws.com` endet, den Sie als Teil der Verbindungszeichenfolge für Ihre Datenbankanwendung angeben.
10. Greifen Sie auf den neuen Endpunkt von einer Ressource in derselben VPC wie der Endpunkt zu. Eine einfache Möglichkeit, diesen Prozess zu testen, besteht darin, eine neue EC2-Instance in dieser VPC zu erstellen. Melden Sie sich dann bei der EC2-Instance an und führen Sie die `psql` Befehle `mysql` oder aus, um eine Verbindung herzustellen, indem Sie den Endpunktwert in Ihrer Verbindungszeichenfolge verwenden.

Erstellen eines Proxy-Endpunktes

Konsole

So erstellen Sie einen Proxy-Endpunkt

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Proxies (Proxys).
3. Klicken Sie auf den Namen des Proxys, für den Sie einen neuen Endpunkt erstellen möchten.

   Die Detailseite für diesen Proxy wird angezeigt.
4. Im Abschnitt Proxy-Endpunkte wählen Sie Proxy-Endpunkt erstellen.

   Das Fenster Proxy-Endpunkt erstellen wird angezeigt.
5. Für Name des Proxy-Endpunkts geben Sie einen beschreibenden Namen Ihrer Wahl ein.
6. Für Ziel-Rolle wählen Sie aus, ob der Endpunkt lese-/schreibgeschützt oder schreibgeschützt sein soll.

   Verbindungen, die Lese-/Schreibendpunkte verwenden, können jede Art von Operationen ausführen, z. B. Data Definition Language (DDL)-Anweisungen, Data Manipulation Language (DML)-Anweisungen und Abfragen. Diese Endpunkte stellen immer eine Verbindung mit der primären Instance des Aurora-Clusters her. Sie können Endpunkte mit Lese-/Schreibzugriff für allgemeine Datenbankoperationen verwenden, wenn Sie nur einen einzelnen Endpunkt in Ihrer Anwendung verwenden. Sie können auch Lese-/Schreibendpunkte für administrative Vorgänge, Online Transaction Processing (OLTP)-Anwendungen und extract-transform-load (ETL)-Aufträge verwenden.

   Verbindungen, die einen schreibgeschützten Endpunkt verwenden, können nur Abfragen durchführen. Wenn es mehrere Reader-Instances im Aurora-Cluster gibt, kann RDS-Proxy für jede Verbindung mit dem Endpunkt eine andere Reader-Instance verwenden. Auf diese Weise kann eine abfrageintensive Anwendung die Clustering-Fähigkeit von Aurora nutzen. Sie können dem Cluster mehr Abfragekapazität hinzufügen, indem Sie weitere Reader-DB-Instances hinzufügen. Diese schreibgeschützten Verbindungen verursachen keinen Overhead für die primäre Instance des Clusters. Auf diese Weise verlangsamen Ihre Berichts- und Analyseabfragen die Schreibvorgänge Ihrer OLTP-Anwendungen nicht.
7. Wählen Sie für Virtual Private Cloud (VPC) die Standardeinstellung für den Zugriff auf den Endpunkt von denselben EC2-Instances oder anderen Ressourcen aus, die normalerweise für den Zugriff auf den Proxy oder die zugehörige Datenbank verwenden. Wenn Sie den VPC-

übergreifenden Zugriff für diesen Proxy einrichten möchten, wählen Sie eine andere VPC als die Standard-VPC aus. Weitere Informationen zum VPC-übergreifenden Zugriff finden Sie unter Zugreifen auf Aurora-Datenbanken über VPCs hinweg.

8. Für Subnetze füllt RDS Proxy standardmäßig dieselben Subnetze wie der zugehörige Proxy aus. Um den Zugriff auf den Endpunkt auf einen Teil des Adressbereichs der VPC zu beschränken, der eine Verbindung herstellen kann, entfernen Sie ein oder mehrere Subnetze.
9. Für die VPC-Sicherheitsgruppe können Sie eine vorhandene Sicherheitsgruppe auswählen oder eine neue erstellen. Standardmäßig füllt RDS Proxy dieselbe Sicherheitsgruppe oder Gruppen wie der zugehörige Proxy aus. Wenn die eingehenden und ausgehenden Regeln für den Proxy für diesen Endpunkt geeignet sind, behalten Sie die Standardauswahl bei.

   Wenn Sie eine neue Sicherheitsgruppe erstellen möchten, geben Sie auf dieser Seite einen Namen für die Sicherheitsgruppe an. Bearbeiten Sie dann die Sicherheitsgruppeneinstellungen später über die EC2-Konsole.
10. Wählen Sie Proxy-Endpunkt erstellen.

AWS CLI

Verwenden Sie den AWS CLI create-db-proxy-endpoint Befehl , um einen Proxy-Endpunkt zu erstellen.

Nutzen Sie die folgenden erforderlichen Parameter:

- `--db-proxy-name` *`value`*
- `--db-proxy-endpoint-name` *`value`*
- `--vpc-subnet-ids` *`list_of_ids`*. Trennen Sie die Subnetz-IDs durch Leerzeichen Sie geben die ID der VPC selbst nicht an.

Sie können auch die folgenden optionalen Parameter angeben:

- `--target-role { READ_WRITE | READ_ONLY }`. Dieser Parameter lautet standardmäßig `READ_WRITE`. Der Wert `READ_ONLY` hat nur Auswirkungen auf von Aurora bereitgestellte Cluster, die eine oder mehrere Reader-DB-Instances enthalten. Wenn der Proxy einem Aurora-Cluster zugeordnet ist, der nur eine Writer-DB-Instance enthält, können Sie nicht angeben`READ_ONLY`. Weitere Informationen zur beabsichtigten Verwendung von schreibgeschützten Endpunkten mit Aurora-Clustern finden Sie unter Verwenden von Reader-Endpunkten mit Aurora-Clustern .

- `--vpc-security-group-ids` *value*. Trennen Sie die Sicherheitsgruppen-IDs durch Leerzeichen Wenn Sie diesen Parameter weglassen, verwendet RDS Proxy die Standardsicherheitsgruppe für die VPC. RDS-Proxy bestimmt die VPC basierend auf den Subnetz-IDs, die Sie für die `--vpc-subnet-ids`-Parameter angeben.

Example

Im folgenden Beispiel wird ein Proxy-Endpunkt mit dem Namen erstell `my-endpoint`.

Für Linux, macOSoder Unix:

```
aws rds create-db-proxy-endpoint \
  --db-proxy-name my-proxy \
  --db-proxy-endpoint-name my-endpoint \
  --vpc-subnet-ids subnet_id subnet_id subnet_id ... \
  --target-role READ_ONLY \
  --vpc-security-group-ids security_group_id ]
```

Windows:

```
aws rds create-db-proxy-endpoint ^
  --db-proxy-name my-proxy ^
  --db-proxy-endpoint-name my-endpoint ^
  --vpc-subnet-ids subnet_id_1 subnet_id_2 subnet_id_3 ... ^
  --target-role READ_ONLY ^
  --vpc-security-group-ids security_group_id
```

RDS-API

Um einen Proxy-Endpunkt zu erstellen, verwenden Sie die RDS-API-Aktion CreateDBProxyEndpoint.

Anzeigen von Proxy-Endpunkten

Konsole

Anzeigen der Details für einen Proxy-Endpunkt

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Proxies (Proxys).

3. Wählen Sie in der Liste den Proxy aus, dessen Endpunkt Sie anzeigen möchten. Klicken Sie auf den Proxy-Namen, um die Detailseite anzuzeigen.
4. Wählen Sie im Abschnitt Proxy-Endpunkte den Endpunkt aus, den Sie anzeigen möchten. Klicken Sie auf seinen Namen, um die Detailseite aufzurufen.
5. Untersuchen Sie die Parameter, für deren Werten Sie sich interessieren. Sie können Eigenschaften wie die Folgenden überprüfen:

   - Ob der Endpunkt lese-/schreibgeschützt oder schreibgeschützt ist.
   - Die Endpunkt-Adresse, die Sie in einer Datenbank-Verbindungszeichenfolge verwenden.
   - Die VPC-Subnetze und -Sicherheitsgruppen, die einem Endpunkt zugeordnet sind.

AWS CLI

Um einen oder mehrere Proxy-Endpunkte anzuzeigen, verwenden Sie den AWS CLI describe-db-proxy-endpoints Befehl .

Sie können die folgenden optionalen Parameter angeben:

- `--db-proxy-endpoint-name`
- `--db-proxy-name`

Das folgende Beispiel beschreibt den `my-endpoint`-Proxy-Endpunkt.

Example

Für Linux, macOSoder Unix:

```
aws rds describe-db-proxy-endpoints \
  --db-proxy-endpoint-name my-endpoint
```

Windows:

```
aws rds describe-db-proxy-endpoints ^
  --db-proxy-endpoint-name my-endpoint
```

RDS-API

Um einen oder mehrere Proxy-Endpunkte zu beschreiben, verwenden Sie die RDS-API-Operation DescribeDBProxyEndpoints.

Ändern eines Proxy-Endpunkts

Konsole

So ändern Sie einen oder mehrere Proxy-Endpunkte

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Proxies (Proxys).
3. Wählen Sie in der Liste den Proxy aus, dessen Endpunkt Sie ändern möchten. Klicken Sie auf den Proxy-Namen, um dessen anzuzeigen
4. Wählen Sie m Abschnitt Proxy-Endpunkte den Endpunkt aus, den Sie ändern möchten. Sie können ihn in der Liste auswählen oder auf seinen Namen klicken, um die Detailseite anzuzeigen.
5. Auf der Seite mit den Proxy-Details unter dem Abschnitt Proxy-Endpunkte wählen Sie Bearbeiten. Oder wählen Sie auf der Detailseite des Proxy-Endpunkts für Aktionen die Option Bearbeiten aus.
6. Ändern Sie wie gewünscht die Werte der Parameter.
7. Wählen Sie Save Changes.

AWS CLI

Um einen Proxy-Endpunkt zu ändern, verwenden Sie den AWS CLI modify-db-proxy-endpoint Befehl mit den folgenden erforderlichen Parametern:

- `--db-proxy-endpoint-name`

Geben Sie Änderungen in den Endpunkteigenschaften an, indem Sie einen oder mehrere der folgenden Parameter verwenden:

- `--new-db-proxy-endpoint-name`
- `--vpc-security-group-ids`. Trennen Sie die Sicherheitsgruppen-IDs durch Leerzeichen

Das folgende Beispiel benennt den `my-endpoint`-Proxy-Endpunkt in `new-endpoint-name`.

Example

Für Linux, macOSoder Unix:

```
aws rds modify-db-proxy-endpoint \
  --db-proxy-endpoint-name my-endpoint \
  --new-db-proxy-endpoint-name new-endpoint-name
```

Windows:

```
aws rds modify-db-proxy-endpoint ^
  --db-proxy-endpoint-name my-endpoint ^
  --new-db-proxy-endpoint-name new-endpoint-name
```

RDS-API

Um einen Proxy-Endpunkt zu ändern, verwenden Sie die RDS-API-Operation ModifyDBProxyEndpoint.

Löschen eines Proxy-Endpunkts

Sie können einen Endpunkt für Ihren Proxy löschen, indem Sie die Konsole, wie im Folgenden beschrieben, verwenden.

> **Note**
>
> Sie können nicht den Standard-Proxy-Endpunkt löschen, den RDS Proxy automatisch für jeden Proxy erstellt.
> Wenn Sie einen Proxy löschen, löscht RDS Proxy automatisch alle zugehörigen Endpunkte.

Konsole

So löschen Sie einen Proxy-Endpunkt mit AWS Management Console

1. Wählen Sie im Navigationsbereich Proxies (Proxys).
2. Wählen Sie in der Liste den Proxy aus, dessen Endpunkt Sie löschen möchten. Klicken Sie auf den Proxy-Namen, um die Detailseite anzuzeigen.

3. Im Abschnitt Proxy-Endpunkte den Endpunkt aus, den Sie löschen möchten. Sie können einen oder mehrere Endpunkte in der Liste auswählen oder auf den Namen eines einzelnen Endpunkts klicken, um die Detailseite anzuzeigen.
4. Auf der Seite mit den Proxy-Details unter dem Abschnitt Proxy-Endpunkte, wählen Sie Löschen. Oder wählen Sie auf der Detailseite des Proxy-Endpunkts für Aktionen die Option Löschen aus.

AWS CLI

Um einen Proxy-Endpunkt zu löschen, führen Sie den delete-db-proxy-endpoint Befehl mit den folgenden erforderlichen Parametern aus:

- `--db-proxy-endpoint-name`

Der folgende Befehl löscht den Proxy-Endpunkt mit dem Namen `my-endpoint`.

Für Linux, macOSoder Unix:

```
aws rds delete-db-proxy-endpoint \
  --db-proxy-endpoint-name my-endpoint
```

Windows:

```
aws rds delete-db-proxy-endpoint ^
  --db-proxy-endpoint-name my-endpoint
```

RDS-API

Um einen Proxy-Endpunkt mit der RDS-API zu löschen, führen Sie die Operation DeleteDBProxyEndpoint aus. Geben Sie den Namen des Proxy-Endpunkts für den `DBProxyEndpointName`-Parameter an.

Limits für Proxy-Endpunkte

RDS Proxy-Endpunkte haben die folgenden Einschränkungen:

- Jeder Proxy hat einen Standard-Endpunkt, den Sie ändern, aber nicht erstellen oder löschen können.
- Die maximale Anzahl von benutzerdefinierten Endpunkten für einen Proxy beträgt 20. Daher kann ein Proxy bis zu 21 Endpunkte haben: den Standard-Endpunkt plus 20, die Sie erstellen.

- Wenn Sie zusätzliche Endpunkte mit einem Proxy verknüpfen, bestimmt RDS Proxy automatisch, welche DB-Instances in Ihrem Cluster für jeden Endpunkt verwendet werden. Sie können bestimmte Instances nicht so auswählen, wie Sie es mit benutzerdefinierten Aurora-Endpunkten können.
- Reader-Endpunkte sind nicht verfügbar für Aurora-Multi-Writer-Cluster.

Überwachen von RDS-Proxy-Metriken mit Amazon CloudWatch

Sie können RDS Proxy überwachen, indem Sie Amazon verwenden CloudWatch. CloudWatch sammelt und verarbeitet Rohdaten aus den Proxys in lesbare near-real-time Metriken. Um diese Metriken in der CloudWatch Konsole zu finden, wählen Sie Metriken, dann RDS und dann Pro-Proxy-Metriken aus. Weitere Informationen finden Sie unter Verwenden von Amazon- CloudWatch Metriken im Amazon CloudWatch -Benutzerhandbuch.

> **Note**
>
> RDS veröffentlicht diese Metriken für jede zugrunde liegende Amazon EC2-Instance, die dem Proxy zugeordnet ist. Ein einzelner Proxy kann von mehr als einer EC2-Instance bedient werden. Verwenden Sie CloudWatch Statistiken, um die Werte für einen Proxy über alle zugehörigen Instances hinweg zu aggregieren.
> Einige dieser Metriken sind möglicherweise erst nach der ersten erfolgreichen Verbindung durch einen Proxy sichtbar.

In den RDS Proxy-Protokollen wird jedem Eintrag der Name des zugehörigen Proxy-Endpunkts vorangestellt. Dieser Name kann der Name sein, den Sie für einen benutzerdefinierten Endpunkt angegeben haben, oder der spezielle Name `default` für den Standardendpunkt eines Proxys, der Lese-/Schreibanforderungen ausführt.

Alle RDS Proxy-Metriken befinden sich in der Gruppe `proxy`.

Jeder Proxy-Endpunkt hat seine eigenen CloudWatch Metriken. Sie können die Nutzung jedes Proxy-Endpunkts unabhängig überwachen. Weitere Informationen zu den Proxy-Endpunkten finden Sie unter Arbeiten mit Amazon RDS Proxy-Endpunkten.

Sie können die Werte für jede Metrik mit einem der folgenden Dimensionssätze aggregieren. Zum Beispiel können Sie, indem Sie den `ProxyName`-Dimensionssatz verwenden, den gesamten Datenverkehr für einen bestimmten Proxy analysieren. Durch die Verwendung der anderen

Dimensionssätze können Sie die Metriken auf verschiedene Arten aufteilen. Sie können die Metriken basierend auf den verschiedenen Endpunkten oder Zieldatenbanken jedes Proxys oder dem Lese-/Schreib- und schreibgeschützten Datenverkehr zu jeder Datenbank aufteilen.

- -Dimensionssatz 1: `ProxyName`
- -Dimensionssatz 2: `ProxyName`, `EndpointName`
- -Dimensionssatz 3: `ProxyName`, `TargetGroup`, `Target`
- -Dimensionssatz 4: `ProxyName`, `TargetGroup`, `TargetRole`

Metrik	Beschreibung	Gültiger Zeitraum	CloudWatch Dimensionssatz
`AvailabilityPercentage`	Der Prozentsatz der Zeit, für die die Zielgruppe in der durch die Dimension angegebenen Rolle verfügbar war. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist `Average`.	1 Minute	Dimension set 4
`ClientConnections`	Die aktuelle Anzahl von Clientverbindungen. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute	Dimension set 1, Dimension set 2
`ClientConnectionsClosed`	Die Anzahl der geschlossenen Clientverbindungen. Die nützlichste	1 Minute und höher	Dimension set 1, Dimension set 2

Metrik	Beschreibung	Gültiger Zeitraum	CloudWatch Dimensionssatz
	Statistik für diese Metrik ist Sum.		
ClientConnectionsNoTLS	Die aktuelle Anzahl von Clientverbindungen ohne TLS (Transport Layer Security). Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist Sum.	1 Minute und höher	Dimension set 1, Dimension set 2
ClientConnectionsReceived	Die Anzahl der empfangenen Clientverbindungsanforderungen. Die nützlichste Statistik für diese Metrik ist Sum.	1 Minute und höher	Dimension set 1, Dimension set 2
ClientConnectionsSetupFailedAuth	Die Anzahl der Clientverbindungsversuche, die aufgrund einer fehlerhaften Authentifizierungs- oder TLS-Konfiguration fehlgeschlagen sind. Die nützlichste Statistik für diese Metrik ist Sum.	1 Minute und höher	Dimension set 1, Dimension set 2

Metrik	Beschreibung	Gültiger Zeitraum	CloudWatch Dimensionssatz
`ClientConnectionsSetupSucceeded`	Die Anzahl der Clientverbindungen, die erfolgreich mit einem Authentifizierungsmechanismus mit oder ohne TLS hergestellt wurden. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute und höher	Dimension set 1, Dimension set 2
`ClientConnectionsTLS`	Die aktuelle Anzahl von Clientverbindungen mit TLS. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute und höher	Dimension set 1, Dimension set 2
`DatabaseConnectionRequests`	Die Anzahl der Anforderungen zum Erstellen einer Datenbankverbindung. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute und höher	Dimension set 1, Dimension set 3, Dimension set 4
`DatabaseConnectionRequestsWithTLS`	Die Anzahl der Anforderungen zum Erstellen einer Datenbankverbindung mit TLS. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute und höher	Dimension set 1, Dimension set 3, Dimension set 4

Metrik	Beschreibung	Gültiger Zeitraum	CloudWatch Dimensionssatz
DatabaseConnections	Die aktuelle Anzahl von Datenbank verbindungen. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist Sum.	1 Minute	Dimension set 1, Dimension set 3, Dimension set 4
DatabaseConnectionsBorrowLatency	Die Zeit in Mikrosekunden, die der überwachte Proxy benötigt, um eine Datenbankverbindung zu erhalten. Die nützlichste Statistik für diese Metrik ist Average.	1 Minute und höher	Dimension set 1, Dimension set 2
DatabaseConnectionsCurrentlyBorrowed	Die aktuelle Anzahl von Datenbank verbindungen im Ausleihstatus. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist Sum.	1 Minute	Dimension set 1, Dimension set 3, Dimension set 4

Metrik	Beschreibung	Gültiger Zeitraum	CloudWatch Dimensionssatz
`DatabaseConnectionsCurrentlyInTransaction`	Die aktuelle Anzahl der Datenbankverbindungen in einer Transaktion. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute	Dimension set 1, Dimension set 3, Dimension set 4
`DatabaseConnectionsCurrentlySessionPinned`	Die aktuelle Anzahl von Datenbankverbindungen, die derzeit aufgrund von Operationen in Clientanforderungen, die den Sitzungsstatus ändern, angeheftet, bzw. fixiert, werden. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute	Dimension set 1, Dimension set 3, Dimension set 4
`DatabaseConnectionsSetupFailed`	Die Anzahl der fehlgeschlagenen Datenbankverbindungsanforderungen. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute und höher	Dimension set 1, Dimension set 3, Dimension set 4

Metrik	Beschreibung	Gültiger Zeitraum	CloudWatch Dimensionssatz
`DatabaseConnectionsSetupSucceeded`	Die Anzahl der erfolgreich aufgebauten Datenbank verbindungen mit oder ohne TLS. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute und höher	Dimension set 1, Dimension set 3, Dimension set 4
`DatabaseConnectionsWithTLS`	Die aktuelle Anzahl von Datenbank verbindungen mit TLS. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute	Dimension set 1, Dimension set 3, Dimension set 4
`MaxDatabaseConnectionsAllowed`	Die maximal zulässige Anzahl von Datenbankverbindungen. Diese Metrik wird jede Minute gemeldet. Die nützlichste Statistik für diese Metrik ist `Sum`.	1 Minute	Dimension set 1, Dimension set 3, Dimension set 4
`QueryDatabaseResponseLatency`	Die Zeit in Mikrosekunden, die die Datenbank benötigt hat, um auf die Abfrage zu antworten. Die nützlichste Statistik für diese Metrik ist `Average`.	1 Minute und höher	Dimension set 1, Dimension set 2, Dimension set 3, Dimension set 4

Metrik	Beschreibung	Gültiger Zeitraum	CloudWatch Dimensionssatz
QueryRequests	Die Anzahl der empfangenen Abfragen. Eine Abfrage, die mehrere Anweisungen enthält, wird als eine Abfrage gezählt. Die nützlichste Statistik für diese Metrik ist Sum.	1 Minute und höher	Dimension set 1, Dimension set 2
QueryRequestsNoTLS	Die Anzahl der Abfragen, die von Nicht-TLS-Verbindungen empfangen wurden. Eine Abfrage, die mehrere Anweisungen enthält, wird als eine Abfrage gezählt. Die nützlichste Statistik für diese Metrik ist Sum.	1 Minute und höher	Dimension set 1, Dimension set 2
QueryRequestsTLS	Die Anzahl der Abfragen, die von TLS-Verbindungen empfangen wurden. Eine Abfrage, die mehrere Anweisungen enthält, wird als eine Abfrage gezählt. Die nützlichste Statistik für diese Metrik ist Sum.	1 Minute und höher	Dimension set 1, Dimension set 2

Metrik	Beschreibung	Gültiger Zeitraum	CloudWatch Dimensionssatz
`QueryResponseLatency`	Die Zeit in Millisekunden zwischen dem Abrufen einer Abfrageanforderung und dem darauf antwortenden Proxy. Die nützlichste Statistik für diese Metrik ist `Average`.	1 Minute und höher	Dimension set 1, Dimension set 2

Protokolle der RDS-Proxy-Aktivität finden Sie unter CloudWatch im AWS Management Console. Jeder Proxy hat einen Eintrag auf der Seite Log groups (Protokollgruppen) .

> **Important**
>
> Diese Protokolle sind zur menschlichen Verwendung zur Fehlerbehebung und nicht für den programmatischen Zugriff bestimmt. Das Format und der Inhalt der Protokolle können geändert werden.
> Insbesondere enthalten ältere Protokolle keine Präfixe, die den Endpunkt für jede Anfrage angeben. In neueren Protokollen wird jedem Eintrag der Name des zugehörigen Proxy-Endpunkts vorangestellt. Dieser Name kann der Name sein, den Sie für einen benutzerdefinierten Endpunkt angegeben haben, oder der spezielle Name `default` für Anforderungen mit dem Standard-Endpunkt eines Proxys.

Arbeiten mit RDS-Proxy-Ereignissen

Ein Ereignis weist auf eine Änderung in einer Umgebung hin, z. B. in einer AWS Umgebung, einem Dienst oder einer Anwendung von einem Software-as-a-Service (SaaS) -Partner. Es kann sich auch um eine Ihrer eigenen benutzerdefinierten Anwendungen oder Dienste handeln. Ein Beispiel: Amazon Aurora generiert ein Ereignis, wenn Sie einen RDS Proxy erstellen oder ändern. Amazon Aurora liefert Ereignisse nahezu EventBridge in Echtzeit an Amazon. Nachfolgend finden Sie eine

Liste von RDS-Proxy-Ereignissen, die Sie abonnieren können, und ein Beispiel für ein RDS-Proxy-Ereignis.

Weitere Informationen zum Arbeiten mit Ereignissen finden Sie in den folgenden Abschnitten:

- Anweisungen zum Anzeigen von Ereignissen mithilfe der AWS Management Console, AWS CLI, oder RDS-API finden Sie unter. Anzeigen von Amazon RDS-Ereignissen
- Informationen zur Konfiguration von Amazon Aurora zum Senden von Ereignissen finden Sie unter Erstellen einer Regel, die bei einem Amazon Aurora-Ereignis ausgelöst wird. EventBridge

RDS-Proxy-Ereignisse

Die folgende Tabelle zeigt die Ereigniskategorie und eine Liste von Ereignissen für den Fall, dass ein RDS Proxy der Quelltyp ist.

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Konfigurationsänderung	RDS-EVENT-0204	RDS hat den DB-Proxy *Name* geändert.	
Konfigurationsänderung	RDS-EVENT-0207	RDS hat den Endpunkt des DB-Proxys *Name* geändert.	
Konfigurationsänderung	RDS-EVENT-0213	RDS hat das Hinzufügen der DB-Instance erkannt und sie automatisch zur Zielgruppe des DB-Proxys *Name* hinzugefügt.	
Konfigurationsänderung	RDS-EVENT-0213	RDS hat das Löschen der DB-Instance *Name* erkannt und sie automatisch der Zielgruppe *Name* des DB-Proxys *Name* hinzugefügt.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Konfigurationsänderung	RDS-EVENT-0214	RDS hat das Löschen der DB-Instance *Name* erkannt und sie automatisch aus der Zielgruppe *Name* des DB-Proxys *Name* entfernt.	
Konfigurationsänderung	RDS-EVENT-0215	RDS hat das Löschen des DB-Clusters *Name* erkannt und ihn automatisch aus der Zielgruppe *Name* des DB-Proxys *Name* entfernt.	
Erstellung	RDS-EVENT-0203	RDS hat den DB-Proxy *Name* erstellt.	
Erstellung	RDS-EVENT-0206	RDS hat den Endpunkt *Name* für den DB-Proxy *Name* erstellt.	
Löschung	RDS-EVENT-0205	RDS hat den DB-Proxy *Name* erstellt.	
Löschung	RDS-EVENT-0208	RDS hat den Endpunkt *Name* für den DB-Proxy *Name* gelöscht.	

Kategorie	RDS-Ereignis-ID	Fehlermeldung	Hinweise
Ausfall	RDS-EVENT-0243	RDS konnte keine Kapazität für den Proxy *Name* bereitstellen, da in Ihren Subnetzen nicht genügend IP-Adressen verfügbar sind: *Name*. Stellen Sie sicher, dass Ihre Subnetze die Mindestanzahl unbenutzter IP-Adressen aufweisen, wie in der RDS-Proxy-Dokumentation empfohlen.	Informationen zur Bestimmung der empfohlenen Anzahl für Ihre Instance-Klasse finden Sie unter Planen der Kapazität von IP-Adressen.
Ausfall	RDS-EVENT-0275	*RDS hat einige Verbindungen zum DB-Proxynamen gedrosselt.* Die Anzahl der gleichzeitigen Verbindungsanfragen vom Client zum Proxy hat das Limit überschritten.	

Es folgt ein Beispiel eines RDS-Proxy-Ereignisses im JSON-Format. Das Ereignis zeigt, dass RDS den Endpunkt `my-endpoint` des RDS Proxy `my-rds-proxy` geändert hat. Die Ereignis-ID lautet RDS-EVENT-0207.

```
{
  "version": "0",
  "id": "68f6e973-1a0c-d37b-f2f2-94a7f62ffd4e",
  "detail-type": "RDS DB Proxy Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-09-27T22:36:43Z",
  "region": "us-east-1",
  "resources": [
     "arn:aws:rds:us-east-1:123456789012:db-proxy:my-rds-proxy"
```

```
  ],
  "detail": {
    "EventCategories": [
      "configuration change"
    ],
    "SourceType": "DB_PROXY",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:db-proxy:my-rds-proxy",
    "Date": "2018-09-27T22:36:43.292Z",
    "Message": "RDS modified endpoint my-endpoint of DB Proxy my-rds-proxy.",
    "SourceIdentifier": "my-endpoint",
    "EventID": "RDS-EVENT-0207"
  }
}
```

Befehlszeilenbeispiele für RDS Proxy

Um zu sehen, wie Kombinationen von Verbindungsbefehlen und SQL-Anweisungen mit RDS Proxy interagieren, sehen Sie sich die folgenden Beispiele an.

Beispiele

- Preserving Connections to a MySQL Database Across a Failover
- Adjusting the max_connections Setting for an Aurora DB Cluster

Example Verbindungen zu einer MySQL-Datenbank über ein Failover beibehalten

Dieses MySQL-Beispiel zeigt, wie offene Verbindungen bei einem Failover weiterhin funktionieren. Ein Beispiel ist, wenn Sie eine Datenbank neu starten oder sie aufgrund eines Problems nicht mehr verfügbar ist. In diesem Beispiel werden ein Proxy mit dem Namen `the-proxy` und ein Aurora-DB-Cluster mit den DB-Instances `instance-8898` und `instance-9814` verwendet. Wenn Sie den `failover-db-cluster`-Befehl über die Linux-Befehlszeile ausführen, wechselt die Schreiber-Instance, mit der der Proxy verbunden ist, zu einer anderen DB-Instance. Sie können sehen, dass sich die dem Proxy zugeordnete DB-Instance ändert, während die Verbindung geöffnet bleibt.

```
$ mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com -u admin_user -p
Enter password:
...

mysql> select @@aurora_server_id;
+--------------------+
```

```
| @@aurora_server_id |
+--------------------+
| instance-9814      |
+--------------------+
1 row in set (0.01 sec)

mysql>
[1]+  Stopped                 mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com
 -u admin_user -p
$ # Initially, instance-9814 is the writer.
$ aws rds failover-db-cluster --db-cluster-identifier cluster-56-2019-11-14-1399
JSON output
$ # After a short time, the console shows that the failover operation is complete.
$ # Now instance-8898 is the writer.
$ fg
mysql -h the-proxy.proxy-demo.us.us-east-1.rds.amazonaws.com -u admin_user -p

mysql> select @@aurora_server_id;
+--------------------+
| @@aurora_server_id |
+--------------------+
| instance-8898      |
+--------------------+
1 row in set (0.01 sec)

mysql>
[1]+  Stopped                 mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com
 -u admin_user -p
$ aws rds failover-db-cluster --db-cluster-identifier cluster-56-2019-11-14-1399
JSON output
$ # After a short time, the console shows that the failover operation is complete.
$ # Now instance-9814 is the writer again.
$ fg
mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com -u admin_user -p

mysql> select @@aurora_server_id;
+--------------------+
| @@aurora_server_id |
+--------------------+
| instance-9814      |
+--------------------+
1 row in set (0.01 sec)
+---------------+---------------+
| Variable_name | Value         |
```

```
+---------------+---------------+
| hostname      | ip-10-1-3-178 |
+---------------+---------------+
1 row in set (0.02 sec)
```

Example Anpassen der Einstellung max_connections für einen Aurora-DB-Cluster.

Dieses Beispiel zeigt, wie Sie die `max_connections`-Einstellung für einen Aurora MySQL-DB-Cluster anpassen können. Dazu erstellen Sie eine eigene DB-Cluster-Parametergruppe basierend auf den Standardparametereinstellungen für Cluster, die mit MySQL 5.7 kompatibel sind. Sie geben einen Wert für die `max_connections`-Einstellung an und überschreiben die Formel, die den Standardwert festlegt. Sie ordnen die DB-Clusterparametergruppe Ihrem DB-Cluster zu.

```
export REGION=us-east-1
export CLUSTER_PARAM_GROUP=rds-proxy-mysql-57-max-connections-demo
export CLUSTER_NAME=rds-proxy-mysql-57

aws rds create-db-parameter-group --region $REGION \
  --db-parameter-group-family aurora-mysql5.7 \
  --db-parameter-group-name $CLUSTER_PARAM_GROUP \
  --description "Aurora MySQL 5.7 cluster parameter group for RDS Proxy demo."

aws rds modify-db-cluster --region $REGION \
  --db-cluster-identifier $CLUSTER_NAME \
  --db-cluster-parameter-group-name $CLUSTER_PARAM_GROUP

echo "New cluster param group is assigned to cluster:"
aws rds describe-db-clusters --region $REGION \
  --db-cluster-identifier $CLUSTER_NAME \
  --query '*[*].{DBClusterParameterGroup:DBClusterParameterGroup}'

echo "Current value for max_connections:"
aws rds describe-db-cluster-parameters --region $REGION \
  --db-cluster-parameter-group-name $CLUSTER_PARAM_GROUP \
  --query '*[*].{ParameterName:ParameterName,ParameterValue:ParameterValue}' \
  --output text | grep "^max_connections"

echo -n "Enter number for max_connections setting: "
read answer

aws rds modify-db-cluster-parameter-group --region $REGION --db-cluster-parameter-
group-name $CLUSTER_PARAM_GROUP \
```

```
  --parameters "ParameterName=max_connections,ParameterValue=$
$answer,ApplyMethod=immediate"

echo "Updated value for max_connections:"
aws rds describe-db-cluster-parameters --region $REGION \
  --db-cluster-parameter-group-name $CLUSTER_PARAM_GROUP \
  --query '*[*].{ParameterName:ParameterName,ParameterValue:ParameterValue}' \
  --output text | grep "^max_connections"
```

Fehlersuche für RDS Proxy

Im Folgenden finden Sie Tipps zur Fehlerbehebung für einige häufige Probleme mit RDS Proxy und Informationen zu CloudWatch Protokollen für RDS Proxy.

In den RDS Proxy-Protokollen wird jedem Eintrag der Name des zugehörigen Proxy-Endpunkts vorangestellt. Dieser Name kann derjenige sein, den Sie für einen benutzerdefinierten Endpunkt angegeben haben. Oder es kann der spezielle Name `default` für den Standardendpunkt eines Proxys sein, der Lese-/Schreibanforderungen ausführt. Weitere Informationen zu den Proxy-Endpunkten finden Sie unter Arbeiten mit Amazon RDS Proxy-Endpunkten.

Themen

Überprüfen der Konnektivität für einen Proxy

Sie können die folgenden Befehle verwenden, um zu überprüfen, ob alle Komponenten wie Proxy, Datenbank und Rechen-Instances in der Verbindung miteinander kommunizieren können.

Untersuchen Sie den Proxy selbst mit dem describe-db-proxies Befehl . Überprüfen Sie auch die zugehörige Zielgruppe mit dem Befehl describe-db-proxy-target-groups. Überprüfen Sie, ob die Details der Ziele mit dem Aurora-Cluster übereinstimmen, den Sie dem Proxy zuordnen möchten. Verwenden Sie Befehle wie die folgenden.

```
aws rds describe-db-proxies --db-proxy-name $DB_PROXY_NAME
aws rds describe-db-proxy-target-groups --db-proxy-name $DB_PROXY_NAME
```

Um zu bestätigen, dass der Proxy eine Verbindung mit der zugrunde liegenden Datenbank herstellen kann, überprüfen Sie mit dem describe-db-proxy-targets Befehl die in den Zielgruppen angegebenen Ziele. Verwenden Sie einen Befehl wie den folgenden.

```
aws rds describe-db-proxy-targets --db-proxy-name $DB_PROXY_NAME
```

Die Ausgabe des describe-db-proxy-targets Befehls enthält ein -`TargetHealth`Feld. Sie können die Felder `State`, `Reason` und `Description` in `TargetHealth` überprüfen, um festzustellen, ob der Proxy mit der zugrunde liegenden DB-Instance kommunizieren kann.

- Der Wert `State` für `AVAILABLE` gibt an, dass der Proxy eine Verbindung mit der DB-Instance herstellen kann.
- Der Wert `State` für `UNAVAILABLE` weist auf ein temporäres oder dauerhaftes Verbindungsproblem hin. Überprüfen Sie in diesem Fall die Felder `Reason` und `Description`. Wenn beispielsweise der `Reason` den Wert `PENDING_PROXY_CAPACITY` hat, versuchen Sie erneut , eine Verbindung herzustellen, nachdem der Proxy seinen Skalierungsvorgang beendet hat. Wenn `Reason` den Wert `UNREACHABLE`, `CONNECTION_FAILED` oder `AUTH_FAILURE` hat, verwenden Sie die Erläuterung aus dem Feld `Description`, um das Problem leichter zu diagnostizieren.
- Das Feld `State` hat möglicherweise für kurze Zeit einen Wert von `REGISTERING`, bevor Sie zu `AVAILABLE` oder `UNAVAILABLE` wechseln.

Wenn der folgende Netcat-Befehl (`nc`) erfolgreich ist, können Sie über die EC2-Instance oder ein anderes System, auf dem Sie angemeldet sind, auf den Proxy-Endpunkt zugreifen. Dieser Befehl meldet einen Fehler, wenn Sie sich nicht in derselben VPC wie der Proxy und die zugehörige Datenbank befinden. Möglicherweise können Sie sich direkt bei der Datenbank anmelden, ohne sich in derselben VPC zu befinden. Sie können sich jedoch nur am Proxy anmelden, wenn Sie sich in derselben VPC befinden.

```
nc -zx MySQL_proxy_endpoint 3306

nc -zx PostgreSQL_proxy_endpoint 5432
```

Sie können die folgenden Befehle verwenden, um sicherzustellen, dass Ihre EC2-Instance über die erforderlichen Eigenschaften verfügt. Insbesondere muss die VPC für die EC2-Instance mit der VPC für die RDS-DB-Instance übereinstimmen, mit der den Aurora-Cluster übereinstimmen, mit dem der Proxy eine Verbindung herstellt.

```
aws ec2 describe-instances --instance-ids your_ec2_instance_id
```

Untersuchen Sie die für den Proxy verwendeten Secrets Manager-Secrets.

```
aws secretsmanager list-secrets
aws secretsmanager get-secret-value --secret-id your_secret_id
```

Stellen Sie sicher, dass das von angezeigte `SecretString` Feld als JSON-Zeichenfolge codiert `get-secret-value` ist, die die `password` Felder `username` und enthält. Das folgende Beispiel zeigt das Format des `SecretString`-Feldes.

```
{
  "ARN": "some_arn",
  "Name": "some_name",
  "VersionId": "some_version_id",
  "SecretString": '{"username":"some_username","password":"some_password"}',
  "VersionStages": [ "some_stage" ],
  "CreatedDate": some_timestamp
}
```

Häufige Probleme und Lösungen

In diesem Abschnitt werden einige häufige Probleme und potenzielle Lösungen bei der Verwendung von RDS Proxy beschrieben.

Wenn die `TargetHealth` Beschreibung nach dem Ausführen des `aws rds describe-db-proxy-targets` CLI-Befehls lautet`Proxy does not have any registered credentials`, überprüfen Sie Folgendes:

- Es sind Anmeldeinformationen registriert, damit der Benutzer auf den Proxy zugreifen kann.
- Die IAM-Rolle für den Zugriff auf das Secrets-Manager-Secret, das vom Proxy verwendet wird, ist gültig.

Beim Erstellen eines DB-Proxys oder beim Herstellen einer Verbindung mit einem DB-Proxy können die folgenden RDS-Ereignisse auftreten.

Kategorie	RDS-Ereignis-ID	Beschreibung
Ausfall	RDS-EVENT-0243	RDS konnte keine Kapazität für den Proxy bereitstellen, da in Ihren Subnetzen nicht genügend IP-Adressen verfügbar sind. Stellen Sie sicher, dass Ihre Subnetze die Mindestanzahl unbenutzter IP-Adressen aufweisen, um das Problem zu lösen. Informationen zur Bestimmung der empfohlenen Anzahl für Ihre Instance-Klasse finden Sie unter Planen der Kapazität von IP-Adressen.
Ausfall	RDS-EVENT-0275	RDS hat einige Verbindungen zum DB-Proxy-*Namen* gedrosselt. Die Anzahl gleichzeitiger Verbindungsanforderungen vom Client zum Proxy hat das Limit überschritten.

Beim Erstellen eines neuen Proxys oder beim Herstellen einer Verbindung mit einem Proxy können die folgenden Probleme auftreten.

Fehler	Ursachen oder Problemumgehungen
`403: The security token included in the request is invalid`	Wählen Sie eine vorhandene IAM-Rolle aus, anstatt eine neue zu erstellen.

Beim Herstellen einer Verbindung mit einem MySQL-Proxy können die folgenden Probleme auftreten.

Fehler	Ursachen oder Problemumgehungen
`ERROR 1040 (HY000): Connections rate limit exceeded (`*`limit_value`*` )`	Die Rate der Verbindungsanforderungen vom Client zum Proxy hat den Grenzwert überschritten.
`ERROR 1040 (HY000): IAM authentication rate limit exceeded`	Die Anzahl der gleichzeitigen Anforderungen mit IAM-Authentifizierung vom Client an den Proxy hat den Grenzwert überschritten.
`ERROR 1040 (HY000): Number simultaneous connections exceeded (`*`limit_value`*` )`	Die Anzahl der gleichzeitigen Verbindungsanforderungen vom Client zum Proxy hat den Grenzwert überschritten.
`ERROR 1045 (28000): Access denied for user '`*`DB_USER`*`'@'%' (using password: YES)`	Das vom Proxy verwendete Secrets Manager-Geheimnis stimmt nicht mit dem Benutzernamen und dem Passwort eines vorhandenen Datenbankbenutzers überein. Aktualisieren Sie entweder die Anmeldeinformationen im Secrets Manager-Geheimnis oder stellen Sie sicher, dass der Datenbankbenutzer vorhanden ist und über das gleiche Passwort wie im Geheimnis verfügt.
`ERROR 1105 (HY000): Unknown error`	Es ist ein unbekannter Fehler aufgetreten.
`ERROR 1231 (42000): Variable`	Der für den `character_set_client` -Parameter gesetzte Wert ist ungültig. Beispielsweise ist der Wert `ucs2` ungültig, da er den MySQL-Server zum Absturz bringen kann.

Fehler	Ursachen oder Problemumgehungen
`''character_set_client'' can't be set to the value of value`	
`ERROR 3159 (HY000): This RDS Proxy requires TLS connections.`	Sie haben die Einstellung Transport Layer Security erfordern im Proxy aktiviert, aber Ihre Verbindung enthielt den Parameter `ssl-mode=DISABLED` im MySQL-Client. Führen Sie eine der folgenden Aufgaben aus: • Deaktivieren Sie die Einstellung Transport Layer Security erfordern. • Stellen Sie eine Verbindung mit der Datenbank mit der Mindestei nstellung `ssl-mode=REQUIRED` im MySQL-Client her.
`ERROR 2026 (HY000): SSL connection error: Internal Server Error`	Der TLS-Handshake an den Proxy ist fehlgeschlagen. Einige mögliche Gründe sind: • SSL ist erforderlich, aber der Server unterstützt dies nicht. • Es ist ein interner Serverfehler aufgetreten. • Es ist ein fehlerhafter Handshake aufgetreten.
`ERROR 9501 (HY000): Timed-out waiting to acquire database connection`	Auf dem Proxy ist beim Herstellen einer Datenbankverbindung eine Zeitüberschreitung aufgetreten. Einige mögliche Gründe sind: • Der Proxy kann keine Datenbankverbindung herstellen, da die maximale Anzahl an Verbindungen erreicht wurde. • Der Proxy kann keine Datenbankverbindung herstellen, da die Datenbank nicht verfügbar ist.

Beim Herstellen einer Verbindung mit einem PostgreSQL-Proxy können die folgenden Probleme auftreten.

Fehler	Ursache	Lösung
`IAM authentication is allowed only with SSL connections.`	Der Benutzer hat versucht, mithilfe der IAM-Authentifizierung mit der Einstellung `sslmode=disable` im PostgreSQL-Client eine Verbindung zur Datenbank herzustellen.	Der Benutzer muss eine Verbindung mit der Datenbank mit der Mindesteinstellung `sslmode=require` im PostgreSQL-Client herstellen. Weitere Informationen finden Sie in der PostgreSQL SSL Support-Dokumentation.
`This RDS Proxy requires TLS connections.`	Der Benutzer hat die Option Transport Layer Security erfordern aktiviert, hat aber versucht, auf dem PostgreSQL-Client eine Verbindung mit `sslmode=disable` herzustellen.	Führen Sie einen der folgenden Schritte aus, um diesen Fehler zu beheben: • Deaktivieren Sie die Option Transport Layer Security erfordern des Proxys. • Herstellen einer Verbindung mit der Datenbank mit der Mindesteinstellung `sslmode=allow` im PostgreSQL-Client.
`IAM authentication failed for user` *`user_name`* `. Check the IAM token for this user and try again.`	Dies kann folgende Ursachen haben: • Der Client hat den falschen IAM-Benutzernamen angegeben. • Der Client hat ein falsches IAM-Autorisierungstoken für den Benutzer angegeben. • Der Client verwendet eine IAM-Richtlinie, die nicht über die erforderlichen Berechtigungen verfügt.	Gehen Sie folgendermaßen vor, um diesen Fehler zu beheben: 1. Bestätigen Sie, dass der bereitgestellte IAM-Benutzer vorhanden ist. 2. Vergewissern Sie sich, dass das IAM-Autorisierungstoken dem bereitgestellten IAM-Benutzer gehört. 3. Bestätigen Sie, dass die IAM-Richtlinie über

Fehler	Ursache	Lösung
	• Der Client hat ein abgelaufenes IAM-Autorisierungstoken für den Benutzer bereitgestellt.	ausreichende Berechtigungen für RDS verfügt. 4. Überprüfen Sie die Gültigkeit des verwendeten IAM-Autorisierungstokens.
`This RDS proxy has no credentials for the role role_name . Check the credentials for this role and try again.`	Es gibt kein Secrets Manager-Secret für diese Rolle.	Fügen Sie ein Secrets Manager-Secret diese Rolle hinzu. Weitere Informationen finden Sie unter AWS Identity and Access Management (IAM-) Richtlinien einrichten.
`RDS supports only IAM, MD5, or SCRAM authentication.`	Der Datenbank-Client, der für die Verbindung mit dem Proxy verwendet wird, nutzt einen Authentifizierungsmechanismus, der derzeit vom Proxy nicht unterstützt wird.	Wenn Sie keine IAM-Authentifizierung verwenden, verwenden Sie die MD5- oder SCRAM-Passwortauthentifizierung.
`A user name is missing from the connection startup packet. Provide a user name for this connection.`	Der Datenbankclient, der zum Herstellen einer Verbindung mit dem Proxy verwendet wird, sendet beim Versuch, eine Verbindung herzustellen, keinen Benutzernamen.	Stellen Sie sicher, dass Sie beim Einrichten einer Verbindung zum Proxy mit dem PostgreSQL-Client Ihrer Wahl einen Benutzernamen definieren.
`Feature not supported: RDS Proxy supports only version 3.0 of the PostgreSQL messaging protocol.`	Der PostgreSQL-Client, mit dem eine Verbindung zum Proxy hergestellt wird, verwendet ein Protokoll, das älter als 3.0 ist.	Verwenden Sie einen neueren PostgreSQL-Client, der das 3.0-Messaging-Protokoll unterstützt. Wenn Sie die `psql` PostgreSQL-CLI verwenden, verwenden Sie Version 7.4 oder höher.

Fehler	Ursache	Lösung
`Feature not supported: RDS Proxy currently doesn't support streaming replication mode.`	Der PostgreSQL-Client, der für die Verbindung mit dem Proxy verwendet wird, versucht, den Streaming-Replikationsmodus zu verwenden, der derzeit vom RDS-Proxy nicht unterstützt wird.	Deaktivieren Sie den Streaming-Replikationsmodus im PostgreSQL-Client, der für die Verbindung verwendet wird.
`Feature not supported: RDS Proxy currently doesn't support the option` *`option_name`* `.`	Über die Startmeldung fordert der PostgreSQL-Client, der für die Verbindung mit dem Proxy verwendet wird, eine Option an, die derzeit vom RDS-Proxy nicht unterstützt wird.	Deaktivieren Sie die Option, die in der obigen Nachricht als nicht unterstützt angezeigt wird, in dem PostgreSQL-Client, der für die Verbindung verwendet wird.
`The IAM authentication failed because of too many competing requests.`	Die Anzahl der gleichzeitigen Anforderungen mit IAM-Authentifizierung vom Client an den Proxy hat den Grenzwert überschritten.	Reduzieren Sie die Rate, mit der Verbindungen mit IAM-Authentifizierung von einem PostgreSQL-Client hergestellt werden.
`The maximum number of client connections to the proxy exceeded` *`number_value`* `.`	Die Anzahl der gleichzeitigen Verbindungsanforderungen vom Client zum Proxy hat den Grenzwert überschritten.	Reduzieren Sie die Anzahl der aktiven Verbindungen von PostgreSQL-Clients zu diesem RDS-Proxy.
`Rate of connection to proxy exceeded` *`number_value`* `.`	Die Rate der Verbindungsanforderungen vom Client zum Proxy hat den Grenzwert überschritten.	Reduzieren Sie die Rate, mit der Verbindungen von einem PostgreSQL-Client hergestellt werden.

Fehler	Ursache	Lösung
`The password that was provided for the role` *`role_name`* `is wrong.`	Das Passwort für diese Rolle stimmt nicht mit dem Secrets Manager-Secret überein.	Überprüfen Sie den Schlüssel für diese Rolle in Secrets Manager, um festzuste llen, ob das Passwort mit dem in Ihrem PostgreSQL-Client verwendeten Passwort übereinstimmt.
`The IAM authentic ation failed for the role` *`role_name`* `. Check the IAM token for this role and try again.`	Es gibt ein Problem mit dem IAM-Token, das für die IAM-Authentifizierung verwendet wird.	Generieren Sie ein neues Authentifizierungstoken und verwenden Sie es in einer neuen Verbindung.
`IAM is allowed only with SSL connections.`	Ein Client hat versucht, eine Verbindung über die IAM-Authentifizierung herzustellen, aber SSL war nicht aktiviert.	Aktivieren Sie SSL im PostgreSQL-Client.
`Unknown error.`	Es ist ein unbekannter Fehler aufgetreten.	Wenden Sie sich an den AWS Support, um das Problem zu untersuchen.

Fehler	Ursache	Lösung
`Timed-out waiting to acquire database connection.`	Auf dem Proxy ist beim Herstellen einer Datenbank verbindung eine Zeitübers chreitung aufgetreten. Einige mögliche Gründe sind: • Der Proxy kann keine Datenbankverbindung herstellen, da die maximale Anzahl an Verbindungen erreicht wurde. • Der Proxy kann keine Datenbankverbindun g herstellen, da die Datenbank nicht verfügbar ist.	Folgende Lösungen sind möglich: • Überprüfen Sie den Status des Ziels der RDS-DB-In stance des Aurora-Clusters, um festzustellen, ob dies nicht verfügbar ist. • Prüfen Sie, ob lang andauernde Transakti onen und/oder Abfragen ausgeführt werden. Diese können Datenbank verbindungen aus dem Verbindungspool für eine lange Zeit belegen.

Fehler	Ursache	Lösung
`Request returned an error: database_error .`	Die vom Proxy hergestellte Datenbankverbindung hat einen Fehler zurückgegeben.	Die Lösung hängt vom spezifischen Datenbank fehler ab. Ein Beispiel is: `Request returned an error: database "your-database-name" does not exist`. Das bedeutet, dass der angegebene Datenbankname nicht auf dem Datenbankserver existiert. Oder es bedeutet, dass der als Datenbankname verwendet e Benutzername (wenn kein Datenbankname angegeben ist) auf dem Server nicht vorhanden ist.

Verwenden von RDS Proxy mit AWS CloudFormation

Sie können RDS Proxy mit AWS CloudFormation nutzen. Auf diese Weise können Sie Gruppen verwandter Ressourcen erstellen. Eine solche Gruppe kann einen Proxy enthalten, der eine Verbindung mit einem neu erstellten Aurora-DB-Cluster herstellen kann. Die RDS-Proxy-Unterstützung in AWS CloudFormation umfasst zwei neue Registrierungstypen: `DBProxy` und `DBProxyTargetGroup`.

Die folgende Auflistung zeigt eine AWS CloudFormation-Beispielvorlage für RDS Proxy.

```
Resources:
 DBProxy:
   Type: AWS::RDS::DBProxy
   Properties:
     DBProxyName: CanaryProxy
     EngineFamily: MYSQL
     RoleArn:
      Fn::ImportValue: SecretReaderRoleArn
     Auth:
```

```
      - {AuthScheme: SECRETS, SecretArn: !ImportValue ProxySecret, IAMAuth: DISABLED}
    VpcSubnetIds:
      Fn::Split: [",", "Fn::ImportValue": SubnetIds]

ProxyTargetGroup:
  Type: AWS::RDS::DBProxyTargetGroup
  Properties:
    DBProxyName: CanaryProxy
    TargetGroupName: default
    DBInstanceIdentifiers:
      - Fn::ImportValue: DBInstanceName
  DependsOn: DBProxy
```

Weitere Informationen zu den Ressourcen in diesem Beispiel finden Sie unter `DBProxy` und `DBProxyTargetGroup`.

Weitere Informationen zu den Ressourcen, die Sie mit AWS CloudFormation erstellen können, finden Sie in der Referenz zu RDS-Ressourcentypen.

Verwenden von RDS Proxy mit globalen Aurora-Datenbanken

Eine globale Aurora-Datenbank ist eine einzige Datenbank, die mehrere AWS-Regionen abdeckt, um globale Lesezugriffe mit niedriger Latenz und eine Notfallwiederherstellung nach regionalen Ausfällen zu ermöglichen. Es bietet eine integrierte Fehlertoleranz für Ihre Bereitstellung, da die DB-Instance nicht auf eine einzelne AWS-Region, sondern auf mehreren Regionen und verschiedenen Availability Zones zurückgreifen kann. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Global Databases.

Sie können RDS Proxy mit jedem DB-Cluster in einer globalen Aurora-Datenbank verwenden. Bevor Sie beginnen, diese Funktionen zusammen zu verwenden, sollten Sie sich mit den folgenden Informationen vertraut machen.

> **Important**
>
> Wenn der DB-Cluster Teil einer globalen Datenbank mit aktivierter Schreibweiterleitung ist, reduzieren Sie den `MaxConnectionsPercent`-Wert Ihres Proxys um das Kontingent, das der Schreibweiterleitung zugewiesen ist. Das Kontingent für die Schreibweiterleitung ist im DB-Cluster-Parameter `aurora_fwd_writer_max_connections_pct` festgelegt.

Informationen zur Schreibweiterleitung finden Sie unter Verwenden der Schreibweiterleitung in einer Amazon Aurora globalen Datenbank.

Einschränkungen für RDS Proxy mit globalen Datenbanken

Wenn im Aurora-DB-Cluster die Schreibweiterleitung aktiviert ist, unterstützt RDS Proxy den `SESSION`-Wert für die `aurora_replica_read_consistency`-Variable nicht. Durch das Festlegen dieses Werts kann unerwartetes Verhalten auftreten.

So funktionieren RDS-Proxy-Endpunkte mit globalen Datenbanken

Wenn Sie verstehen, wie RDS-Proxy-Endpunke mit globalen Datenbanken funktionieren, können Sie Ihre Anwendungen, die Aurora-Datenbanken verwenden, mit diesen beiden Funktionen besser verwalten.

Bei einem Proxy mit dem primären Cluster einer globalen Datenbank als registriertem Ziel funktionieren die Proxy-Endpunkte genauso wie bei jedem beliebigen Aurora-DB-Cluster. Die Lese-/Schreib-Endpunkte des Proxy senden alle Anforderungen an die Writer-Instance des Clusters. Die schreibgeschützten Endpunkte des Proxys senden alle Anfragen an die Reader-Instances. Wenn ein Reader nicht mehr verfügbar ist, während eine Verbindung geöffnet ist, leitet RDS Proxy nachfolgende Abfragen in der Verbindung an eine andere Reader-Instance weiter. Bei einem Proxy mit einem sekundären Cluster als registriertem Ziel werden Anfragen, die an die schreibgeschützten Endpunkte des Proxys gesendet werden, auch an die Reader-Instances gesendet. Da der Cluster keine Writer-Instances hat, schlagen Anfragen, die an Lese/Schreib-Endpunkte gesendet werden, mit dem Fehler „`The target group doesn't have any associated read/write instances`“ fehl.

Eine globale Datenbank-Umstellung und Failover-Vorgänge umfassen einen Rollenwechsel zwischen dem primären und einem der sekundären DB-Cluster. Wenn der ausgewählte sekundäre Cluster zum neuen primären Cluster wird, wird eine seiner Reader-Instances zum Writer hochgestuft. Diese DB-Instance ist jetzt die neue Writer-Instance für den globalen Cluster. Stellen Sie sicher, dass Sie die Schreibvorgänge Ihrer Anwendung an den entsprechenden Lese/Schreib-Endpunkt des Proxys umleiten, der dem neuen primären Cluster zugeordnet ist. Dieser Proxy-Endpunkt kann der Standardendpunkt oder ein benutzerdefinierter Lese/Schreib-Endpunkt sein.

RDS Proxy stellt alle Anfragen über Lese/Schreib-Endpunkte in die Warteschlange und sendet sie an die Schreib-Iinstance des neuen primären Clusters, sobald dieser verfügbar ist. Dies geschieht

unabhängig davon, ob die Umstellung oder der Failover-Vorgang abgeschlossen ist. Während der Umstellung oder des Failovers akzeptiert der Standardendpunkt des Proxys für den alten primären Cluster weiterhin Schreibvorgänge. Sobald dieser Cluster jedoch zu einem sekundären Cluster wird, schlagen alle Schreibvorgänge fehl. Informationen dazu, wie und wann bestimmte globale Umstellungs- oder Failover-Aufgaben ausgeführt werden müssen, finden Sie in den folgenden Themen:

- Globale Datenbank-Umstellung – Durchführen von Umstellungen für Amazon Aurora Global Databases
- Globales Datenbank-Failover – Wiederherstellen einer globalen Amazon Aurora-Datenbank nach einem ungeplanten Ausfall

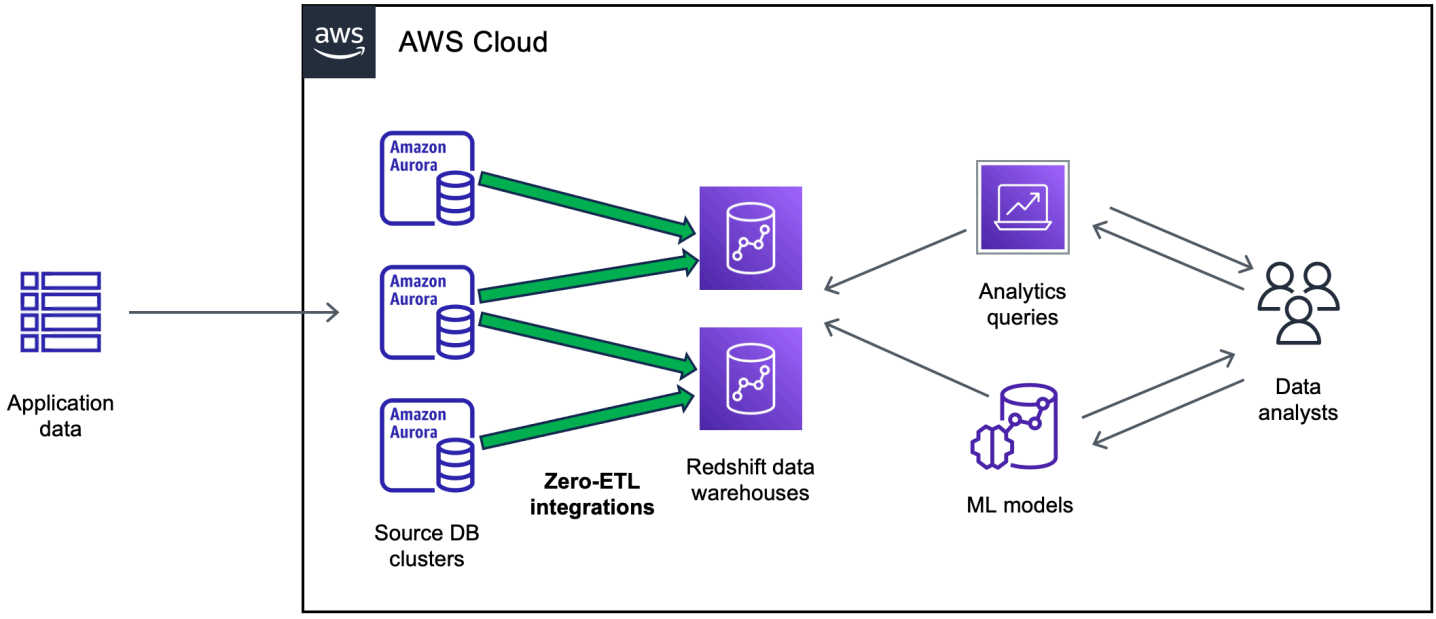
Arbeiten mit AuroraNull-ETL-Integrationen in Amazon Redshift

Eine Aurora-Null-ETL-Integration mit Amazon Redshift ermöglicht nahezu in Echtzeit Analysen und Machine Learning (ML) mit Amazon Redshift auf Transaktionsdaten von Aurora im Petabytemaßstab. Es handelt sich um eine vollständig verwaltete Lösung, um Transaktionsdaten in Amazon Redshift verfügbar zu machen, nachdem sie in einen Aurora DB-Cluster der geschrieben wurden. Beim Extrahieren, Transformieren und Laden (ETL) werden Daten aus mehreren Quellen in einem großen, zentralen Data Warehouse kombiniert.

Eine Zero-ETL-Integration macht die Daten in Ihrem Aurora DB-Cluster in Ihrer nahezu in Echtzeit in Amazon Redshift verfügbar. Sobald sich diese Daten in Amazon Redshift befinden, können Sie Ihre Analyse-, ML- und KI-Workloads mithilfe der integrierten Funktionen von Amazon Redshift unterstützen, z. B. maschinelles Lernen, materialisierte Ansichten, gemeinsame Nutzung von Daten, Verbundzugriff auf mehrere Datenspeicher und Data Lakes sowie Integrationen mit Amazon, Amazon SageMaker und anderen. QuickSight AWS-Services

Um eine Zero-ETL-Integration zu erstellen, geben Sie einen Aurora-DB-Cluster für die als Quelle und ein Amazon Redshift Data Warehouse als Ziel an. Bei der Integration werden Daten aus der Quelldatenbank in das Ziel-Data-Warehouse repliziert.

Das folgende Diagramm verdeutlicht diese Funktionalität:



Die Integration überwacht den Zustand der Datenpipeline und behebt nach Möglichkeit Probleme. Sie können Integrationen aus mehreren Aurora-DB-Clustern von mehreren in einen einzigen Amazon Redshift Redshift-Namespace erstellen, sodass Sie Erkenntnisse über mehrere Anwendungen hinweg gewinnen können.

Informationen zu den Preisen für Zero-ETL-Integrationen finden Sie unter und Amazon Redshift Redshift-Preise.

Themen

Vorteile

AuroraNull-ETL-Integrationen mit Amazon Redshift bieten die folgenden wichtigen Vorteile:

- Sie helfen Ihnen dabei, ganzheitliche Erkenntnisse aus mehreren Datenquellen zu gewinnen.
- Eliminieren Sie die Erfordernis zur Erstellung und Verwaltung komplexer Daten-Pipelines, die Extract, Transform, Load (ETL)-Operationen ausführen. Null-ETL-Integrationen beseitigen die Herausforderungen, die mit dem Aufbau und der Verwaltung von Pipelines einhergehen, indem sie diese für Sie bereitstellen und verwalten.
- Sie reduzieren den Betriebsaufwand und die Kosten, sodass Sie sich ganz auf die Verbesserung Ihrer Anwendungen konzentrieren können.

- Sie können die Analyse- und ML-Funktionen von Amazon Redshift nutzen, um Erkenntnisse aus Transaktions- und anderen Daten zu gewinnen und effektiv auf kritische, zeitkritische Ereignisse zu reagieren.

Die wichtigsten Konzepte

Wenn Sie mit Null-ETL-Integrationen beginnen, sollten Sie die folgenden Konzepte berücksichtigen:

Integration

Eine vollständig verwaltete Datenpipeline, die automatisch Transaktionsdaten und Schemas aus einem Aurora-DB-Cluster einer in ein Amazon Redshift Redshift-Data Warehouse repliziert.

Der Aurora-DB-Cluster der , aus dem Daten repliziert werden. Für Aurora MySQL können Sie einen DB-Cluster angeben, der bereitgestellte DB-Instances oder Aurora Serverless v2 DB-Instances als Quelle verwendet. Für die Aurora PostgreSQL-Vorschau können Sie nur einen Cluster angeben, der bereitgestellte DB-Instances verwendet.

Ziel-Data-Warehouse

Das Data Warehouse von Amazon Redshift, in das die Daten repliziert werden. Es gibt zwei Arten von Data Warehouse: ein bereitgestelltes Cluster-Data-Warehouse und ein Serverless-Data-Warehouse. Ein bereitgestelltes Cluster-Data-Warehouse ist eine Sammlung von Datenverarbeitungsressourcen, den sogenannten Knoten, die zu einer Gruppe, einem sogenannten Cluster, zusammengefasst werden. Ein Serverless-Data-Warehouse besteht aus einer Arbeitsgruppe, die Datenverarbeitungsressourcen speichert, und einem Namespace, in dem die Datenbankobjekte und Benutzer gespeichert sind. In beiden Data Warehouses wird eine Amazon-Redshift-Engine ausgeführt und beide enthalten eine oder mehrere Datenbanken.

DB-Cluster mit mehreren können in dasselbe Ziel schreiben.

Weitere Informationen finden Sie unter Architektur des Data-Warehouse-Systems im Entwicklerhandbuch zu Amazon Redshift.

Einschränkungen

Die folgenden Einschränkungen gelten für Aurora-Null-ETL-Integrationen mit Amazon Redshift.

Themen

Allgemeine Einschränkungen

- Der muss sich in derselben Region wie das Amazon Redshift Redshift-Ziel-Data Warehouse befinden.
- Sie können einen oder eine seiner Instances nicht umbenennen, wenn er über bestehende Integrationen verfügt.
- Sie können keinen löschen, der über bestehende Integrationen verfügt. Sie müssen zuerst alle zugehörigen Integrationen löschen.
- Wenn Sie den beenden, werden die letzten Transaktionen möglicherweise nicht in das Ziel-Data Warehouse repliziert, bis Sie den wieder aufnehmen.
- Wenn Ihr die Quelle einer blauen/grünen Bereitstellung ist, können die blauen und grünen Umgebungen während des Switchovers keine vorhandenen Zero-ETL-Integrationen enthalten. Sie müssen zuerst die Integration löschen und umstellen. Anschließend erstellen Sie die Integration neu.
- Ein DB-Cluster muss mindestens eine DB-Instance enthalten, um die Quelle einer Integration zu sein.
- Wenn der DB-Quell-Cluster in einer globalen Aurora-Datenbank verwendet wird und ein Failover zu einem der sekundären Cluster erfolgt, wird die Integration inaktiv. Sie müssen die Integration löschen und erneut erstellen.
- Sie können keine Integration für eine Quelldatenbank erstellen, für die aktiv eine andere Integration erstellt wird.
- Wenn Sie zum ersten Mal eine Integration erstellen oder wenn eine Tabelle erneut synchronisiert wird, kann das Seeding von Daten von der Quelle zum Ziel je nach Größe der Quelldatenbank 20 bis 25 Minuten oder länger dauern. Diese Verzögerung kann zu einer erhöhten Replikatverzögerung führen.
- Einige Datentypen werden nicht unterstützt. Weitere Informationen finden Sie unter the section called “Datentypunterschiede”.
- Fremdschlüsselverweise mit vordefinierten Tabellenaktualisierungen werden nicht unterstützt. Insbesondere werden `ON UPDATE` Regeln mit `CASCADESET NULL`, und `SET DEFAULT` -Aktionen

nicht unterstützt. `ON DELETE` Der Versuch, eine Tabelle mit solchen Verweisen in einer anderen Tabelle zu erstellen oder zu aktualisieren, führt zu einem Fehlschlag der Tabelle.

- `ALTER TABLE`Partitionsoperationen führen dazu, dass Ihre Tabelle neu synchronisiert wird, um Daten von Aurora nach Amazon Redshift neu zu laden. Die Tabelle kann während der Resynchronisierung nicht abgefragt werden. Weitere Informationen finden Sie unter the section called “Eine oder mehrere meiner Amazon-Redshift-Tabellen erfordern eine erneute Synchronisation”.
- XA-Transaktionen werden nicht unterstützt.
- Objektkennungen (einschließlich Datenbankname, Tabellenname, Spaltennamen und andere) dürfen nur alphanumerische Zeichen, Zahlen, $ und _ (Unterstrich) enthalten.

Einschränkungen von Aurora MySQL

- Auf Ihrem Quell-DB-Cluster muss Aurora MySQL Version 3.05 (kompatibel mit MySQL 8.0.32) oder höher ausgeführt werden.
- Null-ETL-Integrationen benötigen die MySQL-Binärprotokollierung (Binlog), um laufende Datenänderungen zu erfassen. Verwenden Sie keine binlog-basierte Datenfilterung, da dies zu Dateninkonsistenzen zwischen der Quell- und Zieldatenbank führen kann.
- Aurora-MySQL-Systemtabellen, temporäre Tabellen und Ansichten werden nicht in Amazon Redshift repliziert.
- Null-ETL-Integrationen werden nur für Datenbanken unterstützt, die für die Verwendung der InnoDB-Speicher-Engine konfiguriert sind.

Einschränkungen der Aurora PostgreSQL-Vorversion

> **Important**
>
> Die Zero-ETL-Integrationen mit der Amazon Redshift Redshift-Funktion für Aurora PostgreSQL befinden sich in der Vorschauversion. Sowohl die Dokumentation als auch die Funktion können sich ändern. Sie können diese Funktion nur in Testumgebungen verwenden, nicht in Produktionsumgebungen. Weitere Informationen zu den Bedingungen für Vorschauversionen finden Sie unter Betas und Vorversionen in den AWS - Servicebedingungen.

- Auf Ihrem Quell-DB-Cluster muss Aurora PostgreSQL ausgeführt werden (kompatibel mit PostgreSQL 15.4 und Zero-ETL Support).
- Sie können Zero-ETL-Integrationen für Aurora PostgreSQL nur in der Amazon RDS Database Preview-Umgebung im Osten der USA (Ohio) (us-east-2) erstellen und verwalten. AWS-Region Sie können die Vorschauumgebung verwenden, um Beta-, Release Candidate- und frühe Produktionsversionen der PostgreSQL-Datenbank-Engine-Software zu testen.
- Sie können Integrationen für Aurora PostgreSQL nur mit dem erstellen und verwalten. AWS Management Console Sie können die AWS Command Line Interface (AWS CLI), die Amazon RDS-API oder eines der AWS SDKs nicht verwenden.
- Wenn Sie einen Quell-DB-Cluster erstellen, müssen für die von Ihnen gewählte Parametergruppe bereits die erforderlichen DB-Cluster-Parameterwerte konfiguriert sein. Sie können danach keine neue Parametergruppe erstellen und sie dann dem Cluster zuordnen. Eine Liste der erforderlichen Parameter finden Sie unterthe section called “Schritt 1: Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe”.
- Sie können eine Integration nach der Erstellung nicht mehr ändern. Wenn Sie bestimmte Einstellungen ändern müssen, müssen Sie die Integration löschen und neu erstellen.
- Derzeit führen Aurora PostgreSQL-DB-Cluster, die die Quelle einer Integration sind, keine automatische Erfassung logischer Replikationsdaten durch.
- Alle Datenbanken, die im Aurora PostgreSQL-Quell-DB-Cluster erstellt wurden, müssen die UTF-8-Kodierung verwenden.
- Spaltennamen dürfen keines der folgenden Zeichen enthalten: Kommas (,), Semikolons (;), Klammern (), geschweifte Klammern {}, Zeilenumbrüche (\n), Tabulatoren (\ t), Gleichheitszeichen (=) und Leerzeichen.
- Zero-ETL-Integrationen mit Aurora PostgreSQL unterstützen Folgendes nicht:
  - Aurora Serverless v2DB-Instances. Ihr Quell-DB-Cluster muss bereitgestellte DB-Instances verwenden.
  - Benutzerdefinierte Datentypen oder Datentypen, die durch Erweiterungen erstellt wurden.
  - Subtransaktionen auf dem Quell-DB-Cluster.
  - Umbenennen von Schemas oder Datenbanken innerhalb eines Quell-DB-Clusters.
  - Wiederherstellung aus einem DB-Cluster-Snapshot oder Verwendung von Aurora-Cloning zur Erstellung eines Quell-DB-Clusters. Wenn Sie vorhandene Daten in einen Vorschau-Cluster integrieren möchten, müssen Sie die `pg_restore` Dienstprogramme `pg_dump` oder verwenden.
  - Erstellung von logischen Replikationsslots auf der Writer-Instance des Quell-DB-Clusters.

- Große Feldwerte, für die die Oversized-Attribute-Storage-Technik (TOAST) erforderlich ist.
- `ALTER TABLE`Partitionsoperationen. Diese Operationen können dazu führen, dass Ihre Tabelle erneut synchronisiert wird und schließlich in einen `Failed` Status übergeht. Wenn eine Tabelle ausfällt, müssen Sie sie löschen und neu erstellen.

Einschränkungen für Amazon Redshift

Eine Liste der Einschränkungen von Amazon Redshift im Zusammenhang mit Zero-ETL-Integrationen finden Sie unter Überlegungen im Amazon Redshift Management Guide.

Kontingente

Für Ihr Konto gelten die folgenden Kontingente in Bezug auf Aurora-Null-ETL-Integrationen mit Amazon Redshift. Jedes Kontingent gilt pro Region, sofern nicht anders angegeben.

Name	Standard	Beschreibung
Integrationen	100	Die Gesamtzahl der Integrationen innerhalb eines AWS-Konto.
Integrationen pro Ziel-Data-Warehouse	50	Die Anzahl der Integrationen, die Daten an ein einzelnes Ziel-Data-Warehouse von Amazon Redshift senden.
Integrationen pro Quell-Cluster	5 für Aurora MySQL, 1 für Aurora PostgreSQL	Die Anzahl der Integrationen, die Daten aus einem DB-Cluster einer einzelnen senden.

Darüber hinaus legt Amazon Redshift bestimmte Einschränkungen für die Anzahl der zulässigen Tabellen in jeder Datenbank-Instance oder jedem Cluster-Knoten fest. Weitere Informationen finden Sie unter Kontingente und Limits in Amazon Redshift im Verwaltungshandbuch zu Amazon Redshift.

Unterstützte Regionen

Aurora Zero-ETL-Integrationen mit Amazon Redshift sind in einer Teilmenge von verfügbar. AWS-Regionen Eine Liste der unterstützten -Regionen finden Sie unter the section called “Null-ETL-Integrationen ”.

Erste Schritte mit Null-ETL-Integrationen von Aurora in Amazon Redshift

Bevor Sie eine Zero-ETL-Integration mit Amazon Redshift erstellen, konfigurieren Sie Ihren Aurora DB-Cluster für die und Ihr Amazon Redshift Data Warehouse mit den erforderlichen Parametern und Berechtigungen. Während der Einrichtung führen Sie die folgenden Schritte aus:

1. Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe.
2. ???
3. Erstellen eines Ziel-Data-Warehouses in Amazon Redshift.

Wenn Sie diese Aufgaben abgeschlossen haben, fahren Sie mit the section called “Erstellen von Null-ETL-Integrationen” fort.

Sie können die AWS SDKs verwenden, um den Einrichtungsprozess für Sie zu automatisieren. Weitere Informationen finden Sie unter the section called “Richten Sie eine Integration mithilfe der AWS SDKs ein (nur Aurora MySQL)”.

Schritt 1: Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe

Aurora Zero-ETL-Integrationen mit Amazon Redshift erfordern spezifische Werte für die DB-Cluster-Parameter, die die Replikation steuern. Insbesondere erfordert Aurora MySQL eine erweiterte binlog (`aurora_enhanced_binlog`), und Aurora PostgreSQL erfordert eine erweiterte logische Replikation (). `aurora.enhanced_logical_replication`

Um die binäre Protokollierung oder logische Replikation zu konfigurieren, müssen Sie zuerst eine benutzerdefinierte DB-Cluster-Parametergruppe erstellen und diese dann dem Quell-DB-Cluster zuordnen.

Erstellen Sie je nach Quell-DB-Engine eine benutzerdefinierte DB-Cluster-Parametergruppe mit den folgenden Einstellungen. Anweisungen zum Erstellen einer Parametergruppe finden Sie unter .

Aurora MySQL (Aurora-Mysql8.0-Familie):

- `aurora_enhanced_binlog=1`
- `binlog_backup=0`
- `binlog_format=ROW`
- `binlog_replication_globaldb=0`
- `binlog_row_image=full`
- `binlog_row_metadata=full`

Stellen Sie außerdem sicher, dass der `binlog_transaction_compression`-Parameter nicht auf `ON` und der `binlog_row_value_options`-Parameter nicht auf `PARTIAL_JSON` gesetzt ist.

Weitere Informationen zu Aurora MySQL Enhanced Binlog finden Sie unterthe section called “Einrichten eines erweiterten Binärprotokolls”.

Aurora PostgreSQL (Aurora-Postgresql15-Familie):

> **Note**
>
> Für Aurora PostgreSQL-DB-Cluster müssen Sie die benutzerdefinierte Parametergruppe in der Amazon RDS Database Preview-Umgebung im Osten der USA (Ohio) (us-east-2) erstellen. AWS-Region

- `rds.logical_replication=1`
- `aurora.enhanced_logical_replication=1`
- `aurora.logical_replication_backup=0`
- `aurora.logical_replication_globaldb=0`

Durch die Aktivierung der erweiterten logischen Replikation (`aurora.enhanced_logical_replication`) wird der `REPLICA IDENTITY` Parameter automatisch auf gesetzt`FULL`, was bedeutet, dass alle Spaltenwerte in das Write-Ahead-Protokoll (WAL) geschrieben werden. Dadurch werden die IOPS für Ihren Quell-DB-Cluster erhöht.

Schritt 2: Wählen oder erstellen Sie einen

Nachdem Sie eine benutzerdefinierte DB-Cluster-Parametergruppe erstellt haben, wählen oder erstellen Sie einen , den Aurora MySQL- oder Aurora PostgreSQL-DB-Cluster. Dieser wird die Quelle für die Datenreplikation nach Amazon Redshift sein.

Auf dem muss , Aurora MySQL Version 3.05 (kompatibel mit MySQL 8.0.32) oder höher oder Aurora PostgreSQL (kompatibel mit PostgreSQL 15.4 und Zero-ETL Support) ausgeführt werden.

> **Note**
>
> Sie müssen Aurora PostgreSQL-DB-Cluster in der Amazon RDS Database Preview-Umgebung im Osten der USA (Ohio) (us-east-2) erstellen. AWS-Region

Ändern Sie unter Zusätzliche Konfiguration die Standard-DB-Cluster-Parametergruppe in die benutzerdefinierte Parametergruppe, die Sie im vorherigen Schritt erstellt haben.

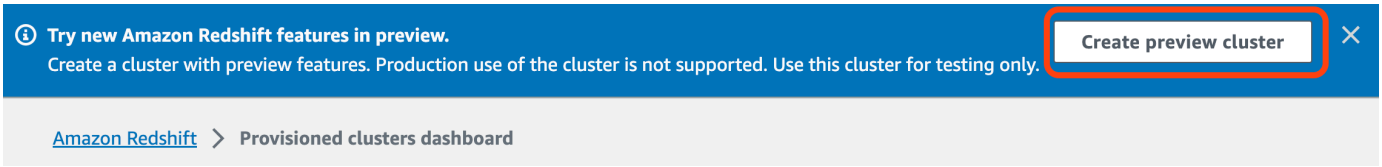
> **Note**
>
> Sie für Aurora MySQL die Parametergruppe dem zuordnen, nachdem der bereits erstellt wurde, müssen Sie die primäre im Cluster neu starten, um die Änderungen zu übernehmen, bevor Sie eine Zero-ETL-Integration erstellen können. Anweisungen finden Sie unter the section called “Neustart eines Aurora DB-Clusters oder einer Instance”.
> Während der Vorabversion der Aurora PostgreSQL Zero-ETL-Integrationen mit Amazon Redshift müssen Sie den Cluster bei der Erstellung des Clusters mit der benutzerdefinierten DB-Cluster-Parametergruppe verknüpfen. Sie können diese Aktion nicht ausführen, nachdem der Quell-DB-Cluster bereits erstellt wurde. Andernfalls müssen Sie den Cluster löschen und neu erstellen.

Schritt 3: Erstellen eines Ziel-Data-Warehouses in Amazon Redshift

Nachdem Sie Ihren erstellt haben, müssen Sie ein Ziel-Data Warehouse in Amazon Redshift erstellen und konfigurieren. Das Data Warehouse muss die folgenden Anforderungen erfüllen:

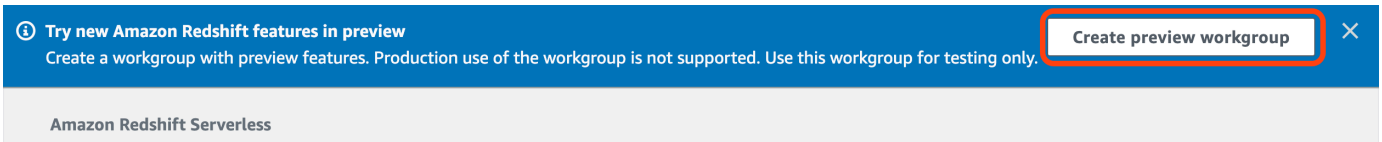
- In der Vorschauversion erstellt (nur für Aurora PostgreSQL-Quellen). Für Aurora MySQL-Quellen müssen Sie Produktionscluster und Arbeitsgruppen erstellen.

- Um einen bereitgestellten Cluster in der Vorschauversion zu erstellen, wählen Sie Vorschau-Cluster erstellen von dem Banner im Dashboard für bereitgestellte Cluster aus. Weitere Informationen finden Sie unter Erstellen eines Vorschau-Clusters.



  Stellen Sie beim Erstellen des Clusters den Vorschau-Track auf `preview_2023` ein.

- Um eine Redshift-Serverless-Arbeitsgruppe in der Vorschauversion zu erstellen, wählen Sie Vorschau-Arbeitsgruppe erstellen von dem Banner im Serverless-Dashboard aus. Weitere Informationen finden Sie unter Erstellen einer Vorschau-Arbeitsgruppe.



- Verwendung eines RA3-Knotentyps (`ra3.xlplusra3.4xlarge`,, oder`ra3.16xlarge`) oder Redshift Serverless.
- Es muss verschlüsselt sein (bei Verwendung eines bereitgestellten Clusters). Weitere Informationen finden Sie unter Datenbankverschlüsselung in Amazon Redshift.

Anweisungen zum Erstellen eines Data Warehouse finden Sie unter Erstellen eines Clusters für bereitgestellte Cluster oder Erstellen einer Arbeitsgruppe mit einem Namespace für Redshift Serverless.

Aktivieren Sie die Berücksichtigung von Groß- und Kleinschreibung im Data Warehouse

Damit die Integration erfolgreich ist, muss der Parameter für die Berücksichtigung von Groß- und Kleinschreibung (`enable_case_sensitive_identifier`) für das Data Warehouse aktiviert sein. Standardmäßig ist die Berücksichtigung von Groß- und Kleinschreibung auf allen bereitgestellten Clustern und Redshift-Serverless-Arbeitsgruppen deaktiviert.

Um die Berücksichtigung von Groß- und Kleinschreibung zu aktivieren, führen Sie je nach Data-Warehouse-Typ die folgenden Schritte aus:

- Bereitgestellter Cluster – Um die Berücksichtigung von Groß- und Kleinschreibung in einem bereitgestellten Cluster zu aktivieren, erstellen Sie eine benutzerdefinierte Parametergruppe

mit aktiviertem `enable_case_sensitive_identifier`-Parameter. Ordnen Sie diese Parametergruppe dann dem Cluster zu. Anweisungen finden Sie unter Verwalten von Parametergruppen mit der Konsole oder Konfigurieren von Parameterwerten mit der AWS CLI.

> **Note**
>
> Denken Sie daran, den Cluster neu zu starten, nachdem Sie ihm die benutzerdefinierte Parametergruppe zugeordnet haben.

- Serverless-Arbeitsgruppe – Um die Berücksichtigung von Groß- und Kleinschreibung in einer Redshift-Serverless-Arbeitsgruppe zu aktivieren, müssen Sie die AWS CLI verwenden. Die Amazon-Redshift-Konsole unterstützt derzeit nicht das Ändern von Redshift-Serverless-Parameterwerten. Senden Sie die folgende Anfrage zur Aktualisierung der Arbeitsgruppe:

```
aws redshift-serverless update-workgroup \
  --workgroup-name target-workgroup \
  --config-parameters
 parameterKey=enable_case_sensitive_identifier,parameterValue=true
```

  Sie müssen eine Arbeitsgruppe nicht neu starten, nachdem Sie ihre Parameterwerte geändert haben.

Konfigurieren der Autorisierung für das Data Warehouse

Nachdem Sie ein Data Warehouse erstellt haben, müssen Sie den Aurora-DB-Cluster der als autorisierte Integrationsquelle konfigurieren. Anweisungen finden Sie unter Konfigurieren der Autorisierung für Ihr Amazon-Redshift-Data-Warehouse.

Richten Sie eine Integration mithilfe der AWS SDKs ein (nur Aurora MySQL)

Anstatt jede Ressource manuell einzurichten, können Sie das folgende Python-Skript ausführen, um die erforderlichen Ressourcen automatisch für Sie einzurichten. Das Codebeispiel verwendet den AWS SDK for Python (Boto3), um einen Aurora MySQL-Quell-DB-Cluster und ein Amazon Redshift Redshift-Ziel-Data Warehouse zu erstellen, jeweils mit den erforderlichen Parameterwerten. Anschließend wird darauf gewartet, dass die Cluster verfügbar sind, bevor eine Zero-ETL-Integration zwischen ihnen erstellt wird. Je nachdem, welche Ressourcen Sie einrichten müssen, können Sie verschiedene Funktionen auskommentieren.

Führen Sie die folgenden Befehle aus, um die erforderlichen Abhängigkeiten zu installieren:

```
pip install boto3
pip install time
```

Innerhalb des Skripts können Sie optional die Namen der Quell-, Ziel- und Parametergruppen ändern. Die letzte Funktion erstellt eine Integration, die `my-integration` nach der Einrichtung der Ressourcen benannt ist.

Python-Codebeispiel

```
import boto3
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default Region.

rds = boto3.client('rds')
redshift = boto3.client('redshift')
sts = boto3.client('sts')

source_cluster_name = 'my-source-cluster' # A name for the source cluster
source_param_group_name = 'my-source-param-group' # A name for the source parameter
 group
target_cluster_name = 'my-target-cluster' # A name for the target cluster
target_param_group_name = 'my-target-param-group' # A name for the target parameter
 group

def create_source_cluster(*args):
    """Creates a source Aurora MySQL DB cluster"""

    response = rds.create_db_cluster_parameter_group(
        DBClusterParameterGroupName=source_param_group_name,
        DBParameterGroupFamily='aurora-mysql8.0',
        Description='For Aurora MySQL zero-ETL integrations'
    )
    print('Created source parameter group: ' + response['DBClusterParameterGroup']
['DBClusterParameterGroupName'])

    response = rds.modify_db_cluster_parameter_group(
        DBClusterParameterGroupName=source_param_group_name,
        Parameters=[
```

```
            {
                'ParameterName': 'aurora_enhanced_binlog',
                'ParameterValue': '1',
                'ApplyMethod': 'pending-reboot'
            },
            {
                'ParameterName': 'binlog_backup',
                'ParameterValue': '0',
                'ApplyMethod': 'pending-reboot'
            },
            {
                'ParameterName': 'binlog_format',
                'ParameterValue': 'ROW',
                'ApplyMethod': 'pending-reboot'
            },
            {
                'ParameterName': 'binlog_replication_globaldb',
                'ParameterValue': '0',
                'ApplyMethod': 'pending-reboot'
            },
            {
                'ParameterName': 'binlog_row_image',
                'ParameterValue': 'full',
                'ApplyMethod': 'pending-reboot'
            },
            {
                'ParameterName': 'binlog_row_metadata',
                'ParameterValue': 'full',
                'ApplyMethod': 'pending-reboot'
            }
        ]
    )
    print('Modified source parameter group: ' +
response['DBClusterParameterGroupName'])

    response = rds.create_db_cluster(
        DBClusterIdentifier=source_cluster_name,
        DBClusterParameterGroupName=source_param_group_name,
        Engine='aurora-mysql',
        EngineVersion='8.0.mysql_aurora.3.05.2',
        DatabaseName='myauroradb',
        MasterUsername='username',
        MasterUserPassword='Password01**'
    )
```

```
    print('Creating source cluster: ' + response['DBCluster']['DBClusterIdentifier'])
    source_arn = (response['DBCluster']['DBClusterArn'])
    create_target_cluster(target_cluster_name, source_arn, target_param_group_name)

    response = rds.create_db_instance(
        DBInstanceClass='db.r6g.2xlarge',
        DBClusterIdentifier=source_cluster_name,
        DBInstanceIdentifier=source_cluster_name + '-instance',
        Engine='aurora-mysql'
    )
    return(response)

def create_target_cluster(target_cluster_name, source_arn, target_param_group_name):
    """Creates a target Redshift cluster"""

    response = redshift.create_cluster_parameter_group(
        ParameterGroupName=target_param_group_name,
        ParameterGroupFamily='redshift-1.0',
        Description='For Aurora MySQL zero-ETL integrations'
    )
    print('Created target parameter group: ' + response['ClusterParameterGroup']
['ParameterGroupName'])

    response = redshift.modify_cluster_parameter_group(
        ParameterGroupName=target_param_group_name,
        Parameters=[
            {
                'ParameterName': 'enable_case_sensitive_identifier',
                'ParameterValue': 'true'
            }
        ]
    )
    print('Modified target parameter group: ' + response['ParameterGroupName'])

    response = redshift.create_cluster(
        ClusterIdentifier=target_cluster_name,
        NodeType='ra3.4xlarge',
        NumberOfNodes=2,
        Encrypted=True,
        MasterUsername='username',
        MasterUserPassword='Password01**',
        ClusterParameterGroupName=target_param_group_name
    )
    print('Creating target cluster: ' + response['Cluster']['ClusterIdentifier'])
```

```
    # Retrieve the target cluster ARN
    response = redshift.describe_clusters(
        ClusterIdentifier=target_cluster_name
    )
    target_arn = response['Clusters'][0]['ClusterNamespaceArn']

    # Retrieve the current user's account ID
    response = sts.get_caller_identity()
    account_id = response['Account']

    # Create a resource policy specifying cluster ARN and account ID
    response = redshift.put_resource_policy(
        ResourceArn=target_arn,
        Policy='''
        {
            \"Version\":\"2012-10-17\",
            \"Statement\":[
                {\"Effect\":\"Allow\",
                \"Principal\":{
                    \"Service\":\"redshift.amazonaws.com\"
                },
                \"Action\":[\"redshift:AuthorizeInboundIntegration\"],
                \"Condition\":{
                    \"StringEquals\":{
                        \"aws:SourceArn\":\"%s\"}
                    }
                },
                {\"Effect\":\"Allow\",
                \"Principal\":{
                    \"AWS\":\"arn:aws:iam::%s:root\"},
                \"Action\":\"redshift:CreateInboundIntegration\"}
            ]
        }
        ''' % (source_arn, account_id)
    )
    return(response)

def wait_for_cluster_availability(*args):
    """Waits for both clusters to be available"""

    print('Waiting for clusters to be available...')

    response = rds.describe_db_clusters(
```

```
        DBClusterIdentifier=source_cluster_name
    )
    source_status = response['DBClusters'][0]['Status']
    source_arn = response['DBClusters'][0]['DBClusterArn']

    response = rds.describe_db_instances(
        DBInstanceIdentifier=source_cluster_name + '-instance'
    )
    source_instance_status = response['DBInstances'][0]['DBInstanceStatus']

    response = redshift.describe_clusters(
        ClusterIdentifier=target_cluster_name
    )
    target_status = response['Clusters'][0]['ClusterStatus']
    target_arn = response['Clusters'][0]['ClusterNamespaceArn']

    # Every 60 seconds, check whether the clusters are available.
    if source_status != 'available' or target_status != 'available' or
 source_instance_status != 'available':
        time.sleep(60)
        response = wait_for_cluster_availability(
            source_cluster_name, target_cluster_name)
    else:
        print('Clusters available. Ready to create zero-ETL integration.')
        create_integration(source_arn, target_arn)
        return

def create_integration(source_arn, target_arn):
    """Creates a zero-ETL integration using the source and target clusters"""

    response = rds.create_integration(
        SourceArn=source_arn,
        TargetArn=target_arn,
        IntegrationName='my-integration'
    )
    print('Creating integration: ' + response['IntegrationName'])

def main():
    """main function"""
    create_source_cluster(source_cluster_name, source_param_group_name)
    wait_for_cluster_availability(source_cluster_name, target_cluster_name)

if __name__ == "__main__":
```

```
    main()
```

Nächste Schritte

Mit einem Aurora-DB-Cluster für die und einem Amazon Redshift Redshift-Ziel-Data Warehouse können Sie jetzt eine Zero-ETL-Integration erstellen und Daten replizieren. Detaillierte Anweisungen finden Sie unter the section called “Erstellen von Null-ETL-Integrationen”.

Erstellen von Null-ETL-Integrationen von Aurora mit Amazon Redshift

Wenn Sie eine Aurora Zero-ETL-Integration erstellen, geben Sie den Aurora-DB-Cluster der und das Amazon Redshift Redshift-Ziel-Data Warehouse an. Sie können auch die Verschlüsselungseinstellungen anpassen und Tags hinzufügen. Aurora erstellt eine Integration zwischen dem und seinem Ziel. Sobald die Integration aktiv ist, werden alle Daten, die Sie in den einfügen, in das konfigurierte Amazon Redshift Redshift-Ziel repliziert.

Themen

Voraussetzungen

Bevor Sie eine Zero-ETL-Integration erstellen, müssen Sie einen und ein Amazon Redshift Redshift-Ziel-Data Warehouse erstellen. Sie müssen auch die Replikation in das Data Warehouse zulassen, indem Sie den als autorisierte Integrationsquelle hinzufügen.

Anweisungen zum Ausführen der einzelnen Schritte finden Sie unter the section called “Erste Schritte mit Null-ETL-Integrationen”.

Erforderliche Berechtigungen

Bestimmte IAM-Berechtigungen sind erforderlich, um eine Null-ETL-Integration zu erstellen. Sie benötigen mindestens die Berechtigungen, um die folgenden Aktionen durchführen zu können:

- Erstellen Sie Zero-ETL-Integrationen für den Aurora DB-Cluster der .
- Anzeigen und Löschen aller Null-ETL-Integrationen.
- Erstellen eingehender Integrationen in das Ziel-Data-Warehouse. Sie können diese Berechtigung entfernen, wenn dasselbe Konto das Amazon Redshift Data Warehouse besitzt und dieses Konto ein autorisierter Prinzipal für dieses Data Warehouse ist. Informationen zum Hinzufügen von autorisierten Prinzipalen finden Sie unter Konfigurieren der Autorisierung für Ihr Amazon Redshift Data Warehouse.

Die folgende Beispielrichtlinie zeigt die Berechtigungen mit den geringsten Berechtigungen, die zum Erstellen und Verwalten von Integrationen erforderlich sind. Möglicherweise benötigen Sie genau diese Berechtigungen nicht, wenn Ihr Benutzer oder Ihre Rolle über umfassendere Berechtigungen verfügt, z. B. über eine `AdministratorAccess` verwaltete Richtlinie.

> **Note**
>
> Redshift-Amazon-Resourcennamen (ARNs) haben das folgende Format. Beachten Sie die Verwendung eines Schrägstrichs (`/`) anstelle eines Doppelpunkts (`:`) vor der Serverless-Namespace-UUID.
>
> - Bereitgestellter Cluster – `arn:aws:redshift:{region}:{account-id}:namespace:namespace-uuid`
> - Serverless – `arn:aws:redshift-serverless:{region}:{account-id}:namespace/namespace-uuid`

Musterrichtlinie

> **Important**
>
> Für die Aurora PostgreSQL-Vorschauversion wurden alle ARNs und Aktionen innerhalb der Amazon RDS Database Preview-Umgebung an den `-preview` Service-Namespace angehängt. Beispiel: `rds-preview:CreateIntegration` und `arn:aws:rds-preview:....`

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rds:CreateIntegration"
        ],
        "Resource": [
            "arn:aws:rds:{region}:{account-id}:cluster:source-db",
            "arn:aws:rds:{region}:{account-id}:integration:*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "rds:DescribeIntegrations"
        ],
        "Resource": ["*"]
    },
    {
        "Effect": "Allow",
        "Action": [
            "rds:DeleteIntegration",
            "rds:ModifyIntegration"
        ],
        "Resource": [
            "arn:aws:rds:{region}:{account-id}:integration:*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "redshift:CreateInboundIntegration"
        ],
        "Resource": [
            "arn:aws:redshift:{region}:{account-id}:namespace:namespace-uuid"
        ]
    }]
}
```

Auswählen eines Ziel-Data-Warehouse in einem anderen Konto

Wenn Sie ein Amazon Redshift Redshift-Ziel-Data Warehouse angeben möchten, das sich in einem anderen befindet AWS-Konto, müssen Sie eine Rolle erstellen, die es Benutzern des aktuellen

Kontos ermöglicht, auf Ressourcen im Zielkonto zuzugreifen. Weitere Informationen finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , dem Sie gehören.

Die Rolle muss über die folgenden Berechtigungen verfügen, die es dem Benutzer ermöglichen, verfügbare von Amazon Redshift bereitgestellte Cluster und Redshift-Serverless-Namespaces im Zielkonto einzusehen.

Erforderliche Berechtigungen und Vertrauensrichtlinie

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "redshift:DescribeClusters",
            "redshift-serverless:ListNamespaces"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Die Rolle muss über die folgende Vertrauensrichtlinie verfügen, die die Zielkonto-ID angibt.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS": "arn:aws:iam::{external-account-id}:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Anweisungen zum Erstellen der Rolle finden Sie unter Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien.

Erstellen von Null-ETL-Integrationen

Sie können und eine Aurora MySQL Zero-ETL-Integration mithilfe der AWS Management Console, der oder der AWS CLI RDS-API erstellen. Um eine Aurora PostgreSQL-Integration zu erstellen, müssen Sie die verwenden. AWS Management Console

RDS-Konsole

So erstellen Sie eine Null-ETL-Integration

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

   Wenn Sie einen Aurora PostgreSQL-DB-Cluster als Quelle der Integration verwenden, müssen Sie sich unter https://us-east-2.console.aws.amazon.com/rds-preview/home?region=us-east-2#databases bei der Amazon RDS Database Preview Environment anmelden.
2. Wählen Sie im linken Navigationsbereich Zero-ETL-Integrationen aus.
3. Wählen Sie Zero-ETL-Integration erstellen aus.
4. Geben Sie für Integrationskennung einen Namen für die Integration ein. Der Name kann bis zu 63 alphanumerische Zeichen umfassen und Bindestriche enthalten.
5. Wählen Sie Weiter.
6. Wählen Sie als Quelle den Aurora DB-Cluster der aus, aus dem die Daten stammen sollen. Auf dem muss oder Aurora PostgreSQL (kompatibel mit PostgreSQL 15.4 und Zero-ETL Support) ausgeführt werden.

   > **Note**
   >
   > Bei MySQL-Quellen benachrichtigt Sie RDS, wenn die DB-Cluster-Parameter nicht korrekt konfiguriert sind. Wenn Sie diese Nachricht erhalten, können Sie entweder Reparieren wählen oder eine manuelle Konfiguration vornehmen. Anweisungen zur manuellen Behebung finden Sie unter the section called “Schritt 1: Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe”.
   > Das Ändern der DB-Cluster-Parameter erfordert einen Neustart. Bevor Sie die Integration erstellen können, muss der Neustart abgeschlossen sein und die neuen Parameterwerte müssen erfolgreich auf den angewendet werden.
7. Wenn Sie einen Aurora PostgreSQL-Quellcluster ausgewählt haben, geben Sie unter Benannte Datenbank die benannte Datenbank an, die als Quelle für Ihre Integration verwendet werden soll.

Das PostgreSQL-Ressourcenmodell ermöglicht die Erstellung mehrerer Datenbanken innerhalb eines einzigen DB-Clusters, aber für jede Zero-ETL-Integration kann nur eine verwendet werden.

Die benannte Datenbank muss aus erstellt werden. `template1` Weitere Informationen finden Sie unter Template Databases in der PostgreSQL-Dokumentation.

8. (Optional) Wenn Sie einen Aurora MySQL-Quell-DB-Cluster ausgewählt haben, wählen Sie Datenfilteroptionen anpassen aus und fügen Sie Ihrer Integration Datenfilter hinzu. Sie können Datenfilter verwenden, um den Umfang der Replikation in das Ziel-Data Warehouse zu definieren. Weitere Informationen finden Sie unter the section called “Datenfilterung für Zero-ETL-Integrationen”.
9. Sobald Ihr erfolgreich konfiguriert wurde, wählen Sie Weiter.
10. Gehen Sie bei Ziel wie folgt vor:

    1. (Optional) Um ein anderes AWS-Konto für das Amazon Redshift Redshift-Ziel zu verwenden, wählen Sie Anderes Konto angeben aus. Geben Sie dann den Namen einer IAM-Rolle mit Berechtigungen zur Anzeige Ihrer Data Warehouses ein. Anweisungen zum Erstellen der IAM-Rolle finden Sie unter the section called “Auswählen eines Ziel-Data-Warehouse in einem anderen Konto”.
    2. Wählen Sie für Amazon Redshift Data Warehouse das Ziel für replizierte Daten aus dem aus. Sie können einen bereitgestellten Amazon-Redshift-Cluster oder einen Redshift-Serverless-Namespace als Ziel auswählen.

> **Note**
>
> RDS benachrichtigt Sie, wenn die Ressourcenrichtlinie oder die Einstellungen zur Berücksichtigung der Groß- und Kleinschreibung für das angegebene Data Warehouse nicht korrekt konfiguriert sind. Wenn Sie diese Nachricht erhalten, können Sie entweder Reparieren wählen oder eine manuelle Konfiguration vornehmen. Anweisungen zur manuellen Behebung finden Sie unter Aktivieren der Groß- und Kleinschreibung für Ihr Data Warehouse und Konfigurieren der Autorisierung für Ihr Data Warehouse im Amazon Redshift Management Guide.
> Das Ändern der Groß- und Kleinschreibung für einen bereitgestellten Redshift-Cluster erfordert einen Neustart. Bevor Sie die Integration erstellen können, muss der Neustart abgeschlossen und der neue Parameterwert erfolgreich auf den Cluster angewendet werden.

> Wenn sich Ihre gewählte Quelle und Ihr Ziel in verschiedenen AWS-Konten befinden, kann Amazon RDS diese Einstellungen nicht für Sie korrigieren. Sie müssen zu dem anderen Konto navigieren und diese manuell in Amazon Redshift korrigieren.

11. Sobald Ihr Ziel-Data Warehouse korrekt konfiguriert ist, wählen Sie Weiter.
12. (Optional) Fügen Sie unter Tags ein oder mehrere Tags zu der Integration hinzu. Weitere Informationen finden Sie unter the section called “Markieren von RDS-Ressourcen”.
13. Geben Sie für Verschlüsselung an, wie Ihre Integration verschlüsselt werden soll. Standardmäßig verschlüsselt RDS alle Integrationen mit einem. AWS-eigener Schlüssel Um stattdessen einen vom Kunden verwalteten Schlüssel auszuwählen, aktivieren Sie die Option Verschlüsselungseinstellungen anpassen und wählen Sie einen KMS-Schlüssel aus, der für die Verschlüsselung verwendet werden soll. Weitere Informationen finden Sie unter the section called “Verschlüsseln von Amazon Aurora-Ressourcen”.

> **Note**
>
> Wenn Sie einen benutzerdefinierten KMS-Schlüssel angeben, muss die Schlüsselrichtlinie die Aktion `kms:CreateGrant` für den Amazon-Redshift-Service-Prinzipal (`redshift.amazonaws.com`) zulassen. Weitere Informationen finden Sie unter Erstellen einer Schlüsselrichtlinie im AWS Key Management Service - Entwicklerhandbuch.

Fügen Sie optional einen Verschlüsselungskontext hinzu. Weitere Informationen finden Sie unter Verschlüsselungskontext im AWS Key Management Service -Entwicklerhandbuch.

14. Wählen Sie Weiter aus.
15. Überprüfen Sie Ihre Integrationseinstellungen und wählen Sie Null-ETL-Integration erstellen aus.

    Wenn die Erstellung fehlschlägt, finden Sie Informationen zur Fehlerbehebung unter the section called “Ich kann keine Null-ETL-Integration erstellen”.

Der Status der Integration lautet während der Erstellung `Creating`. Das Ziel-Data-Warehouse von Amazon Redshift hat den Status `Modifying`. Während dieser Zeit können Sie das Data Warehouse nicht abfragen und keine Konfigurationsänderungen daran vornehmen.

Wenn die Integration erfolgreich erstellt wurde, ändern sich sowohl der Status der Integration als auch der Status des Ziel-Data-Warehouse von Amazon Redshift in `Active`.

AWS CLI

> **Note**
>
> Während der Vorschauversion der Aurora PostgreSQL Zero-ETL-Integrationen können Sie Integrationen nur über die erstellen. AWS Management Console Sie können weder die AWS CLI Amazon RDS-API noch eines der SDKs verwenden.

Um eine Zero-ETL-Integration mit dem zu erstellen AWS CLI, verwenden Sie den Befehl create-integration mit den folgenden Optionen:

- `--integration-name` – Geben Sie einen Namen für die Integration an.
- `--source-arn`— Geben Sie den ARN des Aurora-DB-Clusters der an, der die Quelle für die Integration sein wird.
- `--target-arn` – Geben Sie den ARN des Amazon Redshift Data Warehouse an, das das Ziel für die Integration sein soll.

Example

Für LinuxmacOS, oderUnix:

```
aws rds create-integration \
    --integration-name my-integration \
    --source-arn arn:aws:rds:{region}:{account-id}:my-db \
    --target-arn arn:aws:redshift:{region}:{account-id}:namespace:namespace-uuid
```

Windows:

```
aws rds create-integration ^
    --integration-name my-integration ^
    --source-arn arn:aws:rds:{region}:{account-id}:my-db ^
    --target-arn arn:aws:redshift:{region}:{account-id}:namespace:namespace-uuid
```

RDS-API

> **Note**
>
> Während der Vorschauversion der Aurora PostgreSQL Zero-ETL-Integrationen können Sie Integrationen nur über die erstellen. AWS Management Console Sie können weder die AWS CLI Amazon RDS-API noch eines der SDKs verwenden.

Verwenden Sie die `CreateIntegration`-Operation mit den folgenden Parametern, um mithilfe der Amazon-RDS-API eine Null-ETL-Integration zu erstellen:

- `IntegrationName` – Geben Sie einen Namen für die Integration an.
- `SourceArn`— Geben Sie den ARN des an, der die Quelle für die Integration sein wird.
- `TargetArn` – Geben Sie den ARN des Amazon Redshift Data Warehouse an, das das Ziel für die Integration sein soll.

Nächste Schritte

Nachdem Sie erfolgreich eine Null-ETL-Integration erstellt haben, müssen Sie eine Zieldatenbank in Ihrem Amazon-Redshift-Zielcluster oder Ihrer Zielarbeitsgruppe erstellen. Anschließend können Sie damit beginnen, Daten zum Aurora-DB-Cluster der hinzuzufügen und sie in Amazon Redshift abzufragen. Anweisungen finden Sie unter Erstellen von Zieldatenbanken in Amazon Redshift.

Datenfilterung für Aurora Zero-ETL-Integrationen mit Amazon Redshift

Sie können Datenfilterung für Aurora Zero-ETL-Integrationen verwenden, um den Umfang der Replikation vom Aurora-DB-Cluster der Redshift Redshift-Ziel-Data Warehouse zu definieren. Anstatt alle Daten auf das Ziel zu replizieren, können Sie einen oder mehrere Filter definieren, die bestimmte Tabellen selektiv einbeziehen oder von der Replikation ausschließen. Für Zero-ETL-Integrationen ist nur das Filtern auf Datenbank- und Tabellenebene verfügbar. Sie können nicht nach Spalten oder Zeilen filtern.

Datenfilterung kann nützlich sein, wenn Sie:

- Wenn Sie bestimmte Tabellen aus zwei oder mehr verschiedenen verbinden, benötigen Sie keine vollständigen Daten aus einem der .
- Sparen Sie Kosten, indem Sie Analysen nur mit einer Teilmenge von Tabellen und nicht mit einer ganzen Flotte von Datenbanken durchführen.
- Filtern Sie vertrauliche Informationen wie Telefonnummern, Adressen oder Kreditkarteninformationen aus bestimmten Tabellen heraus.

Sie können Datenfilter zu einer Zero-ETL-Integration hinzufügen AWS Management Console, indem Sie die AWS Command Line Interface (AWS CLI) oder die Amazon RDS-API verwenden.

Wenn die Integration einen bereitgestellten Amazon Redshift Redshift-Cluster als Ziel hat, muss sich der Cluster auf Patch 180 oder höher befinden.

> **Note**
>
> Derzeit können Sie Datenfilterung nur für Integrationen durchführen, die Aurora MySQL-Quellen haben. Die Vorabversion der Aurora PostgreSQL Zero-ETL-Integrationen mit Amazon Redshift unterstützt keine Datenfilterung.

Themen

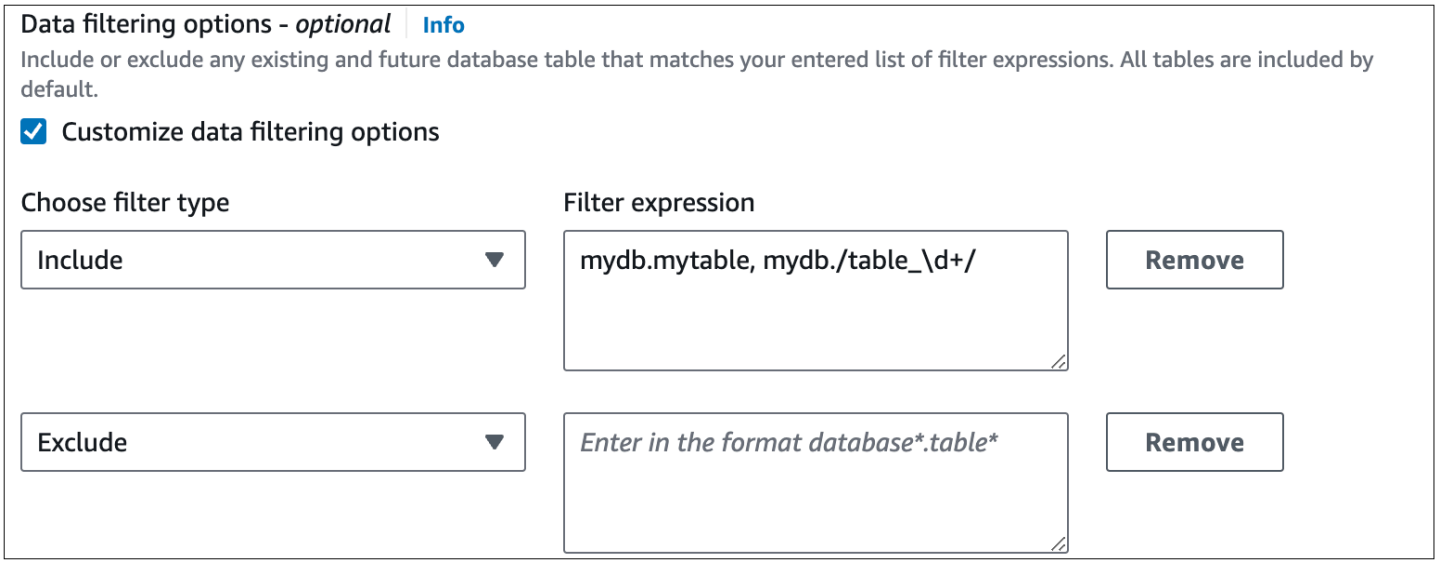
Format eines Datenfilters

Sie können mehrere Filter für eine einzelne Integration definieren. Jeder Filter schließt alle vorhandenen und future Datenbanktabellen ein oder schließt sie aus, die einem der Muster im Filterausdruck entsprechen. Aurora Zero-ETL-Integrationen verwenden die Maxwell-Filtersyntax für die Datenfilterung.

Jeder Filter hat die folgenden Elemente:

Element	Beschreibung
Typ des Filters	Ein `Include` Filtertyp umfasst alle Tabellen, die einem der Muster im Filterausdruck entsprechen. Ein `Exclude` Filtertyp schließt alle Tabellen aus, die einem der Muster entsprechen.
Filterausdruck	Eine durch Kommas getrennte Liste von Mustern. Ausdrücke müssen die Maxwell-Filtersyntax verwenden.
Muster	Ein Filtermuster im Format*`database`*`.`*`table`*. Sie können wörtliche Datenbank- und Tabellennamen (z. B.`mydb.mytable`) angeben oder Platzhalter (*) verwenden. Sie können auch reguläre Ausdrücke im Datenbank- und Tabellennamen definieren. Aurora unterstützt das Filtern nur auf Datenbank- und Tabellenebene. Sie können keine Filter auf Spaltenebene (`database.table.column`) oder Blacklists () einbeziehen. `blacklist: bad_db.*` Eine einzelne Integration kann insgesamt maximal 99 Muster haben. In der Konsole können Sie Muster in einem einzigen Filterausdruck enthalten oder sie auf mehrere Ausdrücke verteilen. Ein einzelnes Muster darf nicht länger als 256 Zeichen sein.

Die folgende Abbildung zeigt die Struktur der Datenfilter in der Konsole:



> **Important**
>
> Nehmen Sie keine personenbezogenen, vertraulichen oder sensiblen Informationen in Ihre Filtermuster auf.

Datenfilter im AWS CLI

Wenn Sie den verwenden AWS CLI , um einen Datenfilter hinzuzufügen, unterscheidet sich die Syntax geringfügig von der der Konsole. Jedes einzelne Muster muss einem eigenen Filtertyp (`Include`oder`Exclude`) zugeordnet werden. Sie können nicht mehrere Muster mit einem einzigen Filtertyp gruppieren.

In der Konsole können Sie beispielsweise die folgenden durch Kommas getrennten Muster in einer einzigen `Include` Anweisung gruppieren:

```
mydb.mytable, mydb./table_\d+/
```

Wenn Sie den verwenden AWS CLI, muss derselbe Datenfilter jedoch das folgende Format haben:

```
'include: mydb.mytable, include: mydb./table_\d+/'
```

Filterlogik

Wenn Sie in Ihrer Integration keine Datenfilter angeben, geht Aurora von einem Standardfilter für aus `include:*.*` und repliziert alle Tabellen in das Ziel-Data Warehouse. Wenn Sie jedoch mindestens einen Filter angeben, beginnt die Logik mit einem angenommenen Wert`exclude:*.*`, was bedeutet, dass alle Tabellen automatisch von der Replikation ausgeschlossen werden. Auf diese Weise können Sie direkt definieren, welche Tabellen und Datenbanken eingeschlossen werden sollen.

Wenn Sie beispielsweise den folgenden Filter definieren:

```
'include: db.table1, include: db.table2'
```

Aurora bewertet den Filter wie folgt:

```
'exclude:*.*, include: db.table1, include: db.table2'
```

Daher db werden nur `table1` und `table2` aus der genannten Datenbank in das Ziel-Data Warehouse repliziert.

Priorität filtern

Aurora wertet Datenfilter in der Reihenfolge aus, in der sie angegeben sind. In der bedeutet dies AWS Management Console, dass Aurora Filterausdrücke von links nach rechts und von oben nach unten auswertet. Wenn Sie ein bestimmtes Muster für den ersten Filter angeben, kann ein zweiter Filter oder sogar ein einzelnes Muster, das unmittelbar danach angegeben wird, dieses überschreiben.

Dies könnte beispielsweise Ihr erster Filter sein `Includebooks.stephenking`, der eine einzelne Tabelle enthält, die innerhalb `stephenking` der `books` Datenbank benannt wurde. Wenn Sie jedoch einen zweiten Filter von hinzufügen `Excludebooks.*`, überschreibt dieser den zuvor definierten `Include` Filter. Somit werden keine Tabellen aus dem `books` Index nach Amazon Redshift repliziert.

Wenn Sie mindestens einen Filter angeben, beginnt die Logik mit einem angenommenen Wert`exclude:*.*`, was bedeutet, dass alle Tabellen automatisch von der Replikation ausgeschlossen werden. Es hat sich daher bewährt, Ihre Filter vom breitesten bis zum am wenigsten breiten Filter zu definieren. Verwenden Sie beispielsweise eine oder mehrere `Include`

Anweisungen, um alle Daten zu definieren, die Sie replizieren möchten. Beginnen Sie dann mit dem Hinzufügen von `Exclude` Filtern, um bestimmte Tabellen selektiv von der Replikation auszuschließen.

Das gleiche Prinzip gilt für Filter, die Sie mit dem definieren. AWS CLI Aurora wertet diese Filtermuster in der Reihenfolge aus, in der sie angegeben wurden, sodass ein Muster eines zuvor angegebenen überschreiben kann.

Beispiele

Die folgenden Beispiele zeigen, wie Datenfilterung für Zero-ETL-Integrationen funktioniert:

- Schließt alle Datenbanken und alle Tabellen ein:

```
'include: *.*'
```

- Schließt alle Tabellen in die `books` Datenbank ein:

```
'include: books.*'
```

- Schließt alle Tabellen mit den folgenden Namen aus`mystery`:

```
'include: *.*, exclude: *.mystery'
```

- Schließt zwei spezifische Tabellen in die `books` Datenbank ein:

```
'include: books.stephen_king, include: books.carolyn_keene'
```

- Schließt alle Tabellen in die `books` Datenbank ein, außer denen, die die Teilzeichenfolge `mystery` enthalten:

```
'include: books.*, exclude: books./.*mystery.*/
```

- Schließt alle Tabellen in die `books` Datenbank ein, außer denen, die beginnen mit`mystery`:

```
'include: books.*, exclude: books./mystery.*/'
```

- Schließt alle Tabellen in die `books` Datenbank ein, außer denen, die mit`mystery`: enden:

```
'include: books.*, exclude: books./.*mystery/'
```

- Schließt alle Tabellen in der `books` Datenbank ein, die mit beginnen`table_`, mit Ausnahme der benannten`table_stephen_king`. Zum Beispiel, `table_movies` oder `table_books` würde repliziert werden, aber nicht`table_stephen_king`.

```
'include: books./table_.*/, exclude: books.table_stephen_king'
```

Hinzufügen von Datenfiltern zu einer Integration

Sie können die Datenfilterung mithilfe der AWS Management Console AWS CLI, der oder der Amazon RDS-API konfigurieren.

> **Important**
>
> Wenn Sie nach dem Erstellen einer Integration einen Filter hinzufügen, bewertet Aurora den Filter neu, als ob er schon immer existiert hätte. Es entfernt alle Daten, die sich derzeit im Amazon Redshift Redshift-Ziel-Data Warehouse befinden und nicht den neuen Filterkriterien entsprechen. Diese Aktion bewirkt, dass alle betroffenen Tabellen erneut synchronisiert werden.

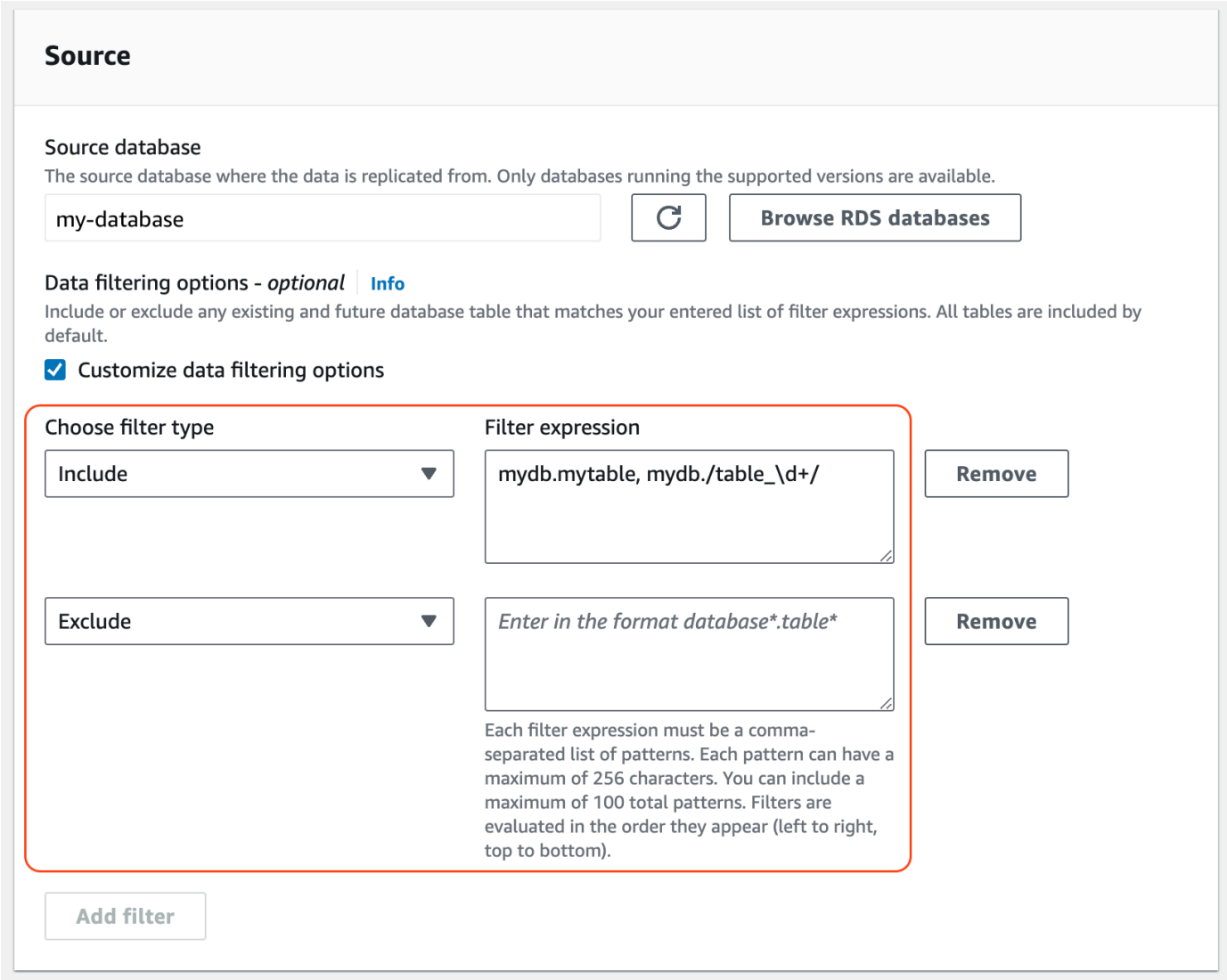
Derzeit können Sie nur Datenfilterung für Integrationen durchführen, die Aurora MySQL-Quellen haben. Die Vorabversion der Aurora PostgreSQL Zero-ETL-Integrationen mit Amazon Redshift unterstützt keine Datenfilterung.

RDS-Konsole

Um Datenfilter zu einer Zero-ETL-Integration hinzuzufügen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Zero-ETL-Integrationen aus. Wählen Sie die Integration aus, zu der Sie Datenfilter hinzufügen möchten, und klicken Sie dann auf Ändern.
3. Fügen Sie unter Quelle eine oder mehrere `Include` `Exclude` AND-Anweisungen hinzu.

   Die folgende Abbildung zeigt ein Beispiel für Datenfilter für eine Integration:



4. Wenn alle Änderungen Ihren Wünschen entsprechen, wählen Sie Weiter und Änderungen speichern.

AWS CLI

Um einer Zero-ETL-Integration mithilfe von Datenfilter hinzuzufügen AWS CLI, rufen Sie den Befehl modify-integration auf. Geben Sie den `--data-filter` Parameter zusätzlich zur Integrations-ID mit einer kommagetrennten Liste von und Maxwell-Filtern an. `Include` `Exclude`

Example

Im folgenden Beispiel werden Filtermuster zu hinzugefügt. `my-integration`

Für LinuxmacOS, oderUnix:

```
aws rds modify-integration \
    --integration-identifier my-integration \
    --data-filter 'include: foodb.*, exclude: foodb.tbl, exclude: foodb./table_\d+/'
```

Windows:

```
aws rds modify-integration ^
    --integration-identifier my-integration ^
    --data-filter 'include: foodb.*, exclude: foodb.tbl, exclude: foodb./table_\d+/'
```

RDS-API

Um eine Zero-ETL-Integration mithilfe der RDS-API zu ändern, rufen Sie den Vorgang auf ModifyIntegration. Geben Sie die Integrations-ID an und stellen Sie eine durch Kommas getrennte Liste von Filtermustern bereit.

Datenfilter aus einer Integration entfernen

Wenn Sie einen Datenfilter aus einer Integration entfernen, bewertet Aurora die verbleibenden Filter neu, als ob der entfernte Filter nie existiert hätte. Aurora repliziert dann alle Daten, die zuvor nicht den Filterkriterien entsprachen (dies aber jetzt tun), in das Amazon Redshift Redshift-Ziel-Data Warehouse.

Durch das Entfernen eines oder mehrerer Datenfilter werden alle betroffenen Tabellen erneut synchronisiert.

Hinzufügen von Daten zu einem Aurora-DB-Cluster einer und deren Abfrage in Amazon Redshift

Zum Erstellen einer Null-ETL-Integration, die Daten von Amazon Aurora in Amazon Redshift repliziert, müssen Sie eine Zieldatenbank in Amazon Redshift erstellen.

Stellen Sie zunächst eine Verbindung mit Ihrem Amazon-Redshift-Cluster oder Ihrer Arbeitsgruppe her und erstellen Sie eine Datenbank mit einem Verweis auf Ihre Integrations-ID. Anschließend können Sie Daten zu Ihrem Aurora-DB-Cluster für die hinzufügen und sehen, wie sie in Amazon Redshift repliziert werden.

Themen

Erstellen einer Zieldatenbank in Amazon Redshift

Bevor Sie mit der Replikation von Daten in Amazon Redshift beginnen können, müssen Sie in Ihrem Ziel-Data-Warehouse eine Zieldatenbank erstellen. Diese Zieldatenbank muss einen Verweis auf die Integrations-ID enthalten. Sie können die Amazon-Redshift-Konsole oder Query Editor v2 verwenden, um die Datenbank zu erstellen.

Anweisungen zum Erstellen einer Zieldatenbank finden Sie unter Erstellen einer Zieldatenbank in Amazon Redshift.

Daten zum hinzufügen

Nachdem Sie Ihre Integration konfiguriert haben, können Sie dem Aurora DB-Cluster der einige Daten hinzufügen, die Sie in Ihr Amazon Redshift Data Warehouse replizieren möchten.

> **Note**
>
> Es gibt Unterschiede zwischen den Datentypen in Amazon Aurora und Amazon Redshift. Eine Tabelle mit Datentypzuordnungen finden Sie unter the section called “Datentypunterschiede”.

Stellen Sie zunächst mit dem MySQL - oder PostgreSQL-Client Ihrer Wahl eine Verbindung zum her. Anweisungen finden Sie unter the section called “Herstellen einer Verbindung mit einem DB-Cluster”.

Erstellen Sie dann eine Tabelle und fügen Sie eine Zeile mit Beispieldaten ein.

> **Important**
>
> Stellen Sie sicher, dass die Tabelle über einen Primärschlüssel verfügt. Andernfalls kann sie nicht in das Ziel-Data-Warehouse repliziert werden.

Die PostgreSQL-Dienstprogramme pg_dump und pg_restore erstellen zunächst Tabellen ohne Primärschlüssel und fügen ihn anschließend hinzu. Wenn Sie eines dieser Dienstprogramme verwenden, empfehlen wir, zuerst ein Schema zu erstellen und dann Daten in einem separaten Befehl zu laden.

MySQL

Im folgenden Beispiel wird das MySQL Workbench-Hilfsprogramm verwendet.

```
CREATE DATABASE my_db;

USE my_db;

CREATE TABLE books_table (ID int NOT NULL, Title VARCHAR(50) NOT NULL, Author
 VARCHAR(50) NOT NULL,
Copyright INT NOT NULL, Genre VARCHAR(50) NOT NULL, PRIMARY KEY (ID));

INSERT INTO books_table VALUES (1, 'The Shining', 'Stephen King', 1977, 'Supernatural
 fiction');
```

PostgreSQL

Das folgende Beispiel verwendet das interaktive psql PostgreSQL-Terminal. Wenn Sie eine Verbindung zum Cluster herstellen, schließen Sie die benannte Datenbank ein, die Sie bei der Erstellung der Integration angegeben haben.

```
psql -h mycluster.cluster-123456789012.us-east-2.rds.amazonaws.com -p 5432 -U username
 -d named_db;

named_db=> CREATE TABLE books_table (ID int NOT NULL, Title VARCHAR(50) NOT NULL,
 Author VARCHAR(50) NOT NULL,
Copyright INT NOT NULL, Genre VARCHAR(50) NOT NULL, PRIMARY KEY (ID));

named_db=> INSERT INTO books_table VALUES (1, "The Shining", "Stephen King", 1977,
 "Supernatural fiction");
```

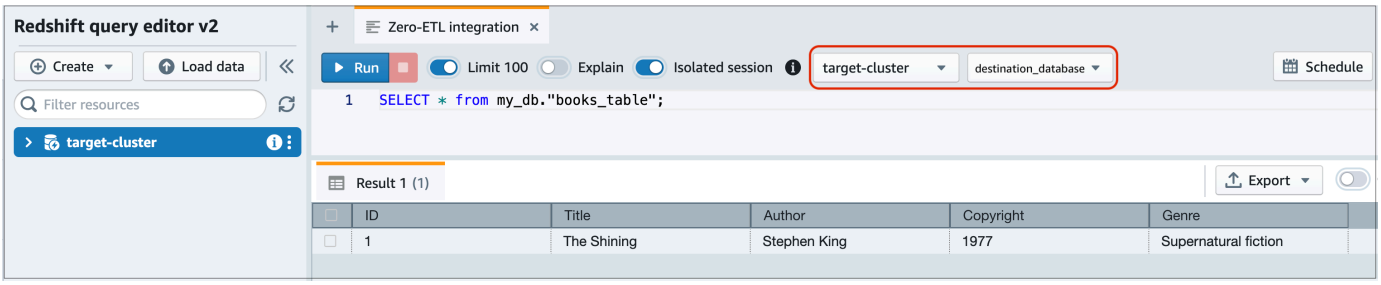
Abfragen Ihrer Aurora-Daten in Amazon Redshift

Nachdem Sie dem Aurora-DB-Cluster der Daten hinzugefügt haben, werden sie in Amazon Redshift repliziert und können abgefragt werden.

So fragen Sie die replizierten Daten ab

1. Navigieren Sie zur Amazon Redshift-Konsole und wählen Sie im linken Navigationsbereich die Option Query Editor v2 aus.
2. Stellen Sie eine Verbindung mit Ihrem Cluster oder Ihrer Arbeitsgruppe her und wählen Sie Ihre aus der Integration erstellte Datenbank im Drop-down-Menü aus (destination_database in diesem Beispiel). Anweisungen zum Erstellen einer Zieldatenbank finden Sie unter Erstellen einer Zieldatenbank in Amazon Redshift.
3. Verwenden Sie eine SELECT-Anweisung, um Ihre Daten abzufragen. In diesem Beispiel können Sie den folgenden Befehl ausführen, um alle Daten aus der Tabelle auszuwählen, die Sie im Aurora DB-Cluster der erstellt haben:

```
SELECT * from my_db."books_table";
```



- *my_db* ist der Name des Aurora-Datenbankschemas. Diese Option wird nur für MySQL-Datenbanken benötigt.
- *books_table* ist der Name der Aurora-Tabelle.

Sie können die Daten auch mit einem Befehlszeilenclient abfragen. Beispielsweise:

```
destination_database=# select * from my_db."books_table";

 ID |       Title |        Author |   Copyright |                 Genre |  txn_seq |
 txn_id
----+-------------+---------------+-------------+-----------------------+----------
+--------+
  1 | The Shining |  Stephen King |        1977 |   Supernatural fiction |        2 |
 12192
```

> **Note**
>
> Um zwischen Groß- und Kleinschreibung zu unterscheiden, verwenden Sie doppelte Anführungszeichen (" ") für Schema-, Tabellen- und Spaltennamen. Weitere Informationen finden Sie unter enable_case_sensitive_identifier.

Datentypunterschiede zwischen Aurora und Amazon Redshift-Datenbanken

Die folgende . Tabellen zeigen die Zuordnungen eines Aurora MySQL- oder Aurora PostgreSQL-Datentyps zu einem entsprechenden Amazon Redshift Redshift-Datentyp. Amazon Aurora unterstützt derzeit nur diese Datentypen für Zero-ETL-Integrationen.

Wenn eine Tabelle in Ihrem einen nicht unterstützten Datentyp enthält, ist die Tabelle nicht mehr synchron und kann vom Amazon Redshift Redshift-Ziel nicht verwendet werden. Das Streaming von der Quelle zum Ziel wird fortgesetzt, aber die Tabelle mit dem nicht unterstützten Datentyp ist nicht verfügbar. Um die Tabelle zu reparieren und sie in Amazon Redshift verfügbar zu machen, müssen Sie die grundlegende Änderung manuell rückgängig machen und dann die Integration aktualisieren, indem Sie `ALTER DATABASE...INTEGRATION REFRESH` ausführen.

Themen

- Aurora MySQL
- Aurora PostgreSQL

Aurora MySQL

Aurora-MySQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
INT	INTEGER	4-Byte-Ganzzahl mit Vorzeichen	
SMALLINT	SMALLINT	2-Byte-Ganzzahl mit Vorzeichen	
TINYINT	SMALLINT	2-Byte-Ganzzahl mit Vorzeichen	

Aurora-MySQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
MEDIUMINT	INTEGER	4-Byte-Ganzzahl mit Vorzeichen	
BIGINT	BIGINT	8-Byte-Ganzzahl mit Vorzeichen	
INT UNSIGNED	BIGINT	8-Byte-Ganzzahl mit Vorzeichen	
TINYINT UNSIGNED	SMALLINT	2-Byte-Ganzzahl mit Vorzeichen	
MEDIUMINT UNSIGNED	INTEGER	4-Byte-Ganzzahl mit Vorzeichen	
BIGINT UNSIGNED	DECIMAL(20,0)	Genauer Zahlenwert mit wählbarer Genauigkeit	
DEZIMAL (p, s) = NUMERISCH (p, s)	DECIMAL (p,s)	Genauer Zahlenwert mit wählbarer Genauigkeit	Eine Genauigkeit von mehr als 38 und eine Skalierung von mehr als 37 werden nicht unterstützt
DEZIMAL (p, s) OHNE VORZEICHEN = NUMERISCH (p, s) OHNE VORZEICHEN	DECIMAL (p,s)	Genauer Zahlenwert mit wählbarer Genauigkeit	Eine Genauigkeit von mehr als 38 und eine Skalierung von mehr als 37 werden nicht unterstützt

Aurora-MySQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
FLOAT4/REAL	REAL	Gleitkommazahl mit einfacher Genauigkeit	
FLOAT4/REAL UNSIGNED	REAL	Gleitkommazahl mit einfacher Genauigkeit	
DOUBLE/REAL/FLOAT8	DOUBLE PRECISION	Double (Gleitkommazahl mit doppelter Genauigkeit)	
DOUBLE/REAL/FLOAT8 UNSIGNED	DOUBLE PRECISION	Double (Gleitkommazahl mit doppelter Genauigkeit)	
BIT (n)	VARBYTE(8)	Binärwert mit variabler Länge	
BINARY(n)	VARBYTE (n)	Binärwert mit variabler Länge	
VARBINARY (n)	VARBYTE (n)	Binärwert mit variabler Länge	
CHAR(n)	VARCHAR (n)	Zeichenkettenwert mit variabler Länge	
VARCHAR (n)	VARCHAR (n)	Zeichenkettenwert mit variabler Länge	

Aurora-MySQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
TEXT	VARCHAR(65535)	Zeichenkettenwert variabler Länge bis zu 65535 Byte	
TINYTEXT	VARCHAR(255)	Zeichenkettenwert variabler Länge bis zu 255 Byte	
MEDIUMTEXT	VARCHAR(65535)	Zeichenkettenwert variabler Länge bis zu 65535 Byte	
LONGTEXT	VARCHAR(65535)	Zeichenkettenwert variabler Länge bis zu 65535 Byte	
ENUM	VARCHAR(1020)	Zeichenkettenwert variabler Länge bis zu 1020 Byte	
SET	VARCHAR(1020)	Zeichenkettenwert variabler Länge bis zu 1020 Byte	
DATUM	DATUM	Kalenderdatum (Jahr, Monat, Tag)	

Aurora-MySQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
DATETIME	TIMESTAMP (ZEITSTEMPEL)	Datum und Uhrzeit (ohne Zeitzone)	
TIMESTAMP(p)	TIMESTAMP (ZEITSTEMPEL)	Datum und Uhrzeit (ohne Zeitzone)	
TIME	VARCHAR(18)	Zeichenkettenwert variabler Länge bis zu 18 Byte	
JAHR	VARCHAR(4)	Zeichenkettenwert variabler Länge bis zu 4 Byte	
JSON	SUPER	Semistrukturierte Daten oder Dokumente als Werte	

Aurora PostgreSQL

Zero-ETL-Integrationen für Aurora PostgreSQL unterstützen keine benutzerdefinierten Datentypen oder Datentypen, die durch Erweiterungen erstellt wurden.

> **Important**
>
> Die Zero-ETL-Integrationen mit der Amazon Redshift Redshift-Funktion für Aurora PostgreSQL befinden sich in der Vorschauversion. Sowohl die Dokumentation als auch die Funktion können sich ändern. Sie können diese Funktion nur in Testumgebungen verwenden, nicht in Produktionsumgebungen. Weitere Informationen zu den Bedingungen

für Vorschauversionen finden Sie unter Betas und Vorversionen in den AWS - Servicebedingungen.

Aurora PostgreSQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
bigint	BIGINT	8-Byte-Ganzzahl mit Vorzeichen	
große Seriennummer	BIGINT	8-Byte-Ganzzahl mit Vorzeichen	
Bit (n)	VARBYTE (n)	Binärwert mit variabler Länge	
etwas variierend (n)	VARBYTE (n)	Binärwert mit variabler Länge	
Bit	VARBYTE (1024000)	Zeichenkettenwert variabler Länge bis zu 1.024.000 Byte	
boolesch	BOOLEAN	Logischer boolescher Wert (wahr/falsch)	
bytea	VARBYTE (1024000)	Zeichenkettenwert variabler Länge bis zu 1.024.000 Byte	
Zeichen (n)	CHAR(n)	Zeichenfolge mit fester Länge	

Aurora PostgreSQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
Zeichen variierend (n)	VARCHAR(65535)	Zeichenkettenwert mit variabler Länge	
date	DATUM	Kalenderdatum (Jahr, Monat, Tag)	• Werte größer als werden `9999-12-31` nicht unterstützt • B.C.-Werte werden nicht unterstützt
double precision	DOUBLE PRECISION	Gleitkommazahlen mit doppelter Genauigkeit	Subnormale Werte werden nicht unterstützt
Ganzzahl	INTEGER	4-Byte-Ganzzahl mit Vorzeichen	
money	DEZIMAL (20,3)	Betrag in der Währung	

Aurora PostgreSQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
numeric(p,s)	DECIMAL (p,s)	Zeichenkettenwert mit variabler Länge	• `NaN`Werte werden nicht unterstützt • Eine Genauigkeit von mehr als 38 und eine Skalierung von mehr als 37 werden nicht unterstützt • Negative Skala wird nicht unterstützt
real	REAL	Gleitkommazahl mit einfacher Genauigkeit	
smallint	SMALLINT	2-Byte-Ganzzahl mit Vorzeichen	
kleine Seriennummer	SMALLINT	2-Byte-Ganzzahl mit Vorzeichen	
serial	INTEGER	4-Byte-Ganzzahl mit Vorzeichen	
text	VARCHAR(65535)	Zeichenkettenwert mit variabler Länge bis zu 65.535 Byte	

Aurora PostgreSQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
Zeit [(p)] [ohne Zeitzone]	VARCHAR (19)	Zeichenkettenwert variabler Länge bis zu 19 Byte	`Infinity`und `-Infinity` Werte werden nicht unterstützt
Zeit [(p)] mit Zeitzone	VARCHAR (22)	Zeichenkettenwert variabler Länge bis zu 22 Byte	• `Infinity`und `-Infinity` Werte werden nicht unterstützt
Zeitstempel [(p)] [ohne Zeitzone]	TIMESTAMP (ZEITSTEMPEL)	Datum und Uhrzeit (ohne Zeitzone)	• `Infinity`und `-Infinity` Werte werden nicht unterstützt • Werte, die größer als `9999-12-31` nicht unterstützt sind • B.C.-Werte werden nicht unterstützt

Aurora PostgreSQL-Datentyp	Amazon-Redshift-Datentyp	Beschreibung	Einschränkungen
Zeitstempel [(p)] mit Zeitzone	TIMESTAMPTZ	Datum und Uhrzeit (mit Zeitzone)	• `Infinity` und `-Infinity` Werte werden nicht unterstützt • Werte, die größer als `9999-12-31` nicht unterstützt sind • B.C.-Werte werden nicht unterstützt

Anzeigen und Überwachen von Null-ETL-Integrationen von Aurora mit Amazon Redshift

Sie können die Details einer Null-ETL-Integration von Amazon Aurora anzeigen, um die zugehörigen Konfigurationsinformationen und den aktuellen Status einzusehen. Sie können außerdem den Status Ihrer Integration überwachen, indem Sie bestimmte Systemansichten in Amazon Redshift abfragen. Darüber hinaus veröffentlicht Amazon Redshift bestimmte integrationsbezogene Metriken auf Amazon CloudWatch, die Sie in der Amazon Redshift Redshift-Konsole einsehen können.

Themen

- Anzeigen von Integrationen
- Überwachen von Integrationen mithilfe von Systemtabellen
- Überwachung von Integrationen mit Amazon EventBridge

Anzeigen von Integrationen

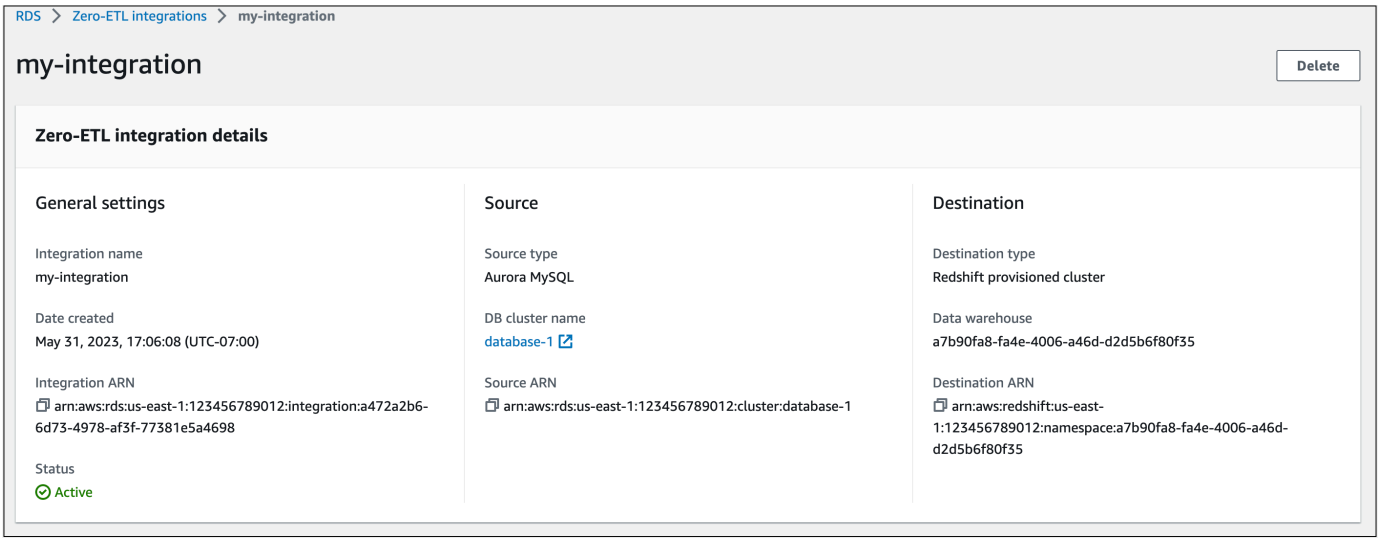
Sie können Aurora Zero-ETL-Integrationen mit Amazon Redshift mithilfe der AWS Management Console, der oder der RDS-API AWS CLI anzeigen.

Konsole

So zeigen Sie die Details einer Null-ETL-Integration an

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

   Wenn die Integration über einen Aurora PostgreSQL-Quell-DB-Cluster verfügt, müssen Sie sich unter https://us-east-2.console.aws.amazon.com/rds-preview/home?region=us-east-2#databases bei der Amazon RDS Database Preview Environment anmelden.
2. Wählen Sie im linken Navigationsbereich Null-ETL-Integrationen aus.
3. Wählen Sie eine Integration aus, um weitere Details zu ihr anzuzeigen, z. B. ihren und ihr Ziel-Data Warehouse.



Eine Integration kann folgende Status aufweisen:

- `Creating` – Die Integration wird erstellt.
- `Active` – Die Integration sendet Transaktionsdaten an das Ziel-Data-Warehouse.
- `Syncing` – Bei der Integration ist ein behebbarer Fehler aufgetreten und die Daten werden erneut gesendet. Betroffene Tabellen können in Amazon Redshift erst abgefragt werden, wenn die Neusynchronisierung abgeschlossen ist.

- `Needs attention` – Bei der Integration ist ein Ereignis oder ein Fehler aufgetreten, für dessen Behebung ein manuelles Eingreifen erforderlich ist. Befolgen Sie zur Behebung des Problems die Anweisungen in der Fehlermeldung auf der Seite mit den Integrationsdetails.
- `Failed` – Bei der Integration ist ein nicht behebbares Ereignis oder ein Fehler aufgetreten, der nicht behoben werden kann. Sie müssen die Integration löschen und erneut erstellen.
- `Deleting` – Die Integration wird gelöscht.

AWS CLI

Um alle Zero-ETL-Integrationen im aktuellen Konto mit dem anzuzeigen, verwenden Sie den Befehl describe-integrations und geben Sie die AWS CLI Option an. `--integration-identifier`

Example

LinuxmacOSUnixFür, oder:

```
aws rds describe-integrations \
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374
```

Windows:

```
aws rds describe-integrations ^
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374
```

RDS-API

Um die Null-ETL-Integration mithilfe der Amazon-RDS-API anzuzeigen, verwenden Sie die Operation `DescribeIntegrations` mit dem Parameter `IntegrationIdentifier`.

Überwachen von Integrationen mithilfe von Systemtabellen

Amazon Redshift verfügt über Systemtabellen und Ansichten, die Informationen zur Funktionsweise des Systems enthalten. Sie können diese Systemtabellen und Ansichten genauso abfragen wie andere Datenbanktabellen. Weitere Informationen zu Systemtabellen und Ansichten in Amazon Redshift finden Sie in der Referenz zu Systemtabellen im Datenbankentwicklerhandbuch zu Amazon Redshift.

Sie können die folgenden Systemansichten und Tabellen abfragen, um Informationen über Ihre Aurora Zero-ETL-Integrationen mit Amazon Redshift zu erhalten:

- SVV_INTEGRATION – Stellt Konfigurationsdetails für Ihre Integrationen bereit.
- SVV_INTEGRATION_TABLE_STATE – Beschreibt den Status jeder Tabelle innerhalb einer Integration.
- SYS_INTEGRATION_TABLE_STATE_CHANGE – Zeigt Protokolle zur Statusänderung von Tabellen für eine Integration an.
- SYS_INTEGRATION_ACTIVITY – Stellt Informationen zu abgeschlossenen Integrationsausführungen bereit.

Alle integrationsbezogenen CloudWatch Amazon-Metriken stammen von Amazon Redshift. Weitere Informationen finden Sie unter Überwachen von Null-ETL-Integrationen im Amazon-Redshift-Verwaltungshandbuch. Derzeit veröffentlicht Amazon Aurora keine Integrationsmetriken für CloudWatch.

Überwachung von Integrationen mit Amazon EventBridge

Amazon Redshift sendet integrationsbezogene Ereignisse an Amazon. EventBridge Eine Liste der Ereignisse und der entsprechenden Ereignis-IDs finden Sie unter Zero-ETL-Integrations-Ereignisbenachrichtigungen mit Amazon EventBridge im Amazon Redshift Management Guide.

Änderung der Aurora Zero-ETL-Integrationen mit Amazon Redshift

Sie können nur den Namen, die Beschreibung und die Datenfilteroptionen für eine Zero-ETL-Integration mit Amazon Redshift ändern. Sie können den AWS KMS Schlüssel, der zur Verschlüsselung der Integration verwendet wird, oder die Quell- oder Zieldatenbanken nicht ändern.

Wenn Sie einer vorhandenen Integration einen Datenfilter hinzufügen, bewertet Aurora den Filter neu, als ob er schon immer existiert hätte. Es entfernt alle Daten, die sich derzeit im Amazon Redshift Redshift-Ziel-Data Warehouse befinden und nicht den neuen Filterkriterien entsprechen. Wenn Sie einen Datenfilter aus einer Integration entfernen, repliziert er alle Daten, die zuvor nicht den Filterkriterien entsprachen (dies jetzt aber tun), in das Ziel-Data Warehouse. Weitere Informationen finden Sie unter the section called “Datenfilterung für Zero-ETL-Integrationen”.

Sie können eine Zero-ETL-Integration mithilfe der AWS Management Console, der oder der AWS CLI Amazon RDS-API ändern.

> **Note**
>
> Derzeit können Sie nur Integrationen ändern, die über Aurora MySQL-Quell-DB-Cluster verfügen. Das Ändern von Integrationen wird für die Vorabversion von Aurora PostgreSQL Zero-ETL-Integrationen mit Amazon Redshift nicht unterstützt.

RDS-Konsole

Um eine Zero-ETL-Integration zu ändern

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Zero-ETL-Integrationen und dann die Integration aus, die Sie ändern möchten.
3. Wählen Sie Ändern und nehmen Sie Änderungen an allen verfügbaren Einstellungen vor.
4. Wenn alle Änderungen Ihren Wünschen entsprechen, wählen Sie Ändern.

AWS CLI

Um eine Zero-ETL-Integration mit dem zu ändern AWS CLI, rufen Sie den Befehl modify-integration auf. Geben Sie zusammen mit dem eine der `--integration-identifier` folgenden Optionen an:

- `--integration-name`— Geben Sie einen neuen Namen für die Integration an.
- `--description`— Geben Sie eine neue Beschreibung für die Integration an.
- `--data-filter`— Geben Sie Datenfilteroptionen für die Integration an. Weitere Informationen finden Sie unter the section called “Datenfilterung für Zero-ETL-Integrationen”.

Example

Die folgende Anfrage ändert eine bestehende Integration.

Für LinuxmacOS, oderUnix:

```
aws rds modify-integration \
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374 \
```

```
    --integration-name my-renamed-integration
```

Windows:

```
aws rds modify-integration ^
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374 ^
    --integration-name my-renamed-integration
```

RDS-API

Um eine Zero-ETL-Integration mithilfe der RDS-API zu ändern, rufen Sie den Vorgang auf ModifyIntegration. Geben Sie die Integrations-ID und die Parameter an, die Sie ändern möchten.

Löschen von Null-ETL-Integrationen von Aurora mit Amazon Redshift

Wenn Sie eine Zero-ETL-Integration löschen, entfernt Aurora sie aus dem Aurora-DB-Cluster der . Ihre Transaktionsdaten werden nicht aus Amazon Aurora oder Amazon Redshift gelöscht, Aurora sendet jedoch keine neuen Daten an Amazon Redshift.

Sie können eine Integration nur löschen, wenn sie den Status`Active`, `FailedSyncing`, oder hat. `Needs attention`

Sie können Zero-ETL-Integrationen mithilfe der AWS Management Console, der oder der AWS CLI RDS-API löschen.

Konsole

So löschen Sie eine Null-ETL-Integration

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

   Wenn die Integration über einen Aurora PostgreSQL-Quell-DB-Cluster verfügt, müssen Sie sich unter https://us-east-2.console.aws.amazon.com/rds-preview/home?region=us-east-2#databases bei der Amazon RDS Database Preview Environment anmelden.
2. Wählen Sie im linken Navigationsbereich Null-ETL-Integrationen aus.
3. Wählen Sie die Null-ETL-Integration aus, die Sie löschen möchten.

4. Klicken Sie auf Aktionen, Löschen und bestätigen Sie den Löschvorgang.

AWS CLI

> **Note**
>
> Während der Vorschauversion der Aurora PostgreSQL Zero-ETL-Integrationen können Sie Integrationen nur über die löschen. AWS Management Console Sie können weder die AWS CLI Amazon RDS-API noch eines der SDKs verwenden.

Verwenden Sie zum Löschen einer Null-ETL-Integration den Befehl delete-integration und geben Sie die Option `--integration-identifier` an.

Example

Für LinuxmacOS, oderUnix:

```
aws rds delete-integration \
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374
```

Windows:

```
aws rds delete-integration ^
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374
```

RDS-API

> **Note**
>
> Während der Vorschauversion der Aurora PostgreSQL Zero-ETL-Integrationen können Sie Integrationen nur über die löschen. AWS Management Console Sie können weder die AWS CLI Amazon RDS-API noch eines der SDKs verwenden.

Verwenden Sie zum Löschen einer Null-ETL-Integration mithilfe der Amazon-RDS-API die Operation `DeleteIntegration` mit dem Parameter `IntegrationIdentifier`.

Fehlerbehebung bei Null-ETL-Integrationen von Aurora mit Amazon Redshift

Sie können den Status einer Null-ETL-Integration überprüfen, indem Sie die Systemtabelle SVV_INTEGRATION in Amazon Redshift abfragen. Wenn die Spalte `state` den Wert `ErrorState` aufweist, bedeutet das, dass ein Fehler vorliegt. Weitere Informationen finden Sie unter the section called “Überwachen mithilfe von Systemtabellen”.

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme bei Null-ETL-Integrationen von Aurora mit Amazon Redshift zu beheben.

Themen

- Ich kann keine Null-ETL-Integration erstellen
- Meine Integration steckt in einem Zustand von Syncing
- Meine Tabellen werden nicht auf Amazon Redshift repliziert
- Eine oder mehrere meiner Amazon-Redshift-Tabellen erfordern eine erneute Synchronisation

Ich kann keine Null-ETL-Integration erstellen

Wenn Sie keine Null-ETL-Integration erstellen können, stellen Sie Folgendes für Ihren DB-Quell-Cluster sicher:

- In Ihrem läuft , Aurora MySQL Version 3.05 (kompatibel mit MySQL 8.0.32) oder höher oder Aurora PostgreSQL (kompatibel mit PostgreSQL 15.4 und Zero-ETL Support).
- Sie haben die Parameter des DB-Clusters korrekt konfiguriert. Wenn die erforderlichen Parameter falsch festgelegt oder nicht mit dem Cluster verknüpft sind, schlägt die Erstellung fehl. Siehe the section called “Schritt 1: Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe”.

Stellen Sie außerdem Folgendes für Ihr Ziel-Data-Warehouse sicher:

- Die Unterscheidung zwischen Groß- und Kleinschreibung ist aktiviert. Siehe Aktivieren der Unterscheidung zwischen Groß- und Kleinschreibung für Ihr Data Warehouse.
- Sie haben den richtigen autorisierten Prinzipal und die richtige Integrationsquelle hinzugefügt. Weitere Informationen finden Sie unter Autorisierung für Ihr Amazon Redshift Data Warehouse konfigurieren.

- Das Data Warehouse ist verschlüsselt (wenn es sich um einen bereitgestellten Cluster handelt). Siehe Amazon Redshift Redshift-Datenbankverschlüsselung.

Meine Integration steckt in einem Zustand von `Syncing`

Ihre Integration zeigt möglicherweise durchgängig den Status an, `Syncing` wenn Sie den Wert eines der erforderlichen DB-Parameter ändern.

Um dieses Problem zu beheben, überprüfen Sie die Werte der Parameter in der Parametergruppe, die dem zugeordnet ist, und stellen Sie sicher, dass sie den erforderlichen Werten entsprechen. Weitere Informationen finden Sie unter the section called “Schritt 1: Erstellen einer benutzerdefinierten DB-Cluster-Parametergruppe”.

Wenn Sie Parameter ändern, stellen Sie sicher, dass Sie den neu starten, um die Änderungen zu übernehmen.

Meine Tabellen werden nicht auf Amazon Redshift repliziert

Ihre Daten werden möglicherweise nicht repliziert, weil eine oder mehrere Ihrer Quelltabellen keinen Primärschlüssel haben. Das Monitoring-Dashboard in Amazon Redshift zeigt den Status dieser Tabellen als an`Failed`, und der Status der gesamten Zero-ETL-Integration ändert sich auf. `Needs attention`

Um dieses Problem zu lösen, können Sie einen vorhandenen Schlüssel in Ihrer Tabelle identifizieren, der zu einem Primärschlüssel werden kann, oder Sie können einen synthetischen Primärschlüssel hinzufügen. Ausführliche Lösungen finden Sie unter Amazon Redshift. die folgenden Ressourcen:

- Behandeln Sie Tabellen ohne Primärschlüssel bei der Erstellung von Amazon Aurora MySQL- oder Amazon RDS for MySQL Zero-ETL-Integrationen mit Amazon Redshift
- Behandeln Sie Tabellen ohne Primärschlüssel bei der Erstellung von Amazon Aurora PostgreSQL Zero-ETL-Integrationen mit Amazon Redshift

Eine oder mehrere meiner Amazon-Redshift-Tabellen erfordern eine erneute Synchronisation

Wenn Sie bestimmte Befehle auf Ihrem DB-Quell-Cluster ausführen, müssen Ihre Tabellen möglicherweise erneut synchronisiert werden. In diesen Fällen zeigt die Systemansicht SVV_INTEGRATION_TABLE_STATE für `table_state` den Wert `ResyncRequired` an.

Dies bedeutet, dass die Integration die Daten für diese spezifische Tabelle vollständig neu von MySQL in Amazon Redshift laden muss.

Wenn die Tabelle mit der erneuten Synchronisation beginnt, wechselt sie in den Status `Syncing`. Sie müssen keine manuellen Maßnahmen ergreifen, um eine Tabelle erneut zu synchronisieren. Während die Tabellendaten erneut synchronisiert werden, können Sie in Amazon Redshift nicht darauf zugreifen.

Im Folgenden finden Sie einige Beispieloperationen, mit denen eine Tabelle in den Status `ResyncRequired` versetzt werden kann, sowie mögliche Alternativen, die Sie in Betracht ziehen sollten.

Operation	Beispiel	Alternative
Hinzufügen einer Spalte an einer bestimmten Position	`ALTER TABLE table_name ADD COLUMN column_name INTEGER NOT NULL first;`	Amazon Redshift unterstützt nicht das Hinzufügen von Spalten an bestimmten Positionen mithilfe der Schlüsselwörter `first` oder `af` Wenn die Reihenfolge der Spalten in der Zieltabelle nicht wichtig ist, fügen Sie die Spalte mit einem einfacheren Befehl am Ende der Tabelle hinzu:

Operation	Beispiel	Alternative
		`ALTER TABLE table_name ADD COLUMN column_name column_type ;`

Operation	Beispiel	Alternative
Hinzufügen einer Zeitstempelspalte mit dem Standardwert CURRENT_TIMESTAMP	`ALTER TABLE table_name ADD COLUMN column_name TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP;`	Der CURRENT_TIMESTAMP Wert für bestehende Tabellenzeilen wird von berechnet und kann in Amazon Redshift ohne vollständige Resynchronisierung der Tabellendaten nicht simuliert werden. Wenn möglich, ändern Sie den Standardwert in eine Literalkonstante wie 2023-01-01 00:00:15, um Latenzen bei der Tabellenv

Operation	Beispiel	Alternative
		erfügbarkeit zu vermeiden.
Ausführen mehrerer Spaltenoperationen innerhalb eines einzigen Befehls	`ALTER TABLE table_name ADD COLUMN column_1, RENAME COLUMN column_2 TO column_3;`	Überlegen Sie, ob Sie den Befehl in zwei separate Operationen, ADD und RENAME, aufteilen sollten, die keine erneute Synchronisation erfordern.

Verwenden von Aurora Serverless v2

Aurora Serverless v2 ist eine On-Demand-Konfiguration mit automatischer Skalierung für Amazon Aurora. Aurora Serverless v2 hilft dabei, die Prozesse zur Überwachung der Workload und zur Anpassung der Kapazität Ihrer Datenbanken zu automatisieren. Die Kapazität wird automatisch basierend auf dem Anwendungsbedarf angepasst. Berechnet werden Ihnen nur Ressourcen, die Ihre DB-Cluster verbrauchen. Daher kann Aurora Serverless v2 Ihnen helfen, innerhalb des Budgets zu bleiben und zu vermeiden, für Computerressourcen zu bezahlen, die Sie nicht verwenden.

Diese Art der Automatisierung ist besonders wertvoll für mehrmandantenfähige Datenbanken, verteilte Datenbanken, Entwicklungs- und Testsysteme sowie andere Umgebungen mit sehr variablen und unvorhersehbaren Workloads.

Themen

Anwendungsfälle für Aurora Serverless v2

Aurora Serverless v2 unterstützt viele verschiedene Datenbank-Workloads. Diese reichen von Entwicklungs- und Testumgebungen über Websites und Anwendungen mit unvorhersehbaren Workloads bis hin zu den anspruchsvollsten, geschäftskritischen Anwendungen, die eine hohe Skalierung und Verfügbarkeit erfordern.

Aurora Serverless v2 ist besonders nützlich für die folgenden Anwendungsfälle:

- Variable Workloads – Sie führen Workloads mit plötzlichen und unvorhersehbaren Aktivitätszuwächsen aus. Ein Beispiel dafür ist eine Verkehrs-Website, für die Aktivitätsspitzen entstehen, wenn es zu regnen beginnt. Eine andere ist eine E-Commerce-Website mit erhöhtem

Datenverkehr, wenn Sie Verkaufs- oder Sonderaktionen anbieten. Mit Aurora Serverless v2 wird Ihre Datenbank automatisch auf die Kapazität skaliert, mit der die Spitzenlast Ihrer Anwendung erfüllt werden kann, und wieder herunterskaliert, wenn die Aktivitätsspitze vorbei ist. Mit Aurora Serverless v2 müssen Sie nicht mehr Spitzen- oder durchschnittliche Kapazitäten bereitstellen. Sie können eine obere Kapazitätsgrenze angeben, um die schlimmste Situation zu bewältigen. Diese Kapazität wird nur genutzt, wenn sie benötigt wird.

Die Granularität der Skalierung in Aurora Serverless v2 hilft Ihnen, die Kapazität genau an die Anforderungen Ihrer Datenbank anzupassen. Für einen bereitgestellten Cluster erfordert die Hochskalierung das Hinzufügen einer ganz neuen DB-Instance. Für ein Aurora Serverless v1-Cluster erfordert die Hochskalierung eine Verdoppelung der Anzahl der Aurora-Kapazitätseinheiten (ACUs) für den Cluster, z. B. von 16 auf 32 oder 32 auf 64. Im Gegensatz dazu kann Aurora Serverless v2 eine halbe ACU hinzufügen, wenn nur ein wenig mehr Kapazität benötigt wird. Es kann 0,5, 1, 1,5, 2 oder zusätzliche halbe ACUs hinzufügen, basierend auf der zusätzlichen Kapazität, die für einen Anstieg der Workload erforderlich ist. Und es kann 0,5, 1, 1,5, 2 oder zusätzliche halbe ACUs entfernen, wenn die Workload abnimmt und diese Kapazität nicht mehr benötigt wird.

- Anwendungen für mehrere Mandanten – Mit Aurora Serverless v2 müssen Sie die Datenbankkapazität nicht für jede Anwendung in Ihrer Flotte einzeln verwalten. Aurora Serverless v2 verwaltet die individuelle Datenbankkapazität für Sie.

  Sie können einen Cluster für jeden Mandanten erstellen. Auf diese Weise können Sie Funktionen wie Klonen, Snapshot-Wiederherstellung und globale Aurora-Datenbanken verwenden, um die hohe Verfügbarkeit und Notfallwiederherstellung für jeden Mandanten zu verbessern.

  Jeder Mandant kann je nach Tageszeit, Jahreszeit, Werbeveranstaltungen usw. bestimmte Perioden mit hoher und geringer Aktivität haben. Jeder Cluster kann einen großen Kapazitätsbereich aufweisen. Auf diese Weise fallen für Cluster mit geringer Aktivität minimale DB-Instance-Gebühren an. Jeder Cluster kann schnell hochskaliert werden, um Perioden mit hoher Aktivität zu bewältigen.
- Neue Anwendungen – Sie stellen eine neue Anwendung bereit und sind sich nicht sicher, welche DB-Instance-Größe Sie benötigen. Durch die Verwendung von Aurora Serverless v2 können Sie einen Cluster mit einer oder mehreren DB-Instances einrichten und es der Datenbank überlassen, gemäß den Kapazitätsanforderungen Ihrer Anwendung automatisch zu skalieren.
- Anwendungen mit gemischter Verwendung – Angenommen, Sie haben eine Anwendung für die Online-Transaktionsverarbeitung (OLTP), erleben aber regelmäßig Spitzen im Abfrageverkehr. Durch Angabe von Hochstufungsstufen für die Aurora Serverless v2-DB-Instances in einem

Cluster können Sie Ihren Cluster so konfigurieren, dass die Reader-DB-Instances unabhängig von der Writer-DB-Instance skalieren können, um die zusätzliche Last zu bewältigen. Wenn die Nutzungsspitze nachlässt, skalieren die Reader-DB-Instances wieder herunter, um der Kapazität der Writer-DB-Instance zu entsprechen.

- Planung der Kapazität – Angenommen, Sie passen normalerweise Ihre Datenbankkapazität an oder überprüfen die optimale Datenbankkapazität für Ihre Workload, indem Sie die DB-Instance-Klassen aller DB-Instances in einem Cluster ändern. Mit Aurora Serverless v2 können Sie diesen Verwaltungsaufwand vermeiden. Sie können die entsprechende minimale und maximale Kapazität ermitteln, indem Sie die Workload ausführen und überprüfen, wie stark die DB-Instances tatsächlich skalieren.

  Sie können vorhandene DB-Instances von bereitgestellt in Aurora Serverless v2 oder von Aurora Serverless v2 in bereitgestellt ändern. In solchen Fällen müssen Sie keinen neuen Cluster und keine neue DB-Instance erstellen.

  Bei einer globalen Aurora-Datenbank benötigen Sie möglicherweise nicht so viel Kapazität für die sekundären Cluster wie im primären Cluster. Sie können Aurora Serverless v2-DB-Instances in den sekundären Clustern verwenden. Auf diese Weise kann die Cluster-Kapazität hochskalieren, wenn eine sekundäre Region hochgestuft wird und die Workload Ihrer Anwendung übernimmt.
- Entwicklung und Tests – Sie können nicht nur Ihre anspruchsvollsten Anwendungen ausführen, sondern Aurora Serverless v2 auch für Entwicklungs- und Testumgebungen verwenden. Mit Aurora Serverless v2 können Sie DB-Instances mit geringer Mindestkapazität erstellen, statt spitzenlastleistungsfähige db.t*-DB-Instance-Klassen zu verwenden. Sie können die maximale Kapazität so hoch einstellen, dass diese DB-Instances weiterhin erhebliche Workloads ausführen können, ohne dass der Speicher knapp wird. Wenn die Datenbank nicht verwendet wird, skalieren alle DB-Instances herunter, um unnötige Gebühren zu vermeiden.

  > **Tip**
  >
  > Um die Verwendung Aurora Serverless v2 in Entwicklungs- und Testumgebungen zu erleichtern, AWS Management Console bietet die die Verknüpfung Einfache Erstellung, wenn Sie einen neuen Cluster erstellen. Wenn Sie die Option Dev/Test (Entwicklung/Test) auswählen, erstellt Aurora einen Cluster mit einer Aurora Serverless v2-DB-Instance und einem Kapazitätsbereich, der für ein Entwicklungs- und Testsystem typisch ist.

Verwenden von Aurora Serverless v2 für vorhandene bereitgestellte Workloads

Angenommen, Sie haben bereits eine Aurora-Anwendung, die auf einem bereitgestellten Cluster ausgeführt wird. Sie können überprüfen, wie die Anwendung mit Aurora Serverless v2 funktionieren würde, indem Sie dem vorhandenen Cluster eine oder mehrere Aurora Serverless v2-DB-Instances als Reader-DB-Instances hinzufügen. Sie können überprüfen, wie oft die Reader-DB-Instances herauf- und herunterskalieren. Sie können den Aurora-Failover-Mechanismus verwenden, um eine Aurora Serverless v2-DB-Instance zum Writer hochzustufen, und überprüfen, wie sie die Lese-/Schreib-Workload bewältigt. Auf diese Weise können Sie mit minimalen Ausfallzeiten und ohne Ändern des Endpunkts, den Ihre Clientanwendungen verwenden, umstellen. Weitere Informationen zum Verfahren zum Konvertieren vorhandener Cluster in Aurora Serverless v2 finden Sie unter Migration zu Aurora Serverless v2.

Vorteile von Aurora Serverless v2

Aurora Serverless v2 ist für variable oder „Spitzen-“Workloads vorgesehen. Bei solch unvorhersehbaren Workloads haben Sie möglicherweise Schwierigkeiten zu planen, wann Ihre Datenbankkapazität geändert werden soll. Möglicherweise haben Sie auch Probleme, Kapazitätsänderungen schnell genug vorzunehmen, indem Sie die bekannten Mechanismen wie das Hinzufügen von DB-Instances oder das Ändern von DB-Instance-Klassen verwenden. Aurora Serverless v2 bietet die folgenden Vorteile zugunsten solcher Anwendungsfälle:

- Einfacheres Kapazitätsmanagement als bereitgestellt – Aurora Serverless v2 reduziert den Aufwand für die Planung von DB-Instance-Größen und die Größenänderung von DB-Instances, wenn sich die Workload ändert. Es reduziert auch den Aufwand, konsistente Kapazität für alle DB-Instances in einem Cluster aufrechtzuerhalten.
- Schnellere und einfachere Skalierung in Zeiten hoher Aktivität – Aurora Serverless v2 skaliert Rechen- und Speicherkapazität nach Bedarf, ohne dass die Client-Transaktionen oder Ihre gesamte Workload gestört werden. Die Möglichkeit, Reader-DB-Instances mit Aurora Serverless v2 zu verwenden, hilft Ihnen, zusätzlich zur vertikalen Skalierung die horizontale Skalierung zu nutzen. Die Möglichkeit, globale Aurora-Datenbanken zu verwenden, bedeutet, dass Sie Ihre Aurora Serverless v2-Lese-Workload über mehrere AWS-Regionen verteilen können. Diese Fähigkeit ist bequemer als die Skalierungsmechanismen für bereitgestellte Cluster. Sie ist auch schneller und stärker granular als die Skalierungsfunktionen in Aurora Serverless v1.

- Kostengünstig in Zeiten geringer Aktivität – Aurora Serverless v2 hilft Ihnen, eine Überbereitstellung Ihrer DB-Instances zu vermeiden. Aurora Serverless v2 fügt Ressourcen in granularen Schritten hinzu, wenn DB-Instances hochskalieren. Sie zahlen nur für die Datenbankressourcen, die Sie verbrauchen. Die Nutzung der Aurora Serverless v2-Ressourcen wird auf Sekundenbasis abgerechnet. Wenn eine DB-Instance herunterskaliert, wird so sofort die reduzierte Ressourcennutzung registriert.
- Größere Funktionsparität mit bereitgestellt – Sie können viele Aurora-Funktionen mit Aurora Serverless v2 verwenden, die für Aurora Serverless v1 nicht verfügbar sind. Mit können Aurora Serverless v2 Sie beispielsweise Reader-DB-Instances, globale Datenbanken, AWS Identity and Access Management (IAM)-Datenbankauthentifizierung und Performance Insights verwenden. Sie können auch viel mehr Konfigurationsparameter verwenden als mit Aurora Serverless v1.

  Mit Aurora Serverless v2 können Sie insbesondere die folgenden Funktionen aus bereitgestellten Clustern nutzen:

  - Reader-DB-Instances – Aurora Serverless v2 kann Reader-DB-Instances für die horizontale Skalierung nutzen. Wenn ein Cluster eine oder mehrere Reader-DB-Instances enthält, kann der Cluster bei Problemen mit der Writer-DB-Instance sofort ein Failover ausführen. Diese Fähigkeit ist mit Aurora Serverless v1 nicht verfügbar.
  - Multi-AZ-Cluster – Sie können die Aurora Serverless v2-DB-Instances eines Clusters auf mehrere Availability Zones (AZs) verteilen. Die Einrichtung eines Multi-AZ-Clusters trägt dazu bei, die Geschäftskontinuität auch in seltenen Fällen von Problemen sicherzustellen, die eine gesamte AZ betreffen. Diese Fähigkeit ist mit Aurora Serverless v1 nicht verfügbar.
  - Globale Datenbanken – Sie können Aurora Serverless v2 in Kombination mit globalen Aurora-Datenbanken verwenden, um zusätzliche schreibgeschützte Kopien Ihres Clusters in anderen AWS-Regionen für Notfallwiederherstellungszwecke zu erstellen.
  - RDS Proxy – Mit Amazon RDS Proxy können Sie Ihren Anwendungen erlauben, Datenbankverbindungen zu bündeln und gemeinsam zu nutzen, um ihre Skalierbarkeit zu verbessern.
- Schnellere, stärker granulare, weniger störende Skalierung als Aurora Serverless v1 – Aurora Serverless v2 kann schneller hoch- und herunterskalieren. Die Skalierung kann die Kapazität um nur 0,5 ACU ändern, anstatt die Anzahl der ACU zu verdoppeln oder zu halbieren. Die Skalierung erfolgt normalerweise ohne Unterbrechung der Verarbeitung. Die Skalierung umfasst im Gegensatz zu Aurora Serverless v1 kein Ereignis, das Sie beachten müssen. Die Skalierung kann erfolgen, während SQL-Anweisungen ausgeführt werden und Transaktionen geöffnet sind, ohne auf einen Ruhepunkt warten zu müssen.

Funktionsweise von Aurora Serverless v2

Die folgende Übersicht beschreibt die Funktionsweise von Aurora Serverless v2.

Themen

Übersicht über Aurora Serverless v2

Amazon Aurora Serverless v2 eignet sich für die anspruchsvollsten, sehr variablen Workloads. Zum Beispiel könnte Ihre Datenbanknutzung für einen kurzen Zeitraum sehr hoch sein, gefolgt von langen Zeiträumen mit nur leichter oder gar keiner Aktivität. Beispiele hierfür sind Einzelhandels-Websites, Spiele oder Sportveranstaltungen mit regelmäßigen Werbeveranstaltungen sowie Datenbanken, die nach Bedarf Berichte erstellen. Andere Beispiele sind Entwicklungs- und Testumgebungen sowie neue Anwendungen, in denen die Nutzung schnell ansteigen könnte. In Fällen wie diesen und vielen anderen ist es mit dem bereitgestellten Modell nicht immer möglich, die Kapazität vorab korrekt zu konfigurieren. Es können auch höhere Kosten entstehen, wenn Sie zu viel Kapazität bereitstellen, die Sie dann nicht benötigen.

Im Gegensatz dazu sind von Aurora bereitgestellte Cluster für stetige Workloads geeignet. Bei bereitgestellten Clustern wählen Sie eine DB-Instance-Klasse mit einer vordefinierten Menge an Speicher, CPU-Leistung, I/O-Bandbreite usw aus. Wenn sich Ihre Workload ändert, ändern Sie die Instance-Klasse Ihres Writers und Ihrer Readers manuell. Das bereitgestellte Modell funktioniert gut, wenn Sie die Kapazität im Vorfeld der erwarteten Verbrauchsmustern anpassen können. Es ist akzeptabel, dass kurze Ausfälle auftreten, während Sie die Instance-Klasse des Writers und der Reader in Ihrem Cluster ändern.

Aurora Serverless v2 ist von Grund auf so konzipiert, dass serverlose DB-Cluster unterstützt werden, die sofort skalierbar sind. Aurora Serverless v2 wurde entwickelt, um das gleiche Maß an Sicherheit und Isolation zu bieten wie mit bereitgestellten Writern und Readern. Diese Aspekte

sind in serverlosen Cloud-Umgebungen mit mehreren Mandanten entscheidend. Der dynamische Skalierungsmechanismus umfasst sehr wenig Aufwand, sodass er schnell auf Änderungen der Datenbank-Workload reagieren kann. Er bietet auch genügend Leistung, um einen drastischen Anstieg beim Bedarf nach Rechenleistung zu meistern.

Durch die Verwendung von Aurora Serverless v2 können Sie einen Aurora-DB-Cluster erstellen, ohne für jeden Writer und Reader an eine bestimmte Datenbankkapazität gebunden zu sein. Sie geben den minimalen und maximalen Bereich für die Kapazität an. Aurora skaliert jeden Aurora Serverless v2-Writer oder -Reader im Cluster innerhalb dieses Kapazitätsbereichs. Durch die Verwendung eines Multi-AZ-Clusters, in dem jeder Writer oder Reader dynamisch skalieren kann, können Sie die dynamische Skalierung und Hochverfügbarkeit nutzen.

Aurora Serverless v2 skaliert die Datenbankressourcen automatisch basierend auf Ihren minimalen und maximalen Kapazitätsspezifikationen. Die Skalierung ist schnell, da die meisten Skalierungsereignisoperationen den Writer oder Reader auf demselben Host halten. In seltenen Fällen, in denen ein Aurora Serverless v2-Writer oder -Reader von einem Host zu einem anderen verschoben wird, verwaltet Aurora Serverless v2 die Verbindungen automatisch. Sie müssen Ihren Datenbank-Client-Anwendungscode oder Ihre Datenbank-Verbindungszeichenfolgen nicht ändern.

Wie bei bereitgestellten Clustern sind bei Aurora Serverless v2 Speicherkapazität und Rechenkapazität getrennt. Wenn wir uns auf Aurora Serverless v2-Kapazität und -Skalierung beziehen, geht es immer um die Rechenkapazität, die zunimmt oder abnimmt. Somit kann Ihr Cluster viele Terabyte an Daten enthalten, auch wenn die CPU und Speicherkapazität auf ein niedriges Niveau herunterskalieren.

Anstelle der Bereitstellung und Verwaltung von Datenbankservern geben Sie die Datenbankkapazität an. Details zur Aurora Serverless v2-Kapazität finden Sie unter Kapazität von Aurora Serverless v2. Die tatsächliche Kapazität jedes Aurora Serverless v2-Writers oder -Readers variiert im Laufe der Zeit, je nach Workload. Details zu diesem Mechanismus finden Sie unter Aurora Serverless v2-Skalierung.

> **Important**
>
> Mit Aurora Serverless v1 verfügt Ihr Cluster über eine einzige Maßeinheit für die Rechenkapazität, die zwischen den minimalen und maximalen Kapazitätswerten skaliert werden kann. Mit Aurora Serverless v2 kann Ihr Cluster zusätzlich zum Writer auch Reader enthalten. Jeder Aurora Serverless v2-Writer und -Reader kann zwischen minimalen und maximalen Kapazitätswerten skalieren. Somit hängt die Gesamtkapazität Ihres Aurora Serverless v2-Clusters sowohl vom Kapazitätsbereich ab, den Sie für Ihren DB-Cluster

definieren, als auch von der Anzahl der Writer und Reader im Cluster. Zu jedem Zeitpunkt wird Ihnen nur die Aurora Serverless v2-Kapazität in Rechnung gestellt, die in Ihrem Aurora-DB-Cluster aktiv genutzt wird.

Konfigurationen für Aurora-DB-Cluster

Für jeden Ihrer Aurora DB-Cluster können Sie eine beliebige Kombination von Aurora Serverless v2-Kapazität, bereitgestellter Kapazität oder beides auswählen.

Sie können einen Cluster einrichten, der beides enthält, Aurora Serverless v2 und bereitgestellte Kapazität. Dies wird als Cluster mit gemischter Konfiguration bezeichnet. Nehmen Sie zum Beispiel an, dass Sie mehr Lese- und Schreibkapazität benötigen, als für einen Aurora Serverless v2-Writer verfügbar ist. In diesem Fall können Sie den Cluster mit einem sehr großen bereitgestellten Writer einrichten. Sie können in diesem Fall immer noch Aurora Serverless v2 für die Reader verwenden. Oder nehmen Sie an, dass die Schreib-Workload für Ihren Cluster variiert, die Lese-Workload jedoch stabil ist. In diesem Fall können Sie Ihren Cluster mit einem Aurora Serverless v2-Writer und einem oder mehreren bereitgestellten Readern einrichten.

Sie können auch einen DB-Cluster einrichten, bei dem die gesamte Kapazität von Aurora Serverless v2 verwaltet wird. Dazu können Sie einen neuen Cluster erstellen und von Anfang an Aurora Serverless v2 verwenden. Oder Sie können die gesamte bereitgestellte Kapazität in einem vorhandenen Cluster durch Aurora Serverless v2 ersetzen. Einige der Upgrade-Pfade älterer Engine-Versionen erfordern z. B., mit einem bereitgestellten Writer zu beginnen und ihn durch einen Aurora Serverless v2-Writer zu ersetzen. Informationen zu den Verfahren zum Erstellen eines neuen DB-Clusters mit Aurora Serverless v2 oder zum Wechseln eines vorhandenen DB-Cluster auf Aurora Serverless v2 finden Sie unter Erstellen eines Aurora Serverless v2-DB Clusters und Umstellung von einem bereitgestellten Cluster zu Aurora Serverless v2.

Wenn Sie Aurora Serverless v2 in einem DB-Cluster überhaupt nicht verwenden, sind alle Writer und Reader im DB-Cluster bereitgestellt. Dies ist die älteste und gebräuchlichste Art von DB-Cluster, mit der die meisten Benutzer vertraut sind. Vor Einführung von Aurora Serverless gab es tatsächlich keinen besonderen Namen für diese Art von Aurora-DB-Cluster. Die bereitgestellte Kapazität ist konstant. Die Gebühren sind relativ einfach zu prognostizieren. Sie müssen jedoch im Vorfeld prognostizieren, wie viel Kapazität Sie benötigen. In einigen Fällen sind Ihre Prognosen möglicherweise ungenau oder Ihr Kapazitätsbedarf kann sich ändern. In diesen Fällen kann Ihr DB-Cluster unterdimensioniert (langsamer als gewünscht) oder überdimensioniert (teurer als gewünscht) sein.

Kapazität von Aurora Serverless v2

Die Maßeinheit für Aurora Serverless v2 ist die Aurora-Kapazitätseinheit (ACU). Die Kapazität von Aurora Serverless v2 ist nicht an die DB-Instance-Klassen gebunden, die Sie für bereitgestellte Cluster verwenden.

Jede ACU ist eine Kombination aus etwa 2 Gibibyte (GiB) Arbeitsspeicher, entsprechender CPU und Netzwerkleistung. Mit dieser Maßeinheit geben Sie den Kapazitätsbereich der Datenbank an. Die Metriken `ServerlessDatabaseCapacity` und `ACUUtilization` helfen Ihnen festzustellen, wie viel Kapazität Ihre Datenbank tatsächlich nutzt und wo diese Kapazität innerhalb des angegebenen Bereichs liegt.

Zu jedem Zeitpunkt verfügt jeder Aurora Serverless v2-DB-Writer oder -Reader über eine Kapazität. Die Kapazität wird als Gleitkommazahl dargestellt, die ACUs repräsentiert. Die Kapazität steigt oder nimmt ab, sobald der Writer oder Reader skaliert. Dieser Wert wird jede Sekunde gemessen. Für jeden DB-Cluster, für den Sie Aurora Serverless v2 verwenden möchten, definieren Sie einen Kapazitätsbereich: Die minimalen und maximalen Kapazitätswerte, zwischen denen jeder Aurora Serverless v2-Writer oder -Reader skalieren kann. Der Kapazitätsbereich ist für jeden Aurora Serverless v2-Writer oder -Reader in einem DB-Cluster gleich. Jeder Aurora Serverless v2-Writer oder -Reader hat eine eigene Kapazität, die in diesen Bereich fällt.

Die größte Aurora Serverless v2-Kapazität, die Sie definieren können, beträgt 128 ACUs. Alle Überlegungen zur Auswahl des maximalen Kapazitätswerts finden Sie unter Auswählen der maximalen Aurora Serverless v2-Kapazitätseinstellung für einen Cluster.

Die geringste Aurora Serverless v2-Kapazität, die Sie definieren können, beträgt 0,5 ACU. Sie können eine größere Zahl angeben, wenn sie kleiner oder gleich Ihrem maximalen Kapazitätswert ist. Wenn Sie die Mindestkapazität auf eine kleine Zahl festlegen, können leicht geladene DB-Cluster minimale Rechenressourcen verbrauchen. Gleichzeitig bleiben sie bereit, Verbindungen sofort anzunehmen und hochzuskalieren, wenn ihre Aktivität ansteigt.

Wir empfehlen, das Minimum auf einen Wert festzulegen, der es jedem DB-Writer oder -Reader ermöglicht, den Arbeitssatz der Anwendung im Pufferpool zu halten. Auf diese Weise wird der Inhalt des Pufferpools in Zeiten geringer Aktivität nicht verworfen. Alle Überlegungen zur Auswahl des minimalen Kapazitätswerts finden Sie unter Auswählen der minimalen Aurora Serverless v2-Kapazitätseinstellung für einen Cluster.

Je nachdem, wie Sie die Reader in einem Multi-AZ-DB-Cluster konfigurieren, können ihre Kapazitäten an die Kapazität des Writers gebunden oder davon unabhängig sein. Weitere Informationen zur Vorgehensweise finden Sie unter Aurora Serverless v2-Skalierung.

Die Überwachung von Aurora Serverless v2 umfasst die Messung der Kapazitätswerte für den Writer und die Reader in Ihrem DB-Cluster im Zeitverlauf. Wenn Ihre Datenbank nicht auf die Mindestkapazität herunterskaliert, können Sie Maßnahmen ergreifen, z. B. den minimalen Wert anpassen und Ihre Datenbankanwendung optimieren. Wenn Ihre Datenbank ihre maximale Kapazität konsequent erreicht, können Sie Maßnahmen wie die Erhöhung des maximalen Werts ergreifen. Sie können auch Ihre Datenbankanwendung optimieren und die Abfragelast auf mehr Reader verteilen.

Die Gebühren für die Aurora Serverless v2-Kapazität werden in Form von ACU-Stunden gemessen. Informationen darüber, wie Aurora Serverless v2-Gebühren berechnet werden, finden Sie auf der Seite Aurora-Preisübersicht.

Angenommen, die Gesamtzahl der Writer und Reader in Ihrem Cluster ist N. In diesem Fall verbraucht der Cluster ungefähr *n* x *minimum ACUs*, wenn Sie keine Datenbankoperationen ausführen. Aurora selbst führt möglicherweise Überwachungs- oder Wartungsvorgänge durch, die eine geringe Last verursachen. Dieser Cluster verbraucht nicht mehr als *n* x *maximum ACUs*, wenn die Datenbank mit voller Kapazität läuft.

Weitere Informationen zur Auswahl geeigneter minimaler und maximaler ACU-Werte finden Sie unter Auswählen des Aurora Serverless v2-Kapazitätsbereichs für einen Aurora-Cluster. Die minimalen und maximalen ACU-Werte, die Sie angeben, wirken sich auch auf die Funktionsweise einiger Aurora-Konfigurationsparameter für Aurora Serverless v2 aus. Weitere Informationen zur Wechselwirkung zwischen dem Kapazitätsbereich und den Konfigurationsparametern finden Sie unter Arbeiten mit Parametergruppen für Aurora Serverless v2.

Aurora Serverless v2-Skalierung

Für jeden Aurora Serverless v2-Writer oder -Reader verfolgt Aurora kontinuierlich die Auslastung von Ressourcen wie CPU, Arbeitsspeicher und Netzwerk. Diese Messungen werden zusammen als Last bezeichnet. Die Last umfasst die von Ihrer Anwendung ausgeführten Datenbankoperationen. Außerdem umfasst sie auch die Hintergrundverarbeitung für den Datenbankserver und Aurora-Verwaltungsaufgaben. Wenn die Kapazität durch einen dieser Faktoren eingeschränkt wird, wird Aurora Serverless v2 hochskaliert. Aurora Serverless v2 skaliert auch hoch, wenn Leistungsprobleme erkannt werden, die dadurch gelöst werden können. Sie können die Ressourcenauslastung und deren Auswirkung auf die Aurora Serverless v2-Skalierung überwachen, indem Sie die Verfahren

in Wichtige CloudWatch Amazon-Metriken für Aurora Serverless v2 und Überwachung der Aurora Serverless v2-Leistung mit Performance Insights verwenden.

Die Last kann je nach Writer und Reader in Ihrem DB-Cluster variieren. Der Writer verarbeitet alle DDL-Anweisungen (Data Definition Language), wie `CREATE TABLE` ,`ALTER TABLE` und `DROP TABLE`. Außerdem verarbeitet der Writer alle DML-Anweisungen (Data Manipulation Language), wie `INSERT` und `UPDATE`. Reader können schreibgeschützte Anweisungen verarbeiten, z. B. `SELECT`-Abfragen.

Skalierung ist die Operation, die die Aurora Serverless v2-Kapazität für Ihre Datenbank erhöht oder senkt. Mit Aurora Serverless v2 verfügt jeder Writer und Reader über einen eigenen aktuellen Kapazitätswert, der in ACUs gemessen wird. Aurora Serverless v2 skaliert einen Writer oder Reader auf eine höhere Kapazität, wenn die aktuelle Kapazität zu niedrig ist, um die Last zu bewältigen. Der Writer oder Reader wird auf eine geringere Kapazität skaliert, wenn seine aktuelle Kapazität höher als erforderlich ist.

Im Gegensatz zu Aurora Serverless v1, bei der skaliert wird, indem die Kapazität bei jedem Erreichen eines Schwellenwerts verdoppelt wird, kann Aurora Serverless v2 die Kapazität inkrementell erhöhen. Wenn Ihr Workload-Bedarf die aktuelle Datenbankkapazität eines Writers oder Readers erreicht, erhöht Aurora Serverless v2 die Anzahl der ACUs für diesen Writer oder Reader. Aurora Serverless v2 skaliert die Kapazität in den inkrementellen Schritten, die erforderlich sind, um die beste Leistung für die genutzten Ressourcen zu bieten. Die Skalierung erfolgt in inkrementellen Schritten ab 0,5 ACU. Je größer die aktuelle Kapazität, desto größer ist das Skalierungsinkrement und desto schneller kann die Skalierung erfolgen.

Da die Aurora Serverless v2 Skalierung so häufig, granular und unterbrechungsfrei ist, verursacht sie keine diskreten Ereignisse in AWS Management Console der Art und Weise, wie dies Aurora Serverless v1 tut. Stattdessen können Sie die Amazon- CloudWatch Metriken wie `ServerlessDatabaseCapacity` und messen `ACUUtilization` und ihre Mindest-, Höchst- und Durchschnittswerte im Laufe der Zeit verfolgen. Weitere Informationen über Aurora-Metriken finden Sie unter Überwachung von Metriken in einem Amazon-Aurora-Cluster. Tipps zur Überwachung von Aurora Serverless v2 finden Sie unter Wichtige CloudWatch Amazon-Metriken für Aurora Serverless v2.

Sie können wählen, ob ein Reader gleichzeitig mit dem zugehörigen Writer oder unabhängig vom Writer skalieren soll. Dazu geben Sie die Hochstufungsstufe für diesen Reader an.

- Reader in den Hochstufungsstufen 0 und 1 skalieren gleichzeitig mit dem Writer. Dieses Skalierungsverhalten macht Reader in den Prioritätsstufen 0 und 1 ideal verfügbar. Das liegt daran,

dass sie immer auf die richtige Kapazität dimensioniert sind, um die Workload des Writers im Falle eines Failovers zu übernehmen.

- Reader der Hochstufungsstufen 2 bis 15 skalieren unabhängig vom Writer. Jeder Reader bleibt innerhalb der minimalen und maximalen ACU-Werte, die Sie für Ihren Cluster angegeben haben. Wenn ein Reader unabhängig von der zugehörigen Writer-DB skaliert, kann er inaktiv werden und herunterskalieren, während der Writer weiterhin ein hohes Transaktionsvolumen verarbeitet. Er ist nach wie vor als Failover-Ziel verfügbar, wenn keine anderen Reader in niedrigeren Hochstufungsstufen zur Verfügung stehen. Wenn der Reader jedoch zum Writer hochgestuft wird, muss er möglicherweise hochskalieren, um die volle Workload des Writers zu bewältigen.

Weitere Informationen zu Hochstufungsstufen finden Sie unter Auswählen der Hochstufungsstufe für einen Aurora Serverless v2-Reader.

Die Begriffe Skalierungpunkte und zugehörige Timeout-Perioden von Aurora Serverless v1 finden in Aurora Serverless v2 keine Anwendung. Die Aurora Serverless v2-Skalierung kann auftreten, während Datenbankverbindungen geöffnet sind, während SQL-Transaktionen in Bearbeitung sind, während Tabellen gesperrt sind und während temporäre Tabellen verwendet werden. Aurora Serverless v2 wartet nicht auf einen Ruhepunkt, um mit der Skalierung zu beginnen. Die Skalierung unterbricht keine laufenden Datenbankoperationen.

Wenn Ihre Workload mehr Lesekapazität benötigt, als mit einem einzigen Writer und einem einzigen Reader verfügbar ist, können Sie dem Cluster mehrere Aurora Serverless v2-Reader hinzufügen. Jeder Aurora Serverless v2-Reader kann innerhalb der minimalen und maximalen Kapazitätswerte skalieren, die Sie für Ihren DB-Cluster angegeben haben. Sie können den Reader-Endpunkt des Clusters verwenden, um schreibgeschützte Sitzungen an die Reader zu leiten und die Last des Writers zu reduzieren.

Ob Aurora Serverless v2 die Skalierung durchführt und wie schnell die Skalierung nach dem Start erfolgt, hängt auch von den minimalen und maximalen ACU-Einstellungen für den Cluster ab. Darüber hinaus hängt es davon ab, ob ein Reader so konfiguriert ist, dass er zusammen mit dem Writer oder unabhängig davon skaliert wird. Details zu den Faktoren, die Auswirkungen auf die Aurora Serverless v2-Skalierung haben, finden Sie unter Performance und Skalierung für Aurora Serverless v2.

> **Note**
>
> Derzeit skalieren Aurora Serverless v2-Writer und -Reader nicht herunter bis auf null ACU. Inaktive Aurora Serverless v2-Writer und -Reader können auf den minimalen ACU-Wert herunterskalieren, den Sie für den Cluster angegeben haben.
> Dieses Verhalten ist anders als bei Aurora Serverless v1, bei der nach einer Zeit der Inaktivität eine Pause erfolgen kann, aber dann einige Zeit benötigt wird, den Betrieb fortzusetzen, wenn Sie eine neue Verbindung öffnen. Wenn Ihr DB-Cluster mit Aurora Serverless v2-Kapazität einige Zeit nicht benötigt wird, können Sie Cluster genau wie bereitgestellte DB-Cluster anhalten und starten. Informationen zum Anhalten und Starten von Clustern finden Sie unter Stoppen und Starten eines Amazon Aurora-DB-Clusters.

Aurora Serverless v2 und hohe Verfügbarkeit

Hohe Verfügbarkeit für einen Aurora-DB-Cluster wird erreicht, indem Sie ihn zu einem Multi-AZ-DB-Cluster hochstufen. Ein Multi-AZ-Aurora-DB-Cluster verfügt jederzeit über Rechenkapazität in mehr als einer Availability Zone (AZ). Diese Konfiguration hält Ihre Datenbank auch im Falle eines größeren Ausfalls betriebsbereit. Aurora führt ein automatisches Failover im Falle eines Problems durch, das den Writer oder sogar die gesamte AZ betrifft. Mit Aurora Serverless v2 können Sie wählen, ob die Standby-Rechenkapazität zusammen mit der Kapazität des Schreibers hoch- oder herunterskaliert werden soll. Auf diese Weise ist die Rechenkapazität in der zweiten AZ bereit, die aktuelle Workload jederzeit zu übernehmen. Gleichzeitig kann die Rechenkapazität in allen AZs herunterskalieren, wenn die Datenbank inaktiv ist. Weitere Informationen zur Funktionsweise von Aurora mit AWS-Regionen und Availability Zones finden Sie unter Hohe Verfügbarkeit für Aurora-DB-Instances.

Die Aurora Serverless v2-Multi-AZ-Fähigkeit verwendet Reader zusätzlich zum Writer. Die Unterstützung für Reader ist neu für Aurora Serverless v2 im Gegensatz zu Aurora Serverless v1. Sie können bis zu 15 Aurora Serverless v2-Reader hinzufügen, die sich über 3 AZs auf einen Aurora-DB-Cluster verteilen.

Für geschäftskritische Anwendungen, die auch im Falle eines Problems, das Ihren gesamten Cluster oder die gesamte AWS Region betrifft, verfügbar bleiben müssen, können Sie eine globale Aurora-Datenbank einrichten. Sie können Aurora Serverless v2-Kapazität in den sekundären Clustern verwenden, damit sie im Falle einer Notfallwiederherstellung zur Übernahme bereit sind. Sie können auch herunterskalieren, wenn die Datenbank nicht ausgelastet ist. Weitere Informationen zu globalen Aurora-Datenbanken finden Sie unter Verwenden von Amazon Aurora Global Databases.

Aurora Serverless v2 funktioniert wie für Failover und andere Hochverfügbarkeitsfunktionen bereitgestellt. Weitere Informationen finden Sie unter Hohe Verfügbarkeit für Amazon Aurora.

Angenommen, Sie möchten maximale Verfügbarkeit für Ihre Aurora Serverless v2-Cluster sicherstellen. Sie können zusätzlich zum Writer einen Reader erstellen. Wenn Sie dem Reader die Hochstufungsstufe 0 oder 1 zuweisen, geschieht jede Skalierung sowohl für den Writer als auch für den Reader. Auf diese Weise ist ein Reader mit identischer Kapazität im Falle eines Failovers immer zur Übernahme für den Writer bereit.

Angenommen, Sie möchten Quartalsberichte für Ihr Unternehmen erstellen, während Ihr Cluster weiterhin Transaktionen verarbeitet. Wenn Sie dem Cluster einen Aurora Serverless v2-Reader hinzufügen und ihm eine Hochstufungsstufe zwischen 2 und 15 zuweisen, können Sie sich direkt mit diesem Reader verbinden, um die Berichte zu erstellen. Abhängig davon, wie arbeitsspeicherintensiv und CPU-intensiv die Berichtsabfragen sind, kann dieser Reader hochskalieren, um die Workload zu bewältigen. Anschließend kann er wieder herunterskalieren, wenn die Berichte erstellt sind.

Aurora Serverless v2 und Speicher

Der Speicher für jeden Aurora-DB-Cluster besteht aus sechs Kopien aller Ihrer Daten, die auf drei AZs verteilt sind. Diese integrierte Datenreplikation gilt unabhängig davon, ob Ihr DB-Cluster zusätzlich zum Writer auch Reader enthält. Auf diese Weise sind Ihre Daten sicher, auch bei Problemen, die sich auf die Rechenkapazität des Clusters auswirken.

Aurora Serverless v2-Speicher hat die gleichen Zuverlässigkeits- und Haltbarkeitseigenschaften wie unter Amazon Aurora-Speicher und -Zuverlässigkeit beschrieben. Das liegt daran, dass der Speicher für Aurora-DB-Cluster identisch funktioniert, unabhängig davon, ob die Rechenkapazität Aurora Serverless v2 verwendet oder bereitgestellt wird.

Konfigurationsparameter für Aurora-Cluster

Sie können Cluster- und Datenbankkonfigurationsparameter für Cluster mit Aurora Serverless v2-Kapazität genauso anpassen wie für bereitgestellte DB-Clustern. Einige kapazitätsbezogene Parameter werden für Aurora Serverless v2 jedoch unterschiedlich behandelt. In einem Cluster mit gemischter Konfiguration gelten die Parameterwerte, die Sie für diese kapazitätsbezogenen Parameter angeben, weiterhin für bereitgestellte Writer und Reader.

Fast alle Parameter funktionieren für Aurora Serverless v2-Writer und Reader auf die gleiche Weise wie für bereitgestellte Writer und Reader. Ausnahmen sind einige Parameter, die Aurora während der

Skalierung automatisch anpasst, und einige Parameter, die von Aurora als feste Werte beibehalten werden, die von der maximalen Kapazitätseinstellung abhängen.

Beispielsweise erhöht sich die für den Puffer-Cache reservierte Speichermenge, wenn ein Writer oder Reader hochskaliert, und nimmt beim Herunterskalieren ab. Auf diese Weise kann Arbeitsspeicher freigegeben werden, wenn Ihre Datenbank nicht ausgelastet ist. Umgekehrt legt Aurora die maximale Anzahl von Verbindungen automatisch auf einen Wert fest, der basierend auf der maximalen Kapazitätseinstellung angemessen ist. Auf diese Weise werden aktive Verbindungen nicht unterbrochen, wenn die Last sinkt und Aurora Serverless v2 herunterskaliert. Weitere Informationen zum Umgang von Aurora Serverless v2 mit bestimmten Parametern finden Sie unter Arbeiten mit Parametergruppen für Aurora Serverless v2.

Anforderungen und Einschränkungen für Aurora Serverless v2

Wenn Sie einen Cluster erstellen, in dem Sie Aurora Serverless v2 DB-Instances verwenden möchten, achten Sie auf die folgenden Anforderungen und Einschränkungen.

Themen

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Aurora-Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen zur Verfügbarkeit von Versionen und Regionen im Zusammenhang mit Aurora und Aurora Serverless v2 finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2.

Das folgende Beispiel zeigt die - AWS CLI Befehle zur Bestätigung der genauen DB-Engine-Werte, die Sie mit Aurora Serverless v2 für eine bestimmte verwenden können AWS-Region. Der `--db-instance-class`-Parameter für Aurora Serverless v2 ist immer `db.serverless`. Der `--engine`-Parameter kann `aurora-mysql` oder `aurora-postgresql` sein. Ersetzen Sie die entsprechenden Werte `--region` und `--engine` zur Bestätigung der `--engine-version`-Werte, die Sie verwenden können. Wenn der Befehl keine Ausgabe erzeugt, Aurora Serverless v2 ist für diese Kombination aus AWS-Region und DB-Engine nicht verfügbar.

```
aws rds describe-orderable-db-instance-options --engine aurora-mysql --db-instance-
class db.serverless \
  --region my_region --query 'OrderableDBInstanceOptions[].[EngineVersion]' --output
 text

aws rds describe-orderable-db-instance-options --engine aurora-postgresql --db-
instance-class db.serverless \
  --region my_region --query 'OrderableDBInstanceOptions[].[EngineVersion]' --output
 text
```

Für Cluster, die Aurora Serverless v2 verwenden, muss ein Kapazitätsbereich angegeben sein

Ein Aurora-Cluster muss über ein `ServerlessV2ScalingConfiguration`-Attribut verfügen, bevor Sie DB-Instances hinzufügen können, die die `db.serverless`-DB-Instance-Klasse verwenden. Dieses Attribut gibt den Kapazitätsbereich an. Die Aurora Serverless v2-Kapazität reicht von mindestens 0,5 Aurora-Kapazitätseinheiten (ACU) bis 128 ACU in inkrementellen Schritten von 0,5 ACU. Jede ACU bietet das Äquivalent von ungefähr 2 Gibibyte (GiB) RAM und zugehörige CPU- und Netzwerkressourcen. Details darüber, wie Aurora Serverless v2 die Einstellungen des Kapazitätsbereichs verwendet, finden Sie unter Funktionsweise von Aurora Serverless v2.

Sie können die minimalen und maximalen ACU-Werte in der angeben AWS Management Console , wenn Sie einen Cluster und eine zugehörige Aurora Serverless v2 DB-Instance erstellen. Sie können auch die `--serverless-v2-scaling-configuration`-Option in der AWS CLI angeben. Oder Sie können den `ServerlessV2ScalingConfiguration`-Parameter mit der Amazon-RDS-API angeben. Sie können dieses Attribut angeben, wenn Sie einen Cluster erstellen oder einen vorhandenen Cluster ändern. Informationen zu den Verfahren zum Festlegen des Kapazitätsbereichs finden Sie unter Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster. Eine ausführliche Diskussion darüber, wie minimale und maximale Kapazitätswerte ausgewählt werden und wie sich diese Einstellungen auf einige Datenbankparameter auswirken, finden Sie unter Auswählen des Aurora Serverless v2-Kapazitätsbereichs für einen Aurora-Cluster.

Einige bereitgestellte Funktionen werden in Aurora Serverless v2 nicht unterstützt

Die folgenden Funktionen der von Aurora bereitgestellten DB-Instances sind derzeit für Amazon Aurora Serverless v2 nicht verfügbar:

- Datenbankaktivitäts-Streams (DAS)
- Cluster-Cacheverwaltung für Aurora PostgreSQL. Der `apg_ccm_enabled`-Konfigurationsparameter gilt nicht für Aurora Serverless v2-DB-Instances.

Einige Aurora-Funktionen arbeiten mit Aurora Serverless v2, können jedoch Probleme verursachen, wenn Ihr Kapazitätsbereich niedriger ist als für die Speicheranforderungen dieser Funktionen mit Ihrer spezifischen Workload erforderlich. In diesem Fall funktioniert Ihre Datenbank möglicherweise nicht so gut wie gewohnt oder kann auf out-of-memory Fehler stoßen. Empfehlungen zum Einstellen des entsprechenden Kapazitätsbereichs finden Sie unter Auswählen des Aurora Serverless v2-Kapazitätsbereichs für einen Aurora-Cluster. Informationen zur Fehlerbehebung, wenn in Ihrer Datenbank out-of-memory Fehler aufgrund eines falsch konfigurierten Kapazitätsbereichs auftreten, finden Sie unter Fehler vermeiden out-of-memory .

Aurora Auto Scaling wird nicht unterstützt. Diese Art der Skalierung fügt basierend auf der CPU-Auslastung neue Reader hinzu, um zusätzliche leseintensive Workloads zu bewältigen. Die Skalierung auf der Grundlage der CPU-Auslastung ist für jedoch nicht sinnvollAurora Serverless v2. Alternativ können Sie Aurora Serverless v2-Reader-DB-Instances im Vorfeld erstellen und sie auf geringe Kapazität herunterskaliert lassen. Dies ist eine schnellere und weniger störende Methode, um die Lesekapazität eines Clusters zu skalieren, als neue DB-Instances dynamisch hinzuzufügen.

Einige Aurora Serverless v2-Aspekte unterscheiden sich von Aurora Serverless v1

Wenn Sie ein -Aurora Serverless v1Benutzer sind und dies zum ersten Mal verwendenAurora Serverless v2, lesen Sie die Unterschiede zwischen den Aurora Serverless v1 Anforderungen Aurora Serverless v2 und , um zu verstehen, wie sich die Anforderungen zwischen Aurora Serverless v1 und unterscheidenAurora Serverless v2.

Erstellen eines DB-Clusters, das Aurora Serverless v2

Wenn Sie einen Aurora-Cluster erstellen möchten, dem Sie Aurora Serverless v2-DB-Instances hinzufügen können, folgen Sie dem gleichen Verfahren wie in Erstellen eines Amazon Aurora-DB Clusters. Mit Aurora Serverless v2 sind Ihre Cluster mit bereitgestellten Clustern austauschbar. Es sind Cluster möglich, in denen einige DB-Instances Aurora Serverless v2 verwenden und andere DB-Instances bereitgestellt werden.

Themen

- Einstellungen für Aurora Serverless v2-DB-Cluster
- Erstellen eines Aurora Serverless v2-DB Clusters
- Eine Aurora Serverless v2 Writer-DB-Instance erstellen

Einstellungen für Aurora Serverless v2-DB-Cluster

Stellen Sie sicher, dass die Anfangseinstellungen des Clusters die unter aufgeführten Anforderungen erfüllenAnforderungen und Einschränkungen für Aurora Serverless v2. Geben Sie die folgenden Einstellungen an, um sicherzustellen, dass Sie dem Cluster Aurora Serverless v2-DB-Instances hinzufügen können:

AWS-Region

Erstellen Sie den Cluster in einem Land AWS-Region , in dem Aurora Serverless v2 DB-Instances verfügbar sind. Einzelheiten zu verfügbaren Regionen finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2.

DB-Engine-Version

Wählen Sie eine Engine-Version aus, die mit Aurora Serverless v2 kompatibel ist. Weitere Informationen über die Aurora Serverless v2-Versionsanforderungen finden Sie unter Anforderungen und Einschränkungen für Aurora Serverless v2.

DB-Instance-Klasse

Wenn Sie einen Cluster mit dem erstellen AWS Management Console, wählen Sie gleichzeitig die DB-Instance-Klasse für die Writer-DB-Instance aus. Wählen Sie die DB-Instance-Klasse Serverless aus. Wenn Sie diese DB-Instance-Klasse auswählen, geben Sie auch den Kapazitätsbereich für die Writer-DB-Instance an. Derselbe Kapazitätsbereich gilt für alle anderen Aurora Serverless v2-DB-Instances, die Sie diesem Cluster hinzufügen.

Wenn Sie die Option Serverless für die DB-Instance-Klasse nicht sehen, stellen Sie sicher, dass Sie eine DB-Engine-Version ausgewählt haben, die für Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2 unterstützt wird.

Wenn Sie die AWS CLI oder die Amazon RDS-API verwenden, lautet der Parameter, den Sie für die DB-Instance-Klasse angebendb.serverless.

Capacity range (Kapazitätsbereich)

Geben Sie die Werte der minimalen und maximalen Aurora-Kapazitätseinheit (ACU) ein, die für alle DB-Instances im Cluster gelten. Diese Option ist sowohl auf der Seite Create cluster (Cluster erstellen) als auch auf der Seite Add reader (Reader hinzufügen) der Konsole verfügbar, wenn Sie Serverless für die DB-Instance-Klasse auswählen.

Wenn Sie die ACU-Felder Minimum und Maximum nicht sehen, stellen Sie sicher, dass Sie die Serverless-DB-Instance-Klasse für die Writer-DB-Instance ausgewählt haben.

Wenn Sie den Cluster zunächst mit einer bereitgestellten DB-Instance erstellen, geben Sie nicht die minimalen und maximalen ACUs an. In diesem Fall können Sie den Cluster später ändern und diese Einstellung hinzufügen. Sie können dem Cluster auch eine Aurora Serverless v2-Reader-DB-Instance hinzufügen. Im Rahmen dieses Prozesses geben Sie den Kapazitätsbereich an.

Solange Sie den Kapazitätsbereich für Ihren Cluster nicht angegeben haben, können Sie dem Cluster keine Aurora Serverless v2 DB-Instances mithilfe der AWS CLI oder der RDS-API hinzufügen. Wenn Sie versuchen, eine Aurora Serverless v2-DB-Instance hinzuzufügen, wird eine Fehlermeldung ausgegeben. In den AWS CLI oder den RDS-API-Verfahren wird der Kapazitätsbereich durch das `ServerlessV2ScalingConfiguration` Attribut dargestellt.

Bei Clustern, die mehr als eine Reader-DB-Instance enthalten, spielt die Failover-Priorität jeder Aurora Serverless v2-Reader-DB-Instance eine wichtige Rolle dabei, wie diese DB-Instance hoch- oder herunterskaliert. Sie können die Priorität nicht angeben, wenn Sie den Cluster erstellen. Denken Sie an diese Eigenschaft, wenn Sie Ihrem Cluster eine zweite oder weitere Reader-DB-Instance hinzufügen. Weitere Informationen finden Sie unter Auswählen der Hochstufungsstufe für einen Aurora Serverless v2-Reader.

Erstellen eines Aurora Serverless v2-DB Clusters

Sie können die AWS Management Console, oder RDS-API verwenden AWS CLI, um einen Aurora Serverless v2 DB-Cluster zu erstellen.

Konsole

Erstellen Sie einen Cluster mit einem Aurora Serverless v2-Writer wie folgt

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.

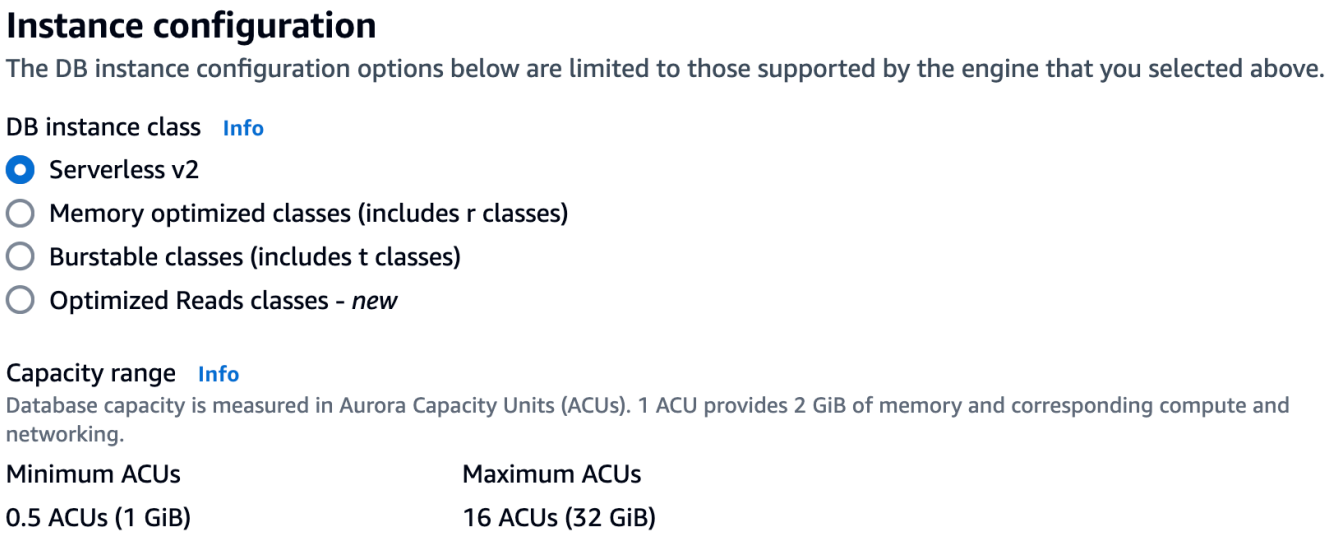
3. Wählen Sie Create database (Datenbank erstellen) aus. Wählen Sie auf der angezeigten Seite die folgenden Optionen aus:

   - Wählen Sie als Engine-Typ Aurora (MySQL-kompatibel) oder Aurora (PostgreSQL-kompatibel).
   - Wählen Sie unter Version eine der unterstützten Versionen fürUnterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2.

4. Wählen Sie als DB-Instance-Klasse Serverless v2 aus.

5. Für den Kapazitätsbereich können Sie den Standardbereich akzeptieren. Sie können auch andere Mindest- und Höchstwerte für die Kapazitätseinheiten festlegen. Sie können zwischen mindestens 0,5 ACU bis maximal 128 ACU in Schritten von 0,5 ACU wählen.

   Weitere Informationen zu Aurora Serverless v2-Kapazitätseinheiten finden Sie unter Kapazität von Aurora Serverless v2 und Performance und Skalierung für Aurora Serverless v2.

6. Wählen Sie beliebige andere DB-Cluster-Einstellungen aus, wie unter beschriebenEinstellungen für Aurora-DB-Cluster.

7. Wählen Sie Create database, um Ihren Aurora-DB-Cluster mit einer Aurora Serverless v2 DB-Instance als Writer-Instance zu erstellen, die auch als primäre DB-Instance bezeichnet wird.

CLI

Um einen DB-Cluster zu erstellen, der mit Aurora Serverless v2 DB-Instances kompatibel ist AWS CLI, folgen Sie dem CLI-Verfahren unterErstellen eines Amazon Aurora-DB Clusters. Fügen Sie die folgenden Parameter in Ihren `create-db-cluster`-Befehl ein:

- --region *AWS_Region_where_Aurora Serverless v2_instances_are_available*
- --engine-version *serverless_v2_compatible_engine_version*
- MinCapacity*--serverless-v2-scaling-configuration = Mindestkapazität, = Höchstkapazität MaxCapacity*

Das folgende Beispiel zeigt, wie ein Aurora Serverless v2-DB-Cluster erstellt wird.

```
aws rds create-db-cluster \
    --db-cluster-identifier my-serverless-v2-cluster \
    --region eu-central-1 \
    --engine aurora-mysql \
    --engine-version 8.0.mysql_aurora.3.04.1 \
    --serverless-v2-scaling-configuration MinCapacity=1,MaxCapacity=4 \
    --master-username myuser \
    --manage-master-user-password
```

> **Note**
>
> Wenn Sie einen Aurora Serverless v2 DB-Cluster mit dem erstellen, erscheint der Engine-Modus in der Ausgabe als und nicht. AWS CLI`provisioned` `serverless` Der Engine-Modus `serverless` bezieht sich auf Aurora Serverless v1.

Dieses Beispiel spezifiziert die `--manage-master-user-password` Option, das Administratorkennwort zu generieren und es in Secrets Manager zu verwalten. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager. Alternativ können Sie die Option `--master-password` verwenden, um das Passwort selbst festzulegen und zu verwalten.

Weitere Informationen über die Aurora Serverless v2-Versionsanforderungen finden Sie unter Anforderungen und Einschränkungen für Aurora Serverless v2. Informationen über die zulässigen Werte für den Kapazitätsbereich und was diese Werte darstellen, finden Sie unter Kapazität von Aurora Serverless v2 und Performance und Skalierung für Aurora Serverless v2.

Wenn Sie überprüfen möchten, ob ein vorhandener Cluster die angegebenen Kapazitätseinstellungen hat, sehen Sie sich die Ausgabe des `describe-db-clusters`-Befehls für das `ServerlessV2ScalingConfiguration`-Attribut an. Dieses Attribut sieht ähnlich wie folgt aus.

```
"ServerlessV2ScalingConfiguration": {
    "MinCapacity": 1.5,
    "MaxCapacity": 24.0
}
```

> **Tip**
>
> Wenn Sie beim Erstellen des Clusters die minimalen und maximalen ACU-Werte nicht angeben, können Sie diese Einstellungen später mit dem `modify-db-cluster`-Befehl hinzufügen. Bis dahin können Sie dem Cluster keine Aurora Serverless v2-DB-Instances hinzufügen. Wenn Sie versuchen, eine `db.serverless`-DB-Instance hinzuzufügen, wird eine Fehlermeldung ausgegeben.

API

Wenn Sie einen DB-Cluster mit der RDS API erstellen möchten, der mit Aurora Serverless v2-DB-Instances kompatibel ist, folgen Sie dem API-Verfahren unter Erstellen eines Amazon Aurora-DB Clusters. Wählen Sie die folgenden Einstellungen aus. Stellen Sie sicher, dass die `CreateDBCluster`-Operation die folgenden Parameter enthält:

```
EngineVersion serverless_v2_compatible_engine_version
ServerlessV2ScalingConfiguration with MinCapacity=minimum_capacity and
 MaxCapacity=maximum_capacity
```

Weitere Informationen über die Aurora Serverless v2-Versionsanforderungen finden Sie unter Anforderungen und Einschränkungen für Aurora Serverless v2. Informationen über die zulässigen Werte für den Kapazitätsbereich und was diese Werte darstellen, finden Sie unter Kapazität von Aurora Serverless v2 und Performance und Skalierung für Aurora Serverless v2.

Wenn Sie überprüfen möchten, ob ein vorhandener Cluster die angegebenen Kapazitätseinstellungen hat, sehen Sie sich die Ausgabe der `DescribeDBClusters`-Operation für das `ServerlessV2ScalingConfiguration`-Attribut an. Dieses Attribut sieht ähnlich wie folgt aus.

```
"ServerlessV2ScalingConfiguration": {
    "MinCapacity": 1.5,
    "MaxCapacity": 24.0
}
```

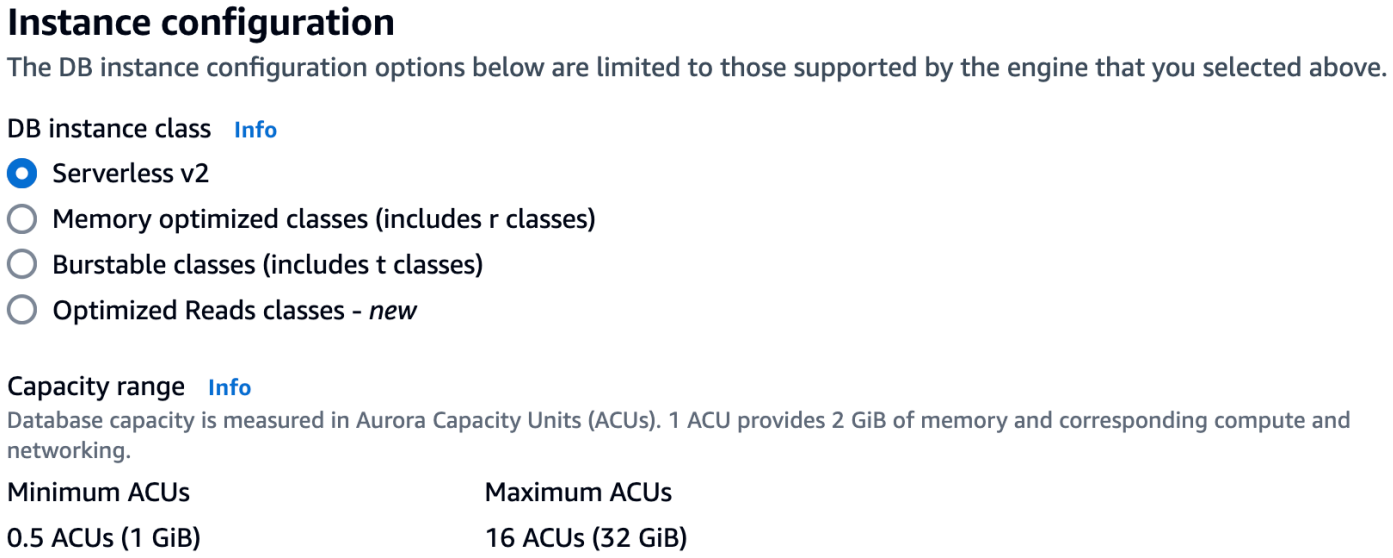
> **Tip**
>
> Wenn Sie beim Erstellen des Clusters die minimalen und maximalen ACU-Werte nicht angeben, können Sie diese Einstellungen später mit der `ModifyDBCluster`-Operation hinzufügen. Bis dahin können Sie dem Cluster keine Aurora Serverless v2-DB-Instances hinzufügen. Wenn Sie versuchen, eine `db.serverless`-DB-Instance hinzuzufügen, wird eine Fehlermeldung ausgegeben.

Eine Aurora Serverless v2 Writer-DB-Instance erstellen

Konsole

Wenn Sie mit dem einen DB-Cluster erstellen AWS Management Console, geben Sie gleichzeitig die Eigenschaften der Writer-DB-Instance an. Damit die Writer-DB-Instance Aurora Serverless v2 verwendet, wählen Sie die DB-Instance-Klasse Serverless aus.

Anschließend legen Sie den Kapazitätsbereich für den Cluster fest, indem Sie die Werte für die minimale und maximale Aurora-Kapazitätseinheit (ACU) angeben. Diese minimalen und maximalen Werte gelten für jede Aurora Serverless v2-DB-Instance im Cluster.



Wenn Sie bei der Ersterstellung des Clusters keine Aurora Serverless v2-DB-Instance erstellen, können Sie später eine oder mehrere Aurora Serverless v2-DB-Instances hinzufügen. Befolgen Sie hierzu die Verfahren unter Hinzufügen eines Aurora Serverless v2-Readers und Konvertieren eines bereitgestellten Writers oder Readers in Aurora Serverless v2. Sie geben den Kapazitätsbereich zu

dem Zeitpunkt an, an dem Sie dem Cluster die erste Aurora Serverless v2-DB-Instance hinzufügen. Sie können den Kapazitätsbereich später ändern, indem Sie die Schritte unter Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster befolgen.

CLI

Wenn Sie mit dem einen Aurora Serverless v2 DB-Cluster erstellen AWS CLI, fügen Sie die Writer-DB-Instance explizit mit dem Befehl create-db-instance hinzu. Schließen Sie den folgenden Parameter ein:

- `--db-instance-class db.serverless`

Das folgende Beispiel zeigt, wie eine Writer-DB-Instance von Aurora Serverless v2 erstellt wird.

```
aws rds create-db-instance \
    --db-cluster-identifier my-serverless-v2-cluster \
    --db-instance-identifier my-serverless-v2-instance \
    --db-instance-class db.serverless \
    --engine aurora-mysql
```

Verwaltung von Aurora Serverless v2 DB-Clustern

Mit Aurora Serverless v2 sind Ihre Cluster mit bereitgestellten Clustern austauschbar. Die Aurora Serverless v2-Eigenschaften gelten für eine oder mehrere DB-Instances innerhalb eines Clusters. Daher sind die Verfahren zum Erstellen von Clustern, zum Ändern von Clustern, zum Erstellen und Wiederherstellen von Snapshots usw. im Grunde die gleichen wie bei anderen Arten von Aurora-Clustern. Allgemeine Verfahren zum Verwalten von Aurora-Clustern und DB-Instances finden Sie unter Verwalten eines Amazon Aurora-DB-Clusters.

In den folgenden Themen erfahren Sie mehr über Überlegungen zur Verwaltung von Clustern, die Aurora Serverless v2 DB-Instances enthalten.

Themen

- Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster
- Überprüfen des Kapazitätsbereichs für Aurora Serverless v2
- Hinzufügen eines Aurora Serverless v2-Readers
- Konvertieren eines bereitgestellten Writers oder Readers in Aurora Serverless v2

- Konvertieren eines Aurora Serverless v2-Writers oder -Readers in bereitgestellt
- Auswählen der Hochstufungsstufe für einen Aurora Serverless v2-Reader
- Verwenden von TLS/SSL mit Aurora Serverless v2
- Anzeigen von Aurora Serverless v2-Writern und -Readern
- Protokollierung für Aurora Serverless v2

Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster

Wenn Sie die Konfigurationsparameter oder andere Einstellungen für Cluster mit Aurora Serverless v2-DB-Instances oder die DB-Instances selbst ändern möchten, folgen Sie denselben allgemeinen Verfahren wie für bereitgestellte Cluster. Details hierzu finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Die wichtigste Einstellung, die für Aurora Serverless v2 einzigartig ist, ist der Kapazitätsbereich. Nachdem Sie die Werte für die minimale und maximale Aurora-Kapazitätseinheit (ACU) für einen Aurora-Cluster festgelegt haben, müssen Sie die Kapazität der Aurora Serverless v2-DB-Instances im Cluster aktiv anpassen. Aurora übernimmt diesen Schritt nicht. Diese Einstellung wird auf Cluster-Ebene verwaltet. Für jede Aurora Serverless v2-DB-Instance im Cluster gelten die gleichen minimalen und maximalen ACU-Werte.

Sie können die folgenden spezifischen Werte festlegen:

- Minimum ACUs (Minimale ACUs) – Die Aurora Serverless v2-DB-Instance kann die Kapazität auf diese Anzahl von ACUs reduzieren.
- Maximum ACUs (Maximale ACUs) – Die Aurora Serverless v2-DB-Instance kann die Kapazität auf diese Anzahl von ACUs erhöhen.

> **Note**
>
> Wenn Sie den Kapazitätsbereich für einen DB-Cluster von Aurora Serverless v2 ändern, erfolgt die Änderung sofort, unabhängig davon, ob Sie sie sofort oder während des nächsten geplanten Wartungsfensters anwenden möchten.

Weitere Informationen zu den Auswirkungen des Kapazitätsbereichs und zur Überwachung und Feinabstimmung finden Sie unter Wichtige CloudWatch Amazon-Metriken für Aurora Serverless v2

und Performance und Skalierung für Aurora Serverless v2. Ihr Ziel ist es, sicherzustellen, dass die maximale Kapazität für den Cluster hoch genug ist, um Spitzen bei der Workload zu bewältigen, und die miminale Kapazität niedrig genug ist, um die Kosten zu minimieren, wenn der Cluster nicht aktiv ist.

Angenommen, Sie bestimmen basierend auf Ihrer Überwachung, dass der ACU-Bereich für den Cluster höher, niedriger, breiter oder schmaler sein sollte. Sie können die Kapazität eines Aurora-Clusters mit der, der oder der Amazon RDS-API auf einen bestimmten Bereich von ACUs festlegen. AWS Management Console AWS CLI Dieser Kapazitätsbereich gilt für jede Aurora Serverless v2-DB-Instance im Cluster.

Angenommen, Ihr Cluster hat einen Kapazitätsbereich von 1 bis 16 ACUs und enthält zwei Aurora Serverless v2-DB-Instances. Dann verbraucht der Cluster insgesamt zwischen 2 ACUs (bei Inaktivität) und 32 ACUs (bei Vollauslastung). Wenn Sie den Kapazitätsbereich in 8 bis 20,5 ACUs ändern, verbraucht der Cluster jetzt 16 ACUs bei Inaktivität und bei voller Auslastung bis zu 41 ACUs.

Aurora legt automatisch bestimmte Parameter für Aurora Serverless v2-DB-Instances auf Werte fest, die vom maximalen ACU-Wert im Kapazitätsbereich abhängen. Eine Liste dieser Parameter finden Sie unter Maximale Anzahl der Verbindungen für Aurora Serverless v2. Bei statischen Parametern, die von dieser Berechnungsart abhängen, wird der Wert beim Neustart der DB-Instance erneut ausgewertet. So können Sie den Wert solcher Parameter aktualisieren, indem Sie die DB-Instance neu starten, nachdem Sie den Kapazitätsbereich geändert haben. Wenn Sie wissen möchten, ob Sie Ihre DB-Instance neu starten müssen, um Parameteränderungen zu übernehmen, überprüfen Sie das `ParameterApplyStatus`-Attribut der DB-Instance. Der Wert `pending-reboot` gibt an, dass ein Neustart Änderungen auf einige Parameterwerte anwendet.

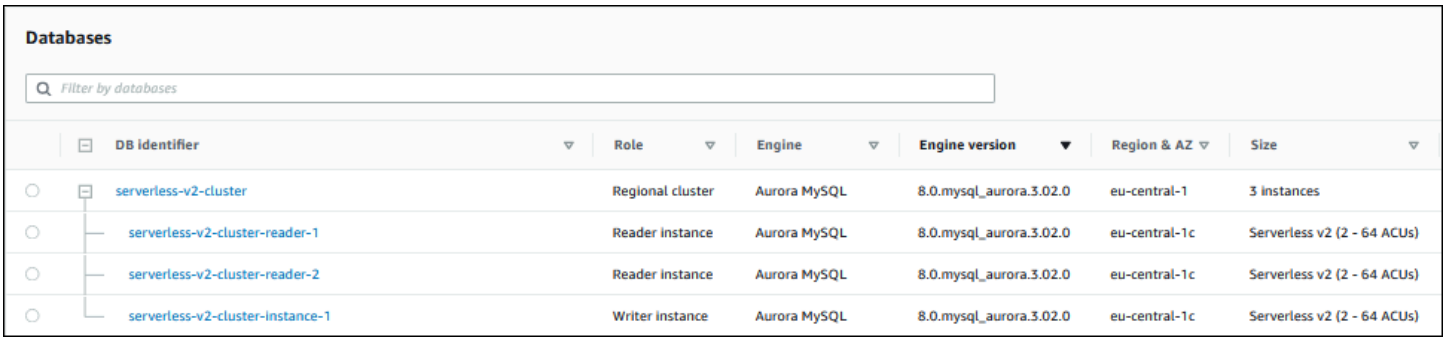
Konsole

Sie können den Kapazitätsbereich eines Clusters, der Aurora Serverless v2-DB-Instances enthält, über die AWS Management Console festlegen.

Wenn Sie die Konsole verwenden, legen Sie den Kapazitätsbereich für den Cluster zu dem Zeitpunkt fest, zu dem Sie dem Cluster die erste Aurora Serverless v2-DB-Instance hinzufügen. Diesen Schritt können Sie ausführen, wenn Sie beim Erstellen des Clusters die DB-Instance-Klasse Serverless v2 für die Writer-DB-Instance auswählen. Sie können diesen Schritt auch ausführen, wenn Sie beim Hinzufügen einer Aurora Serverless v2-Reader-DB-Instance zum Cluster die DB-Instance-Klasse Serverless auswählen. Möglich ist dieser Schritt auch, wenn Sie eine vorhandene bereitgestellte DB-Instance im Cluster in die DB-Instance-Klasse Serverless konvertieren. Die Vollversionen dieser Verfahren finden Sie unter Eine Aurora Serverless v2 Writer-DB-Instance erstellenHinzufügen eines

Aurora Serverless v2-Readers, und Konvertieren eines bereitgestellten Writers oder Readers in Aurora Serverless v2.

Der jeweilige Kapazitätsbereich, den Sie auf Cluster-Ebene festlegen, gilt für alle Aurora Serverless v2-DB-Instances in Ihrem Cluster. Die folgende Abbildung zeigt einen Cluster mit mehreren Aurora Serverless v2-Reader-DB-Instances. Jede Instance hat einen identischen Kapazitätsbereich von 2 bis 64 ACU.

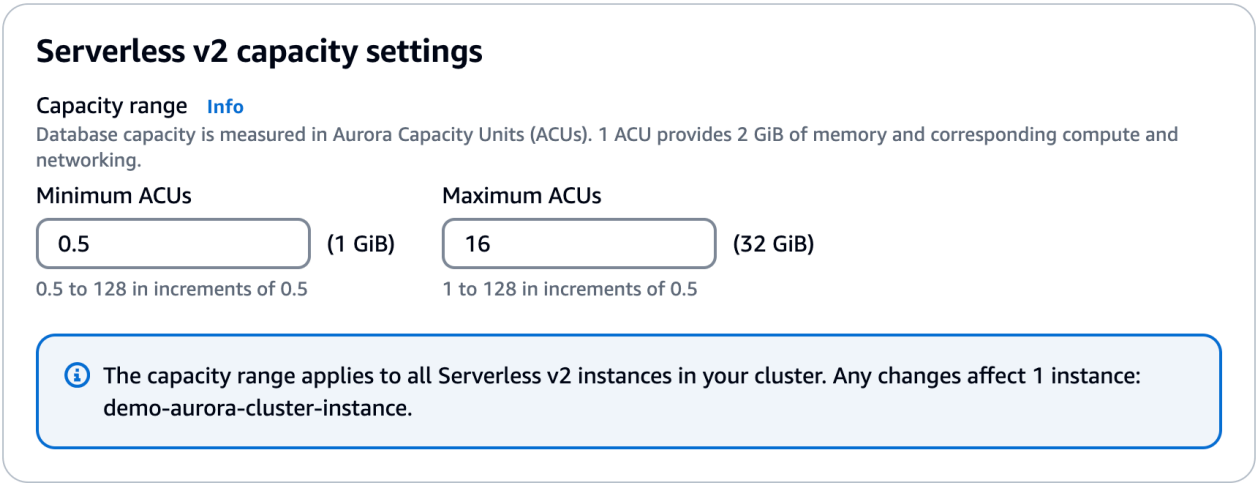


So ändern Sie den Kapazitätsbereich eines Aurora Serverless v2-Clusters

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den Cluster, der Ihre Aurora Serverless v2-DB-Instances enthält, aus der Liste aus. Der Cluster muss bereits mindestens eine Aurora Serverless v2-DB-Instance enthalten. Andernfalls zeigt Aurora den Abschnitt Capacity range (Kapazitätsbereich) nicht an.
4. Wählen Sie für Actions (Aktionen) die Option Modify (Ändern) aus.
5. Wählen Sie im Abschnitt Capacity range (Kapazitätsbereich) Folgendes aus:

    a. Geben Sie einen Wert für Minimum ACUs (Minimale ACUs) ein. Die Konsole zeigt den zulässigen Wertebereich an. Sie können eine Mindestkapazität von 0,5 bis 128 ACUs wählen. Sie können eine maximale Kapazität von 1 bis 128 ACUs wählen. Sie können die Kapazitätswerte in Schritten von 0,5 ACU anpassen.

    b. Geben Sie einen Wert für Maximum ACUs (Maximale ACUs) ein. Dieser Wert muss gleich oder größer als der Wert für Minimum ACUs (Minimale ACUs) sein. Die Konsole zeigt den zulässigen Wertebereich an. Die folgende Abbildung zeigt diese Auswahl.



6. Klicken Sie auf Weiter. Die Seite Summary of modifications (Zusammenfassung der Änderungen) wird angezeigt.
7. Wählen Sie Apply immediately (Sofort anwenden) aus.

   Die Kapazitätsänderung erfolgt sofort, unabhängig davon, ob Sie sie sofort oder während des nächsten geplanten Wartungsfensters anwenden möchten.
8. Wählen Sie Modify cluster (Cluster ändern), um die Zusammenfassung der Änderungen zu akzeptieren. Sie können auch Back (Zurück) wählen, um Ihre Änderungen zu bearbeiten, oder Cancel (Abbrechen), um Ihre Änderungen zu verwerfen.

AWS CLI

Um die Kapazität eines Clusters festzulegen, in dem Sie Aurora Serverless v2 DB-Instances mithilfe von verwenden möchten AWS CLI, führen Sie den modify-db-cluster AWS CLI Befehl aus. Legen Sie die Option `--serverless-v2-scaling-configuration` fest. Der Cluster enthält möglicherweise bereits eine oder mehrere Aurora Serverless v2-DB-Instances oder Sie können die DB-Instances später hinzufügen. Gültige Werte für die Felder `MinCapacity` und `MaxCapacity` sind unter anderem folgende:

- `0.5`, `1`, `1.5`, 2 usw. in Schritten von 0,5 bis maximal 128.

In diesem Beispiel legen Sie den ACU-Bereich eines Aurora-DB-Clusters namens `sample-cluster` auf ein Minimum von `48.5` und maximal 64 fest.

```
aws rds modify-db-cluster --db-cluster-identifier sample-cluster \
```

```
--serverless-v2-scaling-configuration MinCapacity=48.5,MaxCapacity=64
```

Die Kapazitätsänderung erfolgt sofort, unabhängig davon, ob Sie sie sofort oder während des nächsten geplanten Wartungsfensters anwenden möchten.

Danach können Sie dem Cluster Aurora Serverless v2-DB-Instances hinzufügen und jede neue DB-Instance kann zwischen 48,5 und 64 ACUs skaliert werden. Der neue Kapazitätsbereich gilt auch für alle Aurora Serverless v2-DB-Instances, die sich bereits im Cluster befanden. Die DB-Instances skalieren bei Bedarf hoch oder herunter, um in den neuen Kapazitätsbereich zu gelangen.

Weitere Beispiele für die Einstellung des Kapazitätsbereichs über die CLI finden Sie unter Auswählen des Aurora Serverless v2-Kapazitätsbereichs für einen Aurora-Cluster.

Um die Skalierungskonfiguration eines Aurora Serverless DB-Clusters mithilfe von zu ändern AWS CLI, führen Sie den modify-db-cluster AWS CLI Befehl aus. Geben Sie die Option `--serverless-v2-scaling-configuration` an, um die minimale und die maximale Kapazität zu konfigurieren. Zu den gültigen Kapazitätswerten gehören die folgenden:

- Aurora MySQL: `0.5`, `1`, `1.5`, `2` usw. in Schritten von 0,5 ACUs bis maximal `128`.
- Aurora PostgreSQL: `0.5`, `1`, `1.5`, `2` usw. in Schritten von 0,5 ACUs bis maximal `128`.

Im folgenden Beispiel ändern Sie die Skalierungskonfiguration einer Aurora Serverless v2-DB-Instance mit dem Namen `sample-instance`, die Teil eines Clusters namens `sample-cluster` ist.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster --db-cluster-identifier sample-cluster \
--serverless-v2-scaling-configuration MinCapacity=8,MaxCapacity=64
```

Windows:

```
aws rds modify-db-cluster --db-cluster-identifier sample-cluster ^
--serverless-v2-scaling-configuration MinCapacity=8,MaxCapacity=64
```

RDS-API

Sie können die Kapazität einer Aurora-DB-Instance über die API-Operation ModifyDBCluster festlegen. Geben Sie den Parameter `ServerlessV2ScalingConfiguration` an. Gültige Werte für die Felder `MinCapacity` und `MaxCapacity` sind unter anderem folgende:

- `0.5`, `1`, `1.5`, 2 usw. in Schritten von 0,5 bis maximal 128.

Sie können die Skalierungskonfiguration eines Clusters, der Aurora Serverless v2-DB-Instances enthält, über die API-Operation ModifyDBCluster ändern. Geben Sie den Parameter `ServerlessV2ScalingConfiguration` an, um die minimale und die maximale Kapazität zu konfigurieren. Zu den gültigen Kapazitätswerten gehören die folgenden:

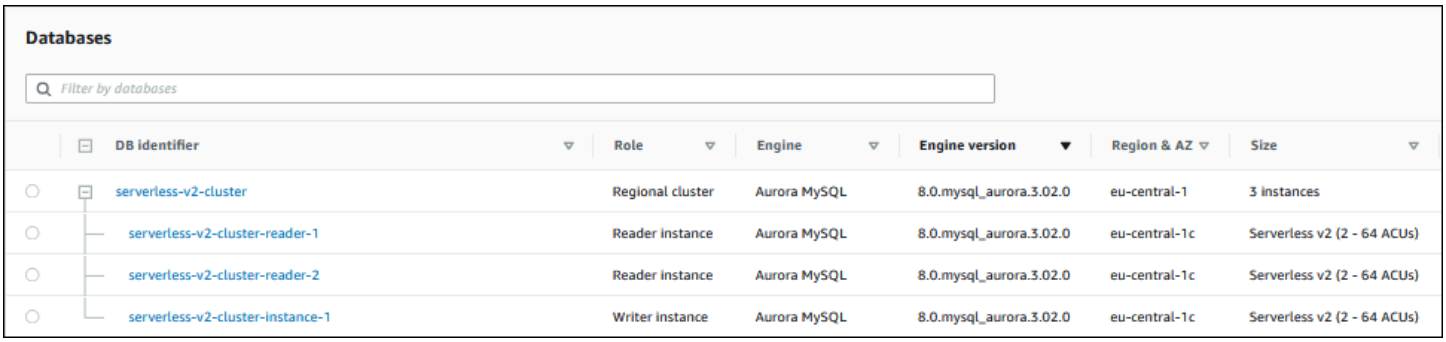
- Aurora MySQL: `0.5`, `1`, `1.5`, 2 usw. in Schritten von 0,5 ACUs bis maximal 128.
- Aurora PostgreSQL: `0.5`, `1`, `1.5`, 2 usw. in Schritten von 0,5 ACUs bis maximal 128.

Die Kapazitätsänderung erfolgt sofort, unabhängig davon, ob Sie sie sofort oder während des nächsten geplanten Wartungsfensters anwenden möchten.

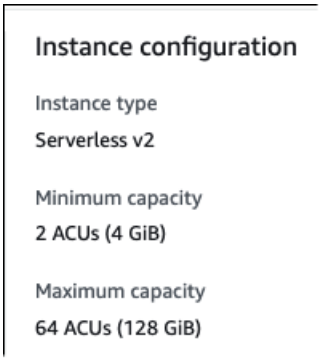
Überprüfen des Kapazitätsbereichs für Aurora Serverless v2

Das Verfahren zur Überprüfung des Kapazitätsbereichs für Ihren Aurora Serverless v2-Cluster erfordert, dass Sie zuerst einen Kapazitätsbereich festlegen. Wenn Sie dies noch nicht getan haben, gehen Sie wie unter Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster beschrieben vor.

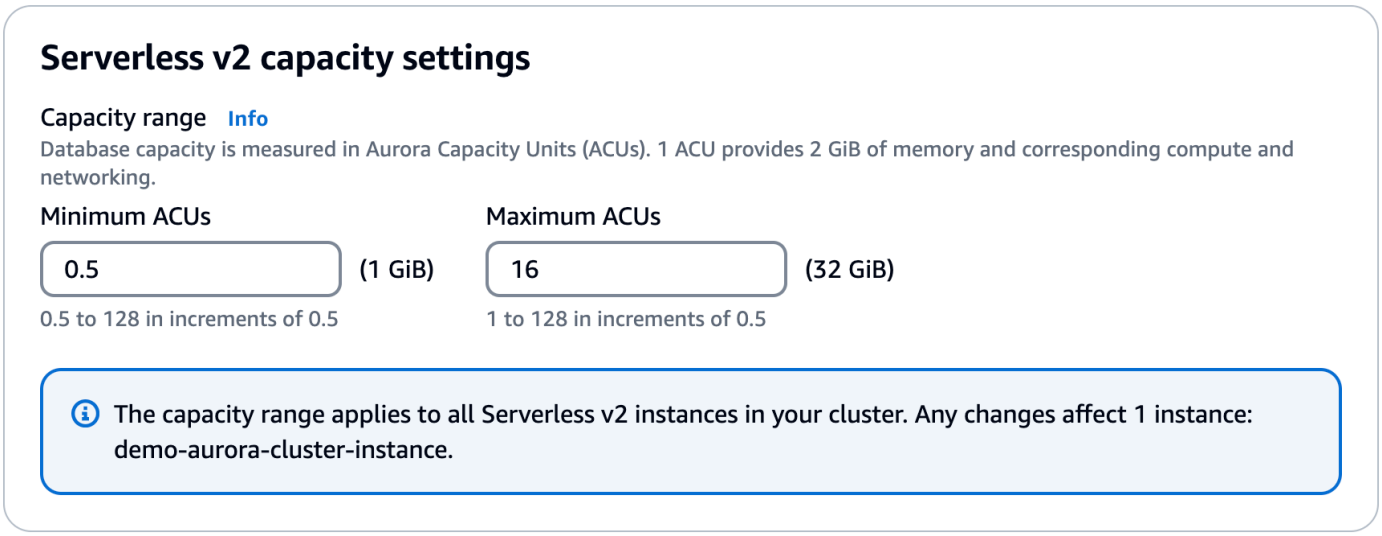
Der jeweilige Kapazitätsbereich, den Sie auf Cluster-Ebene festlegen, gilt für alle Aurora Serverless v2-DB-Instances in Ihrem Cluster. Die folgende Abbildung zeigt einen Cluster mit mehreren Aurora Serverless v2-DB-Instances. Jede Instance hat einen identischen Kapazitätsbereich.



Sie können auch die Detailseite für alle Aurora Serverless v2-DB-Instances im Cluster anzeigen. Der Kapazitätsbereich der DB-Instances wird auf dem Tab Configuration (Konfiguration) angezeigt.



Sie können den aktuellen Kapazitätsbereich für den Cluster auch auf der Seite Modify (Ändern) für den Cluster sehen. Die folgende Abbildung veranschaulicht die Vorgehensweise. An diesem Punkt können Sie den Kapazitätsbereich ändern. Alle Möglichkeiten, wie Sie den Kapazitätsbereich einstellen oder ändern können, finden Sie unter Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster.



Überprüfen des aktuellen Kapazitätsbereichs für einen Aurora-Cluster

Sie können den Kapazitätsbereich überprüfen, der für Aurora Serverless v2-DB-Instances in einem Cluster konfiguriert ist, indem Sie sich das `ServerlessV2ScalingConfiguration`-Attribut für den Cluster ansehen. Das folgende AWS CLI -Beispiel zeigt einen Cluster mit einer minimalen Kapazität von 0,5 Aurora-Kapazitätseinheiten (ACU) und einer maximalen Kapazität von 16 ACUs.

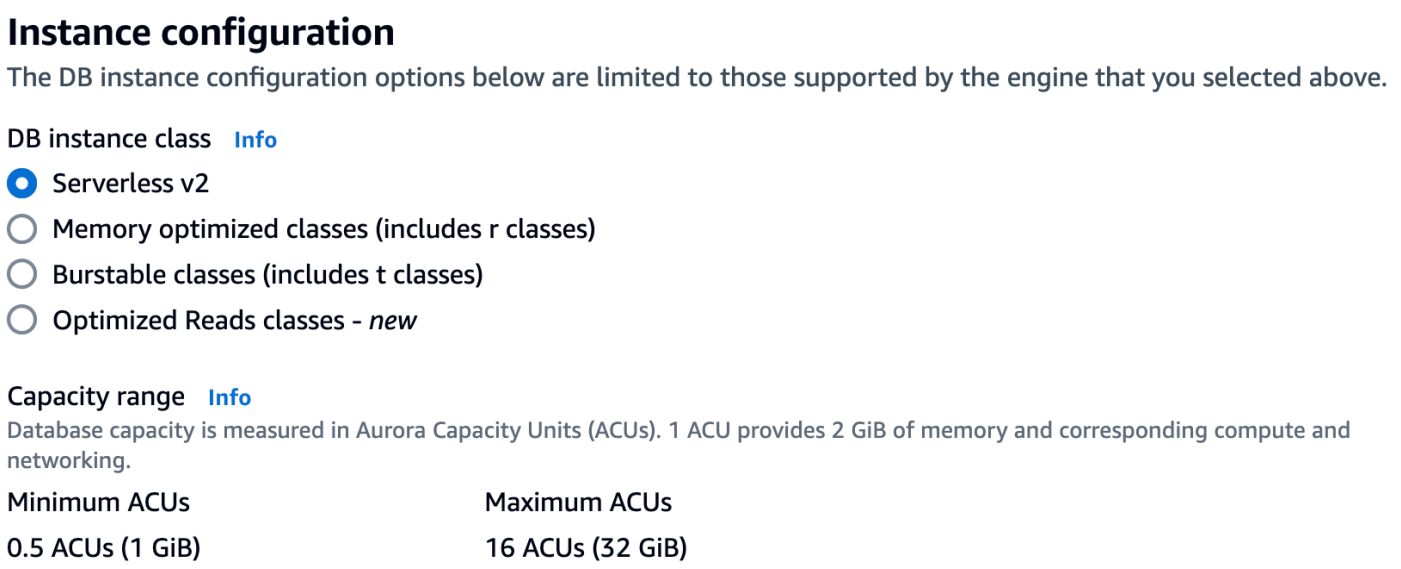
```
$ aws rds describe-db-clusters --db-cluster-identifier serverless-v2-64-acu-cluster \
  --query 'DBClusters[*].[ServerlessV2ScalingConfiguration]'
[
    [
```

```
        {
            "MinCapacity": 0.5,
            "MaxCapacity": 16.0
        }
    ]
]
```

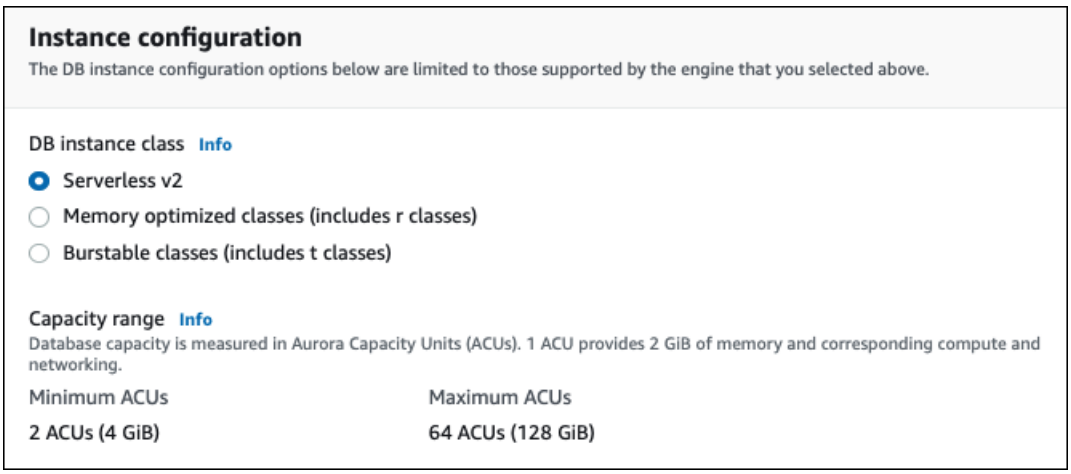
Hinzufügen eines Aurora Serverless v2-Readers

Wenn Sie Ihrem Cluster eine Aurora Serverless v2-Reader-DB-Instance hinzufügen möchten, folgen Sie dem gleichen allgemeinen Verfahren wie in Hinzufügen von Aurora-Replicas zu einem DB-Cluster. Wählen Sie die Instance-Klasse Serverless v2 für die neue DB-Instance aus.

Wenn die Reader-DB-Instance die erste Aurora Serverless v2-DB-Instance im Cluster ist, wählen Sie auch den Kapazitätsbereich aus. Die folgende Abbildung zeigt die Steuerelemente, mit denen Sie die minimalen und maximalen Aurora-Kapazitätseinheiten (ACUs) angeben. Diese Einstellung gilt für diese Reader-DB-Instance und für alle weiteren Aurora Serverless v2-DB-Instances, die Sie dem Cluster hinzufügen. Jede Aurora Serverless v2-DB-Instance kann zwischen dem minimalen und dem maximalen ACU-Wert skaliert werden.



Wenn Sie dem Cluster bereits Aurora Serverless v2-DB-Instances hinzugefügt haben, wird Ihnen beim Hinzufügen weiterer Aurora Serverless v2-Reader-DB-Instances der aktuelle Kapazitätsbereich angezeigt. Die folgende Abbildung zeigt diese schreibgeschützten Steuerelemente.



Wenn Sie den Kapazitätsbereich für den Cluster ändern möchten, gehen Sie vor, wie in Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster bechrieben.

Bei Clustern, die mehr als eine Reader-DB-Instance enthalten, spielt die Failover-Priorität jeder Aurora Serverless v2-Reader-DB-Instance eine wichtige Rolle dabei, wie diese DB-Instance hoch- oder herunterskaliert. Sie können die Priorität nicht angeben, wenn Sie den Cluster erstellen. Denken Sie an diese Eigenschaft, wenn Sie Ihrem Cluster einen zweiten Reader oder eine weitere DB-Instance hinzufügen. Weitere Informationen finden Sie unter Auswählen der Hochstufungsstufe für einen Aurora Serverless v2-Reader.

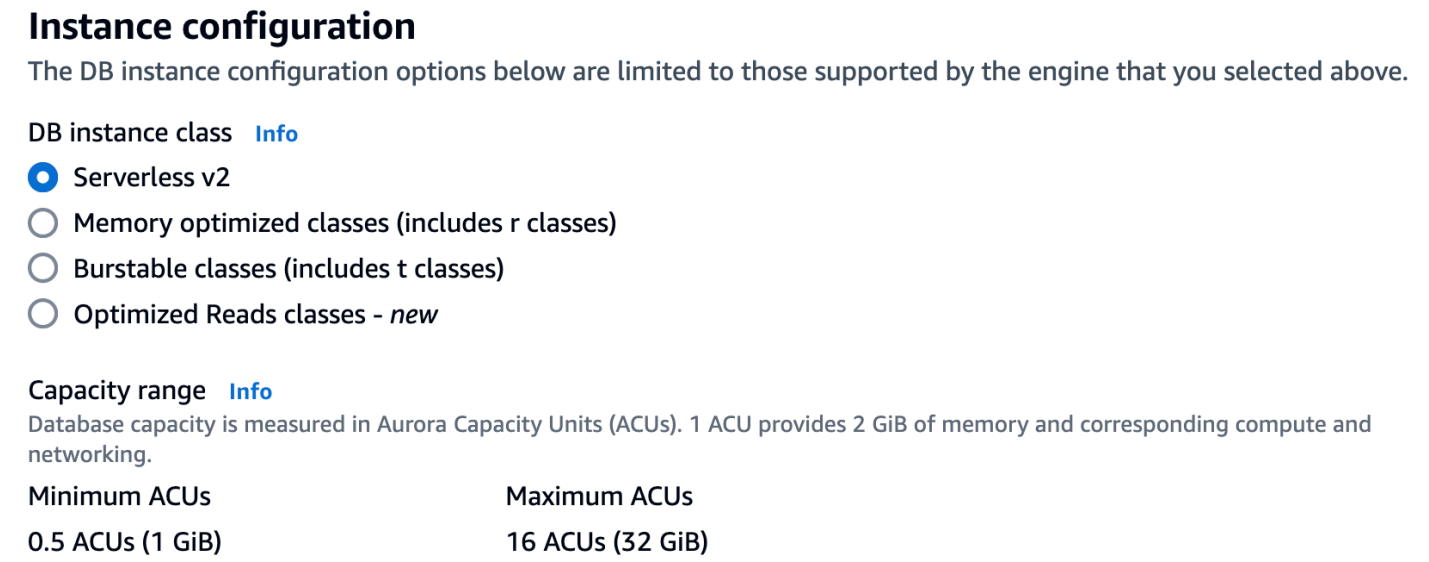
Weitere Möglichkeiten zum Anzeigen des aktuellen Kapazitätsbereichs für einen Cluster finden Sie unter Überprüfen des Kapazitätsbereichs für Aurora Serverless v2.

Konvertieren eines bereitgestellten Writers oder Readers in Aurora Serverless v2

Sie können eine bereitgestellte DB-Instance konvertieren, um Aurora Serverless v2 zu verwenden. Befolgen Sie dazu die Anleitung unter Ändern einer DB-Instance in einem DB-Cluster. Der Cluster muss die Anforderungen in Anforderungen und Einschränkungen für Aurora Serverless v2 erfüllen. Aurora Serverless v2-DB-Instances erfordern beispielsweise, dass der Cluster bestimmte Mindest-Engine-Versionen ausführt.

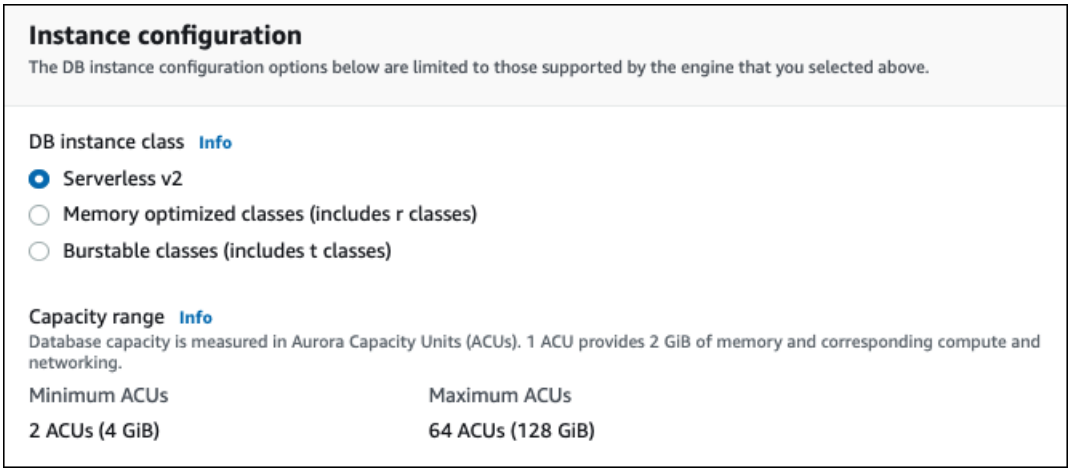
Angenommen, Sie konvertieren einen laufenden bereitgestellten Cluster, um Aurora Serverless v2 zu nutzen. In diesem Fall können Sie Ausfallzeiten minimieren, indem Sie im ersten Schritt des Umstellungsprozesses eine DB-Instance in Aurora Serverless v2 konvertieren. Das vollständige Verfahren finden Sie unter Umstellung von einem bereitgestellten Cluster zu Aurora Serverless v2.

Wenn die DB-Instance, die Sie konvertieren, die erste Aurora Serverless v2-DB-Instance im Cluster ist, wählen Sie den Kapazitätsbereich für den Cluster im Rahmen der Operation Modify (Ändern) aus. Dieser Kapazitätsbereich gilt für jede Aurora Serverless v2-DB-Instance, die Sie dem Cluster hinzufügen. Die folgende Abbildung zeigt die Seite, auf der Sie die minimalen und maximalen Aurora-Kapazitätseinheiten (ACUs) angeben.



Weitere Informationen zur Bedeutung des Kapazitätsbereichs finden Sie unter Kapazität von Aurora Serverless v2.

Wenn der Cluster bereits eine oder mehrere Aurora Serverless v2-DB-Instances enthält, sehen Sie den vorhandenen Kapazitätsbereich, wenn Sie die Operation Modify (Ändern) verwenden. Die folgende Abbildung zeigt ein Beispiel für dieses Informationsfeld.



Wenn Sie den Kapazitätsbereich für den Cluster ändern möchten, nachdem Sie weitere Aurora Serverless v2-DB-Instances hinzugefügt haben, gehen Sie vor, wie in Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster bechrieben.

Konvertieren eines Aurora Serverless v2-Writers oder -Readers in bereitgestellt

Sie können eine Aurora Serverless v2-DB-Instance in eine bereitgestellte DB-Instance konvertieren. Befolgen Sie dazu die Anleitung unter Ändern einer DB-Instance in einem DB-Cluster. Wählen Sie eine andere DB-Instance-Klasse als Serverless aus.

Sie können eine Aurora Serverless v2-DB-Instance in eine bereitgestellte Instance konvertieren, wenn sie eine größere Kapazität benötigt, als mit den maximalen Aurora-Kapazitätseinheiten (ACUs) einer Aurora Serverless v2-DB-Instance verfügbar ist. Zum Beispiel haben die größten DB-Instance-Klassen db.r5 und db.r6g eine größere Speicherkapazität als die Kapazität, auf die eine Aurora Serverless v2-DB-Instance skalieren kann.

> **Tip**
>
> Einige der älteren DB-Instance-Klassen wie db.r3 und db.t2 sind für die Aurora-Versionen, die Sie mit Aurora Serverless v2 verwenden, nicht verfügbar. Informationen dazu, wie Sie feststellen können, welche DB-Instance-Klassen beim Konvertieren einer Aurora Serverless v2-DB-Instance in eine bereitgestellte Instance verwendet werden können, finden Sie unter Unterstützte DB-Engines für DB-Instance-Klassen.

Wenn Sie die Writer-DB-Instance Ihres Clusters von Aurora Serverless v2 in eine bereitgestellte Instance konvertieren, können Sie die Vorgehensweise unter Umstellung von einem bereitgestellten Cluster zu Aurora Serverless v2 verwenden. Stellen Sie eine der Reader-DB-Instances im Cluster von Aurora Serverless v2 auf eine bereitgestellte Instance um. Führen Sie ein Failover durch, damit diese bereitgestellte DB-Instance zur Writer-Instance wird.

Jeder Kapazitätsbereich, den Sie zuvor für den Cluster angegeben haben, bleibt bestehen, auch wenn alle Aurora Serverless v2-DB-Instances aus dem Cluster entfernt werden. Wenn Sie den Kapazitätsbereich ändern möchten, können Sie den Cluster ändern, wie in Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster erläutert.

Auswählen der Hochstufungsstufe für einen Aurora Serverless v2-Reader

Bei Clustern mit mehreren Aurora Serverless v2-DB-Instances oder mit einer Mischung aus bereitgestellten und Aurora Serverless v2-DB-Instances achten Sie auf die Einstellung der Hochstufungsstufe für jede einzelne Aurora Serverless v2-DB-Instance. Diese Einstellung steuert mehr Verhaltensweisen für Aurora Serverless v2-DB-Instances als für bereitgestellte DB-Instances.

In der AWS Management Console geben Sie diese Einstellung mithilfe der Failover-Priorität unter Zusätzliche Konfiguration für die Seiten Create database, Modify instance und Add reader pages an. Sie sehen diese Eigenschaft für vorhandene DB-Instances in der optionalen Spalte Priority tier(Prioritätsstufe) auf der Seite Databases (Datenbanken). Diese Eigenschaft können Sie auch der Detailseite für einen DB-Cluster oder eine DB-Instance entnehmen.

Bei bereitgestellten DB-Instances bestimmt die Auswahl der Stufe 0 bis 15 nur die Reihenfolge, in der Aurora entscheidet, welche Reader-DB-Instance während eines Failover-Vorgangs zum Writer hochgestuft werden soll. Für Aurora Serverless v2-Reader-DB-Instances bestimmt die Stufennummer auch, ob die DB-Instance auf die Kapazität der Writer-DB-Instance hochskaliert oder unabhängig und basierend auf ihrer eigenen Workload skaliert wird. Aurora Serverless v2-Reader-DB-Instances in Stufe 0 oder 1 werden auf einer minimalen Kapazität gehalten, die mindestens so hoch ist wie die der Writer-DB-Instance. Auf diese Weise sind sie im Falle eines Failovers zur Übernahme von der Writer-DB-Instance bereit. Wenn die Writer-DB-Instance eine bereitgestellte DB-Instance ist, schätzt Aurora die entsprechende Aurora Serverless v2-Kapazität. Sie verwendet diese Schätzung als Mindestkapazität für die Aurora Serverless v2-Reader-DB-Instance.

Aurora Serverless v2-Reader-DB-Instances der Stufen 2 bis 15 haben nicht die gleiche Einschränkung ihrer minimalen Kapazität. Wenn sie inaktiv sind, können sie auf den minimalen Aurora-Kapazitätseinheitwert (ACU) herunterskaliert werden, der im Kapazitätsbereich des Clusters angegeben ist.

Das folgende AWS CLI Linux-Beispiel zeigt, wie Sie die Upgrade-Stufen aller DB-Instances in Ihrem Cluster untersuchen können. Das letzte Feld enthält den Wert `True` für die Writer-DB-Instance und `False` für alle Reader-DB-Instances.

```
$ aws rds describe-db-clusters --db-cluster-identifier promotion-tier-demo \
  --query 'DBClusters[*].DBClusterMembers[*].
[PromotionTier,DBInstanceIdentifier,IsClusterWriter]' \
  --output text

1   instance-192  True
```

```
1   tier-01-4840  False
10  tier-10-7425  False
15  tier-15-6694  False
```

Das folgende AWS CLI Linux-Beispiel zeigt, wie Sie die Upgrade-Stufe einer bestimmten DB-Instance in Ihrem Cluster ändern können. Mit den Befehlen wird zuerst die DB-Instance geändert und eine neue Hochstufungsstufe festgelegt. Dann wird gewartet, bis die DB-Instance wieder verfügbar ist, und die neue Hochstufungsstufe für die DB-Instance bestätigt.

```
$ aws rds modify-db-instance --db-instance-identifier instance-192 --promotion-tier 0
$ aws rds wait db-instance-available --db-instance-identifier instance-192
$ aws rds describe-db-instances --db-instance-identifier instance-192 \
  --query '*[].[PromotionTier]' --output text
0
```

Weitere Hilfestellung zum Angeben von Hochstufungsstufen für verschiedene Anwendungsfälle finden Sie unter Aurora Serverless v2-Skalierung.

Verwenden von TLS/SSL mit Aurora Serverless v2

Aurora Serverless v2 kann das TLS-/SSL-Protokoll (Transport Layer Security/Secure Sockets Layer) verwenden, um die Kommunikation zwischen Clients und den Aurora Serverless v2-DB-Instances zu verschlüsseln. Die TLS-/SSL-Versionen 1.0, 1.1 und 1.2 werden unterstützt. Allgemeine Informationen zur Verwendung von TLS/SSL mit Aurora finden Sie unter Verwenden von TLS mit DB-Clustern von Aurora MySQL.

Weitere Informationen zum Verbinden mit der Aurora MySQL-Datenbank über den MySQL-Client finden Sie unter Verbinden mit einer DB-Instance, auf der die MySQL-Datenbank-Engine ausgeführt wird.

Aurora Serverless v2 unterstützt alle für den MySQL-Client (`mysql`) und PostgreSQL-Client (`psql`) verfügbaren TLS-/SSL-Modi, einschließlich der in der folgenden Tabelle aufgeführten.

Beschreibung des TLS-/SSL-Modus	mysql-	psql
Verbinden ohne Verwendung von TLS/SSL	DISABLED	disable

Beschreibung des TLS-/SSL-Modus	mysql-	psql
Verbindung zuerst mit TLS/SSL probieren, bei Bedarf aber auf Nicht-SSL zurückgreifen	PREFERRED	bevorzugen (Standard)
Verwendung von TLS/SSL erzwingen	REQUIRED	require
SSL erzwingen und die Zertifizierungsstelle (CA) überprüfen.	VERIFY_CA	verify-ca
TLS/SSL erzwingen, CA überprüfen und CA-Hostnamen überprüfen	VERIFY_IDENTITY	verify-full

Aurora Serverless v2 nutzt Platzhalter-Zertifikate. Wenn Sie bei Verwendung von TLS/SSL die Option "CA überprüfen" oder "CA und CA-Hostnamen überprüfen" angeben, laden Sie zuerst den Amazon Root CA 1 Trust Store von Amazon Trust Services herunter. Danach können Sie diese PEM-formatierte Datei in Ihrem Client-Befehl identifizieren. Gehen Sie folgendermaßen vor, um diesen Vorgang mit dem PostgreSQL-Client auszuführen.

Für LinuxmacOS, oderUnix:

```
psql 'host=endpoint user=user sslmode=require sslrootcert=amazon-root-CA-1.pem
 dbname=db-name'
```

Weitere Informationen zum Arbeiten mit der Aurora PostgreSQL-Datenbank unter Verwendung des Postgres-Clients finden Sie unter Herstellen einer Verbindung zu einer DB-Instance, in der die PostgreSQL-Datenbank-Engine ausgeführt wird.

Weitere Informationen zum Verbinden mit Aurora-DB-Clustern im Allgemeinen finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

Unterstützte Verschlüsselungssammlungen für Verbindungen mit Aurora Serverless v2-DB-Clustern

Durch die Verwendung von konfigurierbaren Chiffrier-Suiten können Sie mehr Kontrolle über die Sicherheit Ihrer Datenbankverbindungen haben. Sie können eine Liste von Verschlüsselungssammlungen angeben, die Sie zum Sichern von TLS/SSL-Verbindungen zu Ihrer Datenbank des Clients zulassen möchten. Mit konfigurierbaren Chiffrier-Suiten können Sie die Verbindungsverschlüsselung steuern, die Ihr Datenbankserver akzeptiert. Dadurch wird die Verwendung von Verschlüsselungsverfahren verhindert, die nicht sicher sind oder nicht mehr verwendet werden.

Aurora Serverless v2-DB-Cluster, die auf Aurora MySQL basieren, unterstützen dieselben Verschlüsselungssammlungen wie von Aurora MySQL bereitgestellte DB-Cluster. Weitere Informationen über diese Verschlüsselungssammlungen finden Sie unter Konfigurieren von Cipher-Suites für Verbindungen mit Aurora-MySQL-DB-Clustern.

Aurora Serverless v2-DB-Cluster, die auf Aurora MySQL basieren, unterstützen dieselben Verschlüsselungssammlungen wie von Aurora PostgreSQL bereitgestellte DB-Cluster. Weitere Informationen über diese Verschlüsselungssammlungen finden Sie unter Konfigurieren von Chiffrier-Suiten für Verbindungen mit Aurora-PostgreSQL-DB-Clustern.

Anzeigen von Aurora Serverless v2-Writern und -Readern

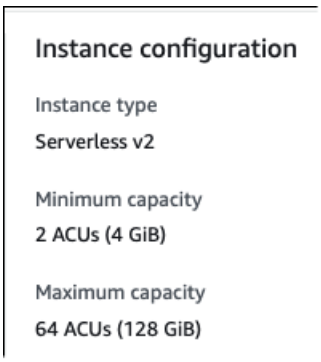
Sie können sich die Details von Aurora Serverless v2-DB-Instances auf die gleiche Weise anzeigen lassen wie für bereitgestellte DB-Instances. Befolgen Sie hierzu das allgemeine Verfahren unter Anzeigen eines Amazon Aurora-DB-Clusters. Ein Cluster könnte alle Aurora Serverless v2-DB-Instances, alle bereitgestellten DB-Instances oder jeweils einige davon enthalten.

Nachdem Sie eine oder mehrere Aurora Serverless v2-DB-Instances erstellt haben, können Sie anzeigen, welche DB-Instances den Typ Serverless (Serverlos) und welche den Typ Instance haben. Außerdem können Sie die minimalen und maximalen Aurora-Kapazitätseinheiten (ACUs) anzeigen, die die Aurora Serverless v2-DB-Instance verwenden kann. Jede ACU ist eine Kombination aus Rechenkapazität (CPU) und Arbeitsspeicherkapazität (RAM). Dieser Kapazitätsbereich gilt für jede Aurora Serverless v2-DB-Instance im Cluster. Informationen zum Verfahren zur Überprüfung des Kapazitätsbereichs eines Clusters oder einer Aurora Serverless v2-DB-Instance im Cluster finden Sie unter Überprüfen des Kapazitätsbereichs für Aurora Serverless v2.

In der AWS Management Console sind Aurora Serverless v2 DB-Instances in der Spalte Größe auf der Datenbankseite markiert. Bei bereitgestellten DB-Instances wird der Name einer DB-Instance-

Klasse wie r6g.xlarge angezeigt. Die Aurora Serverless-DB-Instances zeigen Serverless (Serverlos) für die DB-Instance-Klasse sowie die minimale und maximale Kapazität der DB-Instance an. Es wird beispielsweise Serverless v2 (4–64 ACUs) oder Serverless v2 (1–40 ACUs) angezeigt.

Die gleichen Informationen finden Sie auf dem Tab Configuration (Konfiguration) für jede Aurora Serverless v2-DB-Instance in der Konsole. Sie sehen beispielsweise einen Abschnitt Instance type (Instance-Typ) wie den folgenden. Hier ist der Wert Instance type (Instance-Typ) Serverless v2, der Wert Minimum capacity (Minimale Kapazität) beträgt 2 ACUs (4 GiB) und der Wert Maximum capacity (Maximale Kapazität) ist auf 64 ACUs (128 GiB) festgelegt.



Sie können die Kapazität jeder einzelnen Aurora Serverless v2-DB-Instance im Zeitverlauf überwachen. Auf diese Weise können Sie die minimalen, maximalen und durchschnittlichen ACUs überprüfen, die von jeder DB-Instance verbraucht werden. Sie können auch überprüfen, wie nahe die DB-Instance an ihre minimale oder maximale Kapazität gekommen ist. Um solche Details in der zu sehen AWS Management Console, sehen Sie sich die Diagramme der CloudWatch Amazon-Metriken auf der Registerkarte Überwachung für die DB-Instance an. Weitere Informationen über die angezeigten Metriken und ihre Interpretation finden Sie unter Wichtige CloudWatch Amazon-Metriken für Aurora Serverless v2.

Protokollierung für Aurora Serverless v2

Wenn Sie die Datenbankprotokollierung aktivieren möchten, geben Sie die Protokolle an, die mithilfe von Konfigurationsparametern in Ihrer benutzerdefinierten Parametergruppe aktiviert werden sollen.

Für Aurora MySQL können Sie die folgenden Protokolle aktivieren.

Aurora MySQL	Beschreibung
`general_log`	Erstellt das allgemeine Protokoll. Stellen Sie zum Einschalten auf 1. Die Standardeinstellung ist aus (0).
`log_queries_not_using_indexes`	Protokolliert alle Abfragen im Slow-Query-Protokoll, das keinen Index verwendet. Die Standardeinstellung ist aus (0). Stellen Sie auf 1 ein, um dieses Protokoll zu aktivieren.
`long_query_time`	Verhindert, dass Fast-Running-Queries im langsamen Slow-Query-Protokoll protokoll iert werden. Kann auf einen Gleitkommawert zwischen 0 und 31536000 gesetzt werden. Die Standardeinstellung ist 0 (nicht aktiv).
`server_audit_events`	Die Liste der Ereignisse, die in den Protokollen erfasst werden sollen. Unterstützte Werte sind `CONNECT`, `QUERY`, `QUERY_DCL` , `QUERY_DDL` , `QUERY_DML` und `TABLE`.
`server_audit_logging`	Setzen Sie den Parameter auf 1, um die Serverprüfungsprotokollierung zu aktivieren. Wenn Sie diese Option aktivieren, können Sie die Prüfereignisse angeben, an die gesendet CloudWatch werden soll, indem Sie sie im `server_audit_events` Parameter auflisten.
`slow_query_log`	Erstellt ein Slow-Query-Protokoll. Auf 1 setzen, um das Slow-Query-Protokoll zu aktivieren. Die Standardeinstellung ist aus (0).

Weitere Informationen finden Sie unter Verwenden von Advanced Auditing in einem Amazon Aurora MySQL DB-Cluster.

Für Aurora PostgreSQL können Sie die folgenden Protokolle auf Ihren Aurora Serverless v2-DB-Instances aktivieren.

Aurora PostgreSQL	Beschreibung
`log_connections`	Protokolliert jede erfolgreiche Verbindung.
`log_disconnections`	Protokolliert das Ende einer Sitzung einschließlich der Dauer.
`log_lock_waits`	Der Standardwert ist 0 (aus). Stellen Sie auf 1 ein, um die Wartezeiten für die Sperrung zu protokollieren.
`log_min_duration_statement`	Die Mindestdauer (in Millisekunden), die eine Anweisung vor der Protokollierung ausgeführt wird.
`log_min_messages`	Legt die Nachrichtenebenen fest, die protokolliert werden. Unterstützte Werte sind , , , , , , , , , , und `debug5`, `debug4`, `debug3`, `debug2`, `debug1`, `info`, `notice`, `warning`, `error`, `log`, `fatal`, `panic`. Zum Protokollieren von Leistungsdaten im `postgres`-Protokoll, setzen Sie den Wert auf `debug1` .
`log_temp_files`	Protokolliert die Verwendung von temporären Dateien, die über den angegebenen Kilobyte (kB) liegen.
`log_statement`	Steuert die spezifischen SQL-Anweisungen, die protokolliert werden. Unterstützte Werte sind `none`, `ddl`, `mod` und `all`. Der Standardwert ist `none`.

Themen

- Protokollierung mit Amazon CloudWatch

- Aurora Serverless v2Logs in Amazon anzeigen CloudWatch
- Kapazität mit Amazon überwachen CloudWatch

Protokollierung mit Amazon CloudWatch

Nachdem Sie das Verfahren unter verwendet haben, Protokollierung für Aurora Serverless v2 um auszuwählen, welche Datenbankprotokolle aktiviert werden sollen, können Sie auswählen, welche Protokolle auf Amazon hochgeladen („veröffentlicht“) werden sollen CloudWatch.

Sie können Amazon verwenden CloudWatch , um Protokolldaten zu analysieren, Alarme zu erstellen und Metriken anzuzeigen. Standardmäßig sind Fehlerprotokolle für aktiviert und Aurora Serverless v2 werden automatisch in hochgeladen CloudWatch. Sie können auch andere Protokolle von Aurora Serverless v2 DB-Instances in hochladen CloudWatch.

Dann wählen Sie aus, in welche dieser Protokolle Sie hochladen möchten CloudWatch, indem Sie die Einstellungen für Protokollexporte in AWS Management Console oder die `--enable-cloudwatch-logs-exports` Option in der verwenden AWS CLI.

Sie können wählen, in welche Ihrer Aurora Serverless v2 Protokolle Sie hochladen möchten CloudWatch. Weitere Informationen finden Sie unter Verwenden von Advanced Auditing in einem Amazon Aurora MySQL DB-Cluster.

Wie bei jedem Typ von Aurora-DB-Cluster können Sie die standardmäßige DB-Cluster-Parametergruppe nicht ändern. Erstellen Sie stattdessen Ihre eigene DB-Cluster-Parametergruppe basierend auf einem Standardparameter für Ihren DB-Cluster und Engine-Typ. Sie sollten Ihre benutzerdefinierte DB-Cluster-Parametergruppe erstellen, bevor Sie Ihren Aurora Serverless v2-DB-Cluster erstellen, damit Sie diese auswählen können, wann Sie eine Datenbank in der Konsole erstellen.

> **Note**
>
> Bei Aurora Serverless v2 können Sie sowohl DB-Cluster- als auch DB-Parametergruppen erstellen. Im Gegensatz dazu können Sie bei Aurora Serverless v1 nur DB-Cluster-Parametergruppen erstellen.

Aurora Serverless v2Logs in Amazon anzeigen CloudWatch

Nachdem Sie das Verfahren unter Protokollierung mit Amazon CloudWatch verwendet haben, um auszuwählen, welche Datenbankprotokolle aktiviert werden sollen, können Sie den Inhalt der Protokolle anzeigen.

Weitere Informationen zur Verwendung CloudWatch mit Aurora MySQL- und Aurora PostgreSQL-Protokollen finden Sie unter Überwachen von Protokollereignissen in Amazon CloudWatch und. Veröffentlichen von Aurora-PostgreSQL-Protokollen in Amazon CloudWatch Logs

So zeigen Sie Protokolle für Ihren Aurora Serverless v2-DB-Cluster an:

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wähle deine AWS-Region.
3. Wählen Sie Protokollgruppen.
4. Wählen Sie Ihr DB-Cluster-Protokoll für Aurora Serverless v2 in der Liste aus. Bei Protokollen ist das Benennungsmuster wie folgt.

   ```
   /aws/rds/cluster/cluster-name/log_type
   ```

> **Note**
>
> Für Aurora-MySQL-kompatible DB-Cluster von Aurora Serverless v2 enthält das Fehlerprotokoll auch dann Skalierungsereignisse für Pufferpools, wenn keine Fehler vorliegen.

Kapazität mit Amazon überwachen CloudWatch

Mit Aurora Serverless v2 CloudWatch können Sie die Kapazität und Auslastung aller Aurora Serverless v2 DB-Instances in Ihrem Cluster überwachen. Sie können Metriken auf Instance-Ebene anzeigen, um die Kapazität jeder einzelnen Aurora Serverless v2-DB-Instance beim Hoch- und Herunterskalieren zu überprüfen. Sie können die kapazitätsbezogenen Metriken auch mit anderen Metriken vergleichen, um zu sehen, wie sich Änderungen an Workloads auf den Ressourcenverbrauch auswirken. Sie können beispielsweise `ServerlessDatabaseCapacity` mit `DatabaseUsedMemory`, `DatabaseConnections` und `DMLThroughput` vergleichen, um einzuschätzen, wie Ihr DB-Cluster während des Betriebs reagiert. Weitere Informationen zu den

kapazitätsbezogenen Metriken, die für Aurora Serverless v2 gelten, finden Sie unter Wichtige CloudWatch Amazon-Metriken für Aurora Serverless v2.

So überwachen Sie die Kapazität Ihres Aurora Serverless v2-DB-Clusters:

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Metrics (Metriken) aus. Alle verfügbaren Metriken werden in der Konsole als Karten angezeigt, gruppiert nach Servicename.
3. Wählen Sie RDS.
4. (Optional) Verwenden Sie das Feld Suchen (Search), um die Metriken zu finden, die für Aurora Serverless v2 besonders wichtig sind: `ServerlessDatabaseCapacity`, `ACUUtilization`, `CPUUtilization` und `FreeableMemory`.

Wir empfehlen Ihnen, ein CloudWatch Dashboard einzurichten, um Ihre Aurora Serverless v2 DB-Cluster-Kapazität anhand der kapazitätsbezogenen Metriken zu überwachen. Wie das geht, erfahren Sie unter Dashboards erstellen mit. CloudWatch

Weitere Informationen zur Verwendung von Amazon CloudWatch mit Amazon Aurora finden Sie unterVeröffentlichen von Amazon Aurora MySQL-Protokollen in Amazon CloudWatch Logs.

Performance und Skalierung für Aurora Serverless v2

Die folgenden Verfahren und Beispiele zeigen, wie Sie den Kapazitätsbereich für Aurora Serverless v2-Cluster und ihre zugehörigen DB-Instances festlegen können. Sie können die folgenden Verfahren auch verwenden, um zu überwachen, wie ausgelastet Ihre DB-Instances sind. Anschließend können Sie anhand Ihrer Ergebnisse feststellen, ob Sie den Kapazitätsbereich nach oben oder unten anpassen müssen.

Stellen Sie sicher, dass Sie mit der Funktionsweise der Skalierung in Aurora Serverless v2 vertraut sind. Der Skalierungsmechanismus ist anders als in Aurora Serverless v1. Details hierzu finden Sie unter Aurora Serverless v2-Skalierung.

Inhalt

Auswählen des Aurora Serverless v2-Kapazitätsbereichs für einen Aurora-Cluster

Bei Aurora Serverless v2-DB-Instances legen Sie den Kapazitätsbereich, der für alle DB-Instances in Ihrem DB-Cluster gilt, beim Hinzufügen der ersten Aurora Serverless v2-DB-Instance zum DB-Cluster fest. Weitere Informationen zum entsprechenden Verfahren finden Sie unter Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster.

Sie können den Kapazitätsbereich für einen vorhandenen Cluster auch ändern. In den folgenden Abschnitten wird ausführlicher beschrieben, wie Sie geeignete Mindest- und Höchstwerte auswählen und was passiert, wenn Sie den Kapazitätsbereich ändern. Durch Ändern des Kapazitätsbereichs können sich beispielsweise die Standardwerte einiger Konfigurationsparameter ändern. Das Anwenden aller Parameteränderungen kann einen Neustart jeder Aurora Serverless v2-DB-Instance erfordern.

Themen

- Beispiel: Ändern des Aurora Serverless v2-Kapazitätsbereichs eines Aurora-PostgreSQL-Clusters

Auswählen der minimalen Aurora Serverless v2-Kapazitätseinstellung für einen Cluster

Es ist verlockend, immer 0,5 für die miminale Aurora Serverless v2-Kapazitätseinstellung auszuwählen. Dieser Wert ermöglicht es der DB-Instance, am meisten herunterzuskalieren, wenn sie vollständig inaktiv ist. Je nachdem, wie Sie diesen Cluster verwenden und wie die anderen Einstellungen konfiguriert sind, ist jedoch ein anderer Wert ggf. am effektivsten. Berücksichtigen Sie bei der Auswahl der Mindestkapazitätseinstellung die folgenden Faktoren:

- Die Skalierungsrate für eine Aurora Serverless v2-DB-Instance hängt von ihrer aktuellen Kapazität ab. Je höher die aktuelle Kapazität, desto schneller kann sie hochskalieren. Wenn die DB-Instance schnell auf eine sehr hohe Kapazität hochskalieren muss, sollten Sie die Mindestkapazität auf einen Wert einstellen, bei dem die Skalierungsrate Ihren Anforderungen entspricht.
- Wenn Sie die DB-Instance-Klasse Ihrer DB-Instances in Erwartung einer besonders hohen oder niedrigen Workload in der Regel ändern, können Sie diese Erfahrung verwenden, um den entsprechenden Aurora Serverless v2-Kapazitätsbereich grob einzuschätzen. Informationen zum Ermitteln der Speichergröße, die in Zeiten mit geringem Datenverkehr verwendet werden soll, finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.

  Angenommen, Sie verwenden die DB-Instance-Klasse db.r6g.xlarge, wenn Ihr Cluster eine geringe Workload hat. Diese DB-Instance-Klasse verfügt über 32 GiB Speicher. Somit können Sie eine minimale Einstellung der Aurora-Kapazitätseinheit (ACU) von 16 angeben, um eine Aurora Serverless v2-DB-Instance einzurichten, die auf ungefähr dieselbe Kapazität herunterskalieren kann. Das liegt daran, dass jede ACU ungefähr 2 GiB Speicher entspricht. Sie können einen etwas niedrigeren Wert angeben, damit die DB-Instance weiter herunterskaliert wird, falls Ihre db.r6g.xlarge-DB-Instance manchmal nicht ausgelastet war.
- Wenn Ihre Anwendung dann am effizientesten arbeitet, wenn die DB-Instances eine bestimmte Datenmenge im Puffer-Cache haben, sollten Sie eine minimale ACU-Einstellung angeben, bei der der Speicher groß genug ist, um die häufig aufgerufenen Daten zu speichern. Andernfalls werden einige Daten im Puffer-Cache bereinigt, wenn Aurora Serverless v2-DB-Instances auf eine niedrigere Speichergröße herunterskalieren. Wenn die DB-Instances dann wieder hochskaliert werden, werden die Informationen im Zeitverlauf wieder in den Puffer-Cache eingelesen. Wenn für das Einlesen der Daten wieder in den Puffercache eine erhebliche I/O-Menge erforderlich ist, ist es möglicherweise effektiver, einen höheren minimalen ACU-Wert auszuwählen.
- Wenn Ihre Aurora Serverless v2-DB-Instances die meiste Zeit mit einer bestimmten Kapazität ausgeführt werden, erwägen Sie, eine Mindestkapazitätseinstellung anzugeben, die zwar niedriger

als diese Baseline, aber nicht zu niedrig ist. Aurora Serverless v2 DB-Instances können am effektivsten abschätzen, wie viel und wie schnell hochskaliert werden muss, wenn die aktuelle Kapazität nicht deutlich niedriger als die erforderliche Kapazität ist.

- Wenn Ihre bereitgestellte Workload Speicheranforderungen hat, die für kleine DB-Instance-Klassen wie T3 oder T4g zu hoch sind, wählen Sie eine minimale ACU-Einstellung, die ähnlichen Speicher bietet wie eine R5- oder R6g-DB-Instance.

  Insbesondere empfehlen wir die folgende Mindestkapazität für die Verwendung mit den angegebenen Funktionen (diese Empfehlungen können sich ändern):

  - Performance Insights – 2 ACUs
  - Globale Aurora-Datenbanken – 8 ACUs (gilt nur für die primäre AWS-Region)
- In einigen Fällen enthält Ihr Cluster möglicherweise Aurora Serverless v2-Reader-DB-Instances, die unabhängig vom Writer skalieren. In einem solchen Fall wählen Sie eine Mindestkapazitätseinstellung aus, die hoch genug ist, damit die Reader-DB-Instances die Änderungen vom Writer anwenden können, ohne in Rückstand zu geraten, wenn die Writer-DB-Instance mit einer schreibintensiven Workload beschäftigt ist. Wenn Sie die Replikatverzögerung bei Readern beobachten, die sich in den Hochstufungsstufen 2 bis 15 befinden, sollten Sie die Mindestkapazitätseinstellung für Ihren Cluster ggf. erhöhen. Weitere Informationen zur Entscheidung, ob Reader-DB-Instances zusammen mit dem Writer oder unabhängig skaliert werden, finden Sie unter Auswählen der Hochstufungsstufe für einen Aurora Serverless v2-Reader.
- Wenn Sie einen DB-Cluster mit Aurora Serverless v2 Leser-DB-Instances haben, skalieren die Leser nicht zusammen mit der Writer-DB-Instance, wenn die Promotion-Stufe der Leser nicht 0 oder 1 ist. In diesem Fall kann das Festlegen einer geringen Mindestkapazität zu einer übermäßigen Replikationsverzögerung führen. Das liegt daran, dass die Reader möglicherweise nicht genug Kapazität haben, um Änderungen vom Writer zu übernehmen, wenn die Datenbank ausgelastet ist. Wir empfehlen, dass Sie die Mindestkapazität auf einen Wert festlegen, der einer vergleichbaren Speicher- und CPU-Menge entspricht wie bei der Writer-DB-Instance.
- Der Wert des `max_connections`-Parameters für Aurora Serverless v2-DB-Instances basiert auf der Speichergröße, die von den maximalen ACUs abgeleitet wird. Wenn Sie jedoch eine Mindestkapazität von 0,5 ACUs auf PostgreSQL-kompatible DB-Instances angeben,`max_connections` ist der Höchstwert bei 2.000 begrenzt.

  Wenn Sie beabsichtigen, den Aurora-PostgreSQL-Cluster für einen Workload mit hohem Verbindungsdurchsatz zu verwenden, sollten Sie eine Mindest-ACU-Einstellung von 1 oder höher verwenden. Details darüber, wie Aurora Serverless v2 den `max_connections`-

Konfigurationsparameter behandelt, finden Sie unter Maximale Anzahl der Verbindungen für Aurora Serverless v2.

- Die Zeit, die eine Aurora Serverless v2-DB-Instance benötigt, um von ihrer minimalen Kapazität auf ihre maximale Kapazität zu skalieren, hängt von der Differenz zwischen ihren minimalen und maximalen ACU-Werten ab. Wenn die aktuelle Kapazität der DB-Instance groß ist, skaliert Aurora Serverless v2 in größeren Schritten, als wenn die DB-Instance mit einer geringen Kapazität beginnt. Wenn Sie also eine relativ große maximale Kapazität angeben und die DB-Instance die meiste Zeit in diesem Kapazitätsbereich bleibt, sollten Sie erwägen, die minimale ACU-Einstellung zu erhöhen. Auf diese Weise kann eine inaktive DB-Instance schneller wieder auf maximale Kapazität skaliert werden.

Auswählen der maximalen Aurora Serverless v2-Kapazitätseinstellung für einen Cluster

Es ist verlockend, immer einen hohen Wert für die maximale Aurora Serverless v2-Kapazitätseinstellung auszuwählen. Eine große maximale Kapazität ermöglicht es der DB-Instance, bei intensiver Workload am stärksten hochzuskalieren. Mit einem niedrigen Wert entfällt die Möglichkeit unerwarteter Gebühren. Je nachdem, wie Sie diesen Cluster verwenden und die anderen Einstellungen konfigurieren, kann der effektivste Wert höher oder niedriger sein, als Sie ursprünglich dachten. Berücksichtigen Sie bei der Auswahl der maximalen Kapazitätseinstellung die folgenden Faktoren:

- Die maximale Kapazität muss mindestens so hoch sein wie die Mindestkapazität. Sie können die minimale und maximale Kapazität auf den gleichen Wert festlegen. In diesem Fall skaliert sich die Kapazität jedoch niemals hoch oder herunter. Daher ist die Verwendung identischer Werte für die minimale und maximale Kapazität außerhalb von Testsituationen nicht geeignet.
- Die maximale Kapazität muss höher als 0,5 ACU sein. Sie können die minimale und maximale Kapazität in den meisten Fällen auf den gleichen Wert festlegen. Sie können 0,5 jedoch nicht sowohl für das Minimum als auch für das Maximum angeben. Verwenden Sie einen Wert von 1 oder höher für die maximale Kapazität.
- Wenn Sie die DB-Instance-Klasse Ihrer DB-Instances in Erwartung einer besonders hohen oder niedrigen Workload in der Regel ändern, können Sie diese Erfahrung verwenden, um den entsprechenden Aurora Serverless v2-Kapazitätsbereich einzuschätzen. Informationen zum Ermitteln der Speichergröße, die in Zeiten mit hohem Datenverkehr verwendet werden soll, finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.

Angenommen, Sie verwenden die DB-Instance-Klasse db.r6g.4xlarge, wenn Ihr Cluster eine hohe Workload hat. Diese DB-Instance-Klasse verfügt über 128 GiB Speicher. Somit können Sie eine maximale ACU-Einstellung von 64 angeben, um eine Aurora Serverless v2-DB-Instance einzurichten, die auf ungefähr dieselbe Kapazität hochskalieren kann. Das liegt daran, dass jede ACU ungefähr 2 GiB Speicher entspricht. Sie können einen etwas höheren Wert angeben, damit die DB-Instance weiter hochskalieren kann, falls Ihre db.r6g.4xlarge-DB-Instance manchmal nicht genug Kapazität hat, um die Workload effektiv zu bewältigen.

- Wenn Sie eine Haushaltsobergrenze für Ihre Datenbankauslastung haben, wählen Sie einen Wert, der innerhalb dieser Obergrenze bleibt, auch wenn alle Ihre Aurora Serverless v2-DB-Instances ständig mit maximaler Kapazität laufen. Denken Sie daran, dass wenn Sie n Aurora Serverless v2-DB-Instances in Ihrem Cluster haben, die theoretische maximale Aurora Serverless v2-Kapazität, die der Cluster jederzeit verbrauchen kann, n-mal die maximale ACU-Einstellung für den Cluster ist. (Der tatsächlich verbrauchte Betrag ist möglicherweise geringer, wenn beispielsweise einige Reader unabhängig vom Writer skalieren.)
- Wenn Sie Aurora Serverless v2-Reader-DB-Instances dazu verwenden, den schreibgeschützten Workload der Writer-DB-Instance teilweise auszulagern, können Sie möglicherweise eine niedrigere Maximalkapazitätseinstellung auswählen. Damit berücksichtigen Sie die Tatsache, dass jede Reader-DB-Instance nicht gleichermaßen hoch skaliert werden muss wie im Falle, dass der Cluster nur eine einzelne DB-Instance enthält.
- Angenommen, Sie möchten sich vor übermäßiger Auslastung aufgrund falsch konfigurierter Datenbankparameter oder ineffizienter Abfragen in Ihrer Anwendung schützen. In diesem Fall können Sie eine versehentliche Überbeanspruchung vermeiden, indem Sie eine maximale Kapazitätseinstellung wählen, die niedriger ist als die absolut höchste, die Sie festlegen können.
- Wenn Spitzen aufgrund realer Benutzeraktivitäten zwar selten sind, aber dennoch auftreten, können Sie diese Situationen bei der Auswahl der maximalen Kapazitätseinstellung berücksichtigen. Wenn die Priorität darin besteht, dass die Anwendung weiterhin mit voller Leistung und Skalierbarkeit ausgeführt wird, können Sie eine maximale Kapazitätseinstellung angeben, die höher ist, als Sie bei normaler Auslastung beobachten. Wenn es akzeptabel ist, dass die Anwendung bei sehr extremen Aktivitätsspitzen mit reduziertem Durchsatz ausgeführt wird, können Sie eine etwas niedrigere maximale Kapazitätseinstellung wählen. Stellen Sie sicher, dass Sie eine Einstellung auswählen, die immer noch über genügend Speicher- und CPU-Ressourcen verfügt, damit die Anwendung weiterhin ausgeführt wird.
- Wenn Sie Einstellungen in Ihrem Cluster aktivieren, die die Speicherauslastung für jede DB-Instance erhöhen, berücksichtigen Sie diesen Speicher bei der Entscheidung über den maximalen ACU-Wert. Zu diesen Einstellungen gehören diejenigen für Performance Insights, parallele Aurora

MySQL-Abfragen, Aurora MySQL-Leistungsschema und Aurora MySQL-Binärprotokollreplikation. Stellen Sie sicher, dass der maximale ACU-Wert Aurora Serverless v2-DB-Instances erlaubt, ausreichend hoch zu skalieren, um die Workload zu bewältigen, wenn diese Funktion verwendet wird. Informationen zur Fehlerbehebung von Problemen, die durch die Kombination einer niedrigen maximalen ACU-Einstellung und Aurora-Funktionen verursacht werden, die Speicher-Overhead verursachen, finden Sie unter Fehler vermeiden out-of-memory .

Beispiel: Ändern des Aurora Serverless v2-Kapazitätsbereichs eines Aurora-MySQL-Clusters

Das folgende AWS CLI Beispiel zeigt, wie der ACU-Bereich für Aurora Serverless v2 DB-Instances in einem vorhandenen Aurora MySQL-Cluster aktualisiert wird. Anfänglich beträgt der Kapazitätsbereich für den Cluster 8 bis 32 ACUs.

```
aws rds describe-db-clusters --db-cluster-identifier serverless-v2-cluster \
  --query 'DBClusters[*].ServerlessV2ScalingConfiguration|[0]'
{
    "MinCapacity": 8.0,
    "MaxCapacity": 32.0
}
```

Die DB-Instance ist inaktiv und wird auf 8 ACUs herunterskaliert. Die folgenden kapazitätsbezogenen Einstellungen gelten zu diesem Zeitpunkt für die DB-Instance. Zum Darstellen der Größe des Pufferpools in leicht lesbaren Einheiten teilen wir ihn durch 2 hoch 30, was zu einer Messung in Gibibyte (GiB) führt. Das liegt daran, dass speicherbezogene Messungen für Aurora Einheiten verwenden, die auf Zweierpotenzen und nicht auf Zehnerpotenzen basieren.

```
mysql> select @@max_connections;
+-------------------+
| @@max_connections |
+-------------------+
|              3000 |
+-------------------+
1 row in set (0.00 sec)

mysql> select @@innodb_buffer_pool_size;
+---------------------------+
| @@innodb_buffer_pool_size |
+---------------------------+
```

```
|                9294577664 |
+---------------------------+
1 row in set (0.00 sec)

mysql> select @@innodb_buffer_pool_size / pow(2,30) as gibibytes;
+-----------+
| gibibytes |
+-----------+
|   8.65625 |
+-----------+
1 row in set (0.00 sec)
```

Als Nächstes ändern wir den Kapazitätsbereich für den Cluster. Nachdem der `modify-db-cluster`-Befehl abgeschlossen ist, beträgt der ACU-Bereich für den Cluster 12,5 bis 80.

```
aws rds modify-db-cluster --db-cluster-identifier serverless-v2-cluster \
  --serverless-v2-scaling-configuration MinCapacity=12.5,MaxCapacity=80

aws rds describe-db-clusters --db-cluster-identifier serverless-v2-cluster \
  --query 'DBClusters[*].ServerlessV2ScalingConfiguration|[0]'
{
    "MinCapacity": 12.5,
    "MaxCapacity": 80.0
}
```

Durch Ändern des Kapazitätsbereichs können sich die Standardwerte einiger Konfigurationsparameter ändern. Aurora kann einige dieser neuen Standardwerte sofort anwenden. Einige der Parameteränderungen werden jedoch erst nach einem Neustart wirksam. Der Status `pending-reboot` gibt an, dass ein Neustart erforderlich ist, um einige Parameteränderungen anzuwenden.

```
aws rds describe-db-clusters --db-cluster-identifier serverless-v2-cluster \
  --query '*[].{DBClusterMembers:DBClusterMembers[*].
{DBInstanceIdentifier:DBInstanceIdentifier,DBClusterParameterGroupStatus:DBClusterParameterGrou
[0]'
{
    "DBClusterMembers": [
        {
            "DBInstanceIdentifier": "serverless-v2-instance-1",
            "DBClusterParameterGroupStatus": "pending-reboot"
        }
    ]
```

```
}
```

Zu diesem Zeitpunkt ist der Cluster inaktiv und die DB-Instance `serverless-v2-instance-1` verbraucht 12,5 ACUs. Der `innodb_buffer_pool_size`-Parameter ist bereits basierend auf der aktuellen Kapazität der DB-Instance angepasst. Der `max_connections`-Parameter spiegelt immer noch den Wert der früheren maximalen Kapazität wider. Das Zurücksetzen dieses Werts erfordert einen Neustart der DB-Instance.

> **Note**
>
> Wenn Sie den `max_connections` Parameter direkt in einer benutzerdefinierten DB-Parametergruppe festlegen, ist kein Neustart erforderlich.

```
mysql> select @@max_connections;
+-------------------+
| @@max_connections |
+-------------------+
|              3000 |
+-------------------+
1 row in set (0.00 sec)

mysql> select @@innodb_buffer_pool_size;
+---------------------------+
| @@innodb_buffer_pool_size |
+---------------------------+
|               15572402176 |
+---------------------------+
1 row in set (0.00 sec)

mysql> select @@innodb_buffer_pool_size / pow(2,30) as gibibytes;
+---------------+
| gibibytes     |
+---------------+
| 14.5029296875 |
+---------------+
1 row in set (0.00 sec)
```

Jetzt starten wir die DB-Instance neu und warten darauf, dass sie wieder verfügbar ist.

```
aws rds reboot-db-instance --db-instance-identifier serverless-v2-instance-1
```

```
{
  "DBInstanceIdentifier": "serverless-v2-instance-1",
  "DBInstanceStatus": "rebooting"
}

aws rds wait db-instance-available --db-instance-identifier serverless-v2-instance-1
```

Der `pending-reboot`-Status ist gelöscht. Der Wert `in-sync` bestätigt, dass Aurora alle ausstehenden Parameteränderungen übernommen hat.

```
aws rds describe-db-clusters --db-cluster-identifier serverless-v2-cluster \
  --query '*[].{DBClusterMembers:DBClusterMembers[*].
{DBInstanceIdentifier:DBInstanceIdentifier,DBClusterParameterGroupStatus:DBClusterParameterGrou
[0]'
{
    "DBClusterMembers": [
        {
            "DBInstanceIdentifier": "serverless-v2-instance-1",
            "DBClusterParameterGroupStatus": "in-sync"
        }
    ]
}
```

Der `innodb_buffer_pool_size`-Parameter hat sich auf seine endgültige Größe für eine inaktive DB-Instance erhöht. Der `max_connections`-Parameter wurde erhöht, um einen vom maximalen ACU-Wert abgeleiteten Wert widerzuspiegeln. Die Formel, die Aurora für `max_connections` verwendet, führt zu einem Anstieg von 1.000, wenn sich die Speichergröße verdoppelt.

```
mysql> select @@innodb_buffer_pool_size;
+---------------------------+
| @@innodb_buffer_pool_size |
+---------------------------+
|               16139681792 |
+---------------------------+
1 row in set (0.00 sec)

mysql> select @@innodb_buffer_pool_size / pow(2,30) as gibibytes;
+-----------+
| gibibytes |
+-----------+
|  15.03125 |
+-----------+
```

```
1 row in set (0.00 sec)

mysql> select @@max_connections;
+-------------------+
| @@max_connections |
+-------------------+
|              4000 |
+-------------------+
1 row in set (0.00 sec)
```

Wir setzen den Kapazitätsbereich auf 0,5—128 ACUs und starten die DB-Instance neu. Jetzt hat die inaktive DB-Instance eine Puffer-Cache-Größe von weniger als 1 GiB. Daher messen wir sie nun in Mebibyte (MiB). Der `max_connections`-Wert 5.000 wird von der Speichergröße der maximalen Kapazitätseinstellung abgeleitet.

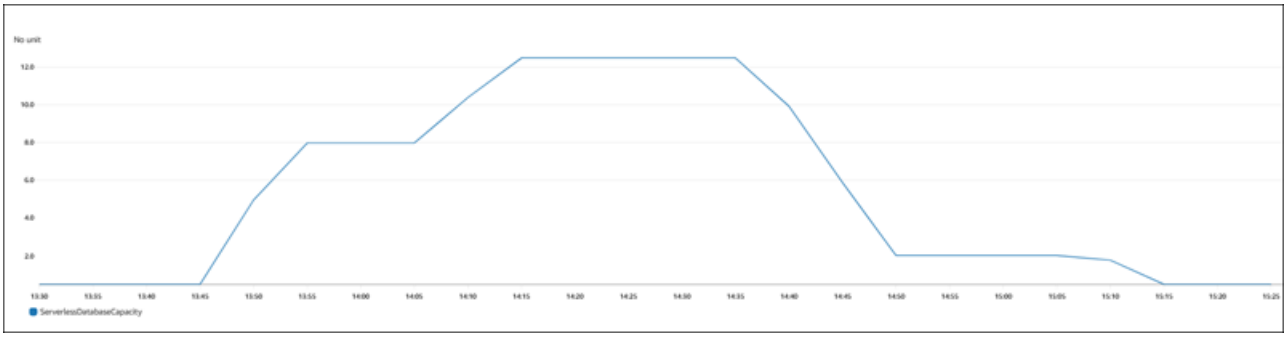
```
mysql> select @@innodb_buffer_pool_size / pow(2,20) as mebibytes, @@max_connections;
+-----------+-------------------+
| mebibytes | @@max_connections |
+-----------+-------------------+
|       672 |              5000 |
+-----------+-------------------+
1 row in set (0.00 sec)
```

Beispiel: Ändern des Aurora Serverless v2-Kapazitätsbereichs eines Aurora-PostgreSQL-Clusters

Das folgende CLI-Beispiel zeigt, wie Sie den ACU-Bereich für DB-Instances von Aurora Serverless v2 in einem bestehenden Aurora-PostgreSQL-Cluster aktualisieren.

1. Der Kapazitätsbereich für den Cluster beginnt bei 0,5 bis 1 ACU.
2. Ändern Sie den Kapazitätsbereich auf 8 bis 32 ACUs.
3. Ändern Sie den Kapazitätsbereich auf 12,5 bis 80 ACUs.
4. Ändern Sie den Kapazitätsbereich auf 0,5 bis 128 ACUs.
5. Legen Sie die Kapazität wieder auf den ursprünglichen Bereich von 0,5 bis 1 ACU fest.

Die folgende Abbildung zeigt die Kapazitätsänderungen in Amazon CloudWatch.



Die DB-Instance ist inaktiv und wird auf 0,5 ACUs herunterskaliert. Die folgenden kapazitätsbezogenen Einstellungen gelten zu diesem Zeitpunkt für die DB-Instance.

```
postgres=> show max_connections;
 max_connections
-----------------
 189
(1 row)

postgres=> show shared_buffers;
 shared_buffers
----------------
 16384
(1 row)
```

Als Nächstes ändern wir den Kapazitätsbereich für den Cluster. Nachdem der `modify-db-cluster`-Befehl abgeschlossen ist, beträgt der ACU-Bereich für den Cluster 8,0 bis 32.

```
aws rds describe-db-clusters --db-cluster-identifier serverless-v2-cluster \
  --query 'DBClusters[*].ServerlessV2ScalingConfiguration|[0]'
{
    "MinCapacity": 8.0,
    "MaxCapacity": 32.0
}
```

Durch Ändern des Kapazitätsbereichs können sich die Standardwerte einiger Konfigurationsparameter ändern. Aurora kann einige dieser neuen Standardwerte sofort anwenden. Einige der Parameteränderungen werden jedoch erst nach einem Neustart wirksam. Der Status `pending-reboot` gibt an, dass ein Neustart erforderlich ist, um einige Parameteränderungen anzuwenden.

```
aws rds describe-db-clusters --db-cluster-identifier serverless-v2-cluster \
```

```
  --query '*[].{DBClusterMembers:DBClusterMembers[*].
{DBInstanceIdentifier:DBInstanceIdentifier,DBClusterParameterGroupStatus:DBClusterParameterGrou
[0]'
{
    "DBClusterMembers": [
        {
            "DBInstanceIdentifier": "serverless-v2-instance-1",
            "DBClusterParameterGroupStatus": "pending-reboot"
        }
    ]
}
```

Zu diesem Zeitpunkt ist der Cluster inaktiv und die DB-Instance `serverless-v2-instance-1` verbraucht 8,0 ACUs. Der `shared_buffers`-Parameter ist bereits basierend auf der aktuellen Kapazität der DB-Instance angepasst. Der `max_connections`-Parameter spiegelt immer noch den Wert der früheren maximalen Kapazität wider. Das Zurücksetzen dieses Werts erfordert einen Neustart der DB-Instance.

> **Note**
>
> Wenn Sie den `max_connections` Parameter direkt in einer benutzerdefinierten DB-Parametergruppe festlegen, ist kein Neustart erforderlich.

```
postgres=> show max_connections;
 max_connections
-----------------
 189
(1 row)

postgres=> show shared_buffers;
 shared_buffers
----------------
 1425408
(1 row)
```

Wir starten die DB-Instance neu und warten darauf, dass sie wieder verfügbar ist.

```
aws rds reboot-db-instance --db-instance-identifier serverless-v2-instance-1
{
  "DBInstanceIdentifier": "serverless-v2-instance-1",
```

```
  "DBInstanceStatus": "rebooting"
}

aws rds wait db-instance-available --db-instance-identifier serverless-v2-instance-1
```

Nachdem die DB-Instance neu gestartet wurde, ist der Status `pending-reboot` gelöscht. Der Wert `in-sync` bestätigt, dass Aurora alle ausstehenden Parameteränderungen übernommen hat.

```
aws rds describe-db-clusters --db-cluster-identifier serverless-v2-cluster \
  --query '*[].{DBClusterMembers:DBClusterMembers[*].
{DBInstanceIdentifier:DBInstanceIdentifier,DBClusterParameterGroupStatus:DBClusterParameterGrou
[0]'
{
    "DBClusterMembers": [
        {
            "DBInstanceIdentifier": "serverless-v2-instance-1",
            "DBClusterParameterGroupStatus": "in-sync"
        }
    ]
}
```

Nach dem Neustart zeigt `max_connections` den Wert der neuen maximalen Kapazität an.

```
postgres=> show max_connections;
 max_connections
-----------------
 5000
(1 row)

postgres=> show shared_buffers;
 shared_buffers
----------------
 1425408
(1 row)
```

Als Nächstes ändern wir den Kapazitätsbereich für den Cluster auf 12,5 bis 80 ACUs.

```
aws rds modify-db-cluster --db-cluster-identifier serverless-v2-cluster \
  --serverless-v2-scaling-configuration MinCapacity=12.5,MaxCapacity=80

aws rds describe-db-clusters --db-cluster-identifier serverless-v2-cluster \
  --query 'DBClusters[*].ServerlessV2ScalingConfiguration|[0]'
```

```
{
    "MinCapacity": 12.5,
    "MaxCapacity": 80.0
}
```

Zu diesem Zeitpunkt ist der Cluster inaktiv und die DB-Instance `serverless-v2-instance-1` verbraucht 12,5 ACUs. Der `shared_buffers`-Parameter ist bereits basierend auf der aktuellen Kapazität der DB-Instance angepasst. Der `max_connections`-Wert beträgt immer noch 5 000.

```
postgres=> show max_connections;
 max_connections
-----------------
 5000
(1 row)

postgres=> show shared_buffers;
 shared_buffers
----------------
 2211840
(1 row)
```

Wir führen einen weiteren Neustart durch, aber die Parameterwerte bleiben gleich. Dies liegt daran, dass für `max_connections` ein Höchstwert von 5 000 für einen DB-Cluster von Aurora Serverless v2 gilt, auf dem Aurora PostgreSQL ausgeführt wird.

```
postgres=> show max_connections;
 max_connections
-----------------
 5000
(1 row)

postgres=> show shared_buffers;
 shared_buffers
----------------
 2211840
(1 row)
```

Jetzt stellen wir den Kapazitätsbereich zwischen 0,5 und 128 ACUs ein. Der DB-Cluster wird zunächst auf 10 ACUs und dann auf 2 herunterskaliert. Wir starten die DB-Instance neu.

```
postgres=> show max_connections;
```

```
 max_connections
-----------------
 2000
(1 row)

postgres=> show shared_buffers;
 shared_buffers
----------------
 16384
(1 row)
```

Der `max_connections`-Wert für DB-Instances von Aurora Serverless v2 basiert auf der Speichergröße, die von den maximalen ACUs abgeleitet wird. Wenn Sie jedoch eine Mindestkapazität von 0,5 ACUs auf PostgreSQL-kompatible DB-Instances angeben, ist der Höchstwert von `max_connections` auf 2.000 begrenzt.

Jetzt legen wir die Kapazität wieder auf den ursprünglichen Bereich von 0,5 bis 1 ACU fest und starten die DB-Instance neu. Der `max_connections`-Parameter ist auf seinen ursprünglichen Wert zurückgekehrt.

```
postgres=> show max_connections;
 max_connections
-----------------
 189
(1 row)

postgres=> show shared_buffers;
 shared_buffers
----------------
 16384
(1 row)
```

Arbeiten mit Parametergruppen für Aurora Serverless v2

Wenn Sie Ihren Aurora Serverless v2-DB-Cluster erstellen, wählen Sie eine bestimmte Aurora-DB-Engine und eine zugehörige DB-Cluster-Parametergruppe. Wenn Sie nicht damit vertraut sind, wie Aurora Parametergruppen verwendet, um Konfigurationseinstellungen konsistent auf Cluster anzuwenden, finden Sie weitere Informationen unter Arbeiten mit Parametergruppen. Alle diese Verfahren zum Erstellen, Ändern, Anwenden sowie andere Aktionen für Parametergruppen gelten für Aurora Serverless v2.

Die Parametergruppen-Funktion funktioniert im Allgemeinen für bereitgestellte Cluster und Cluster, dieAurora Serverless v2-DB-Instances enthalten, gleich:

- Die Standardparameterwerte für alle DB-Instances im Cluster werden von der Cluster-Parametergruppe definiert.
- Sie können einige Parameter für bestimmte DB-Instances überschreiben, indem Sie eine benutzerdefinierte DB-Parametergruppe für diese DB-Instances angeben. Diesen Vorgang können Sie während des Debuggens oder der Leistungsoptimierung für bestimmte DB-Instances durchführen. Angenommen, Sie haben einen Cluster, der einige Aurora Serverless v2-DB-Instances und einige bereitgestellte DB-Instances enthält. In diesem Fall können Sie mithilfe einer benutzerdefinierten DB-Parametergruppe einige andere Parameter für die bereitgestellten DB-Instances angeben.
- Bei Aurora Serverless v2 können Sie alle Parameter verwenden, die den Wert `provisioned` im `SupportedEngineModes`-Attribut der Parametergruppe aufweisen. In Aurora Serverless v1 können Sie nur die Teilmenge von Parametern verwenden, die `serverless` im `SupportedEngineModes`-Attribut enthalten.

Themen

Standard-Parameterwerte

Der entscheidende Unterschied zwischen bereitgestellten DB-Instances und Aurora Serverless v2-DB-Instances besteht darin, dass Aurora alle benutzerdefinierten Parameterwerte für bestimmte Parameter außer Kraft setzt, die sich auf die Kapazität der DB-Instance beziehen. Die benutzerdefinierten Parameterwerte gelten weiterhin für alle bereitgestellten DB-Instances in Ihrem Cluster. Weitere Details darüber, wie Aurora Serverless v2-DB-Instances die Parameter aus Aurora-Parametergruppen interpretieren, finden Sie unter Konfigurationsparameter für Aurora-Cluster. Die spezifischen Parameter, die Aurora Serverless v2 außer Kraft setzen, finden Sie unter Parameter, die Aurora anpasst, während Aurora Serverless v2 hoch- und herunterskaliert und Parameter, die Aurora basierend auf der maximalen Kapazität von Aurora Serverless v2 berechnet.

Sie können eine Liste der Standardwerte für die Standardparametergruppen für die verschiedenen Aurora-DB-Engines abrufen, indem Sie den describe-db-cluster-parametersCLI-Befehl verwenden und die AWS-Region abfragen. Die folgenden Werte können Sie für die Optionen `--db-parameter-group-family` und `-db-parameter-group-name` für Engine-Versionen verwenden, die mit Aurora Serverless v2 kompatibel sind.

Datenbank-Engine und -Version	Parametergruppenfamilie	Name der Standard-Parametergruppe
Aurora-MySQL-Version 3	`aurora-mysql8.0`	`default.aurora-mysql8.0`
Aurora-PostgreSQL-Version 13.x	`aurora-postgresql13`	`default.aurora-postgresql13`
Aurora-PostgreSQL-Version 14.x	`aurora-postgresql14`	`default.aurora-postgresql14`
Aurora-PostgreSQL-Version 15.x	`aurora-postgresql15`	`default.aurora-postgresql15`
Aurora PostgreSQL Version 16.x	`aurora-postgresql16`	`default.aurora-postgresql16`

Im folgenden Beispiel wird eine Liste von Parametern aus der Standard-DB-Cluster-Gruppe für Aurora-MySQL-Version 3 und Aurora PostgreSQL 13 abgerufen. Dies sind die Aurora-MySQL- und Aurora-PostgreSQL-Versionen, die Sie mit Aurora Serverless v2 verwenden.

FürLinux, oder: macOS Unix

```
aws rds describe-db-cluster-parameters \
  --db-cluster-parameter-group-name default.aurora-mysql8.0 \
  --query 'Parameters[*].
{ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} |
    [?contains(SupportedEngineModes, `provisioned`) == `true`] | [*].[ParameterName]' \
  --output text

aws rds describe-db-cluster-parameters \
  --db-cluster-parameter-group-name default.aurora-postgresql13 \
```

```
  --query 'Parameters[*].
{ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} |
    [?contains(SupportedEngineModes, `provisioned`) == `true`] | [*].[ParameterName]' \
  --output text
```

Windows:

```
aws rds describe-db-cluster-parameters ^
  --db-cluster-parameter-group-name default.aurora-mysql8.0 ^
  --query 'Parameters[*].
{ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} |
    [?contains(SupportedEngineModes, `provisioned`) == `true`] | [*].[ParameterName]' ^
  --output text

aws rds describe-db-cluster-parameters ^
  --db-cluster-parameter-group-name default.aurora-postgresql13 ^
  --query 'Parameters[*].
{ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} |
    [?contains(SupportedEngineModes, `provisioned`) == `true`] | [*].[ParameterName]' ^
  --output text
```

Maximale Anzahl der Verbindungen für Aurora Serverless v2

Sowohl für Aurora MySQL als auch für Aurora PostgreSQL halten Aurora Serverless v2-DB-Instances den Parameter `max_connections` konstant, damit Verbindungen nicht unterbrochen werden, wenn die DB-Instance herunterskaliert wird. Der Standardwert für diesen Parameter leitet sich von einer Formel ab, die auf der Speichergröße der DB-Instance beruht. Weitere Informationen zur Formel und zu den Standardwerten für bereitgestellte DB-Instance-Klassen finden Sie unter Maximale Verbindungen zu einer Aurora MySQL-DB-Instance und Maximale Verbindungen zu einer Aurora PostgreSQL-DB-Instance.

Wenn Aurora Serverless v2 die Formel auswertet, verwendet es die Speichergröße basierend auf den maximalen Aurora-Kapazitätseinheiten (ACUs) für die DB-Instance, nicht den aktuellen ACU-Wert. Wenn Sie den Standardwert ändern, empfehlen wir, eine Variante der Formel zu verwenden, anstatt einen konstanten Wert anzugeben. Auf diese Weise kann Aurora Serverless v2 basierend auf der maximalen Kapazität eine angemessene Einstellung verwenden.

Wenn Sie die maximale Kapazität eines DB-Clusters von Aurora Serverless v2 ändern, müssen Sie die DB-Instances von Aurora Serverless v2 neu starten, um den `max_connections`-Wert zu aktualisieren. Dies liegt daran, dass es sich bei `max_connections` um einen statischen Parameter für Aurora Serverless v2 handelt.

Die folgende Tabelle zeigt die Standardwerte für `max_connections` für Aurora Serverless v2 basierend auf dem maximalen ACU-Wert.

Maximale ACUs	Standardmäßige maximale Verbindungen für Aurora MySQL	Standardmäßige maximale Verbindungen für Aurora PostgreSQL
1	90	189
4	135	823
8	1.000	1.669
16	2.000	3.360
32	3,000	5,000
64	4.000	5,000
128	5,000	5,000

> **Note**
>
> Der `max_connections`-Wert für DB-Instances von Aurora Serverless v2 basiert auf der Speichergröße, die von den maximalen ACUs abgeleitet wird. Wenn Sie jedoch eine Mindestkapazität von 0,5 ACUs auf PostgreSQL-kompatible DB-Instances angeben,ist der Höchstwert von `max_connections` auf 2.000 begrenzt.

Konkrete Beispiele, die zeigen, wie sich `max_connections` mit dem maximalen ACU-Wert ändert, finden Sie unter Beispiel: Ändern des Aurora Serverless v2-Kapazitätsbereichs eines Aurora-MySQL-Clusters und Beispiel: Ändern des Aurora Serverless v2-Kapazitätsbereichs eines Aurora-PostgreSQL-Clusters.

Parameter, die Aurora anpasst, während Aurora Serverless v2 hoch- und herunterskaliert

Bei der automatischen Skalierung muss Aurora Serverless v2 in der Lage sein, Parameter zu ändern, damit jede DB-Instance optimal für die erhöhte oder verringerte Kapazität funktioniert. Daher können Sie einige Parameter im Zusammenhang mit der Kapazität nicht außer Kraft setzen. Vermeiden Sie bei einigen Parametern, die Sie außer Kraft setzen können, eine Hartcodierung fester Werte. Die folgenden Überlegungen gelten für diese Einstellungen, die sich auf die Kapazität beziehen.

Bei Aurora MySQL ändert Aurora Serverless v2 die Größe einiger Parameter während der Skalierung dynamisch. Für die folgenden Parameter verwendet Aurora Serverless v2 keine benutzerdefinierten Parameterwerte, die Sie angeben:

- `innodb_buffer_pool_size`
- `innodb_purge_threads`
- `table_definition_cache`
- `table_open_cache`

Bei Aurora PostgreSQL ändert Aurora Serverless v2 die Größe der folgenden Parameter während der Skalierung dynamisch. Für die folgenden Parameter verwendet Aurora Serverless v2 keine benutzerdefinierten Parameterwerte, die Sie angeben:

- `shared_buffers`

Für alle anderen Parameter als die hier aufgelisteten funktionieren DB-Instances von Aurora Serverless v2 genauso wie bereitgestellte DB-Instances. Der Standardparameterwert wird von der Cluster-Parametergruppe geerbt. Sie können den Standardwert für den gesamten Cluster mit einer benutzerdefinierten Cluster-Parametergruppe ändern. Den Standardwert für bestimmte DB-Instances können Sie auch mithilfe einer benutzerdefinierten DB-Parametergruppe ändern. Die dynamischen Parameter werden sofort aktualisiert. Änderungen an statischen Parametern werden erst wirksam, nachdem Sie die DB-Instance neu gestartet haben.

Parameter, die Aurora basierend auf der maximalen Kapazität von Aurora Serverless v2 berechnet

Für die folgenden Parameter verwendet Aurora PostgreSQL auch Standardwerte, die genau wie bei `max_connections` von der Speichergröße basierend auf der maximalen ACU-Einstellung abgeleitet werden:

- `autovacuum_max_workers`
- `autovacuum_vacuum_cost_limit`
- `autovacuum_work_mem`
- `effective_cache_size`
- `maintenance_work_mem`

Fehler vermeiden out-of-memory

Wenn eine Ihrer Aurora Serverless v2-DB-Instances konsequent die Grenze ihrer maximalen Kapazität erreicht, weist Aurora auf diese Bedingung hin, indem die DB-Instance auf den Status `incompatible-parameters` festgelegt wird. Während die DB-Instance den Status `incompatible-parameters` aufweist, sind einige Operationen blockiert. Beispielsweise können Sie die Engine-Version nicht aktualisieren.

In der Regel wechselt Ihre DB-Instance in diesen Status, wenn sie aufgrund von out-of-memory Fehlern häufig neu gestartet wird. Aurora zeichnet ein Ereignis auf, wenn diese Art von Neustart stattfindet. Sie können das Ereignis anzeigen, indem Sie die Vorgehensweise unter Anzeigen von Amazon RDS-Ereignissen befolgen. Eine ungewöhnlich hohe Speicherauslastung kann aufgrund von Overhead durch Aktivieren von Einstellungen wie Performance Insights und IAM-Authentifizierung auftreten. Sie kann auch durch eine hohe Workload Ihrer DB-Instance oder durch die Verwaltung der Metadaten entstehen, die mit einer großen Anzahl von Schemaobjekten verknüpft sind.

Wenn die Speicherauslastung sinkt, sodass die DB-Instance ihre maximale Kapazität nicht sehr oft erreicht, ändert Aurora den Status der DB-Instance automatisch wieder in `available`.

Zur Wiederherstellung nach diesem Zustand können Sie einige oder alle der folgenden Aktionen ausführen:

- Erhöhen Sie die untere Kapazitätsgrenze für Aurora Serverless v2-DB-Instances durch Ändern des Mindestwerts der Aurora-Kapazitätseinheit (ACU) für den Cluster. Dadurch werden Probleme vermieden, bei denen eine inaktive Datenbank auf eine Kapazität mit weniger Speicher

heruntergeskaliert wird, als für die in Ihrem Cluster aktivierten Funktionen benötigt wird. Nachdem Sie die ACU-Einstellungen für den Cluster geändert haben, starten Sie die Aurora Serverless v2-DB-Instance neu. Dadurch wird geprüft, ob Aurora den Status wieder auf `available` zurücksetzen kann.

- Erhöhen Sie die untere Kapazitätsgrenze für Aurora Serverless v2-DB-Instances durch Ändern des maximalen Werts der Aurora-Kapazitätseinheit (ACU) für den Cluster. Auf diese Weise werden Probleme vermieden, bei denen eine ausgelastete Datenbank nicht auf eine Kapazität mit genügend Speicher für die in Ihrem Cluster aktivierten Funktionen und die Datenbank-Workload hochskaliert werden kann. Nachdem Sie die ACU-Einstellungen für den Cluster geändert haben, starten Sie die Aurora Serverless v2-DB-Instance neu. Dadurch wird geprüft, ob Aurora den Status wieder auf `available` zurücksetzen kann.
- Deaktivieren Sie Konfigurationseinstellungen, die Speicher-Overhead erfordern. Angenommen, Sie haben Funktionen wie AWS Identity and Access Management (IAM), Performance Insights oder Aurora MySQL-Binärprotokollreplikation aktiviert, verwenden sie aber nicht. In diesem Fall können Sie sie deaktivieren. Oder Sie können die minimalen und maximalen Kapazitätswerte für den Cluster nach oben korrigieren, um den von diesen Funktionen verwendeten Speicher zu berücksichtigen. Richtlinien zur Auswahl der minimalen und maximalen Kapazitätseinstellungen finden Sie unter Auswählen des Aurora Serverless v2-Kapazitätsbereichs für einen Aurora-Cluster.
- Reduzieren Sie die Workload der DB-Instance. Beispielsweise können Sie dem Cluster Reader-DB-Instances hinzufügen, um die Last von schreibgeschützten Abfragen auf weitere DB-Instances zu verteilen.
- Optimieren Sie den von Ihrer Anwendung verwendeten SQL-Code, um weniger Ressourcen zu verwenden. Sie können beispielsweise Ihre Abfragepläne untersuchen, das langsame Abfrageprotokoll überprüfen oder die Indizes in Ihren Tabellen anpassen. Außerdem können Sie andere traditionelle Arten von SQL-Optimierung durchführen.

Wichtige CloudWatch Amazon-Metriken für Aurora Serverless v2

Informationen zu den ersten Schritten mit Amazon CloudWatch für Ihre Aurora Serverless v2 DB-Instance finden Sie unterAurora Serverless v2Logs in Amazon anzeigen CloudWatch. Weitere Informationen zur Überwachung von Aurora-DB-Clustern finden CloudWatch Sie unterÜberwachen von Protokollereignissen in Amazon CloudWatch.

Anhand der `ServerlessDatabaseCapacity` Metrik können Sie Ihre Aurora Serverless v2 DB-Instances anzeigen CloudWatch , um die von jeder DB-Instance verbrauchte Kapazität zu überwachen. Sie können auch alle CloudWatch Aurora-Standardmetriken wie

`DatabaseConnections` und überwachen`Queries`. Die vollständige Liste der CloudWatch Messwerte, die Sie für Aurora überwachen können, finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora. Die Metriken sind in Metriken auf Clusterebene für Amazon Aurora und Metriken auf Instance-Ebene für Amazon Aurora in Metriken auf Cluster-Ebene und auf Instance-Ebene unterteilt.

Es ist wichtig, die folgenden Metriken CloudWatch auf Instance-Ebene zu überwachen, damit Sie verstehen, wie Ihre Aurora Serverless v2 DB-Instances nach oben und unten skalieren. Alle diese Metriken werden jede Sekunde berechnet. Auf diese Weise können Sie den aktuellen Status Ihrer Aurora Serverless v2-DB-Instances überwachen. Sie können Alarme einstellen, um sich gegebenenfalls benachrichtigen zu lassen, wenn sich eine Aurora Serverless v2-DB-Instance einem Schwellenwert für kapazitätsbezogene Metriken nähert. Sie können feststellen, ob die minimalen und maximalen Kapazitätseinstellungen angemessen sind oder ob Sie sie anpassen müssen. Sie können bestimmen, worauf Sie sich konzentrieren müssen, um die Effizienz Ihrer Datenbank zu optimieren.

- `ServerlessDatabaseCapacity`: Als Metrik auf Instance-Ebene gibt sie die Anzahl der ACUs an, die durch die aktuelle DB-Instance-Kapazität repräsentiert werden. Als Metrik auf Cluster-Ebene repräsentiert sie den Durchschnitt der `ServerlessDatabaseCapacity`-Werte aller Aurora Serverless v2-DB-Instances im Cluster. Diese Metrik ist nur eine Metrik auf Cluster-Ebene in Aurora Serverless v1. In Aurora Serverless v2 ist sie auf DB-Instance-Ebene und auf Cluster-Ebene verfügbar.
- `ACUUtilization`: Diese Metrik ist neu in Aurora Serverless v2. Dieser Wert wird als Prozentsatz dargestellt. Er wird als Wert der `ServerlessDatabaseCapacity`-Metrik geteilt durch den maximalen ACU-Wert des DB-Clusters berechnet. Beachten Sie die folgenden Richtlinien, um diese Metrik zu interpretieren und Maßnahmen zu ergreifen:
  - Wenn sich diese Metrik dem Wert `100.0` nähert, ist die DB-Instance so hoch wie möglich hochskaliert. Erwägen Sie, die maximale ACU-Einstellung für den Cluster zu erhöhen. Auf diese Weise können sowohl Writer- als auch Reader-DB-Instances auf eine höhere Kapazität skaliert werden.
  - Angenommen, eine schreibgeschützte Workload bewirkt, dass sich eine Reader-DB-Instance einem `ACUUtilization`-Wert von `100.0` nähert, während die Writer-DB-Instance ihrer maximalen Kapazität nicht annähernd erreicht. Erwägen Sie in diesem Fall, dem Cluster zusätzliche Reader-DB-Instances hinzuzufügen. Auf diese Weise können Sie den schreibgeschützten Teil der Workload auf mehrere DB-Instances verteilen und so die Last jeder Reader-DB-Instance reduzieren.

  - Angenommen, Sie führen eine Produktionsanwendung aus, bei der Leistung und Skalierbarkeit die Hauptüberlegungen sind. In diesem Fall können Sie den maximalen ACU-Wert für den Cluster auf eine hohe Zahl festlegen. Ihr Ziel besteht darin, die `ACUUtilization`-Metrik immer unter `100.0` zu halten. Mit einem hohen maximalen ACU-Wert können Sie sicher sein, dass genügend Spielraum vorhanden ist, falls unerwartete Spitzen bei der Datenbankaktivität auftreten. Berechnet wird Ihnen nur die tatsächlich verbrauchte Datenbankkapazität.

- `CPUUtilization`: Diese Metrik wird in Aurora Serverless v2 anders interpretiert als in bereitgestellten DB-Instances. Bei Aurora Serverless v2 ist dieser Wert ein Prozentsatz, der als der aktuell CPU-Verbrauch dividiert durch die CPU-Kapazität berechnet wird, die unter dem maximalen ACU-Wert des DB-Clusters verfügbar ist. Aurora überwacht diesen Wert automatisch und skaliert Ihre Aurora Serverless v2-DB-Instance, wenn die DB-Instance konsequent einen hohen Anteil ihrer CPU-Kapazität verbraucht.

  Wenn sich diese Metrik dem Wert `100.0` nähert, hat die DB-Instance ihre maximale CPU-Kapazität erreicht. Erwägen Sie, die maximale ACU-Einstellung für den Cluster zu erhöhen. Wenn sich diese Metrik dem Wert `100.0` nähert, erwägen Sie bei einer Reader-DB-Instance, dem Cluster weitere Reader-DB-Instances hinzuzufügen. Auf diese Weise können Sie den schreibgeschützten Teil der Workload auf mehrere DB-Instances verteilen und so die Last jeder Reader-DB-Instance reduzieren.

- `FreeableMemory`: Dieser Wert stellt die Menge des nicht belegten Speichers dar, die verfügbar ist, wenn die Aurora Serverless v2-DB-Instance auf ihre maximale Kapazität skaliert wird. Für jede ACU, bei der die aktuelle Kapazität unter der maximalen Kapazität liegt, erhöht sich dieser Wert ungefähr um 2 GiB. Daher nähert sich diese Metrik erst null, wenn die DB-Instance so hoch wie möglich hochskaliert ist.

  Wenn sich diese Metrik dem Wert `0` nähert, ist die DB-Instance so weit wie möglich hochskaliert und nähert sich der Grenze ihres verfügbaren Speichers. Erwägen Sie, die maximale ACU-Einstellung für den Cluster zu erhöhen. Wenn sich diese Metrik dem Wert `0` nähert, erwägen Sie bei einer Reader-DB-Instance, dem Cluster weitere Reader-DB-Instances hinzuzufügen. Auf diese Weise können Sie den schreibgeschützten Teil der Workload auf mehrere DB-Instances verteilen und so die Speicherauslastung für jede Reader-DB-Instance reduzieren.

- `TempStorageIops`: Die Anzahl der IOPS, die im lokalen Speicher durchgeführt werden, der der DB-Instance angefügt ist. Dabei sind IOPS für Lese- und Schreibvorgänge enthalten. Diese Metrik stellt eine Zählung dar und wird einmal pro Sekunde gemessen. Dies ist eine neue Metrik für Aurora Serverless v2. Details hierzu finden Sie unter Metriken auf Instance-Ebene für Amazon Aurora.

- `TempStorageThroughput`: Die Menge der mit der DB-Instance verknüpften Daten, die zu und aus dem lokalen Speicher übertragen wurden. Diese Metrik wird in Byte angegeben und einmal pro Sekunde gemessen. Dies ist eine neue Metrik für Aurora Serverless v2. Details hierzu finden Sie unter Metriken auf Instance-Ebene für Amazon Aurora.

In der Regel wird die Hochskalierung von Aurora Serverless v2-DB-Instances größtenteils durch Speicherauslastung und CPU-Aktivität verursacht. Die Metriken `TempStorageIops` und `TempStorageThroughput` können Ihnen helfen, die seltenen Fälle zu diagnostizieren, in denen die Netzwerkaktivität für Übertragungen zwischen Ihrer DB-Instance und lokalen Speichergeräten für unerwartete Kapazitätssteigerungen verantwortlich ist. Wenn Sie andere Netzwerkaktivitäten überwachen möchten, können Sie diese vorhandenen Metriken verwenden:

- `NetworkReceiveThroughput`
- `NetworkThroughput`
- `NetworkTransmitThroughput`
- `StorageNetworkReceiveThroughput`
- `StorageNetworkThroughput`
- `StorageNetworkTransmitThroughput`

Sie können Aurora einige oder alle Datenbankprotokolle veröffentlichen lassen CloudWatch. Sie bestimmen, welche Protokolle veröffentlicht werden sollen, indem Sie in der mit dem Cluster verknüpften DB-Cluster-Parametergruppe Konfigurationsparameter wie `general_log` und `slow_query_log` aktivieren, die mit dem Cluster verknüpft ist, der Ihre Aurora Serverless v2-DB-Instances enthält. Wenn Sie einen Protokollkonfigurationsparameter deaktivieren, wird die Veröffentlichung dieses Protokolls in CloudWatch beendet. Sie können die Logs auch löschen CloudWatch , wenn sie nicht mehr benötigt werden.

Wie wirken sich Aurora Serverless v2 Kennzahlen auf Ihre AWS Rechnung aus

Die Aurora Serverless v2 Gebühren auf Ihrer AWS Rechnung werden auf der Grundlage derselben `ServerlessDatabaseCapacity` Kennzahl berechnet, die Sie überwachen können. Der Abrechnungsmechanismus kann in Fällen, in denen Sie die Aurora Serverless v2 Kapazität nur für einen Teil einer Stunde nutzen, vom berechneten CloudWatch Durchschnitt für diese Kennzahl abweichen. Es kann auch anders sein, wenn die CloudWatch Metrik aufgrund von Systemproblemen für kurze Zeit nicht verfügbar ist. Daher sehen Sie möglicherweise einen etwas

anderen Wert von ACU-Stunden auf Ihrer Rechnung, als wenn Sie die Anzahl selbst anhand des `ServerlessDatabaseCapacity`-Durchschnittswerts berechnen.

Beispiele für CloudWatch Befehle für Aurora Serverless v2 Metriken

Die folgenden AWS CLI Beispiele zeigen, wie Sie die wichtigsten CloudWatch Kennzahlen im Zusammenhang mit überwachen könnenAurora Serverless v2. Ersetzen Sie in jedem Fall die `Value=`-Zeichenfolge für den `--dimensions`-Parameter durch den Bezeichner Ihrer eigenen Aurora Serverless v2-DB-Instance.

Im folgenden Linux-Beispiel werden die minimalen, maximalen und durchschnittlichen Kapazitätswerte für eine DB-Instance angezeigt, die alle 10 Minuten über einen Zeitraum von einer Stunde gemessen werden. Der Linux-Befehl `date` gibt die Start- und Endzeiten relativ zum aktuellen Datum und zur aktuellen Uhrzeit an. Die `sort_by`-Funktion im `--query`-Parameter sortiert die Ergebnisse chronologisch basierend auf dem Feld `Timestamp`.

```
aws cloudwatch get-metric-statistics --metric-name "ServerlessDatabaseCapacity" \
  --start-time "$(date -d '1 hour ago')" --end-time "$(date -d 'now')" --period 600 \
  --namespace "AWS/RDS" --statistics Minimum Maximum Average \
  --dimensions Name=DBInstanceIdentifier,Value=my_instance \
  --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' --output table
```

Die folgenden Linux-Beispiele veranschaulichen die Überwachung der Kapazität jeder DB-Instance in einem Cluster. Sie messen die minimale, maximale und durchschnittliche Kapazitätsauslastung jeder DB-Instance. Die Messungen werden einmal pro Stunde über einen Zeitraum von drei Stunden durchgeführt. Diese Beispiele verwenden die `ACUUtilization`-Metrik, die einen Prozentsatz der Obergrenze für ACUs darstellt, anstelle der `ServerlessDatabaseCapacity`-Metrik, die eine feste Anzahl von ACUs darstellt. Auf diese Weise müssen Sie die tatsächlichen Zahlen für die minimalen und maximalen ACU-Werte im Kapazitätsbereich nicht kennen. Sie können Prozentsätze zwischen 0 und 100 sehen.

```
aws cloudwatch get-metric-statistics --metric-name "ACUUtilization" \
  --start-time "$(date -d '3 hours ago')" --end-time "$(date -d 'now')" --period 3600 \
  --namespace "AWS/RDS" --statistics Minimum Maximum Average \
  --dimensions Name=DBInstanceIdentifier,Value=my_writer_instance \
  --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' --output table

aws cloudwatch get-metric-statistics --metric-name "ACUUtilization" \
```

```
  --start-time "$(date -d '3 hours ago')" --end-time "$(date -d 'now')" --period 3600 \
  --namespace "AWS/RDS" --statistics Minimum Maximum Average \
  --dimensions Name=DBInstanceIdentifier,Value=my_reader_instance \
  --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' --output table
```

Im folgenden Linux-Beispiel werden ähnliche Messungen wie die vorherigen ausgeführt. In diesem Fall gelten die Messungen für die `CPUUtilization`-Metrik Die Messungen werden alle zehn Minuten über einen Zeitraum von einer Stunde durchgeführt. Die Zahlen stellen den Prozentsatz der verwendeten verfügbaren CPU dar, basierend auf den CPU-Ressourcen, die für die maximale Kapazitätseinstellung für die DB-Instance verfügbar sind.

```
aws cloudwatch get-metric-statistics --metric-name "CPUUtilization" \
  --start-time "$(date -d '1 hour ago')" --end-time "$(date -d 'now')" --period 600 \
  --namespace "AWS/RDS" --statistics Minimum Maximum Average \
  --dimensions Name=DBInstanceIdentifier,Value=my_instance \
  --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' --output table
```

Im folgenden Linux-Beispiel werden ähnliche Messungen wie die vorherigen ausgeführt. In diesem Fall gelten die Messungen für die `FreeableMemory`-Metrik Die Messungen werden alle zehn Minuten über einen Zeitraum von einer Stunde durchgeführt.

```
aws cloudwatch get-metric-statistics --metric-name "FreeableMemory" \
  --start-time "$(date -d '1 hour ago')" --end-time "$(date -d 'now')" --period 600 \
  --namespace "AWS/RDS" --statistics Minimum Maximum Average \
  --dimensions Name=DBInstanceIdentifier,Value=my_instance \
  --query 'sort_by(Datapoints[*].
{min:Minimum,max:Maximum,avg:Average,ts:Timestamp},&ts)' --output table
```

Überwachung der Aurora Serverless v2-Leistung mit Performance Insights

Mit Performance Insights können Sie die Leistung von Aurora Serverless v2-DB-Instances überwachen. Informationen zu Performance-Insights-Verfahren finden Sie unter Überwachung mit Performance Insights auf .

Die folgenden neuen Performance-Insights-Zähler gelten für Aurora Serverless v2-DB-Instances:

- `os.general.serverlessDatabaseCapacity` – Die aktuelle Kapazität der DB-Instance in ACUs. Der Wert entspricht der `ServerlessDatabaseCapacity` CloudWatch Metrik für die DB-Instance.
- `os.general.acuUtilization` – Der Anteil der aktuellen Kapazität an der maximal konfigurierten Kapazität in Prozent. Der Wert entspricht der `ACUUtilization` CloudWatch Metrik für die DB-Instance.
- `os.general.maxConfiguredAcu` – Die maximale Kapazität, die Sie für diese Aurora Serverless v2-DB-Instance konfiguriert haben. Sie wird in ACUs gemessen.
- `os.general.minConfiguredAcu` – Die Mindestkapazität, die Sie für diese Aurora Serverless v2-DB-Instance konfiguriert haben. Sie wird in ACUs gemessen.

Eine vollständige Liste der Performance-Insights-Zähler finden Sie unter Performance-Insights-Zählermetriken.

Wenn `vCPU`-Werte für eine Aurora Serverless v2-DB-Instance in Performance Insights angezeigt werden, stellen diese Werte Schätzungen dar, die auf dem ACU-Wert für die DB-Instance basieren. Im Standardintervall von einer Minute werden alle fraktionierten vCPU-Werte auf die nächste ganze Zahl aufgerundet. Für längere Intervalle ist der angezeigte vCPU-Wert der Durchschnitt der ganzzahligen vCPU-Werte für jede Minute.

Behebung von Kapazitätsproblemen bei Aurora Serverless v2

In einigen Fällen wird Aurora Serverless v2 nicht auf die Mindestkapazität herunterskaliert, auch wenn keine Last für die Datenbank vorliegt. Dies kann aus einem der folgenden Gründe geschehen:

- Bestimmte Funktionen können die Ressourcennutzung erhöhen und verhindern, dass die Datenbank auf die Mindestkapazität herunterskaliert wird. Nachstehend sind einige dieser Features aufgeführt:
  - Globale Aurora-Datenbanken
  - CloudWatch Protokolle exportieren
  - Aktivieren von `pg_audit` auf Aurora PostgreSQL kompatiblen DB-Clustern
  - Verbesserte Überwachung
  - Performance Insights

  Weitere Informationen finden Sie unter Auswählen der minimalen Aurora Serverless v2-Kapazitätseinstellung für einen Cluster.

- Wenn eine Reader-Instance nicht auf das Minimum herunterskaliert wird und dieselbe oder eine höhere Kapazität als die Writer-Instance hat, überprüfen Sie die Prioritätsstufe der Reader-Instance. Reader-DB-Instances von Aurora Serverless v2 in Tier 0 oder 1 werden auf einer Mindestkapazität gehalten, die mindestens so hoch ist wie die der Writer-DB-Instance. Ändern Sie die Prioritätsstufe der Reader-Instance in 2 oder höher, sodass sie unabhängig von der Writer-Instance hoch- und herunterskaliert wird. Weitere Informationen finden Sie unter Auswählen der Hochstufungsstufe für einen Aurora Serverless v2-Reader.
- Legen Sie alle Datenbankparameter, die sich auf die Größe des gemeinsam genutzten Speichers auswirken, auf ihre Standardwerte fest. Wenn Sie einen höheren Wert als den Standardwert festlegen, erhöht sich der gemeinsam genutzte Speicherbedarf und verhindert, dass die Datenbank auf die Mindestkapazität herunterskaliert wird. Beispiele sind `max_connections` und `max_locks_per_transaction`.

  > **Note**
  >
  > Das Aktualisieren gemeinsam genutzter Speicherparameter erfordert einen Neustart der Datenbank, damit Änderungen wirksam werden.

- Hohe Datenbank-Workloads können die Ressourcennutzung erhöhen.
- Große Datenbank-Volumes können die Ressourcennutzung erhöhen.

  Amazon Aurora verwendet Speicher- und CPU-Ressourcen für die DB-Cluster-Verwaltung. Aurora benötigt mehr CPU und Arbeitsspeicher, um DB-Cluster mit größeren Datenbank-Volumes zu verwalten. Wenn die Mindestkapazität Ihres Clusters unter der für die Clusterverwaltung erforderlichen Mindestkapazität liegt, skaliert Ihr Cluster nicht auf die Mindestkapazität herunter.
- Hintergrundprozesse wie das Bereinigen können ebenfalls den Ressourcenverbrauch erhöhen.

Wenn die Datenbank immer noch nicht auf die konfigurierte Mindestkapazität herunterskaliert wird, beenden Sie die Datenbank und starten Sie sie neu, um alle Speicherfragmente zurückzugewinnen, die sich im Laufe der Zeit angesammelt haben könnten. Das Stoppen und Starten einer Datenbank führt zu Ausfallzeiten, daher empfehlen wir, achtsam vorzugehen.

Migration zu Aurora Serverless v2

Konvertieren Sie einen vorhandenen DB-Cluster zur Verwendung von Aurora Serverless v2 wie folgt:

- Aktualisieren Sie von einem bereitgestellten Aurora-DB-Cluster aus.

- Aktualisieren Sie von einem Aurora Serverless v1-Cluster aus.
- Migration von einer On-Premises-Datenbank zu einem Aurora Serverless v2-Cluster.

Wenn auf Ihrem aktualisierten Cluster die entsprechende Engine-Version ausgeführt wird, wie unter Anforderungen und Einschränkungen für Aurora Serverless v2 aufgeführt, können Sie mit dem Hinzufügen der Aurora Serverless v2-DB-Instances beginnen. Die erste DB-Instance, die Sie dem aktualisierten Cluster hinzufügen, muss eine bereitgestellte DB-Instance sein. Dann können Sie die Verarbeitung für die Schreib-Workload, die Lese-Workload oder beides auf die Aurora Serverless v2DB-Instances umstellen.

Inhalt

> **Note**
>
> In diesen Themen wird beschrieben, wie ein vorhandener DB-Cluster konvertiert wird. Weitere Informationen zum Erstellen eines neuen DB-Clusters von Aurora Serverless v2 finden Sie unter Erstellen eines DB-Clusters, das Aurora Serverless v2.

Aktualisieren oder Umstellen vorhandener Cluster auf die Verwendung von Aurora Serverless v2

Wenn Ihr bereitgestellter Cluster über eine Engine-Version verfügt, die Aurora Serverless v2 unterstützt, ist für die Umstellung auf Aurora Serverless v2 kein Upgrade erforderlich. In diesem Fall können Sie Ihrem ursprünglichen Aurora Serverless v2-DB-Instances Cluster hinzufügen. Sie können den Cluster umstellen, um alle Aurora Serverless v2-DB-Instances zu verwenden. Sie können auch eine Kombination aus Aurora Serverless v2 und bereitgestellten DB-Instances im selben DB-Cluster verwenden. Die Aurora-Engine-Versionen, die Aurora Serverless v2 unterstützen, finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v2.

Wenn Sie eine niedrigere Engine-Version ausführen, die Aurora Serverless v2 nicht unterstützt, führen Sie diese allgemeinen Schritte aus:

1. Aktualisieren Sie den Cluster.
2. Erstellen Sie eine bereitgestellte Writer-DB-Instance für den aktualisierten Cluster.
3. Ändern Sie den Cluster, sodass er Aurora Serverless v2-DB-Instances verwendet.

> **Important**
>
> Wenn Sie ein größeres Versions-Upgrade auf eine Aurora Serverless v2-kompatible Version unter Verwendung von Snapshot-Wiederherstellung oder -Klonen durchführen, muss die erste DB-Instance, die Sie dem neuen Cluster hinzufügen, eine bereitgestellte DB-Instance sein. Dieser Hinzufügevorgang startet die letzte Phase des Upgrade-Prozesses.
> Bis zu dieser letzten Phase verfügt der Cluster nicht über die Infrastruktur, die für die Unterstützung von Aurora Serverless v2 erforderlich ist. Daher beginnen diese aktualisierten Cluster immer mit einer bereitgestellten Writer-DB-Instance. Dann können Sie die bereitgestellte DB-Instance in eine Aurora Serverless v2-Instance konvertieren oder ein entsprechendes Failover durchführen.

Das Aktualisieren von Aurora Serverless v1 auf Aurora Serverless v2 umfasst das Erstellen eines bereitgestellten Clusters als Zwischenschritt. Anschließend führen Sie dieselben Upgrade-Schritte aus wie beim Start mit einem bereitgestellten Cluster.

Upgrade-Pfade für MySQL-kompatible Cluster zur Verwendung von Aurora Serverless v2

Wenn auf Ihrem ursprünglichen Cluster Aurora MySQL ausgeführt wird, wählen Sie je nach Engine-Version und Engine-Modus Ihres Clusters das entsprechende Verfahren aus.

Wenn Ihr ursprünglicher Aurora-MySQL-Cluster dieser ist	Gehen Sie wie folgt vor, um auf Aurora Serverless v2 umzustellen.
Bereitgestellter Cluster mit Aurora MySQL Version 3, kompatibel mit MySQL 8.0	Dies ist die letzte Phase für alle Konvertierungen aus bestehenden Aurora-MySQL-Clustern. Führen Sie ggf. ein Nebenversions-Upgrade auf Version 3.02.0 oder höher durch. Verwenden Sie eine bereitgestellte DB-Instance für die Writer-DB-Instance. Fügen Sie eine Aurora Serverless v2-Reader-DB-Instance hinzu. Führen Sie ein Failover durch, um diese zur Writer-DB-Instance hochzustufen. (Optional) Konvertieren Sie andere bereitgestellte DB-Instances im Cluster in Aurora Serverless v2. Oder fügen Sie neue DB-Instances von Aurora Serverless v2 hinzu und entfernen Sie die bereitgestellten DB-Instances. Das vollständige Verfahren und Beispiele finden Sie unter Umstellung von einem bereitgestellten Cluster zu Aurora Serverless v2.
Bereitgestellter Cluster mit Aurora MySQL Version 2, kompatibel mit MySQL 5.7	Führen Sie ein Hauptversions-Upgrade auf Aurora MySQL Version 3.02.0 oder höher durch. Befolgen Sie dann die Vorgehensweise für Aurora-MySQL-Version 3, um den Cluster auf die Verwendung von Aurora Serverless v2-DB-Instances umzustellen.

Wenn Ihr ursprünglicher Aurora-MySQL-Cluster dieser ist	Gehen Sie wie folgt vor, um auf Aurora Serverless v2 umzustellen.
Aurora Serverless v1-Cluster mit Aurora MySQL Version 2, kompatibel mit MySQL 5.7	Hilfestellung zur Planung Ihrer Konvertierung von Aurora Serverless v1 finden Sie unter Aurora Serverless v2 und Aurora Serverless v1 im Vergleich. Folgen Sie dann dem Verfahren unter Aktualisieren eines Aurora Serverless v1-Clusters auf Aurora Serverless v2.

Upgrade-Pfade für PostgreSQL-kompatible Cluster zur Verwendung von Aurora Serverless v2

Wenn auf Ihrem ursprünglichen Cluster Aurora PostgreSQL ausgeführt wird, wählen Sie je nach Engine-Version und Engine-Modus Ihres Clusters das entsprechende Verfahren aus.

Wenn Ihr ursprünglicher Aurora-PostgreSQL-Cluster dieser ist	Gehen Sie wie folgt vor, um auf Aurora Serverless v2 umzustellen.
Bereitgestellter Cluster, auf dem Aurora-PostgreSQL-Version 13 ausgeführt wird	Dies ist die letzte Phase für alle Konvertierungen aus bestehenden Aurora-PostgreSQL-Clustern. Führen Sie ggf. ein Nebenversions-Upgrade auf Version 13.6 oder höher durch. Fügen Sie eine bereitgestellte DB-Instance für die Writer-DB-Instance hinzu. Fügen Sie eine Aurora Serverless v2-Reader-DB-Instance hinzu. Führen Sie ein Failover aus, damit diese Aurora Serverless v2-Instance zur Writer-DB-Instance wird. (Optional) Konvertieren Sie andere bereitgestellte DB-Instances im Cluster zu Aurora Serverless v2. Oder fügen Sie neue DB-

Wenn Ihr ursprünglicher Aurora-PostgreSQL-Cluster dieser ist	Gehen Sie wie folgt vor, um auf Aurora Serverless v2 umzustellen.
	Instances von Aurora Serverless v2 hinzu und entfernen Sie die bereitgestellten DB-Instances. Das vollständige Verfahren und Beispiele finden Sie unter Umstellung von einem bereitgestellten Cluster zu Aurora Serverless v2.
Bereitgestellter Cluster mit Aurora PostgreSQL Version 11 oder 12	Führen Sie ein Hauptversions-Upgrade auf Aurora PostgreSQL Version 13.6 oder höher durch. Befolgen Sie dann die Vorgehensweise für Aurora PostgreSQL Version 13, um den Cluster auf die Verwendung von Aurora Serverless v2-DB-Instances umzustellen.
Aurora Serverless v1-Cluster, auf dem Aurora PostgreSQL Version 11 oder 13 ausgeführt wird	Hilfestellung zur Planung Ihrer Konvertierung von Aurora Serverless v1 finden Sie unter Aurora Serverless v2 und Aurora Serverless v1 im Vergleich. Folgen Sie dann dem Verfahren unter Aktualisieren eines Aurora Serverless v1-Clusters auf Aurora Serverless v2.

Umstellung von einem bereitgestellten Cluster zu Aurora Serverless v2

Stellen Sie einen bereitgestellten Cluster wie folgt auf die Verwendung von Aurora Serverless v2 um:

1. Prüfen Sie, ob der bereitgestellte Cluster aktualisiert werden muss, um mit Aurora Serverless v2-DB-Instances verwendet werden zu können. Die Aurora-Versionen, die mit Aurora Serverless v2 kompatibel sind, finden Sie unter Anforderungen und Einschränkungen für Aurora Serverless v2.

   Wenn auf dem bereitgestellten Cluster eine Engine-Version ausgeführt wird, die für Aurora Serverless v2 nicht verfügbar ist, aktualisieren Sie die Engine-Version des Clusters:

- Wenn Sie einen mit MySQL 5.7 kompatiblen bereitgestellten Cluster vorliegen haben, befolgen Sie die Upgrade-Anweisungen für Aurora MySQL Version 3. Verwenden Sie die Verfahren in Erläuterung der Durchführung eines direkten Upgrades.
- Wenn Sie einen mit PostgreSQL kompatiblen bereitgestellten Cluster vorliegen haben, auf dem PostgreSQL Version 11 oder 12 ausgeführt wird, befolgen Sie die Upgrade-Anweisungen für Aurora PostgreSQL Version 13. Verwenden Sie die Verfahren in Durchführen eines Hauptversions-Upgrades.

2. Konfigurieren Sie alle anderen Cluster-Eigenschaften so, dass sie den Aurora Serverless v2-Anforderungen von Anforderungen und Einschränkungen für Aurora Serverless v2 entsprechen.
3. Konfigurieren Sie die Skalierungskonfiguration für den Cluster. Folgen Sie dem Verfahren unter Festlegen des Aurora Serverless v2-Kapazitätsbereichs für einen Cluster.
4. Fügen Sie dem Cluster eine oder mehrere Aurora Serverless v2-DB-Instances hinzu. Gehen Sie vor, wie im allgemeinen Verfahren unter Hinzufügen von Aurora-Replicas zu einem DB-Cluster beschrieben. Geben Sie für jede neue DB-Instance den speziellen DB-Instance-Klassennamen Serverless in der AWS Management Console oder AWS CLI oder `db.serverless` der Amazon RDS-API an.

   In einigen Fällen sind möglicherweise bereits eine oder mehrere bereitgestellte Reader-DB-Instances im Cluster vorhanden. Wenn dies der Fall ist, können Sie einen der Reader in eine Aurora Serverless v2-DB-Instance konvertieren, anstatt eine neue DB-Instance zu erstellen. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Konvertieren eines bereitgestellten Writers oder Readers in Aurora Serverless v2.
5. Führen Sie einen Failover-Vorgang aus, damit eine der Aurora Serverless v2-DB-Instances zur Writer-DB-Instance für den Cluster wird.
6. (Optional) Konvertieren Sie alle bereitgestellten DB-Instances in Aurora Serverless v2 oder entfernen Sie sie aus dem Cluster. Gehen Sie vor, wie im allgemeinen Verfahren unter Konvertieren eines bereitgestellten Writers oder Readers in Aurora Serverless v2 oder Löschen einer DB-Instance aus einem Aurora-DB-Cluster beschrieben.

   > **Tip**
   >
   > Das Entfernen der bereitgestellten DB-Instances ist nicht zwingend erforderlich. Sie können einen Cluster einrichten, der sowohl Aurora Serverless v2 als auch bereitgestellte DB-Instances enthält. Bevor Sie jedoch mit den Leistungs- und Skalierungsmerkmalen von

Aurora Serverless v2-DB-Instances vertraut sind, empfehlen wir Ihnen, Ihre Cluster mit DB-Instances desselben Typs zu konfigurieren.

Das folgende AWS CLI Beispiel zeigt den Switchover-Prozess unter Verwendung eines bereitgestellten Clusters, auf dem Aurora MySQL Version 3.02.0 ausgeführt wird. Der Cluster heißt `mysql-80`. Der Cluster beginnt mit zwei bereitgestellten DB-Instances namens `provisioned-instance-1` und `provisioned-instance-2`, ein Writer und ein Reader. Beide verwenden die `db.r6g.large`-DB-Instance-Klasse.

```
$ aws rds describe-db-clusters --db-cluster-identifier mysql-80 \
  --query '*[].[DBClusterIdentifier,DBClusterMembers[*].
[DBInstanceIdentifier,IsClusterWriter]]' --output text
mysql-80
provisioned-instance-2     False
provisioned-instance-1     True

$ aws rds describe-db-instances --db-instance-identifier provisioned-instance-1 \
  --output text --query '*[].[DBInstanceIdentifier,DBInstanceClass]'
provisioned-instance-1     db.r6g.large

$ aws rds describe-db-instances --db-instance-identifier provisioned-instance-2 \
  --output text --query '*[].[DBInstanceIdentifier,DBInstanceClass]'
provisioned-instance-2     db.r6g.large
```

Wir erstellen eine Tabelle mit einigen Daten. Auf diese Weise können wir bestätigen, dass die Daten und der Betrieb des Clusters vor und nach der Umstellung gleich sind.

```
mysql> create database serverless_v2_demo;
mysql> create table serverless_v2_demo.demo (s varchar(128));
mysql> insert into serverless_v2_demo.demo values ('This cluster started with a
 provisioned writer.');
Query OK, 1 row affected (0.02 sec)
```

Zunächst fügen wir dem Cluster einen Kapazitätsbereich hinzu. Andernfalls erhalten wir einen Fehler beim Hinzufügen von Aurora Serverless v2-DB-Instances zum Cluster. Wenn wir das AWS Management Console für dieses Verfahren verwenden, erfolgt dieser Schritt automatisch, wenn wir die erste Aurora Serverless v2 DB-Instance hinzufügen.

```
$ aws rds create-db-instance --db-instance-identifier serverless-v2-instance-1 \
```

```
  --db-cluster-identifier mysql-80 --db-instance-class db.serverless --engine aurora-
mysql

An error occurred (InvalidDBClusterStateFault) when calling the CreateDBInstance
 operation:
Set the Serverless v2 scaling configuration on the parent DB cluster before creating a
 Serverless v2 DB instance.

$ # The blank ServerlessV2ScalingConfiguration attribute confirms that the cluster
 doesn't have a capacity range set yet.
$ aws rds describe-db-clusters --db-cluster-identifier mysql-80 --query
 'DBClusters[*].ServerlessV2ScalingConfiguration'
[]

$ aws rds modify-db-cluster --db-cluster-identifier mysql-80 \
  --serverless-v2-scaling-configuration MinCapacity=0.5,MaxCapacity=16
{
  "DBClusterIdentifier": "mysql-80",
  "ServerlessV2ScalingConfiguration": {
    "MinCapacity": 0.5,
    "MaxCapacity": 16
  }
}
```

Wir erstellen zwei Reader von Aurora Serverless v2, die an die Stelle der ursprünglichen DB-Instances treten. Dazu geben wir die `db.serverless`-DB-Instance-Klasse für die neuen DB-Instances an.

```
$ aws rds create-db-instance --db-instance-identifier serverless-v2-instance-1 --db-
cluster-identifier mysql-80 --db-instance-class db.serverless --engine aurora-mysql
{
  "DBInstanceIdentifier": "serverless-v2-instance-1",
  "DBClusterIdentifier": "mysql-80",
  "DBInstanceClass": "db.serverless",
  "DBInstanceStatus": "creating"
}

$ aws rds create-db-instance --db-instance-identifier serverless-v2-instance-2 \
  --db-cluster-identifier mysql-80 --db-instance-class db.serverless --engine aurora-
mysql
{
  "DBInstanceIdentifier": "serverless-v2-instance-2",
  "DBClusterIdentifier": "mysql-80",
```

```
  "DBInstanceClass": "db.serverless",
  "DBInstanceStatus": "creating"
}

$ # Wait for both DB instances to finish being created before proceeding.
$ aws rds wait db-instance-available --db-instance-identifier serverless-v2-instance-1
 && \
  aws rds wait db-instance-available --db-instance-identifier serverless-v2-instance-2
```

Wir führen einen Failover-Vorgang aus, damit eine der Aurora Serverless v2-DB-Instances zur Writer-DB-Instance für den Cluster wird.

```
$ aws rds failover-db-cluster --db-cluster-identifier mysql-80 \
  --target-db-instance-identifier serverless-v2-instance-1
{
  "DBClusterIdentifier": "mysql-80",
  "DBClusterMembers": [
    {
      "DBInstanceIdentifier": "serverless-v2-instance-1",
      "IsClusterWriter": false,
      "DBClusterParameterGroupStatus": "in-sync",
      "PromotionTier": 1
    },
    {
      "DBInstanceIdentifier": "serverless-v2-instance-2",
      "IsClusterWriter": false,
      "DBClusterParameterGroupStatus": "in-sync",
      "PromotionTier": 1
    },
    {
      "DBInstanceIdentifier": "provisioned-instance-2",
      "IsClusterWriter": false,
      "DBClusterParameterGroupStatus": "in-sync",
      "PromotionTier": 1
    },
    {
      "DBInstanceIdentifier": "provisioned-instance-1",
      "IsClusterWriter": true,
      "DBClusterParameterGroupStatus": "in-sync",
      "PromotionTier": 1
    }
  ],
  "Status": "available"
```

```
}
```

Es dauert einige Sekunden, bis diese Änderung wirksam wird. Zu diesem Zeitpunkt verfügen wir über einen Aurora Serverless v2-Writer und einen Aurora Serverless v2-Reader. Daher benötigen wir keine der ursprünglich bereitgestellten DB-Instances.

```
$ aws rds describe-db-clusters --db-cluster-identifier mysql-80 \
  --query '*[].[DBClusterIdentifier,DBClusterMembers[*].
[DBInstanceIdentifier,IsClusterWriter]]' \
  --output text
mysql-80
serverless-v2-instance-1        True
serverless-v2-instance-2        False
provisioned-instance-2          False
provisioned-instance-1          False
```

Der letzte Schritt im Umstellungsverfahren besteht darin, beide bereitgestellten DB-Instances zu löschen.

```
$ aws rds delete-db-instance --db-instance-identifier provisioned-instance-2 --skip-
final-snapshot
{
  "DBInstanceIdentifier": "provisioned-instance-2",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql",
  "EngineVersion": "8.0.mysql_aurora.3.02.0",
  "DBInstanceClass": "db.r6g.large"
}

$ aws rds delete-db-instance --db-instance-identifier provisioned-instance-1 --skip-
final-snapshot
{
  "DBInstanceIdentifier": "provisioned-instance-1",
  "DBInstanceStatus": "deleting",
  "Engine": "aurora-mysql",
  "EngineVersion": "8.0.mysql_aurora.3.02.0",
  "DBInstanceClass": "db.r6g.large"
}
```

Abschließend bestätigen wir zur Überprüfung, dass die ursprüngliche Tabelle von der Aurora Serverless v2-Writer-DB-Instance aus zugänglich und beschreibbar ist.

```
mysql> select * from serverless_v2_demo.demo;
+--------------------------------------------------+
| s                                                |
+--------------------------------------------------+
| This cluster started with a provisioned writer.  |
+--------------------------------------------------+
1 row in set (0.00 sec)

mysql> insert into serverless_v2_demo.demo values ('And it finished with a Serverless
 v2 writer.');
Query OK, 1 row affected (0.01 sec)

mysql> select * from serverless_v2_demo.demo;
+--------------------------------------------------+
| s                                                |
+--------------------------------------------------+
| This cluster started with a provisioned writer.  |
| And it finished with a Serverless v2 writer.     |
+--------------------------------------------------+
2 rows in set (0.01 sec)
```

Wir stellen außerdem eine Verbindung mit der Aurora Serverless v2-Reader-DB-Instance her und bestätigen, dass die neu geschriebenen Daten dort auch verfügbar sind.

```
mysql> select * from serverless_v2_demo.demo;
+--------------------------------------------------+
| s                                                |
+--------------------------------------------------+
| This cluster started with a provisioned writer.  |
| And it finished with a Serverless v2 writer.     |
+--------------------------------------------------+
2 rows in set (0.01 sec)
```

Aurora Serverless v2 und Aurora Serverless v1 im Vergleich

Wenn Sie Aurora Serverless v1 bereits verwenden, können Sie sich mit den Hauptunterschieden zwischen Aurora Serverless v1 und Aurora Serverless v2 vertraut machen. Die architektonischen Unterschiede, wie die Unterstützung für Reader-DB-Instances, eröffnen neue Arten von Anwendungsfällen.

Sie können die folgenden Tabellen verwenden, um die wichtigsten Unterschiede zwischen Aurora Serverless v2 und Aurora Serverless v1besser zu verstehen.

Themen

Aurora Serverless v2- und Aurora Serverless v1-Anforderungen im Vergleich

Die folgende Tabelle fasst die verschiedenen Anforderungen zum Ausführen Ihrer Datenbank mit Aurora Serverless v2 oder Aurora Serverless v1 zusammen. Aurora Serverless v2 bietet höhere Versionen der Aurora-MySQL- und Aurora-PostgreSQL-DB-Engines als Aurora Serverless v1.

Funktion	Anforderung von Aurora Serverless v2	Anforderung von Aurora Serverless v1
DB-Engines	Aurora MySQL, Aurora PostgreSQL	Aurora MySQL, Aurora PostgreSQL
Unterstützte Aurora-MySQL-Versionen	Siehe Aurora Serverless v2 mit Aurora MySQL.	Siehe Aurora Serverless v1 mit Aurora MySQL.
Unterstützte Aurora-PostgreSQL-Versionen	Siehe Aurora Serverless v2 mit Aurora PostgreSQL.	Siehe Aurora Serverless v1 mit Aurora PostgreSQL.
Upgraden eines DB-Clusters	Ähnlich wie bei bereitgestellten DB-Clustern können Sie Upgrades manuell durchführen, ohne darauf zu warten, dass Aurora den DB-Cluster für Sie aktualisiert. Weitere Informationen finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.	Nebenversions-Upgrades werden automatisch angewendet, sobald sie verfügbar sind. Weitere Informationen finden Sie unter Aurora Serverless v1- und Aurora-Datenbank-Engine-Versionen.

Funktion	Anforderung von Aurora Serverless v2	Anforderung von Aurora Serverless v1
	Note Um ein Hauptversions-Upgrade von 13.x auf 14.x oder 15.x für einen mit Aurora PostgreSQL kompatiblen DB-Cluster durchzuführen, muss die maximale Kapazität des Clusters mindestens 2 ACUs betragen.	Sie können Hauptversions-Upgrades manuell durchführen. Weitere Informationen finden Sie unter Ändern eines Aurora Serverless v1-DB-Clusters.

Funktion	Anforderung von Aurora Serverless v2	Anforderung von Aurora Serverless v1
Konvertieren von bereitgestellten Clustern aus	Sie können die folgenden Methoden verwenden: • Fügen Sie einem vorhandenen bereitgestellten Cluster eine oder mehrere Aurora Serverless v2-Reader DB-Instances hinzu. Wenn Sie Aurora Serverless v2 für den Writer verwenden möchten, führen Sie ein Failover auf eine der Aurora Serverless v2-DB-Instances durch. Damit der gesamte Cluster Aurora Serverless v2 verwendet, entfernen Sie alle bereitgestellten Writer-DB-Instances, nachdem Sie die Aurora Serverless v2-DB-Instance zum Writer hochgestuft haben. • Erstellen Sie ein neues Cluster mit der entsprechenden DB-Engine und Engine-Version. Verwenden Sie eine der Standardmethoden. Stellen Sie beispielsweise einen Cluster-Snapshot wieder her oder erstellen Sie einen Klon eines vorhandenen Clusters. Wählen Sie Aurora Serverless v2 für einige	Stellen Sie den Snapshot des bereitgestellten Clusters wieder her, um einen neuen Aurora Serverless v1-Cluster zu erstellen.

Funktion	Anforderung von Aurora Serverless v2	Anforderung von Aurora Serverless v1
	oder alle DB-Instances im neuen Cluster. Wenn Sie den neuen Cluster durch Klonen erstellen, können Sie die Engine-Version nicht gleichzeitig aktualisieren. Stellen Sie sicher, dass auf dem ursprünglichen Cluster bereits eine Engine-Version ausgeführt wird, die mit Aurora Serverless v2 kompatibel ist.	
Konvertieren von einem Cluster von Aurora Serverless v1 aus	Folgen Sie dem Verfahren unter Aktualisieren eines Aurora Serverless v1-Clusters auf Aurora Serverless v2.	Nicht zutreffend
Verfügbare DB-Instance-Klassen	Die DB-Instance-Sonderklasse `db.serverless` . In der AWS Management Console ist es als Serverless gekennzeichnet.	Nicht zutreffend. Aurora Serverless v1 verwendet den `serverless` -Engine-Modus.
Port	Jeder Port, der mit MySQL oder PostgreSQL kompatibel ist	Nur MySQL- oder PostgreSQL-Standard-Port
Öffentliche IP-Adresse zulässig?	Ja	Nein

Funktion	Anforderung von Aurora Serverless v2	Anforderung von Aurora Serverless v1
Virtual Private Cloud (VPC) erforderlich?	Ja	Ja. Jeder Aurora Serverless v1-Cluster verbraucht 2 Schnittstellen- und Gateway-Load-Balancer-Endpunkte, die Ihrer VPC zugewiesen sind.

Skalierung und Verfügbarkeit von Aurora Serverless v2 und Aurora Serverless v1 im Vergleich

In der folgenden Tabelle werden die Unterschiede zwischen Aurora Serverless v2 und Aurora Serverless v1 im Hinblick auf Skalierbarkeit und Verfügbarkeit zusammengefasst.

Die Aurora Serverless v2-Skalierung ist reaktionsschneller, stärker granular und weniger störend als die Skalierung in Aurora Serverless v1.Aurora Serverless v2 kann sowohl durch Ändern der Größe der DB-Instance als auch durch Hinzufügen weiterer DB-Instances zum DB-Cluster skaliert werden. Es kann auch skaliert werden, indem Cluster in anderen AWS-Regionen zu einer globalen Aurora-Datenbank hinzugefügt werden. Im Gegensatz dazu skaliert Aurora Serverless v1 nur durch Erhöhung oder Verringerung der Kapazität des Writers. Sämtliche Berechnungen für einen Aurora Serverless v1-Cluster erfolgen in einer einzigen Availability Zone und einer einzigen AWS-Region.

Funktion für Skalierung und Hochverfügbarkeit	Aurora Serverless v2Verhalten	Aurora Serverless v1Verhalten
Minimale Aurora-Kapazitätseinheiten (ACUs) (Aurora MySQL)	0.5	1 wenn der Cluster läuft, 0, wenn der Cluster angehalten wird.
Minimale ACUs (Aurora PostgreSQL)	0.5	2 wenn der Cluster läuft, 0, wenn der Cluster angehalten wird.
Maximale ACUs (Aurora MySQL)	128	256

Funktion für Skalierung und Hochverfügbarkeit	Aurora Serverless v2Verhalten	Aurora Serverless v1Verhalten
Maximale ACUs (Aurora PostgreSQL)	128	384
Stoppen eines Clusters	Sie können den Cluster manuell stoppen und starten, indem Sie die gleiche Cluster-Stopp-und Start-Funktion verwenden wie für bereitges tellte Cluster.	Der Cluster pausiert nach einem Timeout automatisch. Es dauert einige Zeit, bis er wieder verfügbar ist und die Aktivität fortgesetzt wird.
Skalierung von DB-Instances	Skalieren Sie mit einem Mindestinkrement von 0,5 ACU hoch und herunter.	Skalieren Sie durch Verdoppel n bzw. Halbieren der ACUs hoch und herunter.
Anzahl von DB-Instances	Entspricht einem bereitges tellten Cluster: 1 Writer-DB-Instance, bis zu 15 Reader-DB -Instances.	1 DB-Instance, die sowohl Lese- als auch Schreibvo rgänge verarbeitet
Ist die Skalierung möglich, während SQL-Anweisungen ausgeführt werden?	Ja. Bei Aurora Serverless v2 entfällt das Warten auf Ruhepunkt.	Nein. Zum Beispiel wartet die Skalierung auf den Abschluss von lang andauernden Transaktionen, temporären Tabellen und Tabellensperren.
Reader-DB-Instances skalieren zusammen mit dem Writer	Optional.	Nicht zutreffend.
Maximaler Speicher	128 TiB	128 TiB oder 64 TiB, je nach Datenbank-Engine und Version.

Funktion für Skalierung und Hochverfügbarkeit	Aurora Serverless v2Verhalten	Aurora Serverless v1Verhalten
Puffer-Cache wird beim Skalieren beibehalten	Ja. Die Größe des Puffer-Caches wird dynamisch geändert.	Nein. Der Puffer-Cache wird nach der Skalierung wiederverwendet.
Failover	Ja, genauso wie für bereitgestellte Cluster.	Nur bestmöglich, vorbehaltlich der Verfügbarkeit der Kapazität. Langsamer als in Aurora Serverless v2.
Multi-AZ-Fähigkeit	Ja, genauso wie für bereitgestellte Cluster. Ein Multi-AZ-Cluster benötigt eine Reader-DB-Instance in einer zweiten Availability Zone (AZ). Für einen Multi-AZ-Cluster führt Aurora im Falle eines AZ-Fehlers ein Multi-AZ-Failover durch.	Aurora Serverless v1-Cluster führen alle ihre Berechnungen in einer einzigen AZ aus. Die Wiederherstellung im Falle eines AZ-Ausfalls ist nur bestmöglich und unterliegt der Verfügbarkeit der Kapazität.
Globale Aurora-Datenbanken	Ja	Nein
Skalierung basierend auf Speicherauslastung	Ja	Nein
Skalierung basierend auf CPU-Last	Ja	Ja
Skalierung basierend auf Netzwerkverkehr	Ja, basierend auf Speicher- und CPU-Overhead des Netzwerkverkehrs. Der `max_connections` -Parameter bleibt konstant, um einen Abbruch von Verbindungen beim Herunterskalieren zu vermeiden.	Ja, basierend auf der Anzahl der Verbindungen.

Funktion für Skalierung und Hochverfügbarkeit	Aurora Serverless v2Verhalten	Aurora Serverless v1Verhalten
Timeout-Aktion für Skalierungs-Ereignisse	Nein	Ja
Hinzufügen neuer DB-Instances zum Cluster über AWS Auto Scaling	Nicht zutreffend. Sie können Aurora Serverless v2-Reader DB-Instances in den Hochstufungsstufen 2 bis 15 erstellen und sie auf geringe Kapazität herunterskaliert lassen.	Nein. Reader-DB-Instances sind nicht verfügbar.

Funktionsunterstützung von Aurora Serverless v2 und Aurora Serverless v1 im Vergleich

Die folgende Tabelle enthält eine Zusammenfassung folgender Funktionen:

- Funktionen, die in Aurora Serverless v2, aber nicht in Aurora Serverless v1 verfügbar sind
- Funktionen, die in Aurora Serverless v1 und Aurora Serverless v2 unterschiedlich funktionieren
- Funktionen, die derzeit in Aurora Serverless v2 nicht verfügbar sind

Aurora Serverless v2 enthält viele Funktionen aus bereitgestellten Clustern, die für Aurora Serverless v1 nicht verfügbar sind.

Funktion	Aurora Serverless v2-Support	Aurora Serverless v1-Support
Cluster-Topologie	Aurora Serverless v2 ist eine Eigenschaft einzelner DB-Instances. Ein Cluster kann mehrere Aurora Serverless v2DB-Instances oder eine Kombination aus Aurora Serverless v2 und bereitgestellten DB-Instances enthalten.	Aurora Serverless v1-Cluster verwenden nicht den Begriff der DB-Instances. Sie können die Aurora Serverless v1-Eigenschaft nach dem Erstellen des Clusters nicht mehr ändern.

Funktion	Aurora Serverless v2-Support	Aurora Serverless v1-Support
Konfigurationsparameter	Es können fast alle Parameter geändert werden wie in bereitgestellten Clustern. Details hierzu finden Sie unter Arbeiten mit Parametergruppen für Aurora Serverless v2.	Es kann nur eine Teilmenge von Parametern geändert werden.
Parametergruppen	Cluster-Parametergruppen und DB-Parametergruppen Parameter mit dem Wert `provisioned` im Attribut `SupportedEngineModes` sind verfügbar. Dies sind deutlich mehr Parameter als in Aurora Serverless v1.	Nur Cluster-Parametergruppe. Parameter mit dem Wert `serverless` im Attribut `SupportedEngineModes` sind verfügbar.
Verschlüsselung für Cluster-Volume	Optional	Erforderlich Die Einschränkungen in Einschränkungen von Amazon Aurora-verschlüsselten DB-Clustern gelten für alle Aurora Serverless v1-Cluster.
Regionsübergreifende Snapshots	Ja	Der Snapshot muss mit Ihrem eigenen Schlüssel AWS Key Management Service (AWS KMS) verschlüsselt werden.
Automatische Backups, die nach dem Löschen des DB-Clusters beibehalten werden	Ja	Nein

Funktion	Aurora Serverless v2-Support	Aurora Serverless v1-Support
TLS/SSL	Ja. Die Unterstützung ist die gleiche wie für bereitgestellte Cluster. Weitere Informationen zur Nutzung finden Sie unter Verwenden von TLS/SSL mit Aurora Serverless v2.	Ja. Es gibt einige Unterschiede im Hinblick auf den TLS-Unterstützung für bereitgestellte Cluster. Weitere Informationen zur Nutzung finden Sie unter Verwenden von TLS/SSL mit Aurora Serverless v1.
Klonen	Nur von und zu DB-Engine-Versionen, die mit Aurora Serverless v2 kompatibel sind. Sie können das Klonen nicht verwenden, um ein Upgrade von Aurora Serverless v1 oder einer früheren Version eines bereitgestellten Clusters durchzuführen.	Nur von und zu DB-Engine-Versionen, die mit Aurora Serverless v1 kompatibel sind.
Integration in Amazon S3	Ja	Ja
Integration mit AWS Secrets Manager	Nein	Nein
Exportieren von DB-Cluster-Snapshots zu S3	Ja	Nein
Zuweisen einer IAM-Rolle	Ja	Nein
Logs auf Amazon hochladen CloudWatch	Optional. Sie wählen aus, welche Protokolle aktiviert und in welche Protokolle hochgeladen werden sollen. CloudWatch	Alle Protokolle, die aktiviert sind, werden CloudWatch automatisch hochgeladen.
Daten-API verfügbar	Ja	Ja

Funktion	Aurora Serverless v2-Support	Aurora Serverless v1-Support
Abfrage-Editor verfügbar	Ja	Ja
Performance Insights	Ja	Nein
Amazon RDS Proxy verfügbar	Ja	Nein
Babelfish für Aurora PostgreSQL verfügbar	Ja. Unterstützt für Aurora-PostgreSQL-Versionen, die sowohl mit Babelfish als auch Aurora Serverless v2 kompatibel sind.	Nein

Anpassen von Aurora Serverless v1-Anwendungsfälle an Aurora Serverless v2

Abhängig von Ihrem Anwendungsfall für Aurora Serverless v1 können Sie diesen Ansatz wie folgt anpassen, um die Aurora Serverless v2-Funktionen zu nutzen.

Angenommen, Sie haben einen Aurora Serverless v1-Cluster vorliegen, der leicht geladen ist, und Ihre Priorität besteht darin, die kontinuierliche Verfügbarkeit aufrechtzuerhalten und gleichzeitig die Kosten zu minimieren. Mit Aurora Serverless v2 können Sie mit 0,5 eine kleinere Mindesteinstellung für ACU konfigurieren als bei Aurora Serverless v1. Hier beträgt der Mindestwert 1 ACU. Sie können die Verfügbarkeit erhöhen, indem Sie eine Multi-AZ-Konfiguration erstellen, wobei die DB-Instance des Readers ebenfalls auf den Mindestwert von 0,5 ACUs eingestellt ist.

Angenommen, Sie haben einen Aurora Serverless v1-Cluster vorliegen, den Sie in einem Entwicklungs- und Testszenario verwenden. In diesem Fall haben die Kosten ebenfalls eine hohe Priorität, aber der Cluster muss nicht jederzeit verfügbar sein. Derzeit pausiert Aurora Serverless v2 den Cluster nicht automatisch, wenn er vollständig inaktiv ist. Stattdessen können Sie den Cluster manuell stoppen, wenn er nicht benötigt wird, und ihn starten, wenn der nächste Test- oder Entwicklungszyklus ansteht.

Angenommen, Sie haben einen Aurora Serverless v1-Cluster mit einer hohen Workload vorliegen. Ein gleichwertiger Cluster mit Aurora Serverless v2 kann mit größerer Granularität skaliert werden. Aurora Serverless v1 skaliert beispielsweise durch Verdoppelung der Kapazität, z. B. von 64 auf 128 ACU. Im Gegensatz dazu kann Ihre Aurora Serverless v2-DB-Instance auf einen beliebigen Wert zwischen diesen Zahlen skaliert werden.

Angenommen, Ihre Workload erfordert eine höhere Gesamtkapazität, als in Aurora Serverless v1 verfügbar ist. Sie können mehrere Aurora Serverless v2-Reader-DB-Instances verwenden, um die leseintensiven Teile der Workload von der Writer-DB-Instance auszulagern. Sie können leseintensive Workloads auch auf mehrere Reader-DB-Instances verteilen.

Für eine schreibintensive Workload können Sie den Cluster mit einer großen bereitgestellten DB-Instance als Writer konfigurieren. Sie können diesen Vorgang zusammen mit einer oder mehreren Reader-DB-Instances von Aurora Serverless v2 ausführen.

Aktualisieren eines Aurora Serverless v1-Clusters auf Aurora Serverless v2

Der Prozess zum Aktualisieren eines DB-Clusters von Aurora Serverless v1 auf Aurora Serverless v2 umfasst mehrere Schritte. Das liegt daran, dass Sie nicht direkt von Aurora Serverless v1 in Aurora Serverless v2 konvertieren können. Es gibt immer einen Zwischenschritt, bei dem der Aurora Serverless v1-DB-Cluster in einen bereitgestellten Cluster konvertiert wird.

Mit Aurora MySQL kompatible DB-Cluster

Sie können Ihren Aurora Serverless v1 DB-Cluster in einen bereitgestellten DB-Cluster konvertieren und ihn dann mit einer blauen/grünen Bereitstellung aktualisieren und in einen Aurora Serverless v2 DB-Cluster konvertieren. Wir empfehlen dieses Verfahren für Produktionsumgebungen. Weitere Informationen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

Um eine blaue/grüne Bereitstellung für ein Upgrade eines Aurora Serverless v1 Clusters zu verwenden, auf dem Aurora MySQL Version 2 (MySQL 5.7-kompatibel) ausgeführt wird

1. Konvertieren Sie den DB-Cluster von Aurora Serverless v1 in einen bereitgestellten Cluster von Aurora MySQL Version 2. Folgen Sie dem Verfahren unter Konvertieren von Aurora Serverless v1 in bereitgestellt.
2. Erstellen Sie eine blaue/grüne Bereitstellung. Folgen Sie dem Verfahren unter Erstellen einer Blau/Grün-Bereitstellung.
3. Wählen Sie eine Aurora MySQL-Version für den grünen Cluster, die beispielsweise mit Aurora Serverless v2 3.04.1 kompatibel ist.

   Eine Liste kompatibler Versionen finden Sie unter Aurora Serverless v2 mit Aurora MySQL.
4. Ändern Sie die Writer-DB-Instance des grünen Clusters so, dass sie die DB-Instance-Klasse Serverless v2 (db.serverless) verwendet.

Details hierzu finden Sie unter Konvertieren eines bereitgestellten Writers oder Readers in Aurora Serverless v2.

5. Wenn Ihr aktualisiertes Aurora Serverless v2 DB-Cluster verfügbar ist, wechseln Sie vom blauen Cluster zum grünen Cluster.

Mit Aurora PostgreSQL kompatible DB-Cluster

Sie können Ihren Aurora Serverless v1 DB-Cluster in einen bereitgestellten DB-Cluster konvertieren und ihn dann mit einer blauen/grünen Bereitstellung aktualisieren und in einen Aurora Serverless v2 DB-Cluster konvertieren. Wir empfehlen dieses Verfahren für Produktionsumgebungen. Weitere Informationen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.

So verwenden Sie eine blaue/grüne Bereitstellung für ein Upgrade eines Aurora Serverless v1 Clusters, auf dem Aurora PostgreSQL Version 11 ausgeführt wird

1. Konvertieren Sie den DB-Cluster von Aurora Serverless v1 in einen bereitgestellten Cluster von Aurora PostgreSQL. Folgen Sie dem Verfahren unter Konvertieren von Aurora Serverless v1 in bereitgestellt.
2. Erstellen Sie eine blaue/grüne Bereitstellung. Folgen Sie dem Verfahren unter Erstellen einer Blau/Grün-Bereitstellung.
3. Wählen Sie eine Aurora PostgreSQL-Version für den grünen Cluster, die beispielsweise mit 15.3 Aurora Serverless v2 kompatibel ist.

   Eine Liste kompatibler Versionen finden Sie unter Aurora Serverless v2 mit Aurora PostgreSQL.
4. Ändern Sie die Writer-DB-Instance des grünen Clusters so, dass sie die DB-Instance-Klasse Serverless v2 (db.serverless) verwendet.

   Details hierzu finden Sie unter Konvertieren eines bereitgestellten Writers oder Readers in Aurora Serverless v2.
5. Wenn Ihr aktualisiertes Aurora Serverless v2 DB-Cluster verfügbar ist, wechseln Sie vom blauen Cluster zum grünen Cluster.

Sie können Ihren Aurora Serverless v1 DB-Cluster auch direkt von Aurora PostgreSQL Version 11 auf Version 13 aktualisieren, ihn in einen bereitgestellten DB-Cluster konvertieren und dann den bereitgestellten Cluster in einen DB-Cluster konvertieren. Aurora Serverless v2

Um ein Upgrade durchzuführen, konvertieren Sie dann einen Aurora Serverless v1 Cluster, auf dem Aurora PostgreSQL Version 11 ausgeführt wird

1. Führen Sie ein Upgrade des Aurora Serverless v1 Clusters auf eine Aurora PostgreSQL-Version 13 durch, die beispielsweise mit Aurora Serverless v2 13.12 kompatibel ist. Folgen Sie dem Verfahren unter Durchführen eines Upgrades der Hauptversion.

   Eine Liste kompatibler Versionen finden Sie unter Aurora Serverless v2 mit Aurora PostgreSQL.
2. Konvertieren Sie den DB-Cluster von Aurora Serverless v1 in einen bereitgestellten Cluster von Aurora PostgreSQL. Folgen Sie dem Verfahren unter Konvertieren von Aurora Serverless v1 in bereitgestellt.
3. Fügen Sie dem Cluster eine Aurora Serverless v2 Reader-DB-Instance hinzu. Weitere Informationen finden Sie unter Hinzufügen eines Aurora Serverless v2-Readers.
4. Führen Sie einen Failover zur Aurora Serverless v2 DB-Instance durch:

   a. Wählen Sie die Writer-DB-Instance des DB-Clusters aus.

   b. Wählen Sie für Aktionen die Option Failover aus.

   c. Wählen Sie auf der Bestätigungsseite Failover aus.

Für Aurora Serverless v1 DB-Cluster, auf denen Aurora PostgreSQL Version 13 ausgeführt wird, konvertieren Sie den Aurora Serverless v1 Cluster in einen bereitgestellten DB-Cluster und anschließend den bereitgestellten Cluster in einen DB-Cluster. Aurora Serverless v2

So führen Sie ein Upgrade eines Clusters von Aurora Serverless v1 durch, auf dem Aurora PostgreSQL Version 13 ausgeführt wird

1. Konvertieren Sie den DB-Cluster von Aurora Serverless v1 in einen bereitgestellten Cluster von Aurora PostgreSQL. Folgen Sie dem Verfahren unter Konvertieren von Aurora Serverless v1 in bereitgestellt.
2. Fügen Sie dem Cluster eine Aurora Serverless v2 Reader-DB-Instance hinzu. Weitere Informationen finden Sie unter Hinzufügen eines Aurora Serverless v2-Readers.
3. Führen Sie einen Failover zur Aurora Serverless v2 DB-Instance durch:

   a. Wählen Sie die Writer-DB-Instance des DB-Clusters aus.

   b. Wählen Sie für Aktionen die Option Failover aus.

   c. Wählen Sie auf der Bestätigungsseite Failover aus.

Migrieren einer On-Premises-Datenbank zu Aurora Serverless v2

Sie können Ihre On-Premises-Datenbanken zu Aurora Serverless v2 migrieren, genau wie bei bereitgestellten Aurora MySQL und Aurora PostgreSQL.

- Für MySQL-Datenbanken können Sie den `mysqldump`-Befehl verwenden. Weitere Informationen finden Sie unter Importieren von Daten in eine MySQL- oder -MariaDB-Datenbank-Instance mit reduzierter Ausfallzeit.
- Für PostgreSQL-Datenbanken können Sie die Befehle `pg_dump` und `pg_restore` verwenden. Weitere Informationen finden Sie im Blog-Beitrag Best practices for migrating PostgreSQL databases to Amazon RDS and Amazon Aurora (Bewährte Methoden für die Migration von PostgreSQL Datenbanken zu RDS und Amazon Aurora).

Verwenden von Amazon Aurora Serverless v1

Amazon Aurora Serverless v1 (Amazon Aurora Serverless Version 1) ist eine bedarfsabhängige Konfiguration der automatischen Skalierung für Amazon Aurora. Ein Aurora Serverless v1-DB-Cluster ist ein DB-Cluster, der die Rechenkapazität abhängig von den Anforderungen Ihrer Anwendung skaliert. Im Gegensatz dazu wird bei von Aurora bereitgestellten DB-Clustern die Kapazität manuell verwaltet. Aurora Serverless v1 bietet eine relativ einfache, kostengünstige Option für selten oder vorübergehend auftretende oder unvorhersehbare Workloads. Dies ist kosteneffektiv, weil es basierend auf den Anforderungen Ihrer Anwendung automatisch gestartet und die Rechenkapazität skaliert wird, sodass sie mit der Nutzung durch Ihre Anwendung übereinstimmt, und heruntergefahren wird, wenn es nicht verwendet wird.

Weitere Informationen zu den Preisen finden Sie unter Serverless-Preise unter MySQL-kompatible Edition oder PostgreSQL-kompatible Edition auf der Seite Amazon Aurora pricing.

Aurora Serverless v1-Cluster verfügen über die gleiche Art von verteiltem und hochverfügbarem Speicher-Volumen mit hoher Kapazität, das von bereitgestellten DB-Clustern verwendet wird.

Bei einem Aurora Serverless v2-Cluster können Sie auswählen, ob das Cluster-Volume verschlüsselt werden soll.

Bei einem Aurora Serverless v1-Cluster ist das Cluster-Volume immer verschlüsselt. Sie können den Verschlüsselungsschlüssel auswählen, aber Sie können die Verschlüsselung nicht deaktivieren. Das bedeutet, dass Sie für Aurora Serverless v1 die gleichen Vorgänge ausführen können wie für verschlüsselte Snapshots. Weitere Informationen finden Sie unter Aurora Serverless v1 und Snapshots.

Themen

- Wiederherstellen eines Aurora Serverless v1-DB-Clusters
- Ändern eines Aurora Serverless v1-DB-Clusters
- Manuelles Skalieren der Kapazität des Aurora Serverless v1-DB-Clusters
- Anzeigen von Aurora Serverless v1-DB-Clustern
- Löschen eines Aurora Serverless v1-DB-Clusters
- Aurora Serverless v1- und Aurora-Datenbank-Engine-Versionen

> **Important**
>
> Aurora verfügt über zwei Generationen serverloser Technologie: Aurora Serverless v2 und Aurora Serverless v1. Wenn Ihre Anwendung unter MySQL 8.0 oder PostgreSQL 13 ausgeführt werden kann, empfehlen wir Ihnen, Aurora Serverless v2 zu verwenden. Aurora Serverless v2 skaliert schneller und stärker granular. Aurora Serverless v2 bietet außerdem mehr Kompatibilität mit anderen Aurora-Funktionen wie Reader-DB-Instances. Wenn Sie also bereits mit Aurora vertraut sind, müssen Sie nicht so viele neue Verfahren oder Einschränkungen für Aurora Serverless v2 erlernen wie für Aurora Serverless v1. Weitere Informationen über Aurora Serverless v2 finden Sie unter Verwenden von Aurora Serverless v2.

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Aurora-Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen zur Verfügbarkeit von Versionen und Regionen im Zusammenhang mit Aurora und Aurora Serverless v1 finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless Version 1.

Vorteile von Aurora Serverless v1

Aurora Serverless v1 bietet folgende Vorteile:

- Einfacher als bereitgestellt – Aurora Serverless v1 eliminiert einen Großteil der Komplexität bei der Verwaltung von DB-Instances und -Kapazität.
- Skalierbar – Aurora Serverless v1 skaliert Rechen- und Speicherkapazität nahtlos nach Bedarf, ohne dass die Client-Verbindungen gestört werden.

- Kosteneffektiv – Wenn Sie Aurora Serverless v1 verwenden, zahlen Sie nur für die Datenbankressourcen, die Sie verbrauchen – auf Sekundenbasis.
- Hochverfügbarer Speicher – Aurora Serverless v1 verwendet dasselbe fehlertolerante verteilte Speichersystem mit sechsfacher Replikation wie Aurora, um vor Datenverlust zu schützen.

Anwendungsfälle für Aurora Serverless v1

Aurora Serverless v1 ist auf die folgenden Anwendungsfälle ausgelegt:

- Selten verwendete Anwendungen – Sie haben eine Anwendung, die mehrmals pro Tag oder Woche nur für ein paar Minuten verwendet wird, wie beispielsweise eine Blog-Website mit geringem Volumen. Mit Aurora Serverless v1 zahlen Sie nur für die Datenbankressourcen, die Sie verbrauchen – auf Sekundenbasis.
- Neue Anwendungen – Sie stellen eine neue Anwendung bereit und sind sich nicht sicher, welche Instance-Größe Sie benötigen. Mit Aurora Serverless v1 können Sie einen Datenbankendpunkt erstellen und es der Datenbank überlassen, automatisch gemäß den Kapazitätsanforderungen Ihrer Anwendung zu skalieren.
- Variable Workloads – Sie führen eine nur wenig benutzte Anwendung aus, mit Spitzen von 30 Minuten bis zu mehreren Stunden ein paarmal pro Tag oder mehrere Male pro Jahr. Beispiele sind Anwendungen für die Personalabteilung oder für die Erstellung von Budgets oder Betriebsberichten. Mit Aurora Serverless v1 müssen Sie nicht mehr Spitzen- oder durchschnittliche Kapazitäten bereitstellen.
- Unvorhersehbare Workloads – Sie führen tägliche Workloads mit plötzlichen und unvorhersehbaren Aktivitätszuwächsen aus. Ein Beispiel dafür ist eine Verkehrs-Website, für die Aktivitätsspitzen entstehen, wenn es zu regnen beginnt. Mit Aurora Serverless v1 wird Ihre Datenbank automatisch auf die Kapazität skaliert, mit der die Spitzenlast Ihrer Anwendung erfüllt werden kann, und wieder herunterskaliert, wenn die Aktivitätsspitze vorbei ist.
- Entwicklungs- und Testdatenbanken – Ihre Entwickler verwenden Datenbanken während der Arbeitszeit, benötigen sie jedoch nachts oder am Wochenende nicht. Mit Aurora Serverless v1 wird Ihre Datenbank automatisch heruntergefahren, wenn sie nicht verwendet wird.
- Anwendungen für mehrere Mandanten – Mit Aurora Serverless v1 müssen Sie die Datenbankkapazität nicht für jede Anwendung in Ihrer Flotte einzeln verwalten. Aurora Serverless v1 verwaltet die individuelle Datenbankkapazität für Sie.

Einschränkungen von Aurora Serverless v1

Die folgenden Einschränkungen gelten für Aurora Serverless v1:

- Aurora Serverless v1 unterstützt die folgenden Funktionen nicht:
  - Globale Aurora-Datenbanken
  - Aurora-Replikate
  - AWS Identity and Access Management (IAM) Datenbankauthentifizierung
  - Rückverfolgung in Aurora
  - Datenbankaktivitätsstreams
  - Kerberos-Authentifizierung
  - Performance Insights
  - RDS-Proxy
  - Anzeigen von Protokollen in der AWS Management Console
- Verbindungen zu einem Aurora Serverless v1-DB-Cluster werden automatisch geschlossen, wenn sie länger als einen Tag offen gehalten werden.
- Alle Aurora Serverless v1-DB-Cluster haben die folgenden Einschränkungen:
  - Sie können keine Aurora Serverless v1-Snapshots in Amazon-S3-Buckets exportieren.
  - Sie können AWS Database Migration Service und die Erfassung von Datenänderungen (CDC) nicht mit Aurora Serverless v1-DB-Clustern verwenden. Nur bereitgestellte Aurora-DB-Cluster unterstützen CDC mit AWS DMS als Quelle.
  - Sie können Daten nicht als Textdateien in Amazon S3 speichern oder Daten aus Textdateien aus S3 in Aurora Serverless v1 laden.
  - Sie können eine IAM-Rolle nicht einem Aurora Serverless v1-DB-Cluster anfügen. Sie können jedoch Daten aus Amazon S3 in Aurora Serverless v1 laden, indem Sie die `aws_s3`-Erweiterung mit der Funktion `aws_s3.table_import_from_s3` und dem Parameter `credentials` verwenden. Weitere Informationen finden Sie unter Importieren von Amazon S3 in einen Aurora-PostgreSQL-DB-Cluster.
  - Wenn Sie den Query Editor verwenden, wird ein Secrets-Manager-Secret für die DB-Anmeldeinformationen für den Zugriff auf die Datenbank erstellt. Wenn Sie die Anmeldeinformationen aus dem Query Editor löschen, wird das zugehörige Secret auch aus Secrets Manager gelöscht. Sie können dieses Secret nach dem Löschen nicht wiederherstellen.

- Aurora-MySQL-basierte DB-Cluster, auf denen Aurora Serverless v1 ausgeführt wird, unterstützen Folgendes nicht:
  - Aufrufen von AWS Lambda-Funktionen innerhalb des Aurora-MySQL-DB-Clusters. AWS Lambda-Funktionen können jedoch Aufrufe ans Aurora Serverless v1-DB-Cluster tätigen.
  - Wiederherstellen eines Snapshots aus einer DB-Instance, die nicht Aurora MySQL oder RDS for MySQL ist
  - Replizieren von Daten mit auf binären Protokollen basierender Replikation. Diese Einschränkung gilt unabhängig davon, ob Ihr Aurora-MySQL-basierter DB-Cluster Aurora Serverless v1 die Quelle oder das Ziel der Replikation ist. Um Daten aus einer MySQL-DB-Instance außerhalb von Aurora, z. B. aus einer in Amazon EC2 ausgeführten Instance, in einen Aurora Serverless v1-DB-Cluster zu replizieren, sollten Sie die Verwendung von AWS Database Migration Service erwägen. Weitere Informationen finden Sie im AWS Database Migration Service-Benutzerhandbuch.
  - Erstellen von Benutzern mit hostbasiertem Zugriff (`'username'@'IP_address'`). Das liegt daran, dass Aurora Serverless v1 eine Router-Flotte zwischen dem Client und dem Datenbankhost für eine nahtlose Skalierung verwendet. Die IP-Adresse, die der Aurora Serverless-DB-Cluster sieht, ist die des Router-Hosts und nicht die Ihres Clients. Weitere Informationen finden Sie unter Aurora Serverless v1-Architektur.

    Verwenden Sie stattdessen den Platzhalter (`'username'@'%'`).
- Aurora-PostgreSQL-basierte DB-Cluster, auf denen Aurora Serverless v1 ausgeführt wird, haben die folgenden Einschränkungen:
  - Aurora-PostgreSQL-Abfrageplan-Verwaltung (`apg_plan_management`-Erweiterung) wird nicht unterstützt.
  - Die in Amazon RDS PostgreSQL und Aurora PostgreSQL verfügbare logische Replikationsfunktion wird nicht unterstützt.
  - Ausgehende Kommunikation, z. B. Kommunikation, die von Amazon RDS for PostgreSQL-Erweiterungen ermöglicht wird, wird nicht unterstützt. Beispielsweise können Sie mit der Erweiterung `postgres_fdw/dblink` nicht auf externe Daten zugreifen. Weitere Informationen zu RDS PostgreSQL-Erweiterungen finden Sie unter PostgreSQL in Amazon RDS im RDS-Benutzerhandbuch.
  - Derzeit werden bestimmte SQL-Abfragen und -Befehle nicht empfohlen. Dazu gehören empfohlene Sperren auf Sitzungsebene, temporäre Beziehungen, asynchrone Benachrichtigungen (`LISTEN`) und Cursors with Hold (`DECLARE name ... CURSOR WITH`

`HOLD FOR query`). `NOTIFY`-Befehle verhindern außerdem eine Skalierung und werden nicht empfohlen.

Weitere Informationen finden Sie unter Automatische Skalierung für Aurora Serverless v1.

- Sie können das bevorzugte automatisierte Backup-Fenster für einen Aurora Serverless v1-DB-Cluster nicht festlegen.
- Sie können das Wartungszeitfenster für einen DB-Cluster von Aurora Serverless v1 einstellen. Weitere Informationen finden Sie unter Anpassen des bevorzugten DB-Cluster-Wartungsfensters.

Anforderungen an die Konfiguration von Aurora Serverless v1

Beachten Sie beim Erstellen eines Aurora Serverless v1-DB-Clusters die folgenden Anforderungen:

- Verwenden Sie diese spezifischen Portnummern für jede DB-Engine:
  - Aurora MySQL – `3306`
  - Aurora PostgreSQL – `5432`
- Erstellen Sie Ihr Aurora Serverless v1-DB-Cluster in einer Virtual Private Cloud (VPC), basierend auf dem Amazon-VPC-Service. Wenn Sie einen Aurora Serverless v1-DB-Cluster in Ihrer VPC erstellen, verbrauchen Sie zwei (2) der fünfzig (50) Interface- und Gateway Load Balancer-Endpunkte, die Ihrer VPC zugewiesen sind. Diese Endpunkte werden automatisch für Sie erstellt. Wenn Sie Ihr Kontingent erhöhen möchten, wenden Sie sich an AWS Support. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.
- Sie können einem Aurora Serverless v1-DB-Cluster keine öffentliche IP-Adresse geben. Sie können nur von einer VPC aus auf einen Aurora Serverless v1-DB-Cluster zugreifen.
- Erstellen Sie Subnetze in verschiedenen Availability Zones für die DB-Subnetzgruppe, die Sie für Ihren Aurora Serverless v1-DB-Cluster verwenden. Anders ausgedrückt: In einer Availability Zone kann sich nur ein Subnetz befinden.
- Änderungen an einer Subnetzgruppe, die von einem Aurora Serverless v1-DB-Cluster verwendet wird, werden nicht auf den Cluster angewendet.
- Sie können von Aurora Serverless v1 aus auf einen AWS Lambda-DB-Cluster zugreifen. Hierfür müssen Sie Ihre Lambda-Funktion so konfigurieren, dass sie in derselben VPC ausgeführt wird wie Ihr Aurora Serverless v1-DB-Cluster. Weitere Informationen über das Arbeiten mit AWS Lambda finden Sie unter Konfigurieren einer Lambda-Funktion für den Zugriff auf Ressourcen in einer Amazon VPC im AWS Lambda-Entwicklerhandbuch.

Verwenden von TLS/SSL mit Aurora Serverless v1

Aurora Serverless v1 verwendet standardmäßig das TLS-/SSL-Protokoll (Transport Layer Security/ Secure Sockets Layer), um die Kommunikation zwischen Clients und dem Aurora Serverless v1-DB-Cluster zu verschlüsseln. Die TLS-/SSL-Versionen 1.0, 1.1 und 1.2 werden unterstützt. Sie müssen Ihren Aurora Serverless v1-DB-Cluster nicht für die Verwendung von TLS/SSL konfigurieren.

Es gelten jedoch die folgenden Einschränkungen:

- Die Unterstützung von TLS/SSL für Aurora Serverless v1-DB-Cluster ist derzeit in der AWS-Region China (Peking) nicht verfügbar.
- Wenn Sie Datenbankbenutzer für einen Aurora-MySQL-basierten Aurora Serverless v1-DB-Cluster erstellen, verwenden Sie nicht die `REQUIRE`-Klausel für SSL-Berechtigungen. Diese verhindert, dass Benutzer eine Verbindung mit der Aurora-DB-Instance herstellen können.
- Sowohl bei MySQL-Client- als auch PostgreSQL-Client-Dienstprogrammen sind Sitzungsvariablen, die Sie möglicherweise in anderen Umgebungen verwenden, wirkungslos, wenn TLS/SSL zwischen Client und verwendet wir Aurora Serverless v1.
- Beim MySQL-Client müssen Sie beim Verbinden mit dem `VERIFY_IDENTITY`-Modus von TLS/ SSL derzeit den MySQL 8.0-kompatiblen `mysql`-Befehl verwenden. Weitere Informationen finden Sie unter Verbinden mit einer DB-Instance, auf der die MySQL-Datenbank-Engine ausgeführt wird.

Abhängig vom Client, den Sie für die Verbindung mit dem Aurora Serverless v1-DB-Cluster verwenden, müssen Sie möglicherweise TLS/SSL nicht angeben, um eine verschlüsselte Verbindung herzustellen. Um beispielsweise den PostgreSQL-Client zum Verbinden mit einem Aurora Serverless v1-DB-Cluster zu verwenden, auf dem die Aurora-PostgreSQL-kompatible Edition ausgeführt wird, verbinden Sie sich wie gewohnt.

```
psql -h endpoint -U user
```

Nachdem Sie Ihr Passwort eingegeben haben, zeigt der PostgreSQL-Client an, dass Sie die Verbindungsdetails sehen, einschließlich der TLS-/SSL-Version und der Verschlüsselung.

```
psql (12.5 (Ubuntu 12.5-0ubuntu0.20.04.1), server 10.12)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256,
 compression: off)
Type "help" for help.
```

Important

Aurora Serverless v1 verwendet das Protokoll Transport Layer Security/Secure Sockets Layer (TLS/SSL), um Verbindungen standardmäßig zu verschlüsseln, es sei denn, SSL/TLS ist von der Clientanwendung deaktiviert. Die TLS/SSL-Verbindung endet bei der Router-Flotte. Die Kommunikation zwischen der Router-Flotte und Ihrem Aurora Serverless v1-DB-Cluster erfolgt innerhalb der internen Netzwerkgrenze des Services.
Sie können den Status der Clientverbindung überprüfen, um zu prüfen, ob die Verbindung mit Aurora Serverless v1 TLS/SSL-verschlüsselt ist. Die PostgreSQL-Tabellen `pg_stat_ssl` und `pg_stat_activity` und die `ssl_is_used`-Funktion zeigen den TLS/SSL-Status für die Kommunikation zwischen der Clientanwendung und Aurora Serverless v1 nicht an. In ähnlicher Weise kann der TLS/SSL-Status nicht von der `status` MySQL-Anweisung abgeleitet werden.
Die Aurora-Clusterparameter `force_ssl` für PostgreSQL und `require_secure_transport` für MySQL wurden für Aurora Serverless v1 früher nicht unterstützt. Diese Parameter sind jetzt für Aurora Serverless v1 verfügbar. Eine vollständige Liste der von Aurora Serverless v1 unterstützten Parameter finden Sie, indem Sie die DescribeEngineDefaultClusterParameters-API-Operation aufrufen. Weitere Informationen zu Parametergruppen und Aurora Serverless v1 finden Sie unter Parametergruppen für Aurora Serverless v1.

Um den MySQL-Client zum Verbinden mit einem Aurora Serverless v1-DB-Cluster zu verwenden, auf dem die Aurora-MySQL-kompatible Edition ausgeführt wird, geben Sie in Ihrer Anforderung TLS/SSL an. Das folgende Beispiel umfasst den Amazon Root CA 1 Trust Store, der von Amazon Trust Services heruntergeladen wurde und für diese Verbindung erforderlich ist.

```
mysql -h endpoint -P 3306 -u user -p --ssl-ca=amazon-root-CA-1.pem --ssl-mode=REQUIRED
```

Geben Sie bei der Aufforderung Ihr Passwort ein. Kurz darauf öffnet sich der MySQL-Monitor. Sie können sich mit dem `status`-Befehl vergewissern, dass die Sitzung verschlüsselt ist.

```
mysql> status
--------------
mysql  Ver 14.14 Distrib 5.5.62, for Linux (x86_64) using readline 5.1
Connection id:          19
Current database:
Current user:           ***@*******
```

```
SSL:                    Cipher in use is ECDHE-RSA-AES256-SHA
...
```

Weitere Informationen zum Verbinden mit der Aurora MySQL-Datenbank über den MySQL-Client finden Sie unter Verbinden mit einer DB-Instance, auf der die MySQL-Datenbank-Engine ausgeführt wird.

Aurora Serverless v1 unterstützt alle für den MySQL-Client (`mysql`) und PostgreSQL-Client (`psql`) verfügbaren TLS-/SSL-Modi, einschließlich der in der folgenden Tabelle aufgeführten.

Beschreibung des TLS-/SSL-Modus	mysql-	psql
Verbinden ohne Verwendung von TLS/SSL	DISABLED	disable
Verbindung zuerst mit TLS/SSL probieren, bei Bedarf aber auf Nicht-SSL zurückgreifen	PREFERRED	bevorzugen (Standard)
Verwendung von TLS/SSL erzwingen	REQUIRED	require
TLS/SSL erzwingen und CA überprüfen	VERIFY_CA	verify-ca
TLS/SSL erzwingen, CA überprüfen und CA-Hostnamen überprüfen	VERIFY_IDENTITY	verify-full

Aurora Serverless v1 nutzt Platzhalter-Zertifikate. Wenn Sie bei Verwendung von TLS/SSL die Option "CA überprüfen" oder "CA und CA-Hostnamen überprüfen" angeben, laden Sie zuerst den Amazon Root CA 1 Trust Store von Amazon Trust Services herunter. Danach können Sie diese PEM-formatierte Datei in Ihrem Client-Befehl identifizieren. Beim PostgreSQL-Client gehen Sie so vor:

Für Linux, macOSoder Unix:

```
psql 'host=endpoint user=user sslmode=require sslrootcert=amazon-root-CA-1.pem
 dbname=db-name'
```

Weitere Informationen zum Arbeiten mit der Aurora PostgreSQL-Datenbank unter Verwendung des Postgres-Clients finden Sie unter Herstellen einer Verbindung zu einer DB-Instance, in der die PostgreSQL-Datenbank-Engine ausgeführt wird.

Weitere Informationen zum Verbinden mit Aurora-DB-Clustern im Allgemeinen finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

Unterstützte Verschlüsselungssammlungen für Verbindungen mit Aurora Serverless v1-DB-Clustern

Durch die Verwendung von konfigurierbaren Chiffrier-Suiten können Sie mehr Kontrolle über die Sicherheit Ihrer Datenbankverbindungen haben. Sie können eine Liste von Verschlüsselungssammlungen angeben, die Sie zum Sichern von TLS/SSL-Verbindungen zu Ihrer Datenbank des Clients zulassen möchten. Mit konfigurierbaren Chiffrier-Suiten können Sie die Verbindungsverschlüsselung steuern, die Ihr Datenbankserver akzeptiert. Dadurch wird die Verwendung von Verschlüsselungsverfahren verhindert, die nicht sicher sind oder nicht mehr verwendet werden.

Aurora Serverless v1-DB-Cluster, die auf Aurora MySQL basieren, unterstützen dieselben Verschlüsselungssammlungen wie von Aurora MySQL bereitgestellte DB-Cluster. Weitere Informationen über diese Verschlüsselungssammlungen finden Sie unter Konfigurieren von Cipher-Suites für Verbindungen mit Aurora-MySQL-DB-Clustern.

Aurora Serverless v1-DB-Cluster, die auf Aurora PostgreSQL basieren, unterstützen keine Chiffrier-Suiten.

Funktionsweise von Aurora Serverless v1

Im Folgenden erfahren Sie, wie Aurora Serverless v1 funktioniert.

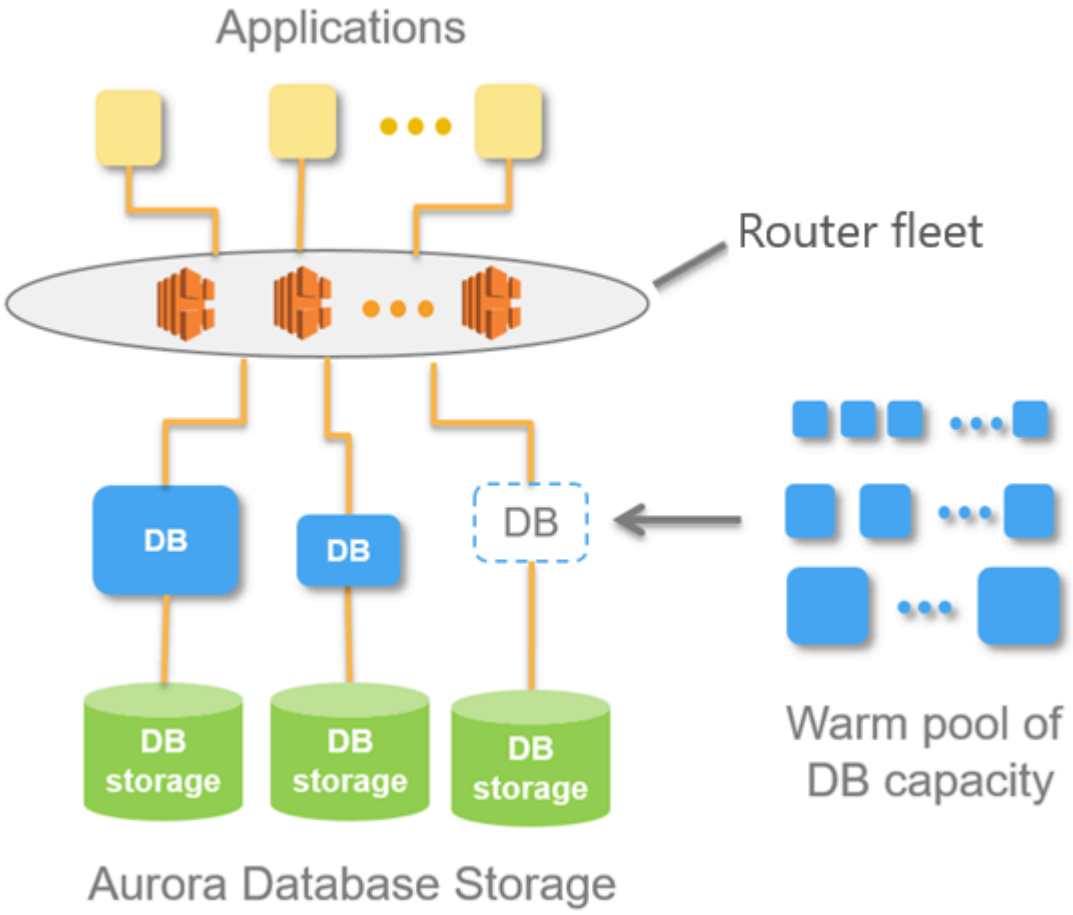
Themen

- Aurora Serverless v1-Architektur
- Automatische Skalierung für Aurora Serverless v1
- Timeout-Aktion für Kapazitätsänderungen
- Pausieren und Fortsetzen für Aurora Serverless v1

- Bestimmen der maximalen Anzahl von Datenbankverbindungen für Aurora Serverless v1
- Parametergruppen für Aurora Serverless v1
- Protokollierung für Aurora Serverless v1
- Aurora Serverless v1 und Wartung
- Aurora Serverless v1 und Failover
- Aurora Serverless v1 und Snapshots

Aurora Serverless v1-Architektur

Die folgende Abbildung zeigt einen Überblick über die Aurora Serverless v1-Architektur.



Anstelle der Bereitstellung und Verwaltung von Datenbankservern geben Sie Aurora Capacity Units (ACUs) an. Jede ACU ist eine Kombination aus etwa 2 Gigabyte (GB) Arbeitsspeicher, entsprechender CPU und Netzwerkleistung. Der Datenbankspeicher wird automatisch von 10 Gibibyte (GiB) auf 128 tebibytes (TiB) skaliert, genau wie Speicher in einem standardmäßigen Aurora-DB-Cluster.

Sie können die minimale und maximale ACU angeben. Die Mindestkapazitätseinheit von Aurora ist die kleinste ACU, auf die das DB-Cluster herabskaliert werden kann. Die maximale Kapazitätseinheit von Aurora ist die größte ACU, auf die das DB-Cluster hinaufskaliert werden kann. Basierend auf Ihren Einstellungen erstellt Aurora Serverless v1 automatisch Skalierungsregeln in Bezug auf Schwellenwerte für CPU-Auslastung, Verbindungen und verfügbaren Arbeitsspeicher.

Aurora Serverless v1 verwaltet den warmen Ressourcenpool in einer AWS-Region, um die Skalierungszeit zu minimieren. Wenn Aurora Serverless v1 dem Aurora-DB-Cluster neue Ressourcen hinzufügt, verwendet es die Routerflotte, um aktive Client-Verbindungen auf die neuen Ressourcen umzustellen. Zu jedem Zeitpunkt werden Ihnen nur die ACUs in Rechnung gestellt, die in Ihrem Aurora DB-Cluster aktiv genutzt werden.

Automatische Skalierung für Aurora Serverless v1

Die Ihrem Aurora Serverless v1-DB-Cluster zugewiesene Kapazität wird basierend auf der von Ihrer Client-Anwendung generierten Last nahtlos auf- und abwärts skaliert. Hier ist die Last die CPU-Auslastung und die Anzahl der Verbindungen. Wenn die Kapazität durch eine dieser beiden Faktoren eingeschränkt wird, wird Aurora Serverless v1 skaliert. Aurora Serverless v1 skaliert auch, wenn Leistungsprobleme erkannt werden, die dadurch gelöst werden können.

Sie können Skalierungsereignisse für Ihre Aurora Serverless v1-Cluster in AWS Management Console einsehen. Während der automatischen Skalierung setzt Aurora Serverless v1 die `EngineUptime`-Metrik zurück. Der Wert des zurückgesetzten Metrikwertes bedeutet weder, dass die nahtlose Skalierung Probleme hatte, noch, dass Aurora Serverless v1 Verbindungen unterbrochen hat. Er ist einfach der Ausgangspunkt für die Betriebszeit bei der neuen Kapazität. Weitere Informationen über Metriken finden Sie unter Überwachung von Metriken in einem Amazon-Aurora-Cluster.

Wenn Ihr Aurora Serverless v1-DB-Cluster keine aktiven Verbindungen hat, kann er auf Kapazität Null skaliert werden (0 ACUs). Weitere Informationen hierzu finden Sie unter Pausieren und Fortsetzen für Aurora Serverless v1.

Wenn er einen Skalierungsvorgang durchführen muss, versucht Aurora Serverless v1 zuerst einen Skalierungspunkt zu identifizieren, ein Moment, in dem keine Anfragen bearbeitet werden. Aurora Serverless v1 kann aus folgenden Gründen möglicherweise keinen Skalierungspunkt finden:

- Lang laufende Anfragen
- Transaktionen in Bearbeitung
- Temporäre Tabellen oder Tabellensperren

Um die Erfolgsrate Ihres Aurora Serverless v1-DB-Clusters bei der Suche nach einem Skalierungspunkt zu erhöhen, empfehlen wir, lang andauernde Abfragen und lang andauernde Transaktionen zu vermeiden. Weitere Informationen zu Operationen zum Blockieren von Skalierungen und wie Sie diese vermeiden können, finden Sie unter Bewährte Methoden für die Arbeit mit Aurora Serverless v1.

Standardmäßig versucht Aurora Serverless v1, einen Skalierungspunkt für 5 Minuten (300 Sekunden) zu finden. Sie können bei der Erstellung oder Änderung des Clusters eine andere Zeitspanne festlegen. Die Timeout-Zeit kann zwischen 60 Sekunden und 10 Minuten (600 Sekunden) liegen. Wenn Aurora Serverless v1 innerhalb des angegebenen Zeitraums keinen Skalierungspunkt finden kann, wird der Autoskalierungsvorgang abgebrochen.

Standardmäßig, wenn automatischen Skalierung vor dem Timeout keinen Skalierungspunkt findet, hält Aurora Serverless v1 den Cluster auf der aktuellen Kapazität. Sie können dieses Standardverhalten bei der Erstellung oder Änderung Ihres Aurora Serverless v1 DB-Clusters ändern, indem Sie die Option Kapazitätsänderung erzwingen auswählen. Weitere Informationen finden Sie unter Timeout-Aktion für Kapazitätsänderungen.

Timeout-Aktion für Kapazitätsänderungen

Wenn die automatische Skalierung abbricht, ohne einen Skalierungspunkt zu finden, behält Aurora standardmäßig die aktuelle Kapazität bei. Sie können festlegen, dass Aurora die Änderung erzwingt, indem Sie die Option Force the capacity change (Kapazitätsänderung erzwingen) aktivieren. Diese Option ist im Abschnitt Autoscaling timeout and action (Autoscaling-Timeout und -Aktion) auf der Seite Create database (Datenbank erstellen) verfügbar, wenn Sie den Cluster erstellen.

Standardmäßig ist die Option Force the capacity change (Kapazitätsänderung erzwingen) deaktiviert. Lassen Sie diese Option deaktiviert, damit die Kapazität Ihres Aurora Serverless v1-DB-Clusters unverändert bleibt, wenn der Skalierungsvorgang ausläuft, ohne einen Skalierungspunkt zu finden.

Wenn Sie diese Option aktivieren, erzwingt Ihr Aurora Serverless v1-DB-Cluster die Kapazitätsänderung auch ohne Skalierungspunkt. Bevor Sie diese Option auswählen, sollten Sie sich der Konsequenzen dieser Auswahl bewusst sein:

- Alle In-Process-Transaktionen werden unterbrochen, und die folgende Fehlermeldung wird angezeigt.

  Aurora MySQL Version 2 – ERROR 1105 (HY000): Die letzte Transaktion wurde aufgrund nahtloser Skalierung abgebrochen. Bitte versuchen Sie es erneut.

Sie können die Transaktion erneut übermitteln, sobald Ihr Aurora Serverless v1-DB-Cluster verfügbar ist.

- Verbindungen zu temporären Tabellen und Sperren werden gelöscht.

  Wir empfehlen, dass Sie die Option Force the capacity change (Kapazitätsänderung erzwingen) nur dann auswählen, wenn Ihre Anwendung nach unterbrochenen Verbindungen oder unvollständigen Transaktionen wiederhergestellt werden kann.

Die Entscheidungen, die Sie in der AWS Management Console treffen, wenn Sie einen Aurora Serverless v1-DB-Cluster erstellen, werden im Objekt `ScalingConfigurationInfo` in den Eigenschaften `SecondsBeforeTimeout` und `TimeoutAction` gespeichert. Der Wert der `TimeoutAction`-Eigenschaft wird bei der Erstellung Ihres Clusters auf einen der folgenden Werte festgelegt:

- `RollbackCapacityChange` – Dieser Wert wird festgelegt, wenn Sie die Option Roll back the capacity change (Rückgängig machen der Kapazitätsänderung) auswählen. Dies ist das Standardverhalten.
- `ForceApplyCapacityChange` – Dieser Wert wird festgelegt, wenn Sie die Option Force the capacity change (Force the capacity change) auswählen.

Sie können den Wert dieser Eigenschaft für einen vorhandenen Aurora Serverless v1 DB-Cluster abrufen, indem Sie den -describe-db-clustersAWS CLIBefehl verwenden, wie im Folgenden gezeigt.

Für Linux, macOSoder Unix:

```
aws rds describe-db-clusters --region region \
  --db-cluster-identifier your-cluster-name \
  --query '*[].{ScalingConfigurationInfo:ScalingConfigurationInfo}'
```

Windows:

```
aws rds describe-db-clusters --region region ^
  --db-cluster-identifier your-cluster-name ^
  --query "*[].{ScalingConfigurationInfo:ScalingConfigurationInfo}"
```

Das folgende Beispiel zeigt die Abfrage und die Antwort für einen Aurora Serverless v1 DB-Cluster mit der Bezeichnung `west-coast-sles` in der Region US-West (Nordkalifornien).

```
$ aws rds describe-db-clusters --region us-west-1 --db-cluster-identifier west-coast-
sles
--query '*[].{ScalingConfigurationInfo:ScalingConfigurationInfo}'

[
    {
        "ScalingConfigurationInfo": {
            "MinCapacity": 1,
            "MaxCapacity": 64,
            "AutoPause": false,
            "SecondsBeforeTimeout": 300,
            "SecondsUntilAutoPause": 300,
            "TimeoutAction": "RollbackCapacityChange"
        }
    }
]
```

Wie die Antwort zeigt, verwendet dieser Aurora Serverless v1-DB-Cluster die Standardeinstellung.

Weitere Informationen finden Sie unter Erstellen eines Aurora Serverless v1-DB Clusters. Nach Erstellung Ihres Aurora Serverless v1, können Sie die Timeout-Aktion und andere Kapazitätseinstellungen jederzeit ändern. Um zu erfahren wie, siehe Ändern eines Aurora Serverless v1-DB-Clusters.

Pausieren und Fortsetzen für Aurora Serverless v1

Sie können festlegen, Ihren Aurora Serverless v1-DB-Cluster nach einer bestimmten Zeit ohne Aktivität zu pausieren. Sie geben die Zeitspanne ohne Aktivität an, bevor der DB-Cluster angehalten wird. Wenn Sie diese Option auswählen, beträgt die standardmäßige Inaktivitätszeit fünf Minuten. Sie können diesen Wert jedoch ändern. Dies ist eine optionale Einstellung.

Wenn der DB-Cluster pausiert wird, findet keine Rechen- oder Speicheraktivität statt, und es wird Ihnen nur die Speicherung in Rechnung gestellt. Wenn beim Anhalten eines Aurora Serverless v1 DB-Clusters Datenbankverbindungen angefordert werden, nimmt der DB-Cluster die Verbindungsanforderungen automatisch wieder auf und bedient sie.

Wenn der DB-Cluster die Aktivität fortsetzt, hat er die gleiche Kapazität wie beim Anhalten des Clusters durch Aurora. Die Anzahl der ACUs hängt davon ab, wie stark Aurora den Cluster nach oben oder unten skaliert hat, bevor er angehalten wurde.

> **Note**
>
> Wenn ein DB-Cluster für mehr als sieben Tage pausiert wird, könnte der DB-Cluster mit einem Snapshot gesichert werden. In diesem Fall stellt Aurora den DB-Cluster aus dem Snapshot wieder her, wenn eine Verbindungsanforderung vorliegt.

Bestimmen der maximalen Anzahl von Datenbankverbindungen für Aurora Serverless v1

Im Folgenden sind einige Beispiele für einen DB-Cluster von Aurora Serverless v1 aufgeführt, der mit MySQL 5.7 kompatibel ist. Sie können einen MySQL-Client oder den Abfrage-Editor verwenden, wenn Sie den Zugriff darauf konfiguriert haben. Weitere Informationen finden Sie unter Ausführen von Abfragen im Abfrage-Editor.

So ermitteln Sie die maximale Anzahl von Datenbankverbindungen

1. Ermitteln Sie den Kapazitätsbereich für Ihren DB-Cluster von Aurora Serverless v1 mithilfe der AWS CLI.

   ```
   aws rds describe-db-clusters \
       --db-cluster-identifier my-serverless-57-cluster \
       --query 'DBClusters[*].ScalingConfigurationInfo|[0]'
   ```

   Das Ergebnis zeigt, dass der Kapazitätsbereich 1 bis 4 ACU beträgt.

   ```
   {
       "MinCapacity": 1,
       "AutoPause": true,
       "MaxCapacity": 4,
       "TimeoutAction": "RollbackCapacityChange",
       "SecondsUntilAutoPause": 3600
   }
   ```

2. Führen Sie die folgende SQL-Abfrage aus, um die maximale Anzahl von Verbindungen zu ermitteln.

   ```
   select @@max_connections;
   ```

Das angezeigte Ergebnis gilt für die Mindestkapazität des Clusters, 1 ACU.

```
@@max_connections
90
```

3. Skalieren Sie den Cluster auf 8–32 ACU.

   Weitere Informationen zur Skalierung finden Sie unter Ändern eines Aurora Serverless v1-DB-Clusters.

4. Bestätigen Sie den Kapazitätsbereich.

```
{
    "MinCapacity": 8,
    "AutoPause": true,
    "MaxCapacity": 32,
    "TimeoutAction": "RollbackCapacityChange",
    "SecondsUntilAutoPause": 3600
}
```

5. Suchen Sie die maximale Anzahl von Verbindungen.

```
select @@max_connections;
```

   Das angezeigte Ergebnis gilt für die Mindestkapazität des Clusters, 8 ACU.

```
@@max_connections
1000
```

6. Skalieren Sie den Cluster auf die maximal mögliche Kapazität, 256–256 ACU.
7. Bestätigen Sie den Kapazitätsbereich.

```
{
    "MinCapacity": 256,
    "AutoPause": true,
    "MaxCapacity": 256,
    "TimeoutAction": "RollbackCapacityChange",
    "SecondsUntilAutoPause": 3600
}
```

8. Suchen Sie die maximale Anzahl von Verbindungen.

```
select @@max_connections;
```

Das angezeigte Ergebnis gilt für 256 ACU.

```
@@max_connections
6000
```

> **Note**
>
> Der Wert `max_connections` skaliert nicht linear mit der Anzahl der ACU.

9. Skalieren Sie den Cluster wieder herunter auf 1–4 ACU.

```
{
    "MinCapacity": 1,
    "AutoPause": true,
    "MaxCapacity": 4,
    "TimeoutAction": "RollbackCapacityChange",
    "SecondsUntilAutoPause": 3600
}
```

Dieses Mal gilt der Wert `max_connections` für 4 ACU.

```
@@max_connections
270
```

10. Lassen Sie den Cluster auf 2 ACU herunterskalieren.

```
@@max_connections
180
```

Wenn Sie den Cluster so konfiguriert haben, dass er nach einer gewissen Zeit im Leerlauf pausiert, skaliert er auf 0 ACU herunter. Allerdings fällt `max_connections` nicht unter den Wert für 1 ACU.

```
@@max_connections
90
```

Parametergruppen für Aurora Serverless v1

Wenn Sie Ihren Aurora Serverless v1-DB-Cluster erstellen, wählen Sie eine bestimmte Aurora-DB-Engine und eine zugehörige DB-Cluster-Parametergruppe. Im Gegensatz zu bereitgestellten Aurora-DB-Clustern, hat ein Aurora Serverless v1-DB-Cluster eine einzige DB-Instance mit Lese-/Schreibzugriff, die nur mit einer DB-Cluster-Parametergruppe — konfiguriert ist. Er hat keine separate DB-Parametergruppe. Während der automatischen Skalierung, muss Aurora Serverless v1 in der Lage sein, Parameter zu ändern, damit der Cluster optimal für die erhöhte oder verringerte Kapazität funktioniert. Das heißt, dass bei einem Aurora Serverless v1-DB-Cluster, einige der Änderungen, die Sie an Parametern für einen bestimmten DB-Engine-Typ vornehmen, möglicherweise nicht gelten.

Zum Beispiel kann ein Aurora-PostgreSQL–basierter Aurora Serverless v1-DB-Cluster `apg_plan_mgmt.capture_plan_baselines` und andere Parameter nicht verwenden, die auf bereitgestellten Aurora PostgreSQL-DB-Clustern für die Verwaltung von Abfrageplänen verwendet werden könnten.

Sie können eine Liste der Standardwerte für die Standardparametergruppen für die verschiedenen Aurora-DB-Engines abrufen, indem Sie den CLI-Befehl describe-engine-default-cluster-parameters verwenden und abfragenAWS-Region. Die folgenden Werte können Sie für die `--db-parameter-group-family`-Option verwenden.

Aurora-MySQL-Version 2	`aurora-mysql5.7`
Aurora-PostgreSQL-Version 11	`aurora-postgresql11`
Aurora PostgreSQL Version 13	`aurora-postgresql13`

Wir empfehlen Ihnen, Ihre AWS CLI mit Ihrer AWS-Zugriffsschlüssel-ID und Ihrem geheimen AWS-Zugriffsschlüssel zu konfigurieren, und Ihre AWS-Region vor der Verwendung der AWS CLI-Befehle einzustellen. Wenn Sie die Region Ihrer CLI-Konfiguration angeben, müssen Sie die `--region`-Parameter beim Ausführen von Befehlen nicht eingeben. Weitere Informationen über die Konfiguration von AWS CLI finden Sie unter Grundlagen der Konfiguration im AWS Command Line Interface-Benutzerhandbuch.

Im folgenden Beispiel wird eine Liste von Parametern aus der Standard-DB-Cluster-Gruppe für Aurora-MySQL-Version 2 gezeigt.

Für Linux, macOSoder Unix:

```
aws rds describe-engine-default-cluster-parameters \
  --db-parameter-group-family aurora-mysql5.7 --query \
  'EngineDefaults.Parameters[*].
{ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} | [?
contains(SupportedEngineModes, `serverless`) == `true`] | [*].{param:ParameterName}' \
  --output text
```

Windows:

```
aws rds describe-engine-default-cluster-parameters ^
   --db-parameter-group-family aurora-mysql5.7 --query ^
   "EngineDefaults.Parameters[*].
{ParameterName:ParameterName,SupportedEngineModes:SupportedEngineModes} | [?
contains(SupportedEngineModes, 'serverless') == `true`] | [*].{param:ParameterName}" ^
   --output text
```

Änderung von Parameterwerten für Aurora Serverless v1

Wie in Arbeiten mit Parametergruppen erläutert, können Sie Werte in einer Standardparametergruppe unabhängig von ihrem Typ (DB-Cluster-Parametergruppe, DB-Parametergruppe) nicht direkt ändern. Stattdessen erstellen Sie eine benutzerdefinierte Parametergruppe basierend auf der standardmäßigen DB-Cluster-Parametergruppe für Ihre Aurora-DB-Engine und ändern die Einstellungen nach Bedarf für diese Parametergruppe. Sie können beispielsweise einige der Einstellungen für Ihren Aurora Serverless v1 DB-Cluster ändern, um Abfragen zu protokollieren oder DB-Engine-spezifische Protokolle in Amazon hochzuladen CloudWatch.

So erstellen Sie eine benutzerdefinierte DB-Cluster-Parametergruppe

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Parameter groups (Parametergruppen).
3. Wählen Sie Parametergruppe erstellen aus, um den Parametergruppe-Detailbereich zu öffnen.
4. Wählen Sie die entsprechende Standard-DB-Cluster-Gruppe für die DB-Engine aus, die Sie für Ihren Aurora Serverless v1-DB-Cluster verwenden möchten. Wählen Sie dabei unbedingt die folgenden Optionen aus:

    a. Wählen Sie unter Parametergruppenfamilie die entsprechende Familie für die von Ihnen gewählte DB-Engine aus. Achten Sie darauf, dass Ihre Auswahl das Präfix `aurora-` im Namen enthält.

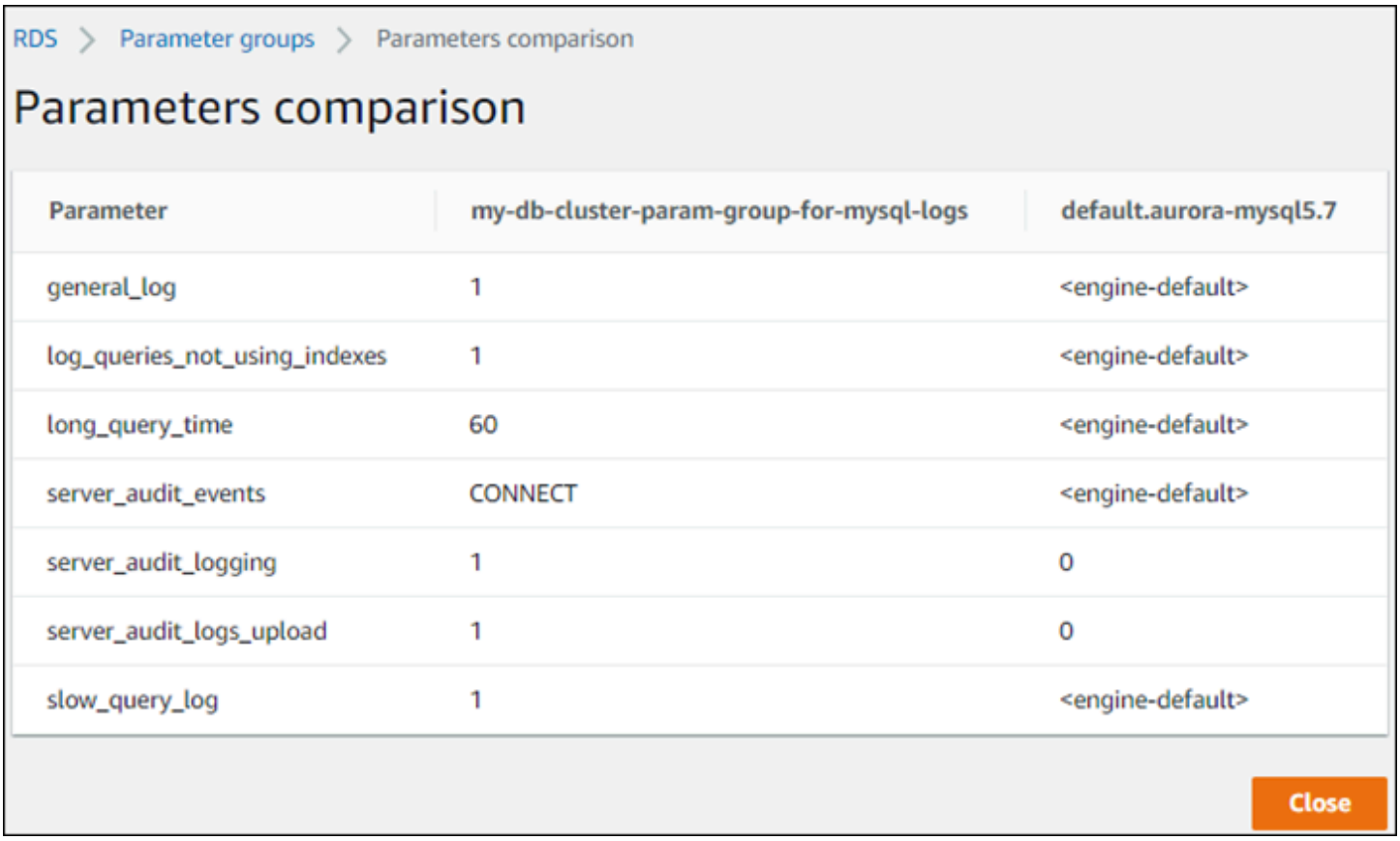
b. Wählen Sie für Typ die Option DB-Cluster-Parametergruppe.

c. Geben Sie für Gruppenname und Beschreibung aussagekräftige Namen für Sie oder andere ein, die möglicherweise mit Ihrem Aurora Serverless v1-DB-Cluster und dessen Parametern arbeiten müssen.

d. Wählen Sie Create aus.

Ihre benutzerdefinierte DB-Cluster-Parametergruppe wird der Liste der Parametergruppen hinzugefügt, die in Ihrer AWS-Region verfügbar sind. Sie können Ihre benutzerdefinierte DB-Cluster-Parametergruppe verwenden, wenn Sie neue Aurora Serverless v1-DB-Cluster erstellen. Sie können auch einen vorhandenen Aurora Serverless v1-DB-Cluster anpassen, sodass ser Ihre benutzerdefinierte DB-Cluster-Parametergruppe verwendet. Nachdem Ihr Aurora Serverless v1-DB-Cluster mit der Verwendung Ihrer benutzerdefinierten DB-Cluster-Parametergruppe begonnen hat, können Sie die Werte für dynamische Parameter mithilfe von AWS Management Console oder AWS CLI ändern.

Sie können auch die Konsole verwenden, um einen side-by-side Vergleich der Werte in Ihrer benutzerdefinierten DB-Cluster-Parametergruppe im Vergleich zur Standard-DB-Cluster-Parametergruppe anzuzeigen, wie im folgenden Screenshot gezeigt.



Wenn Sie Parameterwerte in einem aktiven DB-Cluster ändern, startet Aurora Serverless v1 eine nahtlose Skalierung, um die Parameteränderungen anzuwenden. Wenn Ihr Aurora Serverless v1-DB-Cluster sich in einem pausierten Zustand befindet, wird er fortgesetzt und beginnt mit der Skalierung, damit er die Änderung vornehmen kann. Der Skalierungsvorgang für eine Parametergruppe ändert immer Erzwingen einer Kapazitätsänderung. Beachten Sie daher, dass das Ändern von Parametern zu unterbrochenen Verbindungen führen kann, wenn während der Skalierungsperiode kein Skalierungspunkt gefunden werden kann.

Protokollierung für Aurora Serverless v1

Standardmäßig Aurora Serverless v1 werden Fehlerprotokolle für aktiviert und automatisch in Amazon hochgeladen CloudWatch. Sie können Ihren Aurora Serverless v1 DB-Cluster auch Aurora-Datenbank-Engine-spezifische Protokolle in hochladen lassen CloudWatch. Aktivieren Sie dazu die Konfigurationsparameter in Ihrer benutzerdefinierten DB-Cluster-Parametergruppe. Ihr Aurora Serverless v1 DB-Cluster lädt dann alle verfügbaren Protokolle auf Amazon hoch CloudWatch. An diesem Punkt können Sie verwenden, CloudWatch um Protokolldaten zu analysieren, Alarme zu erstellen und Metriken anzuzeigen.

Für Aurora MySQL zeigt die folgende Tabelle die Protokolle, die Sie aktivieren können. Wenn diese Option aktiviert ist, werden sie automatisch von Ihrem Aurora Serverless v1 DB-Cluster zu Amazon hochgeladen CloudWatch.

Aurora-MySQL-Protokoll	Beschreibung
`general_log`	Erstellt das allgemeine Protokoll. Stellen Sie zum Einschalten auf 1. Die Standardeinstellung ist aus (0).
`log_queries_not_using_indexes`	Protokolliert alle Abfragen im Slow-Query-Protokoll, das keinen Index verwendet. Die Standardeinstellung ist aus (0). Stellen Sie auf 1 ein, um dieses Protokoll zu aktivieren.
`long_query_time`	Verhindert, dass schnell ablaufende Abfragen im Protokoll für langsame Abfragen protokoll iert werden. Kann auf einen Gleitkommawert zwischen 0 und 31.536.000 festgelegt werden. Die Standardeinstellung ist 0 (nicht aktiv).

Aurora-MySQL-Protokoll	Beschreibung
`server_audit_events`	Die Liste der Ereignisse, die in den Protokollen erfasst werden sollen. Unterstützte Werte sind `CONNECT`, `QUERY`, `QUERY_DCL` , `QUERY_DDL` , `QUERY_DML` und `TABLE`.
`server_audit_logging`	Setzen Sie den Parameter auf 1, um die Serverprüfungsprotokollierung zu aktiviere n. Wenn Sie dies aktivieren, können Sie die Audit-Ereignisse angeben, die an gesendet werden sollen, CloudWatch indem Sie sie im `server_audit_events` Parameter auflisten.
`slow_query_log`	Erstellt ein Slow-Query-Protokoll. Auf 1 setzen, um das Slow-Query-Protokoll zu aktivieren. Die Standardeinstellung ist aus (0).

Weitere Informationen finden Sie unter Verwenden von Advanced Auditing in einem Amazon Aurora MySQL DB-Cluster.

Für Aurora PostgreSQL zeigt die folgende Tabelle die Protokolle, die Sie aktivieren können. Wenn diese Option aktiviert ist, werden sie CloudWatch zusammen mit den regulären Fehlerprotokollen automatisch von Ihrem Aurora Serverless v1 DB-Cluster zu Amazon hochgeladen.

Aurora-PostgreSQL-Protokoll	Beschreibung
`log_connections`	Standardmäßig aktiviert und kann nicht geändert werden. Protokolliert Details für alle neuen Client-Verbindungen.
`log_disconnections`	Standardmäßig aktiviert und kann nicht geändert werden. Protokolliert alle Client-Ve rbindungstrennungen.

Aurora-PostgreSQL-Protokoll	Beschreibung
`log_hostname`	Standardmäßig deaktiviert und kann nicht geändert werden. Hostnamen werden nicht protokolliert.
`log_lock_waits`	Der Standardwert ist 0 (aus). Stellen Sie auf 1 ein, um die Wartezeiten für die Sperrung zu protokollieren.
`log_min_duration_statement`	Die Mindestdauer (in Millisekunden), die eine Anweisung vor der Protokollierung ausgeführt wird.
`log_min_messages`	Legt die Nachrichtenebenen fest, die protokolliert werden. Unterstützte Werte sind , , , , , , , , , und `debug5`, `debug4`, `debug3`, `debug2`, `debug1`, `info`, `notice`, `warning`, `error`, `log`, `fatal`, `panic`. Zum Protokollieren von Leistungsdaten im `postgres`-Protokoll, setzen Sie den Wert auf `debug1` .
`log_temp_files`	Protokolliert die Verwendung von temporären Dateien, die über den angegebenen Kilobyte (kB) liegen.
`log_statement`	Steuert die spezifischen SQL-Anweisungen, die protokolliert werden. Unterstützte Werte sind `none`, `ddl`, `mod` und `all`. Der Standardwert ist `none`.

Nachdem Sie die Protokolle für Aurora MySQL oder Aurora PostgreSQL für Ihren Aurora Serverless v1 DB-Cluster aktiviert haben, können Sie die Protokolle in anzeigen CloudWatch.

Anzeigen von Aurora Serverless v1 Protokollen mit Amazon CloudWatch

Aurora Serverless v1 lädt automatisch alle CloudWatch Protokolle, die in Ihrer benutzerdefinierten DB-Cluster-Parametergruppe aktiviert sind, in Amazon hoch („veröffentlicht“). Sie müssen die Protokolltypen nicht auswählen oder angeben. Das Hochladen von Protokollen beginnt, sobald Sie den Protokollkonfigurationsparameter aktivieren. Wenn Sie den Protokoll-Parameter später deaktivieren, werden weitere Uploads angehalten. Alle Protokolle, die bereits veröffentlicht wurden, CloudWatch verbleiben jedoch, bis Sie sie löschen.

Weitere Informationen zur Verwendung von CloudWatch mit Aurora MySQL-Protokollen finden Sie unter Überwachen von Protokollereignissen in Amazon CloudWatch.

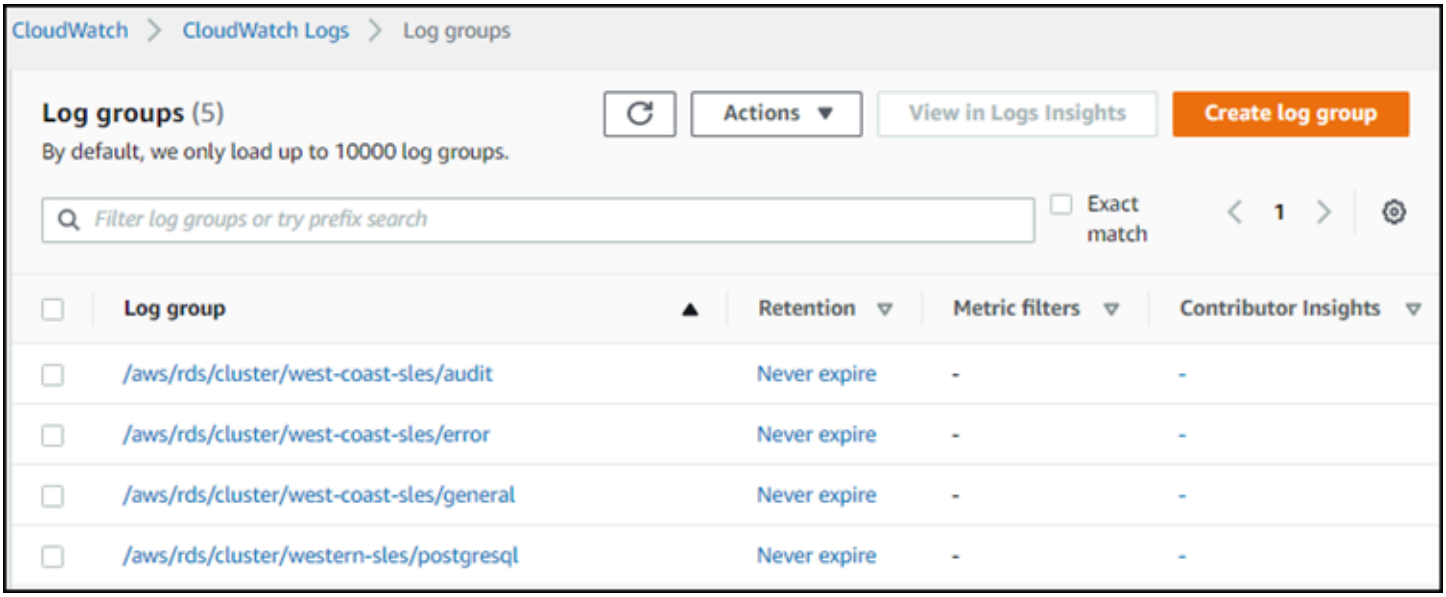
Weitere Informationen zu CloudWatch und Aurora PostgreSQL finden Sie unter Veröffentlichen von Aurora-PostgreSQL-Protokollen in Amazon CloudWatch Logs.

So zeigen Sie Protokolle für Ihren Aurora Serverless v1-DB-Cluster an:

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Ihre AWS-Region.
3. Wählen Sie Protokollgruppen.
4. Wählen Sie Ihr DB-Cluster-Protokoll für Aurora Serverless v1 in der Liste aus. Bei Fehlerprotokollen ist das Benennungsmuster wie folgt:

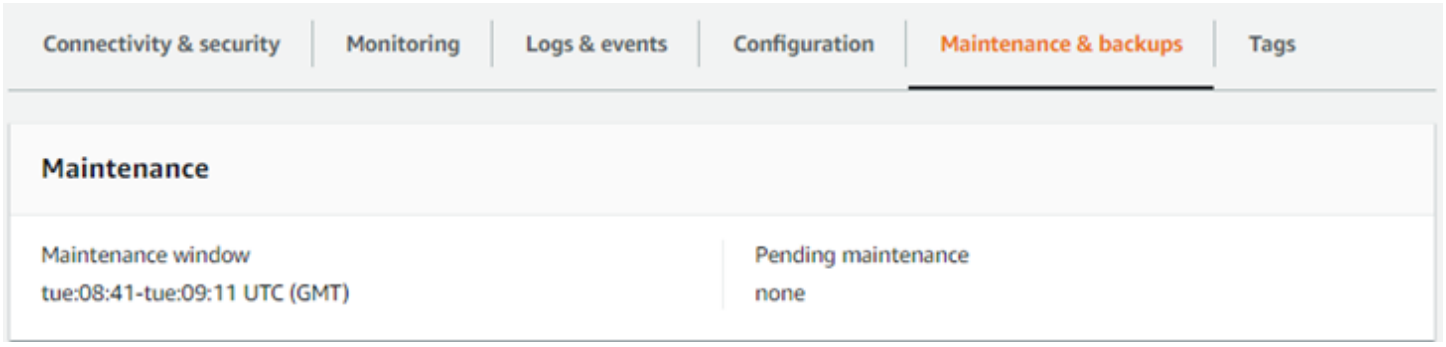
   ```
   /aws/rds/cluster/cluster-name/error
   ```

Im folgenden Screenshot finden Sie beispielsweise Verzeichnisse für Protokolle, die für einen Aurora PostgreSQL Aurora Serverless v1-DB-Cluster namens `western-sles` veröffentlicht wurden. Sie können auch mehrere Verzeichnisse für Aurora MySQL Aurora Serverless v1-DB-Cluster `west-coast-sles` finden. Wählen Sie das gewünschte Protokoll aus, um sich den Inhalt anzusehen.



Aurora Serverless v1 und Wartung

Die Wartung für Aurora Serverless v1-DB-Cluster, wie die Anwendung der neuesten Funktionen, Fehlerbehebungen und Sicherheitsupdates, wird automatisch für Sie durchgeführt. Aurora Serverless v1verfügt über ein Wartungsfenster, das Sie in der AWS Management Console unter Wartung und Sicherungen) für Ihren Aurora Serverless v1-DB-Cluster anzeigen können. Sie finden das Datum und die Uhrzeit, zu der die Wartung möglicherweise durchgeführt wird, und ob Wartungsarbeiten für Ihren Aurora Serverless v1 DB-Cluster ausstehen, wie in der folgenden Abbildung dargestellt.



Sie können das Wartungsfenster festlegen, wenn Sie den Aurora Serverless v1-DB-Cluster erstellen, und Sie können das Fenster später ändern. Weitere Informationen finden Sie unter Anpassen des bevorzugten DB-Cluster-Wartungsfensters.

Wartungsfenster werden für geplante Hauptversions-Upgrades verwendet. Nebenversions-Upgrades und Patches werden sofort während der Skalierung angewendet. Die Skalierung erfolgt entsprechend Ihrer Einstellung für `TimeoutAction`:

- `ForceApplyCapacityChange` – Die Änderung wird sofort angewendet.
- `RollbackCapacityChange` – Aurora aktualisiert den Cluster erzwingend nach 3 Tagen ab dem ersten Patch-Versuch.

Wie bei jeder Änderung, die ohne einen geeigneten Skalierungspunkt erzwungen wird, kann Ihr Workload dadurch unterbrochen werden.

Wann immer möglich, führt Aurora Serverless v1 die Wartung unterbrechungsfrei durch. Wenn eine Wartung erforderlich ist, skaliert Ihr Aurora Serverless v1-DB-Cluster seine Kapazität, damit die erforderlichen Vorgänge durchgeführt werden können. Vor dem Skalieren sucht Aurora Serverless v1 nach einem Skalierungspunkt. Dies geschieht bei Bedarf bis zu drei Tage lang.

Am Ende jedes Tages, an dem Aurora Serverless v1 keinen Skalierungspunkt finden kann, erstellt es ein Cluster-Ereignis. Dieses Ereignis informiert Sie über die ausstehende Wartung und die Notwendigkeit einer Skalierung für die Durchführung der Wartung. Die Benachrichtigung enthält auch das Datum, an dem Aurora Serverless v1 die Skalierung des DB-Clusters erzwingen kann.

Weitere Informationen finden Sie unter Timeout-Aktion für Kapazitätsänderungen.

Aurora Serverless v1 und Failover

Wenn die DB-Instance für einen Aurora Serverless v1-DB-Cluster nicht mehr verfügbar ist oder die Availability Zone (AZ), in der sie sich befindet, ausfällt, erstellt Aurora die DB-Instance in einer anderen AZ neu. Allerdings ist der Aurora Serverless v1-Cluster kein Multi-AZ-Cluster. Das liegt daran, dass er aus einer einzigen DB-Instance in einer einzigen AZ besteht. Dieser Failover-Mechanismus benötigt mehr Zeit als bei einem Aurora-Cluster mit bereitgestellten oder Aurora Serverless v2-Instances. Die Failover-Zeit für Aurora Serverless v1 ist nicht definiert, da sie von der Nachfrage sowie der Kapazität abhängt, die in anderen AZs innerhalb der angegebenen AWS-Region verfügbar ist.

Da Aurora die Datenverarbeitungskapazität und den Speicher voneinander trennt, ist das Speichervolumen für den Cluster auf mehrere AZs verteilt. Ihre Daten bleiben auch bei Ausfällen der DB-Instance oder der zugehörigen AZ verfügbar.

Aurora Serverless v1 und Snapshots

Das Cluster-Volume für einen Aurora Serverless v1-Cluster ist immer verschlüsselt. Sie können den Verschlüsselungsschlüssel auswählen, aber Sie können die Verschlüsselung nicht deaktivieren. Zum

Kopieren oder Freigeben eines Snapshots eines Aurora Serverless v1-Clusters verschlüsseln Sie den Snapshot mit Ihrem eigenen AWS KMS key. Weitere Informationen finden Sie unter Kopieren eines DB-Cluster-Snapshots. Weitere Informationen zur Verschlüsselung und zu Amazon Aurora finden Sie unter Verschlüsseln eines Amazon-Aurora-DB-Clusters.

Erstellen eines Aurora Serverless v1-DB Clusters

Mit dem folgenden Verfahren wird ein Aurora Serverless v1-Cluster ohne eines Ihrer Schemaobjekte oder Daten erstellt. Wenn Sie einen Aurora Serverless v1-Cluster erstellen möchten, der ein Duplikat eines vorhandenen bereitgestellten oder Aurora Serverless v1-Clusters ist, können Sie stattdessen eine Snapshot-Wiederherstellung oder einen Klonvorgang durchführen. Entsprechende Details finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot und Klonen eines Volumes für einen Amazon-Aurora-DB-Cluster. Sie können einen vorhandenen bereitgestellten Cluster nicht in Aurora Serverless v1 konvertieren. Sie können einen vorhandenen Aurora Serverless v1-Cluster auch nicht wieder in einen bereitgestellten Cluster konvertieren.

Wenn Sie einen Aurora Serverless v1-DB-Cluster erstellen, können Sie die Mindest- und Höchstkapazität für den Cluster festlegen. Eine Kapazitätseinheit entspricht einer bestimmten Rechen- und Arbeitsspeicherkonfiguration. Aurora Serverless v1 erstellt Skalierungsregeln in Bezug auf Schwellenwerte für die CPU-Auslastung, Verbindungen und den verfügbaren Arbeitsspeicher. Außerdem erfolgt eine nahtlose Skalierung auf einen Bereich von Kapazitätseinheiten, wie für Ihre Anwendungen erforderlich. Weitere Informationen finden Sie unter Aurora Serverless v1-Architektur.

Sie können die folgenden spezifischen Werte für Ihren Aurora Serverless v1-DB-Cluster festlegen:

- Minimale Aurora Capacity Unit – Aurora Serverless v1 kann die Kapazität bis zu dieser Kapazitätseinheit reduzieren.
- Maximale Aurora Capacity Unit – Aurora Serverless v1 kann die Kapazität bis zu dieser Kapazitätseinheit erhöhen.

Sie können auch die folgenden optionalen Skalierungskonfigurationsoptionen auswählen:

- Bei Zeitüberschreitung Skalierung der Kapazität auf die angegebenen Werte durchsetzen – Sie können diese Einstellung auswählen, wenn Sie möchten, dass Aurora Serverless v1 die Skalierung für Aurora Serverless v1 durchsetzt, auch wenn kein Skalierungspunkt gefunden wird, bevor die Zeitüberschreitung eintritt. Wenn Sie möchten, dass Aurora Serverless v1 Kapazitätsänderungen abbricht, wenn es keinen Skalierungspunkt findet, wählen Sie diese Einstellung nicht. Weitere Informationen finden Sie unter Timeout-Aktion für Kapazitätsänderungen.

- Rechenkapazität nach aufeinanderfolgenden Minuten von Inaktivität anhalten – Sie können diese Einstellung auswählen, wenn Sie möchten, dass Aurora Serverless v1 auf Null skaliert wird, wenn es für einen von Ihnen angegebenen Zeitraum keine Aktivität auf dem DB-Cluster gibt. Wenn diese Einstellung aktiviert ist, setzt der Aurora Serverless v1-DB-Cluster die Verarbeitung automatisch fort und wird auf die notwendige Kapazität skaliert, um den Workload zu verarbeiten, wenn der Datenbankdatenverkehr fortgesetzt wird. Weitere Informationen hierzu finden Sie unter Pausieren und Fortsetzen für Aurora Serverless v1.

Bevor Sie einen Aurora Serverless v1 DB-Cluster erstellen können, benötigen Sie ein AWS Konto. Sie müssen darüber hinaus die Einrichtungsaufgaben für die Arbeit mit Amazon Aurora abgeschlossen haben. Weitere Informationen finden Sie unter Einrichten Ihrer Umgebung für Amazon Aurora. Sie müssen auch andere vorab erforderliche Schritte zum Erstellen eines Aurora-DB-Clusters ausführen. Weitere Informationen hierzu finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Aurora Serverless v1ist nur in bestimmten Versionen AWS-Regionen und nur für bestimmte Aurora MySQL- und Aurora PostgreSQL-Versionen verfügbar. Weitere Informationen finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless Version 1.

> **Note**
>
> Das Cluster-Volume für einen Aurora Serverless v1-Cluster ist immer verschlüsselt. Wenn Sie Ihren Aurora Serverless v1-DB-Cluster erstellen, können Sie die Verschlüsselung nicht deaktivieren, aber Sie können Ihren eigenen Verschlüsselungsschlüssel verwenden. Bei Aurora Serverless v2 können Sie auswählen, ob das Cluster-Volume verschlüsselt werden soll.

Sie können einen Aurora Serverless v1 DB-Cluster mit der AWS Management Console, der oder der AWS CLI RDS-API erstellen.

> **Note**
>
> Wenn beim Versuch, den Cluster zu erstellen, die folgende Fehlermeldung angezeigt wird, benötigt Ihr Konto zusätzliche Berechtigungen.
> `Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.`

Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Aurora.

Sie können keine direkte Verbindung zur DB-Instance in Ihrem Aurora Serverless v1-DB-Cluster herstellen. Um eine Verbindung zum Aurora Serverless v1-DB-Cluster herzustellen, verwenden Sie den Datenbankendpunkt. Sie finden den Endpunkt für Ihren Aurora Serverless v1-DB-Cluster auf der Registerkarte Connectivity & security (Konnektivität und Sicherheit) für Ihren Cluster in der AWS Management Console. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

Konsole

Verwenden Sie das folgende allgemeine Verfahren. Weitere Informationen zum Erstellen eines Aurora-DB-Clusters mit dem AWS Management Console finden Sie unterErstellen eines Amazon Aurora-DB Clusters.

So erstellen Sie einen neuen Aurora Serverless v1-DB-Cluster

1. Melden Sie sich bei der an AWS Management Console.
2. Wählen Sie einen AWS-Region , der unterstütztAurora Serverless v1.
3. Wählen Sie Amazon RDS aus der AWS Serviceliste aus.
4. Wählen Sie Datenbank erstellen aus.
5. Auf der Seite Datenbank erstellen:

    a. Wählen Sie Standard-Erstellung als Datenbankerstellungsmethode.

    b. Fahren Sie fort mit dem Erstellen des Aurora Serverless v1-DB-Clusters, indem Sie den Schritten aus den folgenden Beispielen folgen.

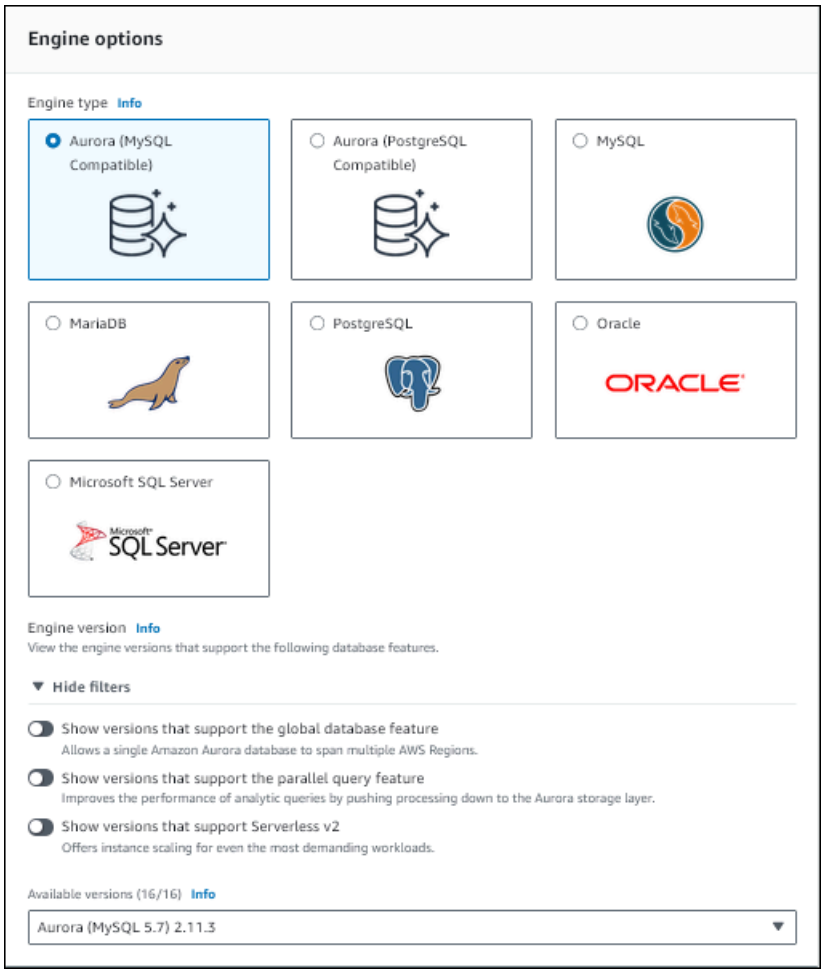
    > **Note**
    >
    > Wenn Sie eine Version der DB-Engine auswählen, die Aurora Serverless v1 nicht unterstützt, wird die Option Serverless für DB-Instance-Klasse nicht angezeigt.

Beispiel für Aurora MySQL

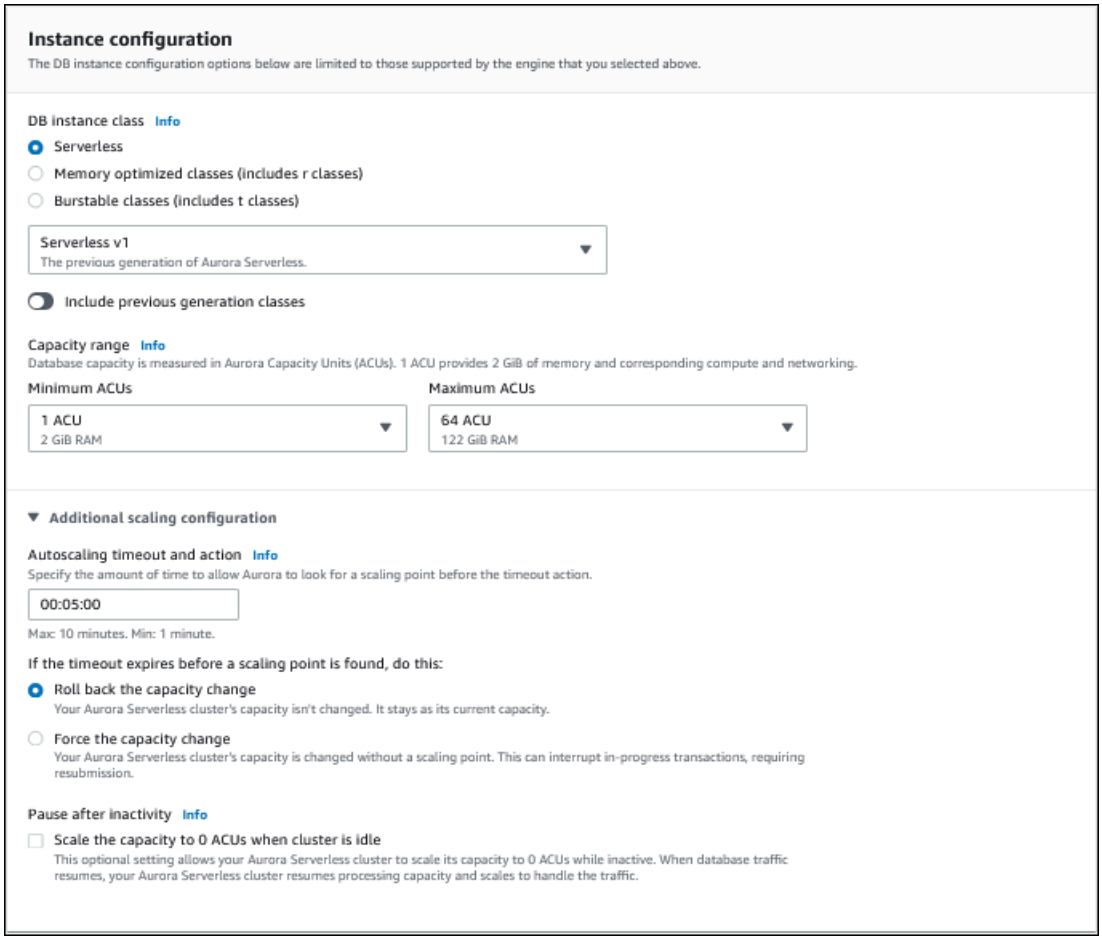
Gehen Sie wie folgt vor:

So erstellen Sie einen Aurora Serverless v1-DB-Cluster für Aurora MySQL

1. Wählen Sie als Engine-Typ Aurora (MySQL Compatibile).
2. Wählen Sie die gewünschte mit Aurora Serverless v1 kompatible Aurora-MySQL-Version für Ihren DB-Cluster aus. Die unterstützten Versionen werden rechts auf der Seite angezeigt.



3. Wählen Sie die DB-Instance-Klasse Serverless aus.
4. Legen Sie den Kapazitätsbereich für den DB-Cluster fest.
5. Passen Sie die Werte im Abschnitt Zusätzliche Skalierungskonfiguration der Seite nach Bedarf an. Weitere Informationen zu Kapazitätseinstellungen finden Sie unter Automatische Skalierung für Aurora Serverless v1.



6. Wenn Sie die Daten-API für Ihren Aurora Serverless v1-DB-Cluster aktivieren möchten, wählen Sie das Kontrollkästchen Data API (Daten-API) unter Additional configuration (Zusätzliche Konfiguration) im Abschnitt Connectivity (Konnektivität) aus.

   Weitere Informationen zur Daten-API finden Sie in der Verwenden der RDS-Daten-API.

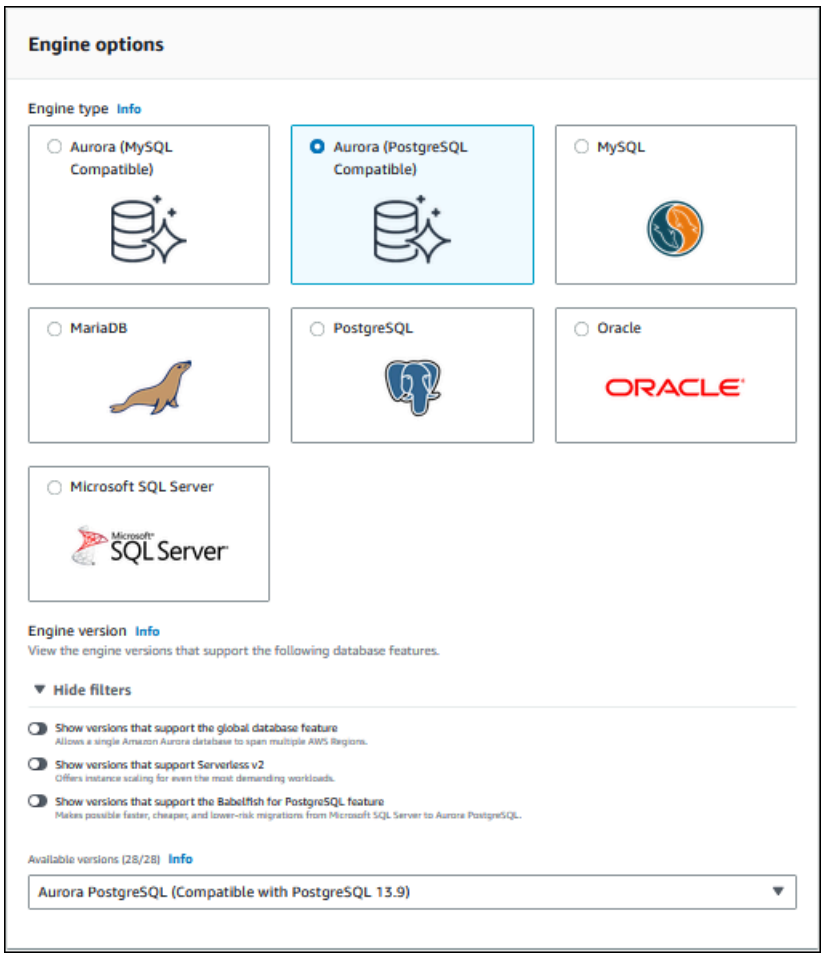
7. Wählen Sie andere Datenbankeinstellungen nach Bedarf und dann Create database (Datenbank erstellen) aus.

Beispiel für Aurora PostgreSQL

Gehen Sie wie folgt vor:

So erstellen Sie einen Aurora Serverless v1-DB-Cluster für Aurora PostgreSQL

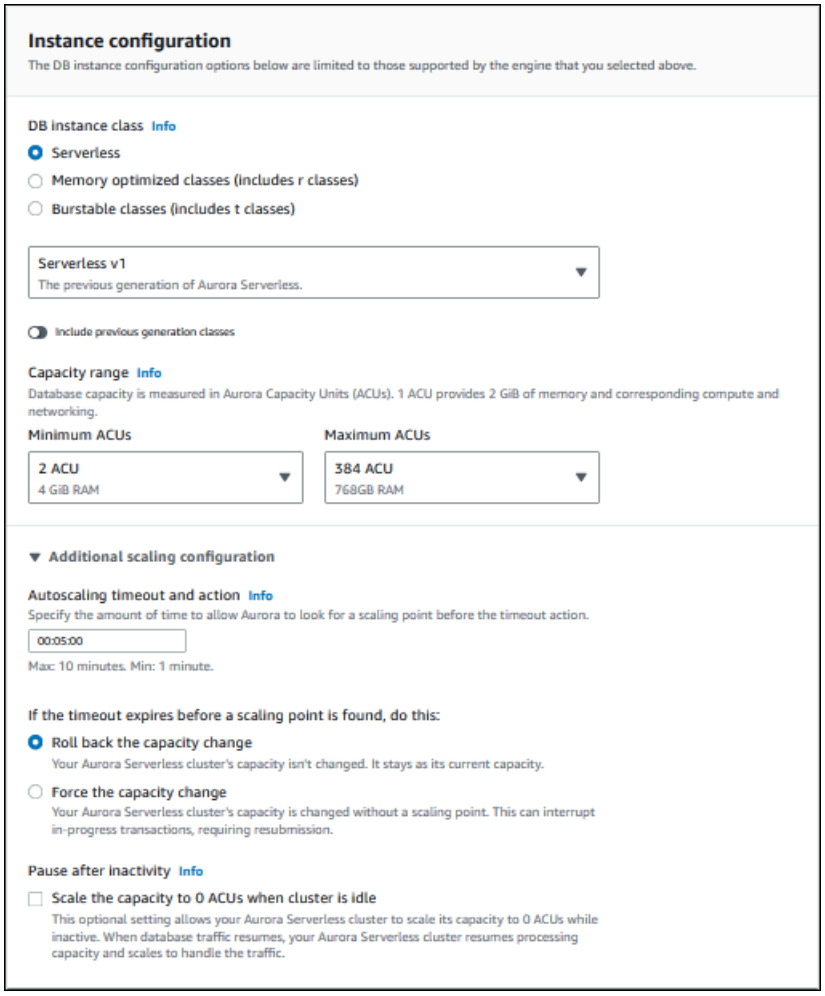
1. Wählen Sie als Engine-Typ Aurora (PostgreSQL Compatibile).
2. Wählen Sie die gewünschte mit Aurora Serverless v1 kompatible Aurora-PostgreSQL-Version für Ihren DB-Cluster aus. Die unterstützten Versionen werden rechts auf der Seite angezeigt.



3. Wählen Sie die DB-Instance-Klasse Serverless aus.
4. Wenn Sie sich für eine Aurora-PostgreSQL-Nebenversion 13 entschieden haben, wählen Sie Serverless v1 aus dem Menü aus.

> **Note**
>
> Aurora PostgreSQL Version 13 unterstützt auch Aurora Serverless v2.

5. Legen Sie den Kapazitätsbereich für den DB-Cluster fest.
6. Passen Sie die Werte im Abschnitt Zusätzliche Skalierungskonfiguration der Seite nach Bedarf an. Weitere Informationen zu Kapazitätseinstellungen finden Sie unter Automatische Skalierung für Aurora Serverless v1.



7. Wenn Sie die Daten-API mit ihrem DB-Cluster von Aurora Serverless v1 verwenden möchten, aktivieren Sie das Kontrollkästchen Daten-API unter Zusätzliche Konfiguration im Abschnitt Konnektivität.

   Weitere Informationen zur Daten-API finden Sie in der Verwenden der RDS-Daten-API.
8. Wählen Sie andere Datenbankeinstellungen nach Bedarf und dann Create database (Datenbank erstellen) aus.

AWS CLI

Um einen neuen Aurora Serverless v1 DB-Cluster mit dem zu erstellen AWS CLI, führen Sie den create-db-clusterBefehl aus und geben Sie `serverless` die `--engine-mode` Option an.

Optional können Sie die Option `--scaling-configuration` angeben, um die minimale Kapazität, die maximale Kapazität und die automatische Pause zu konfigurieren, wenn es keine Verbindungen gibt.

Die folgenden Befehlsbeispiele erstellen einen neuen Serverless DB-Cluster, indem Sie die `--engine-mode`-Option auf `serverless` festlegen. Die Beispiele definieren auch Werte für die `--scaling-configuration`-Option.

Beispiel für Aurora MySQL

Mit den folgenden Befehlen werden neue Aurora MySQL-kompatible Serverless-DB-Cluster erstellt. Gültige Kapazitätswerte für Aurora MySQL sind 1, 2, 4, 8, 16, 32, 64, 128 und 256.

Für LinuxmacOS, oderUnix:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster \
    --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.4 \
    --engine-mode serverless \
    --scaling-configuration
 MinCapacity=4,MaxCapacity=32,SecondsUntilAutoPause=1000,AutoPause=true \
    --master-username username --master-user-password password
```

Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster ^
    --engine aurora-mysql --engine-version 5.7.mysql_aurora.2.11.4 ^
    --engine-mode serverless ^
    --scaling-configuration
 MinCapacity=4,MaxCapacity=32,SecondsUntilAutoPause=1000,AutoPause=true ^
    --master-username username --master-user-password password
```

Beispiel für Aurora PostgreSQL

Mit dem folgenden Befehl wird ein neuer, mit PostgreSQL 13.9 kompatibler Serverless-DB-Cluster erstellt. Gültige Kapazitätswerte für Aurora PostgreSQL sind 2, 4, 8, 16, 32, 64, 192 und 384.

Für LinuxmacOS, oderUnix:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster \
    --engine aurora-postgresql --engine-version 13.9 \
    --engine-mode serverless \
    --scaling-configuration
 MinCapacity=8,MaxCapacity=64,SecondsUntilAutoPause=1000,AutoPause=true \
    --master-username username --master-user-password password
```

Windows:

```
aws rds create-db-cluster --db-cluster-identifier sample-cluster ^
    --engine aurora-postgresql --engine-version 13.9 ^
    --engine-mode serverless ^
    --scaling-configuration
 MinCapacity=8,MaxCapacity=64,SecondsUntilAutoPause=1000,AutoPause=true ^
    --master-username username --master-user-password password
```

RDS-API

Zum Erstellen eines neuen Aurora Serverless v1-DB-Clusters über die RDS-API führen Sie die CreateDBCluster-Operation durch und geben `serverless` als `EngineMode`-Parameter an.

Optional können Sie den Parameter `ScalingConfiguration` angeben, um die minimale Kapazität, die maximale Kapazität und die automatische Pause zu konfigurieren, wenn es keine Verbindungen gibt. Zu den gültigen Kapazitätswerten gehören die folgenden:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128 und 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192 und 384.

Wiederherstellen eines Aurora Serverless v1-DB-Clusters

Sie können einen Aurora Serverless v1-DB-Cluster konfigurieren, wenn Sie einen bereitgestellten DB-Cluster-Snapshot über die AWS Management Console, die AWS CLI oder die RDS-API wiederherstellen.

Wenn Sie einen Snapshot in einem Aurora Serverless v1-DB-Cluster wiederherstellen, können Sie die folgenden Werte festlegen:

- Minimale Aurora Capacity Unit – Aurora Serverless v1 kann die Kapazität bis zu dieser Kapazitätseinheit reduzieren.
- Maximale Aurora Capacity Unit – Aurora Serverless v1 kann die Kapazität bis zu dieser Kapazitätseinheit erhöhen.
- Zeitüberschreitungsaktion – Die Aktion, die ausgeführt werden soll, wenn für eine Kapazitätsänderung eine Zeitüberschreitung eintritt, da kein Skalierungspunkt gefunden werden kann.Aurora Serverless v1 Der -DB-Cluster kann die neuen Kapazitätseinstellungen für Ihren DB-Cluster durchsetzen, wenn Sie die Option Bei Zeitüberschreitung Skalierung der Kapazität auf die angegebenen Werte durchsetzen auswählen. Er kann auch einen Rollback für die

Kapazitätsänderung ausführen, um sie zu stornieren, wenn Sie die Option nicht auswählen. Weitere Informationen finden Sie unter Timeout-Aktion für Kapazitätsänderungen.

- Pause after inactivity (Nach Inaktivität pausieren): Die Zeitdauer, die ohne Datenbankverkehr verstreichen muss, bis auf eine Verarbeitungskapazität von null skaliert wird. Wenn der Datenbankverkehr wieder aufgenommen wird, nimmt Aurora automatisch die Verarbeitungskapazität wieder auf und skaliert sie in Übereinstimmung mit dem Datenverkehr.

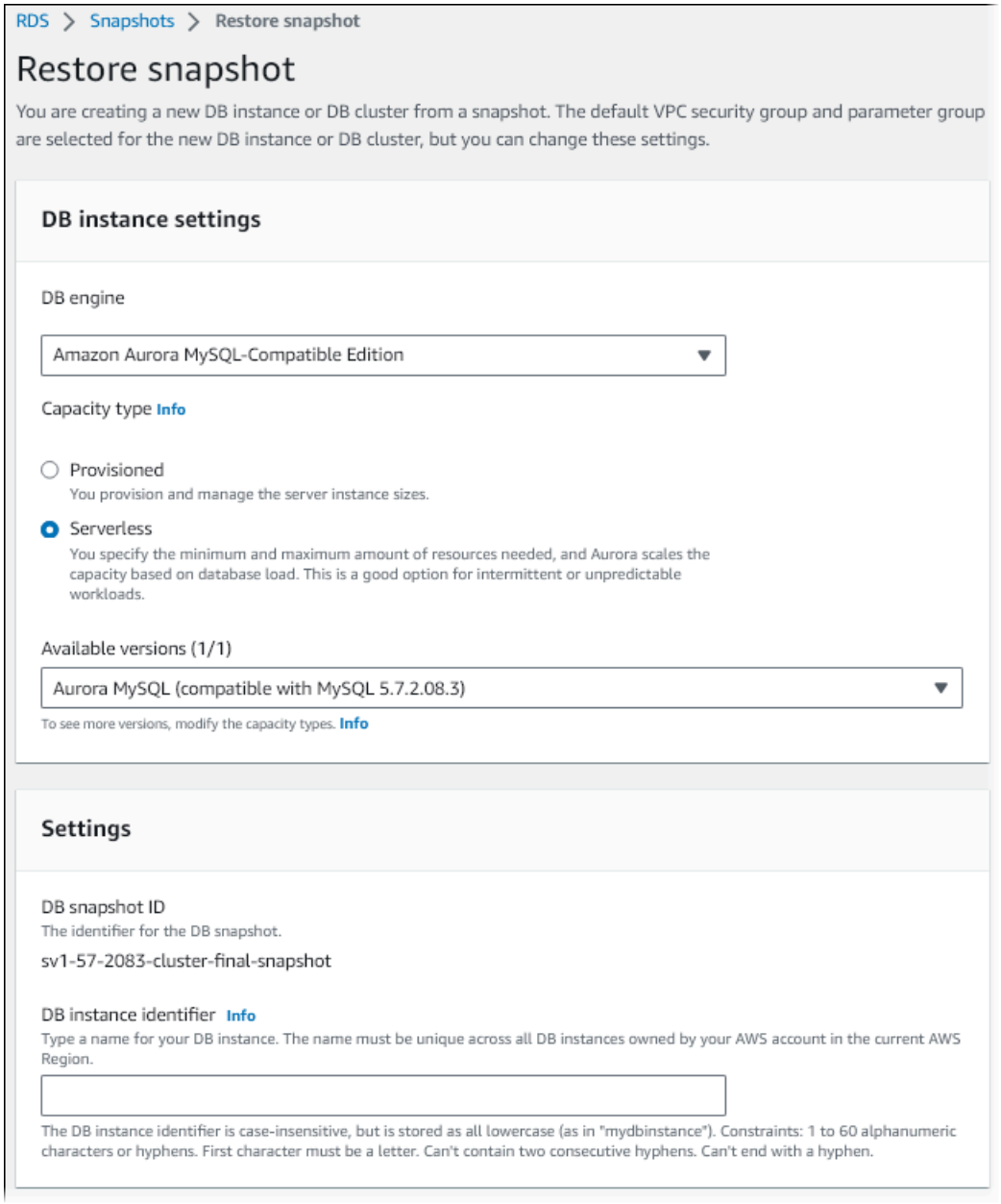
Allgemeine Informationen zum Wiederherstellen eines DB-Clusters aus einem Snapshot finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.

Konsole

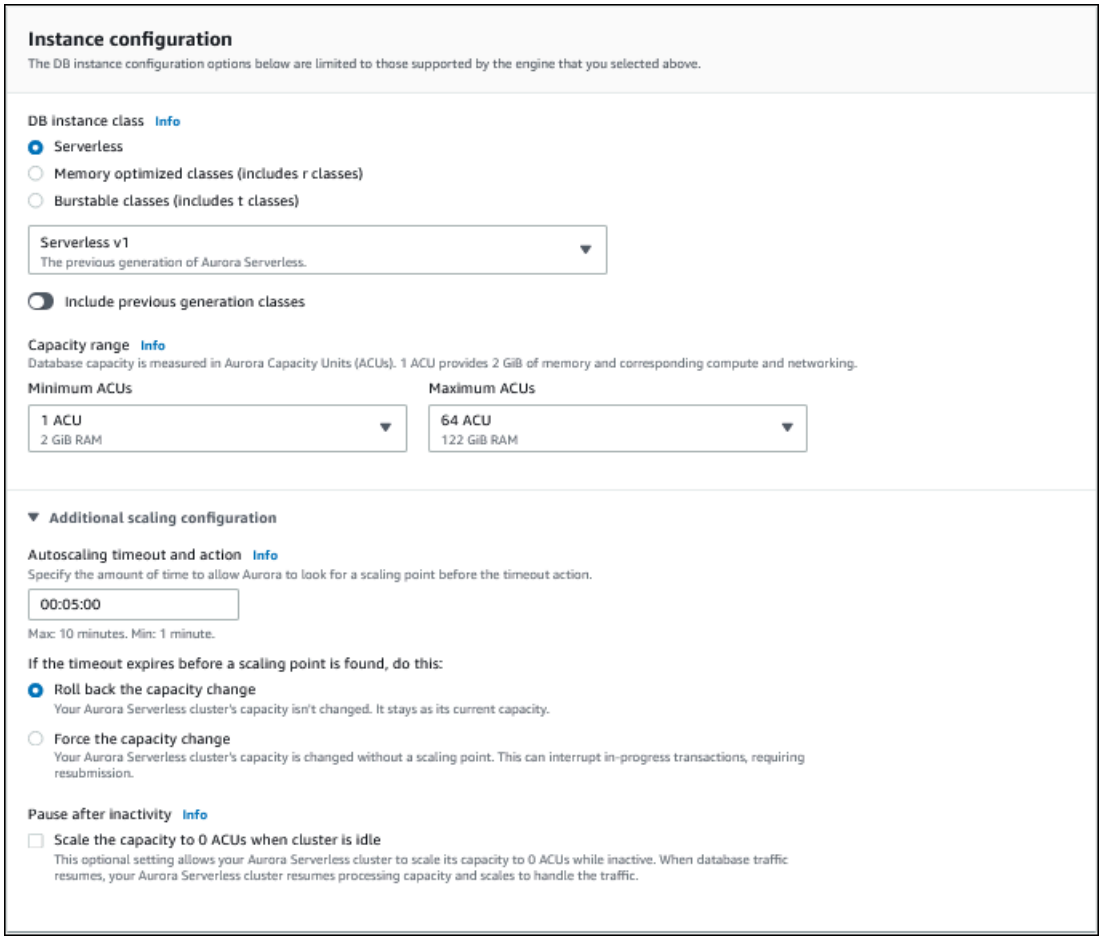
Sie können den Snapshot eines DB-Clusters über die AWS Management Console zu einem Aurora-DB-Cluster wiederherstellen.

Wiederherstellen eines DB-Cluster-Snapshots in einem Aurora DB-Cluster

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der rechten oberen Ecke der AWS Management Console die AWS-Region aus, die Ihr Quell-DB-Cluster hostet.
3. Wählen Sie im Navigationsbereich Snapshots (Snapshots) und dann den wiederherzustellenden DB-Cluster-Snapshot aus.
4. Wählen Sie unter Actions (Aktionen) die Option Restore Snapshot (Snapshot wiederherstellen).
5. Wählen Sie auf der Seite Restore DB Cluster (DB-Cluster wiederherstellen) die Option Serverless (Serverlos) für Capacity type (Kapazitätstyp) aus.



6. Geben Sie in das Feld DB cluster identifier (DB-Cluster-ID) den Namen für das wiederhergestellte DB-Cluster ein und füllen Sie die anderen Felder aus.
7. Ändern Sie im Abschnitt Capacity settings (Kapazitätseinstellungen) die Skalierungskonfiguration.



8. Wählen Sie Restore DB Cluster (DB-Cluster wiederherstellen) aus.

Zum Verbinden eines Aurora Serverless v1-DB-Clusters verwenden Sie den Datenbankendpunkt. Weitere Informationen finden Sie in den Anweisungen in Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

> **Note**
>
> Wenn Sie die folgende Fehlermeldung erhalten, benötigt Ihr Konto zusätzliche Berechtigungen:
> `Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.`
> Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Aurora.

AWS CLI

Sie können einen Aurora Serverless-DB-Cluster konfigurieren, wenn Sie einen bereitgestellten DB-Cluster-Snapshot über die AWS Management Console, die AWS CLI oder die RDS-API wiederherstellen.

Wenn Sie einen Snapshot in einem Aurora Serverless-DB-Cluster wiederherstellen, können Sie die folgenden Werte festlegen:

- Minimale Aurora Capacity Unit – Aurora Serverless kann die Kapazität bis zu dieser Kapazitätseinheit reduzieren.
- Maximale Aurora Capacity Unit – Aurora Serverless kann die Kapazität bis zu dieser Kapazitätseinheit erhöhen.
- Zeitüberschreitungsaktion – Die Aktion, die ausgeführt werden soll, wenn für eine Kapazitätsänderung eine Zeitüberschreitung eintritt, da kein Skalierungspunkt gefunden werden kann.Aurora Serverless v1 Der -DB-Cluster kann die neuen Kapazitätseinstellungen für Ihren DB-Cluster durchsetzen, wenn Sie die Option Bei Zeitüberschreitung Skalierung der Kapazität auf die angegebenen Werte durchsetzen auswählen. Er kann auch einen Rollback für die Kapazitätsänderung ausführen, um sie zu stornieren, wenn Sie die Option nicht auswählen. Weitere Informationen finden Sie unter Timeout-Aktion für Kapazitätsänderungen.
- Pause after inactivity (Nach Inaktivität pausieren): Die Zeitdauer, die ohne Datenbankverkehr verstreichen muss, bis auf eine Verarbeitungskapazität von null skaliert wird. Wenn der Datenbankverkehr wieder aufgenommen wird, nimmt Aurora automatisch die Verarbeitungskapazität wieder auf und skaliert sie in Übereinstimmung mit dem Datenverkehr.

> **Note**
>
> Die Version des DB-Cluster-Snapshots muss mit Aurora Serverless v1 kompatibel sein. Eine Liste der unterstützten Versionen finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless Version 1.

Zum Wiederherstellen eines Snapshots in einem Aurora Serverless v1-Cluster mit MySQL 5.7-Kompatibilität fügen Sie die folgenden Parameter hinzu:

- `--engine` **`aurora-mysql`**
- `--engine-version` **`5.7`**

Mit den Parametern `--engine` und `--engine-version` können Sie einen MySQL 5.7-kompatiblen Aurora Serverless v1-Cluster aus einem MySQL 5.6-kompatiblen Aurora- oder Aurora Serverless v1-Snapshot erstellen. Im folgenden Beispiel wird ein Snapshot aus einem MySQL 5.6-kompatiblen Cluster namens *mydbclustersnapshot* in einem MySQL 5.7-kompatiblen Aurora Serverless v1-Cluster namens *mynewdbcluster*wiederhergestellt.

Für Linux, macOSoder Unix:

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier mynewdbcluster \
    --snapshot-identifier mydbclustersnapshot \
    --engine-mode serverless \
    --engine aurora-mysql \
    --engine-version 5.7
```

Windows:

```
aws rds restore-db-cluster-from-snapshot ^
    --db-instance-identifier mynewdbcluster ^
    --db-snapshot-identifier mydbclustersnapshot ^
    --engine aurora-mysql ^
    --engine-version 5.7
```

Optional können Sie die Option `--scaling-configuration` angeben, um die minimale Kapazität, die maximale Kapazität und die automatische Pause zu konfigurieren, wenn es keine Verbindungen gibt. Zu den gültigen Kapazitätswerten gehören die folgenden:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128 und 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192 und 384.

Im folgenden Beispiel können Sie von einem zuvor erstellten DB-Cluster-Snapshot namens *mydbclustersnapshot* in einem neuen DB-Cluster namens *mynewdbcluster*wiederherstellen. Sie legen `--scaling-configuration` so fest, dass der neue Aurora Serverless v1-DB-Cluster bei Bedarf von 8 ACUs auf 64 ACUs (Aurora-Kapazitätseinheiten) skaliert werden kann, um die Workload zu verarbeiten. Nach Abschluss der Verarbeitung und nach 1000 Sekunden ohne zu unterstützende Verbindungen wird der Cluster heruntergefahren, bis die Verbindungsanforderung zum Neustart auffordert.

Für Linux, macOSoder Unix:

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier mynewdbcluster \
    --snapshot-identifier mydbclustersnapshot \
    --engine-mode serverless --scaling-configuration
 MinCapacity=8,MaxCapacity=64,TimeoutAction='ForceApplyCapacityChange',SecondsUntilAutoPause=10
```

Windows:

```
aws rds restore-db-cluster-from-snapshot ^
    --db-instance-identifier mynewdbcluster ^
    --db-snapshot-identifier mydbclustersnapshot ^
    --engine-mode serverless --scaling-configuration
 MinCapacity=8,MaxCapacity=64,TimeoutAction='ForceApplyCapacityChange',SecondsUntilAutoPause=10
```

RDS-API

Um einen Aurora Serverless v1 -DB-Cluster bei der Wiederherstellung von einem DB-Cluster über die RDS-API zu konfigurieren, führen Sie die Operation RestoreDBClusterFromSnapshot aus und geben Sie `serverless` für den `EngineMode` Parameter an.

Optional können Sie den Parameter `ScalingConfiguration` angeben, um die minimale Kapazität, die maximale Kapazität und die automatische Pause zu konfigurieren, wenn es keine Verbindungen gibt. Zu den gültigen Kapazitätswerten gehören die folgenden:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128 und 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192 und 384.

Ändern eines Aurora Serverless v1-DB-Clusters

Nachdem Sie einen Aurora Serverless v1 DB-Cluster konfiguriert haben, können Sie bestimmte Eigenschaften mit der AWS Management Console AWS CLI, der oder der RDS-API ändern. Die meisten Eigenschaften, die Sie ändern können, sind die gleichen wie für andere Arten von Aurora-Clustern.

Die für Aurora Serverless v1 wichtigsten Änderungen sind folgende:

- Ändern der Skalierungskonfiguration
- Durchführen eines Upgrades der Hauptversion
- Konvertieren von Aurora Serverless v1 in bereitgestellt

Ändern der Skalierungskonfiguration eines DB-Clusters von Aurora Serverless v1

Sie können die minimale und maximale Kapazität für den DB-Cluster festlegen. Jede Kapazitätseinheit entspricht einer bestimmten Rechen- und Arbeitsspeicherkonfiguration. Aurora Serverless erstellt automatisch Skalierungsregeln in Bezug auf Schwellenwerte für die CPU-Auslastung, Verbindungen und den verfügbaren Arbeitsspeicher. Sie können auch festlegen, ob Aurora Serverless die Datenbank anhalten soll, wenn es keine Aktivitäten gibt, und weiterlaufen lassen soll, wenn wieder Aktivitäten beginnen.

Sie können die folgenden spezifischen Werte für die Skalierungskonfiguration festlegen:

- Minimale Aurora Capacity Unit – Aurora Serverless kann die Kapazität bis zu dieser Kapazitätseinheit reduzieren.
- Maximale Aurora Capacity Unit – Aurora Serverless kann die Kapazität bis zu dieser Kapazitätseinheit erhöhen.
- Zeitüberschreitung und Aktion für automatische Skalierung - Dieser Abschnitt gibt an, wie langeAurora Serverless wartet, um einen Skalierungspunkt zu finden, bevor die Zeitüberschreitung eintritt. Sie legt auch fest, was zu tun ist, wenn eine Kapazitätsänderung nicht mehr funktioniert, weil sie keinen Skalierungspunkt findet. Aurora kann die Kapazitätsänderung erzwingen, um die Kapazität so schnell wie möglich auf den angegebenen Wert zu setzen. Die Kapazitätsänderung kann auch zurückgesetzt und somit abgebrochen werden. Weitere Informationen finden Sie unter Timeout-Aktion für Kapazitätsänderungen.
- Pause nach Inaktivität – Verwenden Sie die optionale Einstellung Kapazität auf 0 ACUs skalieren, wenn der Cluster inaktiv ist, um die Datenbank auf eine Verarbeitungskapazität von null zu skalieren, während sie inaktiv ist. Wenn der Datenbankverkehr wieder aufgenommen wird, nimmt Aurora automatisch die Verarbeitungskapazität wieder auf und skaliert sie in Übereinstimmung mit dem Datenverkehr.

Konsole

Sie können die Skalierungskonfiguration eines Aurora-DB-Clusters über die AWS Management Consoleändern.

So ändern Sie einen Aurora Serverless v1-DB-Cluster:

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Aurora Serverless v1DB-Cluster, den Sie ändern möchten.
4. Wählen Sie für Aktionen die Option Cluster ändern.
5. Ändern Sie im Abschnitt Capacity settings (Kapazitätseinstellungen) die Skalierungskonfiguration.
6. Klicken Sie auf Weiter.
7. Überprüfen Sie Ihre Änderungen auf der Seite DB-Cluster ändern und wählen Sie aus, wann diese angewendet werden sollen.
8. Wählen Sie Cluster bearbeiten aus.

AWS CLI

Um die Skalierungskonfiguration eines Aurora Serverless v1 DB-Clusters mithilfe von zu ändern AWS CLI, führen Sie den modify-db-cluster AWS CLI Befehl aus. Geben Sie die Option `--scaling-configuration` an, um die minimale Kapazität, die maximale Kapazität und die automatische Pause zu konfigurieren, wenn es keine Verbindungen gibt. Zu den gültigen Kapazitätswerten gehören die folgenden:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128 und 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192 und 384.

In diesem Beispiel ändern Sie die Skalierungskonfiguration eines Aurora Serverless v1-DB-Clusters namens *`sample-cluster`*.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --scaling-configuration
 MinCapacity=8,MaxCapacity=64,SecondsUntilAutoPause=500,TimeoutAction='ForceApplyCapacityChange
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --scaling-configuration
 MinCapacity=8,MaxCapacity=64,SecondsUntilAutoPause=500,TimeoutAction='ForceApplyCapacityChange
```

RDS-API

Sie können die Skalierungskonfiguration eines Aurora- DB-Clusters über die API-Operation ModifyDBCluster ändern. Geben Sie den Parameter `ScalingConfiguration` an, um die minimale Kapazität, die maximale Kapazität und die automatische Pause zu konfigurieren, wenn es keine Verbindungen gibt. Zu den gültigen Kapazitätswerten gehören die folgenden:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128 und 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192 und 384.

Durchführen eines Upgrades der Hauptversion eines DB-Clusters von Aurora Serverless v1

Sie können die Hauptversion für einen Aurora Serverless v1-DB-Cluster, der mit PostgreSQL 11 kompatibel ist, auf eine entsprechende mit PostgreSQL 13 kompatible Version aktualisieren.

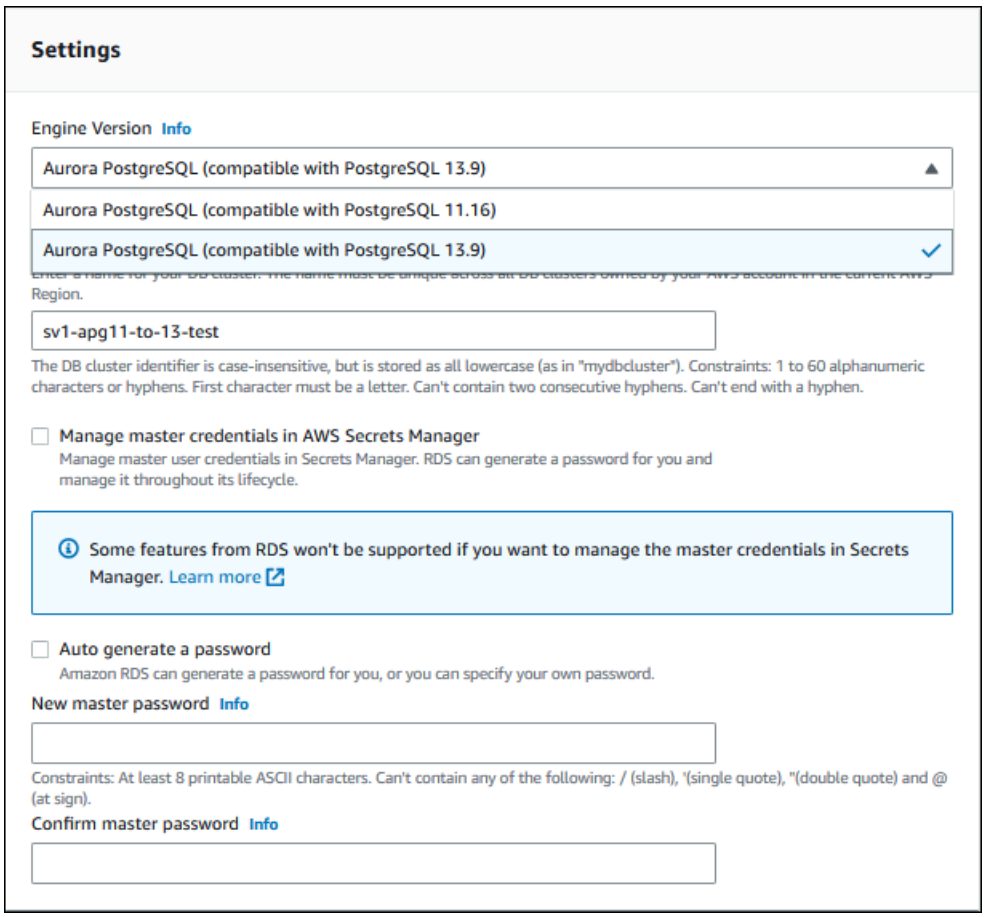
Konsole

Sie können ein direktes Upgrade des DB-Clusters von Aurora Serverless v1 mit der AWS Management Console durchführen.

So führen Sie ein Upgrade eines DB-Clusters von Aurora Serverless v1 durch

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den DB-Cluster von Aurora Serverless v1 aus, für den Sie ein Upgrade durchführen möchten.
4. Wählen Sie für Aktionen die Option Cluster ändern.
5. Wählen Sie für Version eine Versionsnummer von Aurora PostgreSQL Version 13.

   Das folgende Beispiel zeigt ein direktes Upgrade von Aurora PostgreSQL 11.16 auf 13.9.



Wenn Sie ein Hauptversions-Upgrade durchführen, lassen Sie alle anderen Eigenschaften unverändert. Wenn Sie eine der anderen Eigenschaften ändern möchten, führen Sie einen anderen Vorgang Ändern nach Abschluss des Upgrades aus.

6. Klicken Sie auf Weiter.
7. Überprüfen Sie Ihre Änderungen auf der Seite DB-Cluster ändern und wählen Sie aus, wann diese angewendet werden sollen.
8. Wählen Sie Cluster bearbeiten aus.

AWS CLI

Wenn Sie ein direktes Upgrade von einem mit PostgreSQL 11 kompatiblen DB-Cluster von Aurora Serverless v1 auf einen mit PostgreSQL 13 kompatiblen Cluster durchführen möchten, geben Sie den Parameter `--engine-version` mit einer Versionsnummer von Aurora PostgreSQL Version 13 an, die mit Aurora Serverless v1 kompatibel ist. Nehmen Sie außerdem den Parameter `--allow-major-version-upgrade` mit auf.

In diesem Beispiel ändern Sie die Hauptversion eines mit PostgreSQL 11 kompatiblen Aurora Serverless v1-DB-Clusters namens `sample-cluster`. Dadurch wird ein direktes Upgrade auf einen mit PostgreSQL 13 kompatiblen DB-Cluster von Aurora Serverless v1 durchgeführt.

```
aws rds modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --engine-version 13.9 \
    --allow-major-version-upgrade
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --engine-version 13.9 ^
    --allow-major-version-upgrade
```

RDS-API

Wenn Sie ein direktes Upgrade von einem mit PostgreSQL 11 kompatiblen DB-Cluster von Aurora Serverless v1 auf einen mit PostgreSQL 13 kompatiblen Cluster durchführen möchten, geben Sie den Parameter `EngineVersion` mit einer Versionsnummer von Aurora PostgreSQL Version 13 an, die mit Aurora Serverless v1 kompatibel ist. Nehmen Sie außerdem den Parameter `AllowMajorVersionUpgrade` mit auf.

Konvertieren eines DB-Clusters von Aurora Serverless v1 zu einem bereitgestellten Cluster

Sie können einen DB-Cluster von Aurora Serverless v1 zu einem bereitgestellten DB-Cluster konvertieren. Um die Konvertierung durchzuführen, ändern Sie die DB-Instance-Klasse in Bereitgestellt. Sie können diese Konvertierung im Rahmen des Upgrades Ihres DB-Clusters von Aurora Serverless v1 auf Aurora Serverless v2 verwenden. Weitere Informationen finden Sie unter Aktualisieren eines Aurora Serverless v1-Clusters auf Aurora Serverless v2.

Der Konvertierungsprozess erstellt eine Reader-DB-Instance im DB-Cluster, stuft die Reader-Instance zu einer Writer-Instance hoch und löscht dann die ursprüngliche Instance von Aurora Serverless v1. Wenn Sie den DB-Cluster konvertieren, können Sie keine anderen Änderungen gleichzeitig vornehmen, z. B. die DB-Engine-Version oder die DB-Cluster-Parametergruppe ändern. Der Konvertierungsvorgang wird sofort angewendet und kann nicht rückgängig gemacht werden.

Bei der Konvertierung wird ein Backup-DB-Cluster-Snapshot des DB-Clusters für den Fall erstellt, dass ein Fehler auftritt. Der Bezeichner des DB-Cluster-Snapshots hat das Format `pre-modify-engine-mode-`*`DB_cluster_identifier`*`-`*`timestamp`*.

Aurora verwendet die aktuelle Standard-DB-Engine-Nebenversion für den bereitgestellten DB-Cluster.

Wenn Sie keine DB-Instance-Klasse für Ihren konvertierten DB-Cluster angeben, empfiehlt Aurora eine Klasse auf Basis der maximalen Kapazität des ursprünglichen DB-Clusters von Aurora Serverless v1. Die empfohlenen Kapazitäts- und Instance-Klassenzuordnungen sind in der folgenden Tabelle aufgeführt.

Maximale Serverless Kapazität (ACUs)	Bereitgestellte DB-Instance-Klasse
1	db.t3.small
2	db.t3.medium
4	db.t3.large
8	db.r5.large
16	db.r5.xlarge
32	db.r5.2xlarge
64	db.r5.4xlarge
128	db.r5.8xlarge
192	db.r5.12xlarge
256	db.r5.16xlarge
384	db.r5.24xlarge

> **Note**
>
> Abhängig von der ausgewählten DB-Instance-Klasse und Ihrer Datenbanknutzung fallen für einen bereitgestellten DB-Cluster im Vergleich zu Aurora Serverless v1 möglicherweise andere Kosten an.
> Wenn Sie Ihren DB-Cluster von Aurora Serverless v1 in eine burstfähige DB-Instance-Klasse (db.t*) konvertieren, können zusätzliche Kosten für die Verwendung des DB-Clusters anfallen. Weitere Informationen finden Sie unter DB-Instance-Klassenarten.

AWS CLI

Führen Sie den modify-db-cluster AWS CLI Befehl aus, um einen Aurora Serverless v1 DB-Cluster in einen bereitgestellten Cluster zu konvertieren.

Die folgenden Parameter sind erforderlich:

- `--db-cluster-identifier` – Der DB-Cluster von Aurora Serverless v1, den Sie in einen bereitgestellten Cluster konvertieren.
- `--engine-mode` – Verwenden Sie den Wert `provisioned`.
- `--allow-engine-mode-change`
- `--db-cluster-instance-class` – Wählen Sie die DB-Instance-Klasse für den bereitgestellten DB-Cluster auf der Grundlage der Kapazität des DB-Clusters von Aurora Serverless v1.

In diesem Beispiel konvertieren Sie einen DB-Cluster von Aurora Serverless v1 mit dem Namen `sample-cluster` und verwenden die DB-Instance-Klasse `db.r5.xlarge`.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --engine-mode provisioned \
    --allow-engine-mode-change \
    --db-cluster-instance-class db.r5.xlarge
```

Windows:

```
aws rds modify-db-cluster ^
```

```
    --db-cluster-identifier sample-cluster ^
    --engine-mode provisioned ^
    --allow-engine-mode-change ^
    --db-cluster-instance-class db.r5.xlarge
```

RDS-API

Verwenden Sie die API-Operation ModifyDBCluster, um einen DB-Cluster von Aurora Serverless v1 in einen bereitgestellten Cluster zu konvertieren.

Die folgenden Parameter sind erforderlich:

- `DBClusterIdentifier` – Der DB-Cluster von Aurora Serverless v1, den Sie in einen bereitgestellten Cluster konvertieren.
- `EngineMode` – Verwenden Sie den Wert `provisioned`.
- `AllowEngineModeChange`
- `DBClusterInstanceClass` – Wählen Sie die DB-Instance-Klasse für den bereitgestellten DB-Cluster auf der Grundlage der Kapazität des DB-Clusters von Aurora Serverless v1.

Manuelles Skalieren der Kapazität des Aurora Serverless v1-DB-Clusters

In der Regel werden Aurora Serverless v1-DB-Cluster basierend auf dem Workload nahtlos skaliert. Die Kapazität kann jedoch nicht immer schnell genug skaliert werden, um plötzliche Extreme wie einen exponentiellen Anstieg der Transaktionen zu meistern. In solchen Fällen können Sie den Skalierungsvorgang manuell initiieren, indem Sie einen neuen Kapazitätswert festlegen. Nachdem Sie die Kapazität explizit festgelegt haben, skaliert Aurora Serverless v1 den DB-Cluster automatisch. Der Vorgang basiert auf der Ruhepause für die Herunterskalierung.

Sie können die Kapazität eines Aurora Serverless v1-DB-Clusters über die AWS Management Console, die AWS CLI oder die RDS-API explizit auf einen bestimmten Wert festlegen.

Konsole

Sie können die Kapazität eines Aurora-DB-Clusters über die AWS Management Console festlegen.

So ändern Sie einen Aurora Serverless v1-DB-Cluster:

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

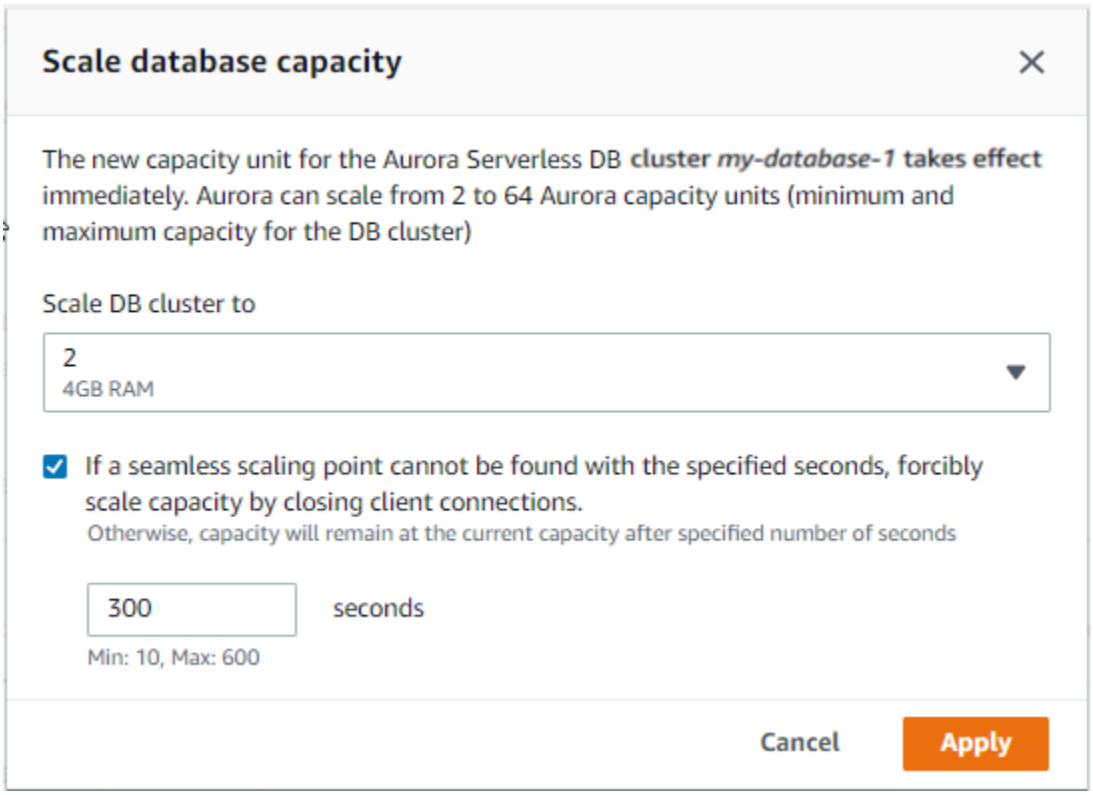
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den Aurora Serverless v1-DB-Cluster aus, den Sie ändern möchten.
4. Wählen Sie für Actions (Aktionen) die Option Set capacity (Kapazität festlegen) aus.
5. Wählen Sie im Fenster Datenbankkapazität skalieren Folgendes aus:

    a. Wählen Sie bei der Dropdown-Auswahl für Scale DB-Cluster to (DB-Cluster skalieren auf) die neue Kapazität aus, die Sie für Ihren DB-Cluster verwenden möchten.

    b. Wählen Sie beim Kontrollkästchen If a seamless scaling point cannot be found (Wenn kein nahtloser Skalierungspunkt gefunden werden kann) das gewünschte Verhalten für die `TimeoutAction`-Einstellung des Aurora Serverless v1-DB-Clusters aus:

    - Deaktivieren Sie diese Option, wenn Sie möchten, dass die Kapazität unverändert bleibt, wenn Aurora Serverless v1 vor dem Timeout keinen Skalierungspunkt finden kann.
    - Aktivieren Sie diese Option, wenn Sie erzwingen möchten, dass der Aurora Serverless v1-DB-Cluster seine Kapazität ändert, auch wenn er vor dem Timeout keinen Skalierungspunkt finden kann. Diese Option kann dazu führen, dass Aurora Serverless v1 Verbindungen unterbricht, die verhindern, dass es einen Skalierungspunkt findet.

    c. Geben Sie im Feld seconds (Sekunden) die Zeit ein, die der Aurora Serverless v1-DB-Cluster vor dem Timeout nach einem Skalierungspunkt suchen soll. Sie können einen Wert zwischen 10 Sekunden und 600 Sekunden (10 Minuten) angeben. Der Standardwert beträgt fünf Minuten (300 Sekunden). Im folgenden Beispiel wird erzwungen, dass der Aurora Serverless v1-DB-Cluster auf 2 ACUs herunterskaliert, auch wenn er innerhalb von fünf Minuten keinen Skalierungspunkt finden kann.



6. Wählen Sie Apply (Anwenden) aus.

Weitere Informationen zu Skalierungspunkten, `TimeoutAction` und Ruhephasen finden Sie unter Automatische Skalierung für Aurora Serverless v1.

AWS CLI

Um die Kapazität eines Aurora Serverless v1-DB-Clusters über die AWS CLI festzulegen, führen Sie den AWS CLI-Befehl modify-current-db-cluster-capacity aus und geben die Option `--capacity` an. Zu den gültigen Kapazitätswerten gehören die folgenden:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128 und 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192 und 384.

In diesem Beispiel legen Sie die Kapazität eines Aurora Serverless v1-DB-Clusters namens *`sample-cluster`* auf *`64`* fest.

```
aws rds modify-current-db-cluster-capacity --db-cluster-identifier sample-cluster --
capacity 64
```

RDS-API

Sie können die Kapazität eines Aurora-DB-Clusters über die API-Operation ModifyCurrentDBClusterCapacity festlegen. Geben Sie den Parameter `Capacity` an. Zu den gültigen Kapazitätswerten gehören die folgenden:

- Aurora MySQL: 1, 2, 4, 8, 16, 32, 64, 128 und 256.
- Aurora PostgreSQL: 2, 4, 8, 16, 32, 64, 192 und 384.

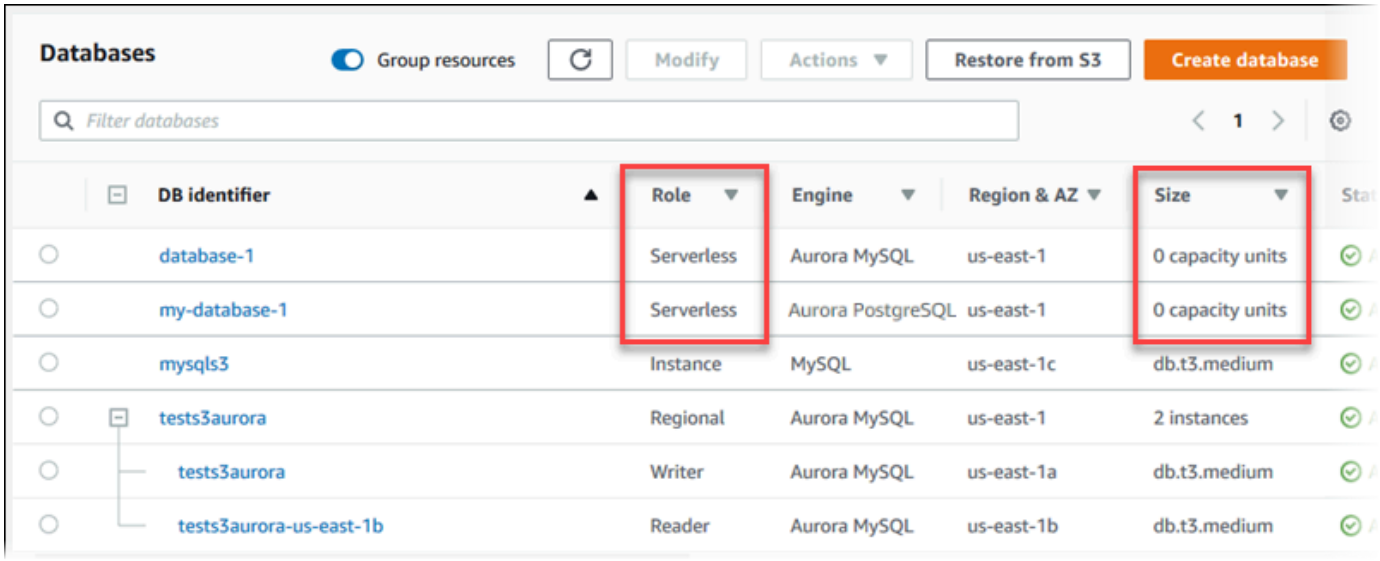
Anzeigen von Aurora Serverless v1-DB-Clustern

Nachdem Sie einen oder mehrere Aurora Serverless v1-DB-Cluster erstellt haben, können Sie anzeigen, welche DB-Cluster den Typ Serverless (Serverlos) und welche den Typ Instance haben. Sie können auch die aktuelle Anzahl von Aurora Capacity Units (ACUs) einsehen, die jeder Aurora Serverless v1-DB-Cluster verwendet. Jede ACU ist eine Kombination aus Rechenkapazität (CPU) und Arbeitsspeicherkapazität (RAM).

So zeigen Sie Ihre Aurora Serverless v1-DB-Cluster an:

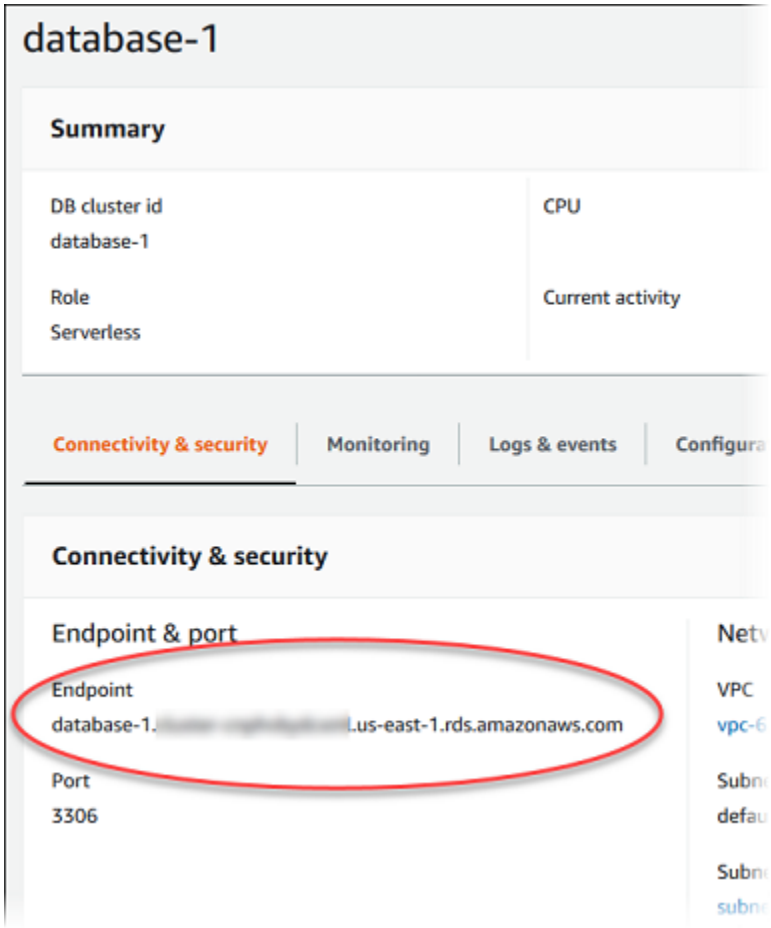
1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie oben rechts in der AWS Management Console die AWS-Region aus, in der Sie die Aurora Serverless v1-DB-Cluster erstellt haben.
3. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.

   Der DB-Cluster-Typ für die einzelnen DB-Cluster wird unter Role (Rolle) angezeigt. Bei den Aurora Serverless v1-DB-Clustern wird Serverless (Serverlos) als Typ angezeigt. Sie können die aktuelle Kapazität eines Aurora Serverless v1-DB-Clusters unter Size (Größe) anzeigen.

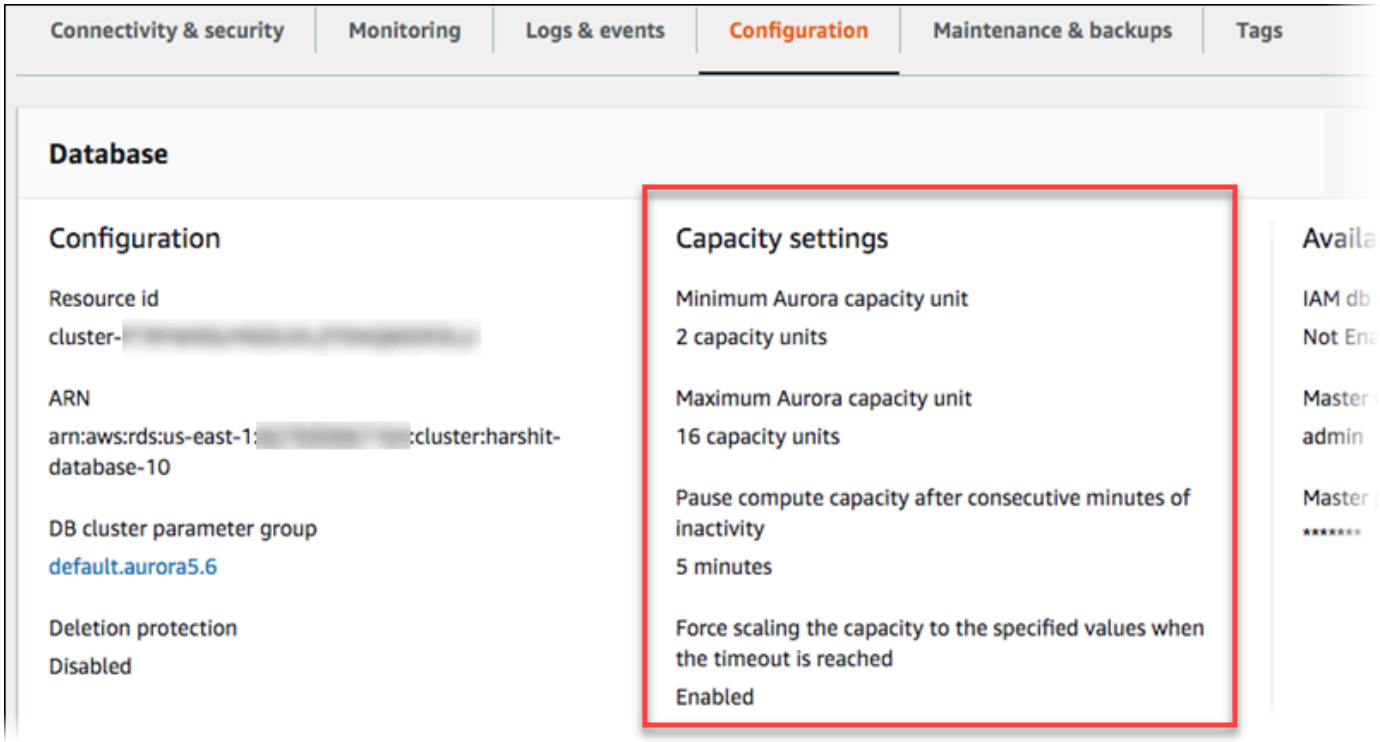


4. Wählen Sie den Namen eines Aurora Serverless v1-DB-Clusters aus, um dessen Details anzuzeigen.

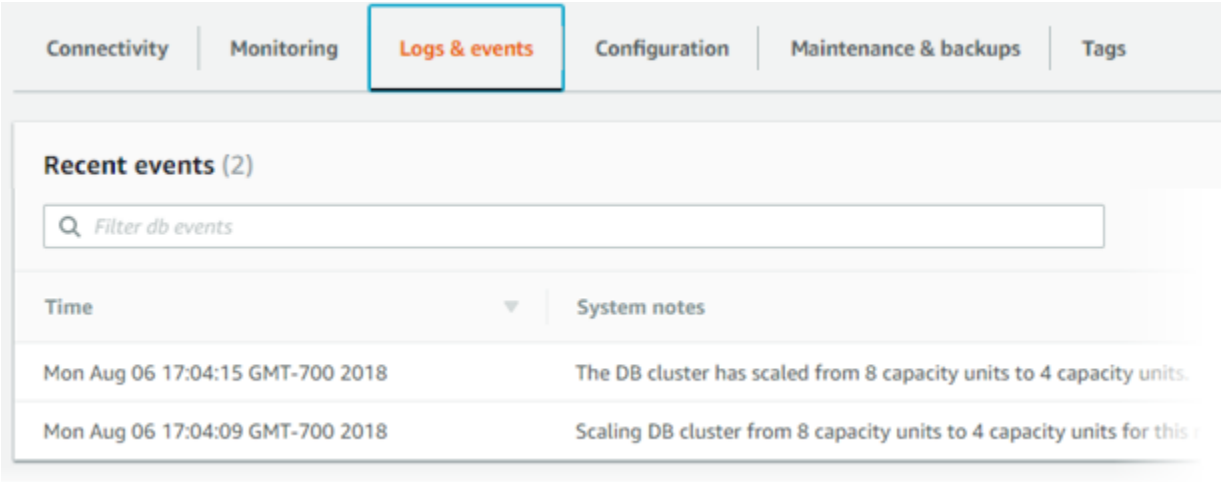
   Beachten Sie auf der Registerkarte Connectivity & security (Konnektivität und Sicherheit) den Datenbankendpunkt. Verwenden Sie diesen Endpunkt, um eine Verbindung zu Ihrem Aurora Serverless v1-DB-Cluster herzustellen.



Wählen Sie die Registerkarte Configuration (Konfiguration) aus, um die Kapazitätseinstellungen anzuzeigen.



Wenn das DB-Cluster nach unten oder oben skaliert, pausiert oder fortgesetzt wird, wird ein Skalierungsereignis generiert. Wählen Sie die Registerkarte Logs & events (Protokolle und Ereignisse) aus, um aktuelle Ereignisse zu sehen. Die folgende Abbildung zeigt Beispiele für diese Ereignisse.



Überwachen der Kapazität und Skalieren von Ereignissen für den Aurora Serverless v1-DB-Cluster

Sie können Ihren Aurora Serverless v1-DB-Cluster in CloudWatch anzeigen, um die dem DB-Cluster zugewiesene Kapazität anhand der Metrik `ServerlessDatabaseCapacity` zu überwachen. Zusätzlich können Sie alle Aurora CloudWatch-Standardmetriken überwachen, wie z. B. `CPUUtilization`, `DatabaseConnections`, `Queries` usw.

Sie können veranlassen, dass Aurora einige oder alle Datenbankprotokolle in CloudWatch veröffentlicht. Sie bestimmen, welche Protokolle veröffentlicht werden sollen, indem Sie in der mit dem `general_log`-Cluster verknüpften DB-Cluster-Parametergruppe Konfigurationsparameter wie `slow_query_log` und Aurora Serverless v1 aktivieren. Anders als bei bereitgestellten Clustern müssen Sie bei Aurora Serverless v1-Clustern in den DB-Cluster-Einstellungen nicht angeben, welche Protokolltypen in CloudWatch hochgeladen werden sollen. Aurora Serverless v1-Cluster laden automatisch alle verfügbaren Protokolle hoch. Wenn Sie einen Protokollkonfigurationsparameter deaktivieren, stoppt die Veröffentlichung des Protokolls in CloudWatch. Sie können die Protokolle auch in CloudWatch löschen, wenn sie nicht mehr benötigt werden.

Erste Schritte mit Amazon CloudWatch für Ihren Aurora Serverless v1-DB-Cluster finden Sie unter Anzeigen von Aurora Serverless v1 Protokollen mit Amazon CloudWatch. Weitere Informationen zur Überwachung von Aurora-DB-Clustern über CloudWatch finden Sie unter Überwachen von Protokollereignissen in Amazon CloudWatch.

Zum Verbinden eines Aurora Serverless v1-DB-Clusters verwenden Sie den Datenbankendpunkt. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

> **Note**
>
> Sie können in Aurora Serverless v1-DB-Clustern keine direkte Verbindung zu bestimmten DB-Instances herstellen.

Löschen eines Aurora Serverless v1-DB-Clusters

Wenn Sie einen Aurora Serverless v1-DB-Cluster über die AWS Management Console erstellen, ist die Option Enable default protection (Standardschutz aktivieren) standardmäßig aktiviert, sofern

sie nicht deaktiviert wurde. Das bedeutet, dass Sie einen Aurora Serverless v1-DB-Cluster, für den Deletion protection (Löschschutz) aktiviert ist, nicht sofort löschen können. Um Aurora Serverless v1-DB-Cluster mit Löschschutz über die AWS Management Console zu löschen, bearbeiten Sie zuerst den Cluster, um diesen Schutz zu entfernen. Informationen zur Verwendung der AWS CLI für diese Aufgabe finden Sie unter AWS CLI.

So deaktivieren Sie den Löschschutz mithilfe der AWS Management Console

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Klicken Sie im Navigationsbereich auf DB clusters (DB-Cluster).
3. Wählen Sie Ihren Aurora Serverless v1-DB-Cluster in der Liste aus.
4. Wählen Sie Modify (Ändern), um die Konfiguration des DB-Clusters zu öffnen. Auf der Seite "DB-Cluster ändern" werden die Einstellungen, Kapazitätseinstellungen und andere Konfigurationsdetails für Ihren Aurora Serverless v1-DB-Cluster geöffnet. Den Löschschutz finden Sie im Bereich Additional configuration (Zusätzliche Konfiguration).
5. Deaktivieren Sie das Kontrollkästchen Enable deletion protection (Löschschutz aktivieren) auf der Eigenschaftenkarte Additional configuration (Zusätzliche Konfiguration).
6. Klicken Sie auf Weiter. Summary of modifications (Zusammenfassung der Änderungen) wird angezeigt.
7. Wählen Sie Modify cluster (Cluster ändern), um die Zusammenfassung der Änderungen zu akzeptieren. Sie können auch Back (Zurück) wählen, um Ihre Änderungen zu bearbeiten, oder Cancel (Abbrechen), um Ihre Änderungen zu verwerfen.

Nachdem der Löschschutz nicht mehr aktiv ist, können Sie Ihren Aurora Serverless v1-DB-Cluster über die AWS Management Console löschen.

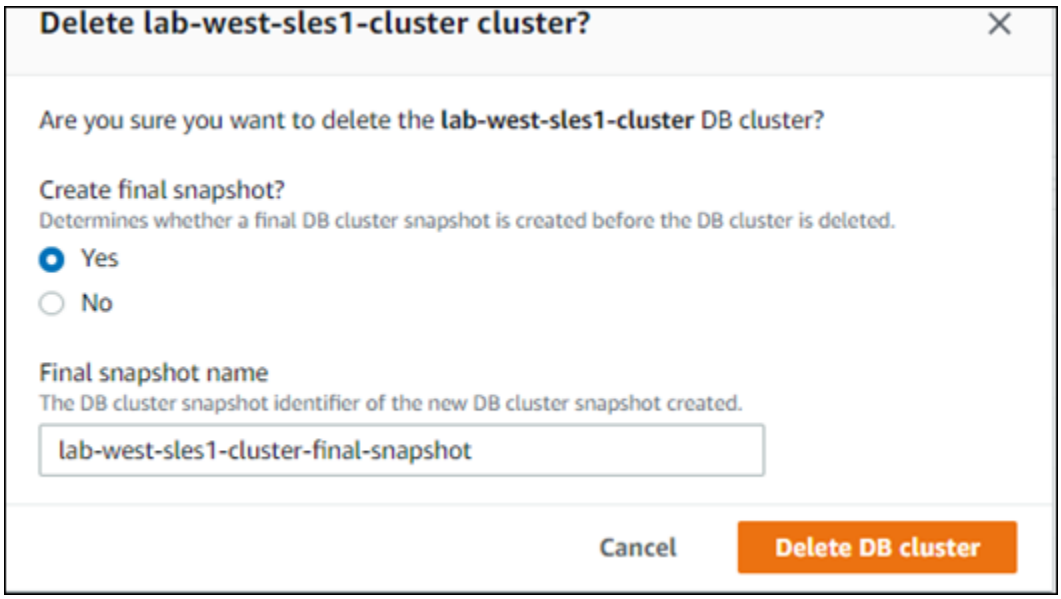
Konsole

So löschen Sie einen Aurora Serverless v1-DB-Cluster:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Bereich Resources (Ressourcen) die Option DB Clusters (DB-Cluster) aus.
3. Wählen Sie den Aurora Serverless v1-DB-Cluster aus, den Sie löschen möchten.

4. Klicken Sie bei Actions auf Delete. Sie werden aufgefordert, zu bestätigen, dass Sie den Aurora Serverless v1-DB-Cluster löschen möchten.
5. Sie sollten die vorausgewählten Optionen beibehalten:

   - Yes (Ja) bei Create final snapshot? (Finalen Snapshot erstellen?)
   - Ihr Aurora Serverless v1-DB-Cluster-Name sowie `-final-snapshot` für Final snapshot name (Name des finalen Snapshots). Sie können jedoch den Namen für Ihren finalen Snapshot in diesem Feld ändern.



   Wenn Sie Nein für Abschließenden Snapshot erstellen? wählen, können Sie Ihren DB-Cluster nicht mithilfe von Snapshots oder point-in-time Wiederherstellung wiederherstellen.
6. Wählen Sie Delete DB cluster (DB-Cluster löschen) aus.

Aurora Serverless v1 löscht Ihren DB-Cluster. Wenn Sie sich für einen finalen Snapshot entschieden haben, wird der Status Ihres Aurora Serverless v1-DB-Clusters zu "Backing-up" (Wird gesichert) geändert, bevor er gelöscht wird und nicht mehr in der Liste erscheint.

AWS CLI

Bevor Sie beginnen, konfigurieren Sie Ihre AWS CLI mit Ihrer AWS-Zugriffsschlüssel-ID, dem geheimen AWS-Zugriffsschlüssel und der AWS-Region, in der sich Ihr Aurora Serverless v1-DB-Cluster befindet. Weitere Informationen finden Sie unter Konfigurationsgrundlagen im AWS Command Line Interface-Benutzerhandbuch.

Sie können einen Aurora Serverless v1-DB-Cluster erst löschen, nachdem Sie für Cluster, die mit dieser Option konfiguriert sind, den Löschschutz deaktiviert haben. Wenn Sie versuchen, einen Cluster zu löschen, bei dem diese Schutzoption aktiviert ist, wird die folgende Fehlermeldung angezeigt.

```
An error occurred (InvalidParameterCombination) when calling the DeleteDBCluster
  operation: Cannot delete protected Cluster, please disable deletion protection and
 try again.
```

Sie können die Löschschutzeinstellung Ihres Aurora Serverless v1 DB-Clusters ändern, indem Sie den modify-db-cluster AWS CLI Befehl verwenden, wie im Folgenden gezeigt:

```
aws rds modify-db-cluster --db-cluster-identifier your-cluster-name --no-deletion-
protection
```

Dieser Befehl liefert die überarbeiteten Eigenschaften für den angegebenen DB-Cluster. Jetzt können Sie den Aurora Serverless v1-DB-Cluster löschen.

Es empfiehlt sich, immer einen finalen Snapshot zu erstellen, wenn Sie einen Aurora Serverless v1-DB-Cluster löschen. Das folgende Beispiel für die Verwendung von AWS CLI delete-db-cluster zeigt Ihnen, wie das geht. Sie geben den Namen Ihres DB-Clusters und einen Namen für den Snapshot an.

Für Linux, macOSoder Unix:

```
aws rds delete-db-cluster --db-cluster-identifier \
  your-cluster-name --no-skip-final-snapshot \
  --final-db-snapshot-identifier name-your-snapshot
```

Windows:

```
aws rds delete-db-cluster --db-cluster-identifier ^
  your-cluster-name --no-skip-final-snapshot ^
  --final-db-snapshot-identifier name-your-snapshot
```

Aurora Serverless v1- und Aurora-Datenbank-Engine-Versionen

Aurora Serverless v1 ist in bestimmten AWS-Regionen und nur für bestimmte Aurora-MySQL- und Aurora-PostgreSQL-Versionen verfügbar. Die aktuelle Liste der AWS-Regionen, die Aurora

Serverless v1 unterstützen, sowie die spezifischen Versionen von Aurora MySQL und Aurora PostgreSQL, die in jeder Region verfügbar sind, finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless Version 1.

Aurora Serverless v1 verwendet die zugehörige Aurora-Datenbank-Engine, um spezifische unterstützte Versionen für jede unterstützte Datenbank-Engine zu ermitteln:

- Aurora MySQL Serverless
- Aurora PostgreSQL Serverless

Wenn Nebenversionen der Datenbank-Engines für Aurora Serverless v1 verfügbar werden, werden sie automatisch in den verschiedenen AWS-Regionen angewendet, in denen Aurora Serverless v1 verfügbar ist. Mit anderen Worten, Sie müssen Ihren Aurora Serverless v1-DB-Cluster nicht aktualisieren, um eine neue Nebenversion für die DB-Engine Ihres Clusters zu erhalten, wenn sie für Aurora Serverless v1 verfügbar ist.

Aurora MySQL Serverless

Wenn Sie Aurora MySQL-Compatible Edition für Ihren Aurora Serverless v1-DB-Cluster verwenden möchten, können Sie eine mit MySQL 5.7 kompatible Versionsnummer von Aurora MySQL Version 2 wählen. Weitere Informationen zu Verbesserungen und Fehlerbehebungen für Aurora MySQL Version 2 finden Sie unter Aktualisierungen der Datenbank-Engine für Amazon Aurora MySQL Version 2 in den Versionshinweisen für Aurora MySQL.

Aurora PostgreSQL Serverless

Wenn Sie Aurora PostgreSQL für Ihren Aurora Serverless v1-DB-Cluster verwenden möchten, können Sie zwischen mit Aurora PostgreSQL 11 und Aurora PostgreSQL 13 kompatiblen Versionen wählen. Nebenversionen für Aurora PostgreSQL-kompatible Edition enthalten nur Änderungen, die abwärtskompatibel sind. Ihr DB-Cluster von Aurora Serverless v1 wird transparent aktualisiert, wenn eine Aurora-PostgreSQL-Nebenversion für Aurora Serverless v1 in Ihrer AWS-Region verfügbar wird.

Beispielsweise wurde die Nebenversion Aurora PostgreSQL 11.16 transparent auf alle Aurora Serverless v1-DB-Cluster angewendet, auf denen die vorherige Aurora-PostgreSQL-Version ausgeführt wurde. Weitere Informationen zum Update von Aurora PostgreSQL Version 11.16 finden Sie unter PostgreSQL 11.16 in den Versionshinweisen für Aurora PostgreSQL.

Verwenden der RDS-Daten-API

Mithilfe der RDS Data API (Data API) können Sie mit einer Webservice-Schnittstelle zu Ihrem Aurora-DB-Cluster arbeiten. Die Daten-API erfordert keine persistente Verbindung zum DB-Cluster. Stattdessen bietet sie einen sicheren HTTP-Endpunkt und die Integration mit AWS SDKs. Über den Endpunkt können Sie SQL-Anweisungen ausführen, ohne Verbindungen zu verwalten.

Benutzer müssen bei Aufrufen an die Daten-API keine Anmeldeinformationen übergeben, da die Daten-API Datenbankanmeldeinformationen verwendet, die in AWS Secrets Manager gespeichert sind. Um Anmeldeinformationen in Secrets Manager zu speichern, müssen Benutzern die entsprechenden Berechtigungen zur Verwendung von Secrets Manager und auch Data API gewährt werden. Weitere Informationen zum Autorisieren von Benutzern finden Sie unter Autorisieren des Zugriffs auf die RDS-Daten-API.

Sie können die Daten-API auch verwenden, um Amazon Aurora in andere AWS Anwendungen wie AWS Lambda AWS AppSync, und zu integrieren AWS Cloud9. Die Daten-API bietet eine sicherere Art der Verwendung AWS Lambda. Sie können damit auf Ihr DB-Cluster zugreifen, ohne eine Lambda-Funktion für den Zugriff auf Ressourcen in einer Virtual Private Cloud (VPC) konfigurieren zu müssen. Weitere Informationen finden Sie unter AWS Lambda, AWS AppSync und AWS Cloud9.

Sie können die Daten-API aktivieren, wenn Sie den Aurora-DB-Cluster erstellen. Sie können die Konfiguration später auch ändern. Weitere Informationen finden Sie unter RDS-Daten-API aktivieren.

Nachdem Sie die Daten-API aktiviert haben, können Sie den Abfrage-Editor auch verwenden, um Ad-hoc-Abfragen auszuführen, ohne ein Abfragetool für den Zugriff auf Aurora in einer VPC zu konfigurieren. Weitere Informationen finden Sie unter Verwenden des Aurora-Abfrage-Editors.

Themen

- Verwendung der Java-Clientbibliothek für die RDS-Daten-API
- Verarbeitung der Ergebnisse der RDS-Daten-API-Abfrage im JSON-Format
- Behebung von Problemen mit der RDS-Daten-API
- Protokollieren von RDS-Daten-API-Aufrufen mit AWS CloudTrail

Verfügbarkeit von Regionen und Versionen

Informationen zu den Regionen und Engine-Versionen, die für die Daten-API verfügbar sind, finden Sie in den folgenden Abschnitten.

Cluster-Typ	Verfügbarkeit von Regionen und Versionen	
Aurora PostgreSQL bereitgestellt und Serverless v2	Daten-API mit Aurora PostgreSQL Serverless v2 und bereitgestellt	
Aurora PostgreSQL Serverlos v1	Daten-API mit Aurora PostgreSQL Serverless v1	
Aurora MySQL Serverlos v1	Daten-API mit Aurora MySQL Serverless v1	

> **Note**
>
> Derzeit ist die Daten-API nicht für von Aurora MySQL bereitgestellte oder serverlose v2-DB-Cluster verfügbar.

Wenn Sie beim Zugriff auf die Daten-API über eine Befehlszeilenschnittstelle oder eine API kryptografische Module benötigen, die durch FIPS 140-2 validiert wurden, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Einschränkungen bei der RDS-Daten-API

Die RDS-Daten-API (Daten-API) hat die folgenden Einschränkungen:

- Sie können Daten-API-Abfragen nur auf Writer-Instances in einem DB-Cluster ausführen. Writer-Instances können jedoch sowohl Schreib- als auch Leseanfragen akzeptieren.
- Mit den globalen Aurora-Datenbanken können Sie die Daten-API sowohl auf primären als auch auf sekundären DB-Clustern aktivieren. Solange ein sekundärer Cluster jedoch nicht zum primären Cluster heraufgestuft wird, hat er keine Writer-Instance. Daher schlagen Daten-API-Abfragen fehl, die Sie an den sekundären Server senden. Sobald eine beworbene sekundäre Instanz über eine verfügbare Writer-Instance verfügt, sollten Daten-API-Abfragen auf dieser DB-Instance erfolgreich sein.
- Performance Insights unterstützt keine Überwachung von Datenbankabfragen, die Sie mithilfe der Daten-API durchführen.
- Die Daten-API wird in T-DB-Instance-Klassen nicht unterstützt.
- Für Aurora PostgreSQL Serverless v2 und bereitgestellte DB-Cluster unterstützt die RDS Data API einige Datentypen nicht. Eine Liste der unterstützten Typen finden Sie unter. the section called “Vergleich mit Serverless v2 und Provisioned und Aurora Serverless v1”
- Für Datenbanken mit Aurora PostgreSQL Version 14 und höher unterstützt die Daten-API nur scram-sha-256 für die Passwortverschlüsselung.

Vergleich der RDS-Daten-API mit Serverless v2 und der bereitgestellten Version und Aurora Serverless v1

In der folgenden Tabelle werden die Unterschiede zwischen der RDS-Daten-API (Daten-API) mit Aurora PostgreSQL Serverless v2 und bereitgestellten DB-Clustern und DB-Clustern beschrieben. Aurora Serverless v1

Unterschied	Aurora PostgreSQL Serverless v2 und bereitgestellt	Aurora Serverless v1
Maximale Anzahl von Anfragen pro Sekunde	Unbegrenzt	1.000
Aktivieren oder Deaktivieren der Daten-API in einer vorhandenen Datenbank mithilfe der RDS-API oder AWS CLI	• RDS-API — Verwenden Sie die `DisableHttpEndpoint` Operationen `EnableHttpEndpoint` und.	• RDS-API — Verwenden Sie den `ModifyDBCluster` Vorgang und geben Sie `false` gegebenen falls `true` oder für den

Unterschied	Aurora PostgreSQL Serverless v2 und bereitgestellt	Aurora Serverless v1
	• AWS CLI — Verwenden Sie die `disable-http-endpoint` Operationen `enable-http-endpoint` und.	`EnableHttpEndpoint` Parameter an. • AWS CLI — Verwenden Sie die `modify-db-cluster` Operation gegebenenfalls mit der `--no-enable-http-endpoint` Option `--enable-http-endpoint` oder.
CloudTrail Ereignisse	Ereignisse aus Daten-API-Aufrufen sind Datenereignisse. Diese Ereignisse werden standardmäßig automatisch in einem Trail ausgeschlossen. Weitere Informationen finden Sie unter the section called “Einschließen von Daten-API-Ereignissen in einen -CloudTrail Trail”.	Ereignisse aus Daten-API -Aufrufen sind Verwaltungsereignisse. Diese Ereignisse werden standardmäßig automatisch in einen Trail aufgenommen. Weitere Informationen finden Sie unter the section called “Ausschließen von Daten-API-Ereignissen aus einem CloudTrail Trail (Aurora Serverless v1nur)”.
Unterstützung mehrerer Anweisungen	Multistatements werden nicht unterstützt. In diesem Fall wird die Daten-API ausgelöst . `ValidationException: Multistatements aren't supported`	Für Aurora PostgreSQL geben Multistatements nur die erste Abfrageantwort zurück. Für Aurora MySQL werden Multistatements nicht unterstützt.
BatchExecuteAussage	Das generierte Feldobjekt im Aktualisierungsergebnis ist leer.	Das generierte Feldobjekt im Aktualisierungsergebnis enthält eingefügte Werte.
Führen Sie SQL aus	Nicht unterstützt	Als veraltet gekennzeichnet

Unterschied	Aurora PostgreSQL Serverless v2 und bereitgestellt	Aurora Serverless v1
ExecuteStatement	`ExecuteStatement` unterstützt das Abrufen mehrdimensionaler Array-Spalten nicht. In diesem Fall wird die Daten-API ausgelöst. `UnsupportedResultException` Die Daten-API unterstützt einige Datentypen nicht, z. B. geometrische und monetäre Typen. In diesem Fall wird die Daten-API ausgelöst. `UnsupportedResultException: The result contains the unsupported data type` *`data_type`* Nur die folgenden Typen werden unterstützt: • `BOOL` • `BYTEA` • `DATE` • `CIDR` • `DECIMAL`, `NUMERIC` • `ENUM` • `FLOAT8`, `DOUBLE PRECISION` • `INET` • `INT`, `INT4`, `SERIAL`	`ExecuteStatement` unterstützt das Abrufen multidimensionaler Array-Spalten und aller erweiterten Datentypen.

Unterschied	Aurora PostgreSQL Serverless v2 und bereitgestellt	Aurora Serverless v1
	• INT2, SMALLINT, SMALLSERIAL • INT8, BIGINT, BIGSERIAL • JSONB, JSON • REAL, FLOAT • TEXT, CHAR(N), VARCHAR, NAME • TIME • TIMESTAMP • UUID • VECTOR Nur die folgenden Array-Typen werden unterstützt: • BOOL[], BIT[] • DATE[] • DECIMAL[] , NUMERIC[] • FLOAT8[], DOUBLE PRECISION[] • INT[], INT4[] • INT2[] • INT8[], BIGINT[] • JSON[] • REAL[], FLOAT[] • TEXT[], CHAR(N)[] , VARCHAR[] , NAME[] • TIME[] • TIMESTAMP[]	

Unterschied	Aurora PostgreSQL Serverless v2 und bereitgestellt	Aurora Serverless v1
	• `UUID[]`	

Autorisieren des Zugriffs auf die RDS-Daten-API

Benutzer können RDS-Daten-API-Operationen (Daten-API) nur aufrufen, wenn sie dazu autorisiert sind. Sie können einem Benutzer die Erlaubnis zur Verwendung der Daten-API erteilen, indem Sie eine AWS Identity and Access Management (IAM-) Richtlinie anhängen, die seine Rechte definiert. Sie können die Richtlinie auch einer Rolle anfügen, wenn Sie IAM-Rollen verwenden. Eine AWS verwaltete Richtlinie umfasst Berechtigungen für die Daten-API. `AmazonRDSDataFullAccess`

Die `AmazonRDSDataFullAccess` Richtlinie umfasst auch Berechtigungen, aus denen der Benutzer den Wert eines Geheimnisses abrufen kann AWS Secrets Manager. Benutzer müssen Secrets Manager verwenden, um Geheimnisse zu speichern, die sie bei ihren Aufrufen der Daten-API verwenden können. Die Verwendung von Geheimnissen bedeutet, dass Benutzer bei ihren Aufrufen der Daten-API keine Datenbankanmeldeinformationen für die Ressourcen angeben müssen, auf die sie abzielen. Die Daten-API ruft Secrets Manager transparent auf, wodurch die Anfrage des Benutzers nach dem Secret zugelassen (oder abgelehnt) wird. Hinweise zum Einrichten von Geheimnissen zur Verwendung mit der Daten-API finden Sie unter. Speichern von Datenbankanmeldedaten in AWS Secrets Manager

Die `AmazonRDSDataFullAccess` Richtlinie bietet vollständigen Zugriff (über die Daten-API) auf Ressourcen. Sie können den Geltungsbereich einschränken, indem Sie eigene Richtlinien definieren, die den Amazon-Ressourcennamen (ARN) einer Ressource angeben.

Die folgende Richtlinie zeigt beispielsweise ein Beispiel für die Mindestberechtigungen, die ein Benutzer für den Zugriff auf die Daten-API für den durch seinen ARN identifizierten DB-Cluster benötigt. Die Richtlinie enthält die nötigen Berechtigungen, um auf Secrets Manager zuzugreifen und die Autorisierung für die DB-Instance für den Benutzer zu erhalten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerDbCredentialsAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
        },
        {
            "Sid": "RDSDataServiceAccess",
            "Effect": "Allow",
            "Action": [
                "rds-data:BatchExecuteStatement",
                "rds-data:BeginTransaction",
                "rds-data:CommitTransaction",
                "rds-data:ExecuteStatement",
                "rds-data:RollbackTransaction"
            ],
            "Resource": "arn:aws:rds:us-east-2:111122223333:cluster:prod"
        }
    ]
}
```

Sie sollten für das Element „Ressourcen“ in Ihren Richtlinienanweisungen (wie im Beispiel gezeigt) einen spezifischen ARN anstelle eines Platzhalters (*) verwenden.

Arbeiten mit der Tag-basierten Autorisierung

RDS Data API (Data API) und Secrets Manager unterstützen beide die Tag-basierte Autorisierung. Tags sind Schlüssel-Wert-Paare, die eine Ressource, z. B. einen RDS-Cluster, mit einem zusätzlichen Zeichenfolgenwert kennzeichnen, z. B.

- `environment:production`
- `environment:development`

Sie können auf Ihre Ressourcen Tags zum Zweck der Kostenzuweisung, der Ausführungsunterstützung, der Zugriffskontrolle und zu vielen weiteren Zwecken anwenden. (Wenn Sie noch keine Tags für Ihre Ressourcen anwenden und Tags anwenden möchten, finden Sie weitere Informationen unter Markieren von Amazon RDS-Ressourcen.) Sie können die Tags in Ihren Richtlinienanweisungen verwenden, um den Zugriff auf die RDS-Cluster einzuschränken, die mit diesen Tags gekennzeichnet sind. Ein Aurora-DB-Cluster könnte beispielsweise Tags besitzen, die die Umgebung als Produktions- oder Entwicklungsumgebung kennzeichnen.

Das folgende Beispiel zeigt, wie Sie in Ihren Richtlinienanweisungen Tags verwenden können. Diese Anweisung erfordert, dass sowohl der Cluster als auch der in der Daten-API-Anforderung übergebene Schlüssel das Tag `environment:production` enthalten.

Die Richtlinie wird wie folgt angewendet: Wenn ein Benutzer mithilfe der Daten-API einen Anruf tätigt, wird die Anfrage an den Dienst gesendet. Die Daten-API überprüft zunächst, ob der in der Anfrage übergebene Cluster-ARN mit `environment:production` gekennzeichnet ist. Anschließend wird Secrets Manager aufgerufen, um den Wert des Geheimnisses des Benutzers in der Anforderung abzurufen. Secrets Manager überprüft auch, ob das Geheimnis des Benutzers mit `environment:production` markiert ist. Wenn ja, verwendet die Daten-API den abgerufenen Wert für das DB-Passwort des Benutzers. Wenn dieser ebenfalls korrekt ist, wird die Daten-API-Anforderung für den Benutzer erfolgreich aufgerufen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecretsManagerDbCredentialsAccess",
            "Effect": "Allow",
            "Action": [
                 "secretsmanager:GetSecretValue"
               ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*",
            "Condition": {
                    "StringEquals": {
                        "aws:ResourceTag/environment": [
                                        "production"
                                       ]
                     }
             }
        },
        {
            "Sid": "RDSDataServiceAccess",
            "Effect": "Allow",
            "Action": [
                  "rds-data:*"
               ],
            "Resource": "arn:aws:rds:us-east-2:111122223333:cluster:*",
            "Condition": {
                    "StringEquals": {
                        "aws:ResourceTag/environment": [
                                        "production"
```

```
                                    ]
                }
            }
        }
    ]
}
```

Das Beispiel zeigt separate Aktionen für `rds-data` und `secretsmanager` für Data API und Secrets Manager. Sie können jedoch Aktionen kombinieren und Tag-Bedingungen auf viele verschiedene Arten definieren, um Ihre spezifischen Anwendungsfälle zu unterstützen. Weitere Informationen finden Sie unter Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für Secrets Manager.

Im Element „Bedingung“ der Richtlinie können Sie Tag-Schlüssel aus den folgenden Optionen auswählen:

- `aws:TagKeys`
- `aws:ResourceTag/${TagKey}`

Weitere Informationen zu Ressourcen-Tags und deren Verwendung `aws:TagKeys` finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Resource-Tags.

> **Note**
>
> Sowohl Daten-API als auch AWS Secrets Manager autorisierte Benutzer. Wenn Sie nicht für alle in einer Richtlinie definierten Aktionen Berechtigungen besitzen, erhalten Sie den Fehler `AccessDeniedException`.

Speichern von Datenbankanmeldedaten in AWS Secrets Manager

Wenn Sie die RDS Data API (Data API) aufrufen, übergeben Sie Anmeldeinformationen für den Aurora-DB-Cluster mithilfe eines Secrets in Secrets Manager. Zum Übermitteln der Anmeldeinformationen auf diese Weise geben Sie den Namen des Secrets oder den Amazon-Ressourcennamen (ARN) des Secrets an.

So speichern Sie DB-Cluster-Anmeldeinformationen in einem Secret

1. Sie können in Secrets Manager einen geheimen Schlüssel erstellen, der Anmeldeinformationen für den Aurora-DB-Cluster enthält.

Anweisungen finden Sie unter Erstellen eines Datenbank-Secrets im AWS Secrets Manager - Benutzerhandbuch.

2. Verwenden Sie die Secrets Manager Manager-Konsole, um die Details für das von Ihnen erstellte Geheimnis anzuzeigen, oder führen Sie den `aws secretsmanager describe-secret` AWS CLI Befehl aus.

   Notieren Sie sich den Namen und den ARN des Secrets. Sie können sie in Aufrufen der Daten-API verwenden.

Weitere Informationen zur Verwendung von Secrets Manager finden Sie im AWS Secrets-Manager-Benutzerhandbuch.

Informationen dazu, wie Amazon Aurora die Identitäts- und Zugriffsverwaltung steuert, finden Sie unter So funktioniert Amazon Aurora mit IAM.

Informationen zum Erstellen einer IAM-Richtlinie finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch. Informationen zum Hinzufügen einer IAM-Richtlinie zu einem Benutzer finden Sie im Abschnitt Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

RDS-Daten-API aktivieren

Um die RDS-Daten-API (Daten-API) zu verwenden, aktivieren Sie sie für Ihren Aurora-DB-Cluster. Sie können die Daten-API aktivieren, wenn Sie den DB-Cluster erstellen oder ändern.

> **Note**
>
> Für Aurora PostgreSQL wird die Daten-API mit Aurora Serverless v2Aurora Serverless v1, und bereitgestellten Datenbanken unterstützt. Für Aurora MySQL wird die Daten-API nur mit Aurora Serverless v1 Datenbanken unterstützt.

Themen

- Aktivieren Sie die RDS-Daten-API, wenn Sie eine Datenbank erstellen
- RDS-Daten-API für eine bestehende Datenbank aktivieren

Aktivieren Sie die RDS-Daten-API, wenn Sie eine Datenbank erstellen

Während Sie eine Datenbank erstellen, die die RDS-Daten-API (Daten-API) unterstützt, können Sie diese Funktion aktivieren. In den folgenden Verfahren wird beschrieben, wie Sie dies tun, wenn Sie die AWS Management Console AWS CLI, oder die RDS-API verwenden.

Konsole

Um die Daten-API bei der Erstellung eines DB-Clusters zu aktivieren, aktivieren Sie das Kontrollkästchen RDS-Daten-API aktivieren im Bereich Konnektivität der Seite Datenbank erstellen, wie im folgenden Screenshot gezeigt.

Anweisungen zum Erstellen einer Datenbank finden Sie im Folgenden:

- Für Aurora PostgreSQL Serverless v2 und bereitgestellte Datenbanken — Erstellen eines Amazon Aurora-DB Clusters
- Aurora Serverless v1Für — Erstellen eines Aurora Serverless v1-DB Clusters

AWS CLI

Um die Daten-API zu aktivieren, während Sie einen Aurora-DB-Cluster erstellen, führen Sie den AWS CLI Befehl create-db-cluster mit der Option aus. `--enable-http-endpoint`

Im folgenden Beispiel wird ein Aurora PostgreSQL-DB-Cluster mit aktivierter Daten-API erstellt.

FürLinux, odermacOS: Unix

```
aws rds create-db-cluster \
    --db-cluster-identifier my_pg_cluster \
    --engine aurora-postgresql \
    --enable-http-endpoint
```

Windows:

```
aws rds create-db-cluster ^
    --db-cluster-identifier my_pg_cluster ^
    --engine aurora-postgresql ^
    --enable-http-endpoint
```

RDS-API

Um die Daten-API zu aktivieren, während Sie einen Aurora-DB-Cluster erstellen, verwenden Sie den Vorgang CreateDBCluster, wobei der Wert des `EnableHttpEndpoint` Parameters auf gesetzt ist. `true`

RDS-Daten-API für eine bestehende Datenbank aktivieren

Sie können einen DB-Cluster ändern, der die RDS-Daten-API (Daten-API) unterstützt, um diese Funktion zu aktivieren oder zu deaktivieren.

Themen

- Daten-API aktivieren oder deaktivieren (Aurora PostgreSQL Serverless v2 und bereitgestellt)
- Daten-API aktivieren oder deaktivieren (Aurora Serverless v1nur)

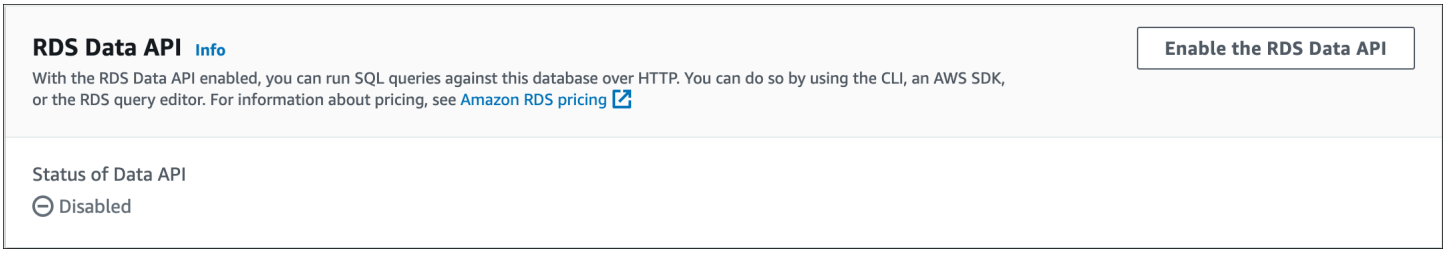
Daten-API aktivieren oder deaktivieren (Aurora PostgreSQL Serverless v2 und bereitgestellt)

Verwenden Sie die folgenden Verfahren, um die Daten-API auf Aurora PostgreSQL Serverless v2 und bereitgestellten Datenbanken zu aktivieren oder zu deaktivieren. Verwenden Sie die Verfahren unter, um die Daten-API für Aurora Serverless v1 Datenbanken zu aktivieren oder zu deaktivieren. the section called “Daten-API aktivieren oder deaktivieren (Aurora Serverless v1nur)”

Konsole

Sie können die Daten-API aktivieren oder deaktivieren, indem Sie die RDS-Konsole für einen DB-Cluster verwenden, der diese Funktion unterstützt. Öffnen Sie dazu die Cluster-Detailseite der Datenbank, für die Sie die Daten-API aktivieren oder deaktivieren möchten, und wechseln Sie auf der Registerkarte Konnektivität und Sicherheit zum Abschnitt RDS-Daten-API. In diesem Abschnitt wird der Status der Daten-API angezeigt und Sie können sie aktivieren oder deaktivieren.

Der folgende Screenshot zeigt, dass die RDS-Daten-API nicht aktiviert ist.



AWS CLI

Um die Daten-API in einer vorhandenen Datenbank zu aktivieren oder zu deaktivieren, führen Sie den AWS CLI Befehl enable-http-endpoint oder disable-http-endpoint aus und geben Sie den ARN Ihres DB-Clusters an.

Das folgende Beispiel aktiviert die Daten-API.

Für LinuxmacOS, oderUnix:

```
aws rds enable-http-endpoint \
    --resource-arn cluster_arn
```

Windows:

```
aws rds enable-http-endpoint ^
    --resource-arn cluster_arn
```

RDS-API

Verwenden Sie die Operationen EnableHttpEndpoint und DisableHttp Endpoint, um die Daten-API in einer vorhandenen Datenbank zu aktivieren oder zu deaktivieren.

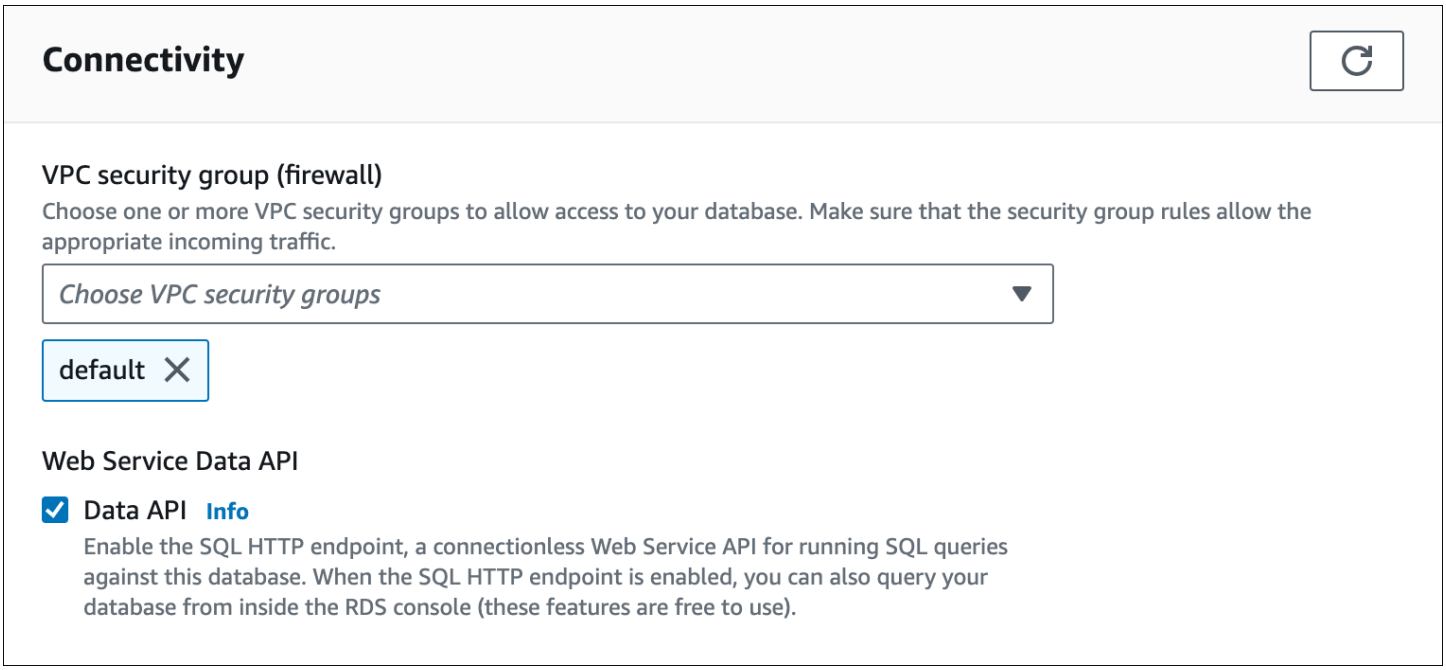
Daten-API aktivieren oder deaktivieren (Aurora Serverless v1nur)

Verwenden Sie die folgenden Verfahren, um die Daten-API in vorhandenen Aurora Serverless v1 Datenbanken zu aktivieren oder zu deaktivieren. Um die Daten-API auf Aurora PostgreSQL Serverless v2 und bereitgestellten Datenbanken zu aktivieren oder zu deaktivieren, verwenden Sie die Verfahren unter. the section called “Daten-API aktivieren oder deaktivieren”

Konsole

Wenn Sie einen Aurora Serverless v1 DB-Cluster ändern, aktivieren Sie die Daten-API im Bereich Konnektivität der RDS-Konsole.

Der folgende Screenshot zeigt die aktivierte Daten-API beim Ändern eines Aurora-DB-Clusters.



Anweisungen zum Ändern eines Aurora Serverless v1 DB-Clusters finden Sie unterÄndern eines Aurora Serverless v1-DB-Clusters.

AWS CLI

Um die Daten-API zu aktivieren oder zu deaktivieren, führen Sie den AWS CLI Befehl modify-db-cluster mit dem `--enable-http-endpoint` oder, falls zutreffend, aus. `--no-enable-http-endpoint`

Im folgenden Beispiel wird die Daten-API aktiviert. `sample-cluster`

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier sample-cluster \
    --enable-http-endpoint
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier sample-cluster ^
    --enable-http-endpoint
```

RDS-API

Um die Daten-API zu aktivieren, verwenden Sie den Vorgang ModifyDBCluster und setzen Sie den Wert von je `EnableHttpEndpoint` nach Bedarf auf `true` oder`false`.

Erstellen eines Amazon VPC-Endpunkts für RDS Data API ()AWS PrivateLink

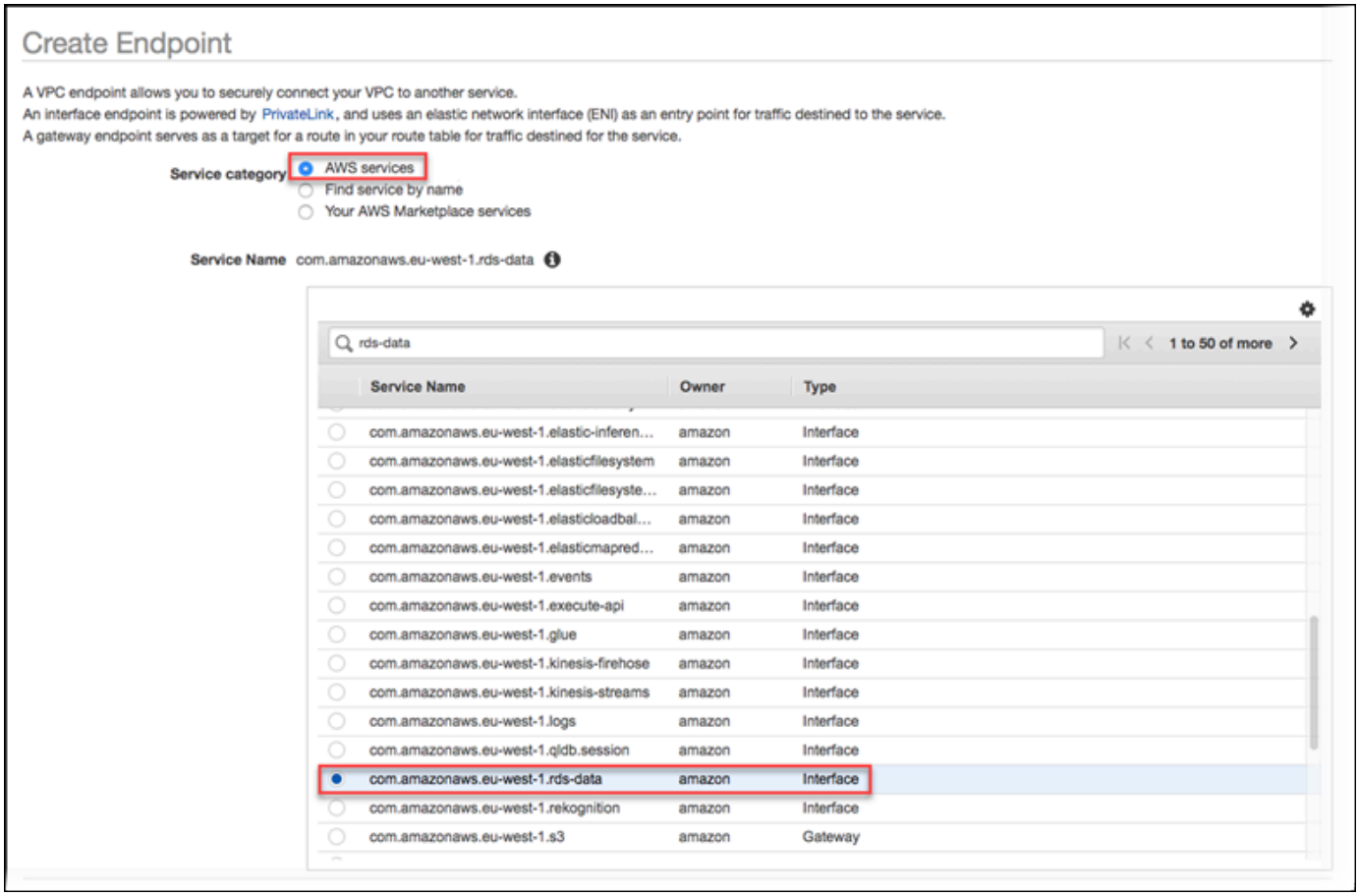
Amazon VPC ermöglicht es Ihnen, AWS Ressourcen wie Aurora-DB-Cluster und -Anwendungen in einer Virtual Private Cloud (VPC) zu starten. AWS PrivateLink bietet private Konnektivität zwischen VPCs und AWS Diensten mit hoher Sicherheit im Amazon-Netzwerk. Mithilfe AWS PrivateLink können Sie Amazon VPC-Endpunkte erstellen, mit denen Sie eine Verbindung zu Diensten über verschiedene Konten und VPCs auf Basis von Amazon VPC herstellen können. Weitere Informationen über AWS PrivateLink finden Sie unter VPC-Endpunktservices (AWS PrivateLink) im Amazon-Virtual-Private-Cloud-Benutzerhandbuch.

Sie können die RDS-Daten-API (Daten-API) mit Amazon VPC-Endpunkten aufrufen. Durch die Verwendung eines Amazon VPC-Endpunkts wird der Datenverkehr zwischen Anwendungen in Ihrer Amazon VPC und der Daten-API im AWS Netzwerk aufrechterhalten, ohne öffentliche IP-Adressen zu verwenden. Amazon-VPC-Endpunkte können Ihnen dabei helfen, Compliance- und behördliche Anforderungen im Zusammenhang mit der Einschränkung der öffentlichen Internetkonnektivität zu erfüllen. Wenn Sie beispielsweise einen Amazon VPC-Endpunkt verwenden, können Sie den Verkehr zwischen einer Anwendung, die auf einer Amazon EC2 EC2-Instance ausgeführt wird, und der Daten-API in den VPCs, die sie enthalten, aufrechterhalten.

Nachdem Sie den Amazon VPC-Endpunkt erstellt haben, können Sie ihn verwenden, ohne Code- oder Konfigurationsänderungen in der Anwendung vorzunehmen.

So erstellen Sie einen Amazon VPC-Endpunkt für die Daten-API

1. Melden Sie sich bei der Amazon VPC-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie Endpunkte und dann Endpunkt erstellen aus.
3. Wählen Sie auf der Seite Create Endpoint (Endpunkt erstellen) für Service category (Servicekategorie) die Option AWS -Services aus. Wählen Sie für Servicename rds-data aus.



4. Wählen Sie für VPC die VPC aus, in der der Endpunkt erstellt werden soll.

   Wählen Sie die VPC aus, die die Anwendung enthält, die Daten-API-Aufrufe ausführt.

5. Wählen Sie für Subnetze das Subnetz für jede Availability Zone (AZ) aus, die von dem AWS Service verwendet wird, auf dem Ihre Anwendung ausgeführt wird.

   Um einen Amazon VPC-Endpunkt zu erstellen, geben Sie den privaten IP-Adressbereich an, in dem auf den Endpunkt zugegriffen werden soll. Wählen Sie dazu das Subnetz für jede Availability Zone aus. Dadurch wird der VPC-Endpunkt auf den privaten IP-Adressbereich

beschränkt, der für jede Availability Zone spezifisch ist. Außerdem wird in jeder Availability Zone ein Amazon VPC-Endpunkt erstellt.

6. Wählen Sie für DNS-Namen aktivieren die Option Für diesen Endpunkt aktivieren aus.

   Private DNS löst den standardmäßigen DNS-Hostnamen der Daten-API (`https://rds-data.`*`region`*`.amazonaws.com`) in die privaten IP-Adressen auf, die mit dem für Ihren Amazon VPC-Endpunkt spezifischen DNS-Hostnamen verknüpft sind. Daher können Sie mit den AWS SDKs AWS CLI oder auf den VPC-Endpunkt der Daten-API zugreifen, ohne Code- oder Konfigurationsänderungen vornehmen zu müssen, um die Endpunkt-URL der Daten-API zu aktualisieren.

7. Wählen Sie für Sicherheitsgruppe eine Sicherheitsgruppe aus, die dem Amazon VPC-Endpunkt zugeordnet werden soll.

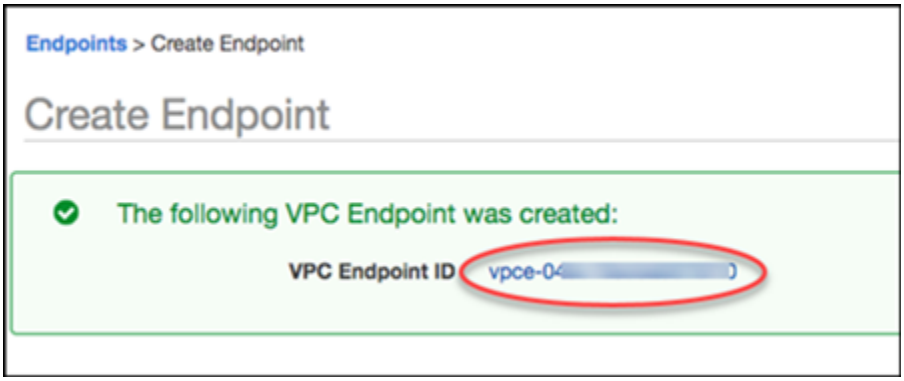
   Wählen Sie die Sicherheitsgruppe aus, die den Zugriff auf den AWS Dienst ermöglicht, auf dem Ihre Anwendung ausgeführt wird. Wenn beispielsweise eine Amazon EC2-Instance Ihre Anwendung ausführt, wählen Sie die Sicherheitsgruppe aus, die den Zugriff auf die Amazon EC2-Instance ermöglicht. Mit der Sicherheitsgruppe können Sie den Datenverkehr zum Amazon VPC-Endpunkt von Ressourcen in Ihrer VPC steuern.

8. Wählen Sie unter Richtlinie die Option Voller Zugriff aus, damit jeder innerhalb der Amazon VPC über diesen Endpunkt auf die Daten-API zugreifen kann. Oder wählen Sie Benutzerdefiniert aus, um eine Richtlinie anzugeben, die den Zugriff einschränkt.

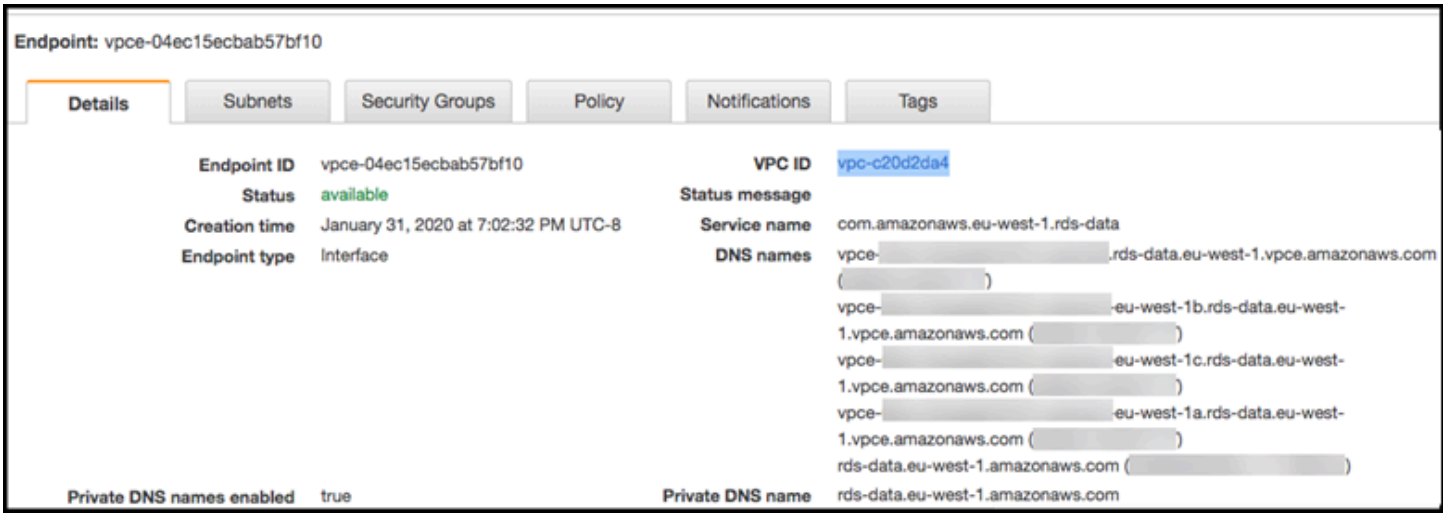
   Wenn Sie Benutzerdefiniert auswählen, geben Sie die Richtlinie im Tool zur Richtlinienerstellung ein.

9. Wählen Sie Endpunkt erstellen aus.

Nachdem der Endpunkt erstellt wurde, wählen Sie den Link in, AWS Management Console um die Endpunktdetails anzuzeigen.



Auf der Registerkarte Details des Endpunkts werden die DNS-Hostnamen angezeigt, die beim Erstellen des Amazon VPC-Endpunkts generiert wurden.



Sie können den Standardendpunkt (`rds-data.`*`region`*`.amazonaws.com`) oder einen der VPC-spezifischen Endpunkte verwenden, um die Daten-API innerhalb der Amazon VPC aufzurufen. Der standardmäßige Daten-API-Endpunkt leitet automatisch an den Amazon VPC-Endpunkt weiter. Dieses Routing tritt auf, weil der private DNS-Hostname beim Erstellen des Amazon VPC-Endpunkts aktiviert wurde.

Wenn Sie einen Amazon VPC-Endpunkt in einem Daten-API-Aufruf verwenden, verbleibt der gesamte Datenverkehr zwischen Ihrer Anwendung und der Daten-API in den Amazon-VPCs, die sie enthalten. Sie können einen Amazon VPC-Endpunkt für jeden Typ von Daten-API-Aufruf verwenden. Informationen zum Aufrufen der Daten-API finden Sie unter. Aufrufen der RDS-Daten-API

Aufrufen der RDS-Daten-API

Wenn die RDS-Daten-API (Daten-API) auf Ihrem Aurora-DB-Cluster aktiviert ist, können Sie SQL-Anweisungen auf dem Aurora-DB-Cluster ausführen, indem Sie die Daten-API oder die AWS CLI.

Die Daten-API unterstützt die von den AWS SDKs unterstützten Programmiersprachen. Weitere Informationen finden Sie unter Tools, auf AWS denen Sie aufbauen können.

Themen

Referenz zu Daten-API-Vorgängen

Die Daten-API bietet die folgenden Operationen zur Ausführung von SQL-Anweisungen.

Daten-API-Operation	AWS CLI Befehl	Beschreibung
`ExecuteStatement`	`aws rds-data execute-statement`	Führt eine SQL-Anweisung in einer Datenbank aus.
`BatchExecuteStatement`	`aws rds-data batch-execute-statement`	Führt eine Batch-SQL-Anweisung über ein Array von Daten für Massen-Update- und -Einfügeoperationen aus. Sie können eine DML-Anweisung (Data Manipulation Language) mit einem Array von Parametersätzen ausführen . Eine Batch-SQL-Anweisung kann gegenüber einzelnen Einfügungs- und Aktualisierungsanweisungen eine erhebliche Leistungsverbesserung bieten.

Sie können beide Vorgänge verwenden, um einzelne SQL-Anweisungen oder Transaktionen auszuführen. Für Transaktionen bietet die Daten-API die folgenden Operationen.

Daten-API-Operation	AWS CLI Befehl	Beschreibung
BeginTransaction	aws rds-data begin-transaction	Startet eine SQL-Transaktion.
CommitTransaction	aws rds-data commit-transaction	Beendet eine SQL-Transaktion und schreibt die Änderungen fest.
RollbackTransaction	aws rds-data rollback-transaction	Führt ein Rollback einer Transaktion durch.

Die Operationen zur Ausführung von SQL-Anweisungen und zur Unterstützung von Transaktionen haben die folgenden gemeinsamen Daten-API-Parameter und AWS CLI -Optionen. Einige Operationen unterstützen andere Parameter oder Optionen.

Daten-API-Operationsparameter	AWS CLI Befehlsoption	Erforderlich	Beschreibung
`resourceArn`	`--resource-arn`	Ja	Der Amazon-Ressourcenname (ARN) des Aurora-DB-Clusters.
`secretArn`	`--secret-arn`	Ja	Der Name oder ARN des Secrets, das Zugriff auf das DB-Cluster ermöglicht.

Sie können Parameter in Daten-API-Aufrufen an `ExecuteStatement` und und verwenden`BatchExecuteStatement`, wenn Sie die AWS CLI Befehle `execute-statement` und ausführen`batch-execute-statement`. Um einen Parameter zu verwenden, geben Sie ein Name-Wert-Paar im Datentyp `SqlParameter` an. Den Wert geben Sie mit dem Datentyp `Field` an. In der folgenden Tabelle sind den Datentypen, die Sie in Daten-API-Aufrufen angeben, JDBC-Datentypen (Java Database Connectivity) zugeordnet.

JDBC-Datentyp	Daten-API-Datentyp
`INTEGER, TINYINT, SMALLINT, BIGINT`	`LONG` (oder `STRING`)
`FLOAT, REAL, DOUBLE`	`DOUBLE`
`DECIMAL`	`STRING`
`BOOLEAN, BIT`	`BOOLEAN`
`BLOB, BINARY, LONGVARBINARY, VARBINARY`	`BLOB`
`CLOB`	`STRING`
Andere Typen (einschließlich datums- und zeitbezogener Typen)	`STRING`

> **Note**
>
> Sie können den Datentyp `LONG` oder `STRING` in Ihrem Daten-API-Aufruf für von der Datenbank zurückgegebene `LONG`-Werte angeben. Wir empfehlen Ihnen, dies zu tun, um zu vermeiden, dass bei extrem großen Zahlen die Genauigkeit verloren geht, was bei der Arbeit mit auftreten kann JavaScript.

Für bestimmte Typen, wie z. B. `DECIMAL` und`TIME`, ist ein Hinweis erforderlich, damit die Daten-API `String` Werte als den richtigen Typ an die Datenbank weitergibt. Um einen Hinweis zu verwenden, schließen Sie Werte für `typeHint` in den Datentyp `SqlParameter` ein. Die folgenden Werte sind für `typeHint` möglich:

- `DATE` – Der entsprechende `String`-Parameter wird als Objekt des Typs `DATE` an die Datenbank gesendet. Das akzeptierte Format ist `YYYY-MM-DD`.
- `DECIMAL` – Der entsprechende `String`-Parameter wird als Objekt des Typs `DECIMAL` an die Datenbank gesendet.
- `JSON` – Der entsprechende `String`-Parameter wird als Objekt des Typs `JSON` an die Datenbank gesendet.

- `TIME` – Der entsprechende `String`-Parameter wird als Objekt des Typs `TIME` an die Datenbank gesendet. Das akzeptierte Format ist `HH:MM:SS[.FFF]`.
- `TIMESTAMP` – Der entsprechende `String`-Parameter wird als Objekt des Typs `TIMESTAMP` an die Datenbank gesendet. Das akzeptierte Format ist `YYYY-MM-DD HH:MM:SS[.FFF]`.
- `UUID` – Der entsprechende `String`-Parameter wird als Objekt des Typs `UUID` an die Datenbank gesendet.

> **Note**
>
> Derzeit unterstützt die Daten-API keine Arrays von Universal Unique Identifiers (UUIDs).

> **Note**
>
> Für Amazon Aurora PostgreSQL gibt die Daten-API immer den Aurora PostgreSQL-Datentyp `TIMESTAMPTZ` in der UTC-Zeitzone zurück.

Aufrufen der RDS-Daten-API mit dem AWS CLI

Sie können die RDS-Daten-API (Daten-API) mit dem aufrufen AWS CLI.

In den folgenden Beispielen wird die AWS CLI for Data API verwendet. Weitere Informationen finden Sie in der AWS CLI -Referenz für die Daten-API.

Ersetzen Sie in jedem Beispiel den Amazon Resource Name (ARN) für den DB-Cluster durch den ARN für Ihren Aurora-DB-Cluster. Ersetzen Sie außerdem den geheimen ARN durch den ARN des geheimen Schlüssels in Secrets Manager, der den Zugriff auf den DB-Cluster ermöglicht.

> **Note**
>
> Sie AWS CLI können Antworten in JSON formatieren.

Themen

- Starten einer SQL-Transaktion
- Ausführen einer SQL-Anweisung

- Ausführen einer Stapel-SQL-Anweisung über ein Daten-Array
- Übergeben einer SQL-Transaktion
- Rollback einer SQL-Transaktion

Starten einer SQL-Transaktion

Sie können eine SQL-Transaktion mit dem CLI-Befehl `aws rds-data begin-transaction` starten. Der Aufruf gibt eine Transaktions-ID zurück.

> **Important**
>
> Innerhalb der Daten-API kommt es bei einer Transaktion zu einem Timeout, wenn innerhalb von drei Minuten keine Aufrufe erfolgen, die ihre Transaktions-ID verwenden. Wenn bei einer Transaktion das Timeout überschritten wird, bevor sie festgeschrieben wurde, wird sie von der Daten-API automatisch zurückgesetzt.
> DDL-Anweisungen (MySQL Data Definition Language) innerhalb einer Transaktion führen zu einem impliziten Commit. Wir empfehlen, dass Sie jede MySQL-DDL-Anweisung in einem separaten `execute-statement` Befehl mit der `--continue-after-timeout` Option ausführen.

Geben Sie zusätzlich zu den allgemeinen Optionen die Option `--database` an, die den Namen der Datenbank enthält.

Der folgende CLI-Befehl beispielsweise startet eine SQL-Transaktion.

Für LinuxmacOS, oderUnix:

```
aws rds-data begin-transaction --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" \
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret"
```

Windows:

```
aws rds-data begin-transaction --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" ^
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "transactionId": "ABC1234567890xyz"
}
```

Ausführen einer SQL-Anweisung

Sie können mittels des CLI-Befehls `aws rds-data execute-statement` eine SQL-Anweisung ausführen.

Sie können die SQL-Anweisung in einer Transaktion ausführen, indem Sie die Transaktions-ID mit der Option `--transaction-id` angeben. Sie können eine SQL-Transaktion mit dem CLI-Befehl `aws rds-data begin-transaction` starten. Sie können eine Transaktion beenden und übergeben, indem Sie den CLI-Befehl `aws rds-data commit-transaction` verwenden.

> **Important**
>
> Wenn Sie die Option `--transaction-id` nicht angeben, werden Änderungen, die sich durch den Aufruf ergeben, automatisch übergeben.

Geben Sie zusätzlich zu den allgemeinen Optionen die folgenden Optionen an:

- `--sql` (erforderlich) – eine SQL-Anweisung, die auf dem DB-Cluster ausgeführt werden soll.
- `--transaction-id` (optional) – die ID einer Transaktion, die über den CLI-Befehl `begin-transaction` gestartet wurde. Geben Sie die Transaktions-ID der Transaktion an, in die Sie die SQL-Anweisung einfügen möchten.
- `--parameters` (optional) – die Parameter für die SQL-Anweisung.
- `--include-result-metadata | --no-include-result-metadata` (optional) – ein Wert, der angibt, ob Metadaten in die Ergebnisse eingefügt werden sollen. Der Standardwert ist `--no-include-result-metadata`.
- `--database` (optional) – der Name der Datenbank.

  Die `--database`-Option funktioniert möglicherweise nicht, wenn Sie eine SQL-Anweisung ausführen, nachdem Sie bei der vorherige Anfrage `--sql "use database_name;"` ausgeführt haben. Es wird empfohlen, die `--database`-Option zu verwenden statt `--sql "use database_name;"`-Anweisungen auszuführen.

- `--continue-after-timeout | --no-continue-after-timeout`(optional) — Ein Wert, der angibt, ob die Anweisung weiter ausgeführt werden soll, nachdem der Aufruf das Daten-API-Timeout-Intervall von 45 Sekunden überschritten hat. Der Standardwert ist `--no-continue-after-timeout`.

  Im Fall von Data Definition Language (DDL)-Anweisungen osllten Sie die Anweisung nach Ablauf des Aufrufs weiter ausführen, um Fehler und die Möglichkeit beschädigter Datenstrukturen zu vermeiden.
- `--format-records-as "JSON"|"NONE"` – Ein optionaler Wert, der angibt, ob die Ergebnismenge als JSON-Zeichenfolge formatiert werden soll. Der Standardwert ist `"NONE"`. Nutzungsinformationen über die Verarbeitung von JSON-Ergebnismengen finden Sie unter Verarbeitung der Ergebnisse der RDS-Daten-API-Abfrage im JSON-Format.

Das DB-Cluster gibt für den Aufruf eine Antwort zurück.

> **Note**
>
> Das Limit für Antwortgrößen beträgt 1 MiB. Wenn der Aufruf mehr als 1 MiB an Antwortdaten zurückgibt, wird der Aufruf beendet.
> Denn Aurora Serverless v1 die maximale Anzahl von Anfragen pro Sekunde beträgt 1.000. Für alle anderen unterstützten Datenbanken gibt es kein Limit.

Der folgende CLI-Befehl führt beispielsweise eine einzelne SQL-Anweisung aus und lässt die Metadaten in den Ergebnissen weg (Standard).

Für LinuxmacOS, oderUnix:

```
aws rds-data execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" \
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" \
--sql "select * from mytable"
```

Windows:

```
aws rds-data execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" ^
```

```
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" ^
--sql "select * from mytable"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "numberOfRecordsUpdated": 0,
    "records": [
        [
            {
                "longValue": 1
            },
            {
                "stringValue": "ValueOne"
            }
        ],
        [
            {
                "longValue": 2
            },
            {
                "stringValue": "ValueTwo"
            }
        ],
        [
            {
                "longValue": 3
            },
            {
                "stringValue": "ValueThree"
            }
        ]
    ]
}
```

Der folgende CLI-Befehl führt eine einzelne SQL-Anweisung in einer Transaktion aus, indem die Option `--transaction-id` angegeben wird.

Für LinuxmacOS, oderUnix:

```
aws rds-data execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" \
```

```
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" \
--sql "update mytable set quantity=5 where id=201" --transaction-id "ABC1234567890xyz"
```

Windows:

```
aws rds-data execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" ^
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" ^
--sql "update mytable set quantity=5 where id=201" --transaction-id "ABC1234567890xyz"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "numberOfRecordsUpdated": 1
}
```

Der folgende CLI-Befehl führt eine einzelne SQL-Anweisung mit Parametern aus.

Für LinuxmacOS, oderUnix:

```
aws rds-data execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" \
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" \
--sql "insert into mytable values (:id, :val)" --parameters "[{\"name\": \"id\",
 \"value\": {\"longValue\": 1}},{\"name\": \"val\", \"value\": {\"stringValue\":
 \"value1\"}}]"
```

Windows:

```
aws rds-data execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" ^
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" ^
--sql "insert into mytable values (:id, :val)" --parameters "[{\"name\": \"id\",
 \"value\": {\"longValue\": 1}},{\"name\": \"val\", \"value\": {\"stringValue\":
 \"value1\"}}]"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "numberOfRecordsUpdated": 1
}
```

Der folgende CLI-Befehl führt eine Data Definition Language (DDL)-SQL-Anweisung aus. Die DDL-Anweisung benennt die Spalte `job` in die Spalte `role` um.

> **Important**
>
> Im Fall von DDL-Anweisungen sollten Sie die Anweisung auch nach Ablauf des Aufrufs weiter ausführen. Wenn eine DDL-Anweisung vor Ende der Ausführung beendet wird, kann dies zu Fehlern und möglicherweise beschädigten Datenstrukturen führen. Um eine Anweisung weiter auszuführen, nachdem ein Aufruf das RDS-Daten-API-Timeout-Intervall von 45 Sekunden überschritten hat, geben Sie die `--continue-after-timeout` Option an.

Für LinuxmacOS, oderUnix:

```
aws rds-data execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" \
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" \
--sql "alter table mytable change column job role varchar(100)" --continue-after-
timeout
```

Windows:

```
aws rds-data execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" ^
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" ^
--sql "alter table mytable change column job role varchar(100)" --continue-after-
timeout
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "generatedFields": [],
    "numberOfRecordsUpdated": 0
}
```

> **Note**
>
> Die `generatedFields`-Daten werden von Aurora PostgreSQL nicht unterstützt. Zum Abrufen der Werte von generierten Feldern verwenden Sie die `RETURNING`-Klausel. Weitere Informationen finden Sie in unter Returning Data From Modified Rows in der PostgreSQL-Dokumentation.

Ausführen einer Stapel-SQL-Anweisung über ein Daten-Array

Sie können eine Batch-SQL-Anweisung über ein Daten-Array ausführen, indem Sie den CLI-Befehl `aws rds-data batch-execute-statement` verwenden. Sie können dieses Befehl verwenden, um einen Massenimport oder eine Update-Operation auszuführen.

Sie können die SQL-Anweisung in einer Transaktion ausführen, indem Sie die Transaktions-ID mit der Option `--transaction-id` angeben. Sie können eine SQL-Transaktion mit dem CLI-Befehl `aws rds-data begin-transaction` starten. Sie können eine Transaktion mit dem CLI-Befehl `aws rds-data commit-transaction` beenden und übergeben.

> **Important**
>
> Wenn Sie die Option `--transaction-id` nicht angeben, werden Änderungen, die sich durch den Aufruf ergeben, automatisch übergeben.

Geben Sie zusätzlich zu den allgemeinen Optionen die folgenden Optionen an:

- `--sql` (erforderlich) – eine SQL-Anweisung, die auf dem DB-Cluster ausgeführt werden soll.

  > **Tip**
  >
  > Fügen Sie bei MySQL-kompatiblen Anweisungen kein Semikolon am Ende des `--sql`-Parameters ein. Ein abschließendes Semikolon kann einen Syntaxfehler verursachen.

- `--transaction-id` (optional) – die ID einer Transaktion, die über den CLI-Befehl `begin-transaction` gestartet wurde. Geben Sie die Transaktions-ID der Transaktion an, in die Sie die SQL-Anweisung einfügen möchten.
- `--parameter-set` (optional) – die Parametersätze für die Batch-Operation.

- `--database` (optional) – der Name der Datenbank.

Das DB-Cluster gibt für den Aufruf eine Antwort zurück.

> **Note**
>
> Es gibt keine feste Obergrenze für die Anzahl der Parametersätze. Die maximale Größe der über die Daten-API übermittelten HTTP-Anfrage beträgt jedoch 4 MiB. Wenn die Anfrage dieses Limit überschreitet, gibt Data API einen Fehler zurück und verarbeitet die Anfrage nicht. Dieses 4-MiB-Limit umfasst die Größe der HTTP-Header und der JSON-Notation in der Anforderung. Die Anzahl der Parametersätze, die Sie einbinden können, hängt demnach von mehreren Faktoren ab, z. B. von der Größe der SQL-Anweisung und der Größe der individuellen Parametersätze.
>
> Das Limit für Antwortgrößen beträgt 1 MiB. Wenn der Aufruf mehr als 1 MiB an Antwortdaten zurückgibt, wird der Aufruf beendet.
>
> Denn Aurora Serverless v1 die maximale Anzahl von Anfragen pro Sekunde beträgt 1.000. Für alle anderen unterstützten Datenbanken gibt es kein Limit.

Der folgende CLI-Befehl führt beispielsweise eine Batch-SQL-Anweisung für ein Daten-Array mit einem Parametersatz aus.

Für LinuxmacOS, oderUnix:

```
aws rds-data batch-execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" \
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" \
--sql "insert into mytable values (:id, :val)" \
--parameter-sets "[[{\"name\": \"id\", \"value\": {\"longValue\": 1}},{\"name\":
 \"val\", \"value\": {\"stringValue\": \"ValueOne\"}}],
[{\"name\": \"id\", \"value\": {\"longValue\": 2}},{\"name\": \"val\", \"value\":
 {\"stringValue\": \"ValueTwo\"}}],
[{\"name\": \"id\", \"value\": {\"longValue\": 3}},{\"name\": \"val\", \"value\":
 {\"stringValue\": \"ValueThree\"}}]]"
```

Windows:

```
aws rds-data batch-execute-statement --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" ^
```

```
--database "mydb" --secret-arn "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret" ^
--sql "insert into mytable values (:id, :val)" ^
--parameter-sets "[[{\"name\": \"id\", \"value\": {\"longValue\": 1}},{\"name\":
 \"val\", \"value\": {\"stringValue\": \"ValueOne\"}}],
[{\"name\": \"id\", \"value\": {\"longValue\": 2}},{\"name\": \"val\", \"value\":
 {\"stringValue\": \"ValueTwo\"}}],
[{\"name\": \"id\", \"value\": {\"longValue\": 3}},{\"name\": \"val\", \"value\":
 {\"stringValue\": \"ValueThree\"}}]]"
```

> **Note**
>
> Verwenden Sie in der Option `--parameter-sets` keine Zeilenumbrüche.

Übergeben einer SQL-Transaktion

Mit dem CLI-Befehl `aws rds-data commit-transaction` können Sie eine SQL-Transaktion beenden, die mit `aws rds-data begin-transaction` gestartet wurde, und die Änderungen übergeben.

Geben Sie zusätzlich zu den allgemeinen Optionen die folgende Option an:

- `--transaction-id` (erforderlich) – die ID einer Transaktion, die über den CLI-Befehl `begin-transaction` gestartet wurde. Geben Sie die Transaktions-ID der Transaktion an, die Sie beenden und übergeben möchten.

Der folgende CLI-Befehl beendet beispielsweise eine SQL-Transaktion und übergibt die Änderungen.

Für LinuxmacOS, oderUnix:

```
aws rds-data commit-transaction --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" \
--secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" \
--transaction-id "ABC1234567890xyz"
```

Windows:

```
aws rds-data commit-transaction --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" ^
--secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" ^
```

```
--transaction-id "ABC1234567890xyz"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "transactionStatus": "Transaction Committed"
}
```

Rollback einer SQL-Transaktion

Mit dem CLI-Befehl `aws rds-data rollback-transaction` können Sie einen Rollback für eine SQL-Transaktion ausführen, die mit `aws rds-data begin-transaction` gestartet wurde. Durch das Rollback einer Transaktion werden für sie ausgeführte Änderungen rückgängig gemacht.

> **Important**
>
> Wenn die Transaktions-ID abgelaufen ist, wurde automatisch ein Rollback für die Transaktion ausgeführt. In diesem Fall gibt ein `aws rds-data rollback-transaction`-Befehl, der die abgelaufene Transaktions-ID angibt, einen Fehler zurück.

Geben Sie zusätzlich zu den allgemeinen Optionen die folgende Option an:

- `--transaction-id` (erforderlich) – die ID einer Transaktion, die über den CLI-Befehl `begin-transaction` gestartet wurde. Geben Sie die Transaktions-ID der Transaktion an, für die Sie ein Rollback ausführen möchten.

Mit dem folgenden AWS CLI Befehl wird beispielsweise eine SQL-Transaktion rückgängig gemacht.

Für LinuxmacOS, oderUnix:

```
aws rds-data rollback-transaction --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" \
--secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" \
--transaction-id "ABC1234567890xyz"
```

Windows:

```
aws rds-data rollback-transaction --resource-arn "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster" ^
```

```
--secret-arn "arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret" ^
--transaction-id "ABC1234567890xyz"
```

Im Folgenden sehen Sie ein Beispiel für die Antwort.

```
{
    "transactionStatus": "Rollback Complete"
    }
```

Aufrufen der RDS-Daten-API aus einer Python-Anwendung

Sie können die RDS-Daten-API (Daten-API) von einer Python-Anwendung aus aufrufen.

Die folgenden Beispiele verwenden das AWS SDK für Python (Boto). Weitere Informationen zu Boto finden Sie in der AWS SDK for Python (Boto 3)-Dokumentation.

Ersetzen Sie in jedem Beispiel den Amazon Resource Name (ARN) des DB-Clusters durch den ARN für Ihren Aurora-DB-Cluster. Ersetzen Sie außerdem den geheimen ARN durch den ARN des geheimen Schlüssels in Secrets Manager, der den Zugriff auf den DB-Cluster ermöglicht.

Themen

- Ausführen einer SQL-Abfrage
- Ausführen einer DML SQL-Anweisung
- Ausführen einer SQL-Transaktion

Ausführen einer SQL-Abfrage

Sie können eine `SELECT`-Anweisung ausführen und die Ergebnisse mit einer Python-Anwendung abrufen.

Im folgenden Beispiel wird eine SQL-Abfrage ausgeführt.

```
import boto3

rdsData = boto3.client('rds-data')

cluster_arn = 'arn:aws:rds:us-east-1:123456789012:cluster:mydbcluster'
secret_arn = 'arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret'

response1 = rdsData.execute_statement(
```

```
            resourceArn = cluster_arn,
            secretArn = secret_arn,
            database = 'mydb',
            sql = 'select * from employees limit 3')

print (response1['records'])
[
    [
        {
            'longValue': 1
        },
        {
            'stringValue': 'ROSALEZ'
        },
        {
            'stringValue': 'ALEJANDRO'
        },
        {
            'stringValue': '2016-02-15 04:34:33.0'
        }
    ],
    [
        {
            'longValue': 1
        },
        {
            'stringValue': 'DOE'
        },
        {
            'stringValue': 'JANE'
        },
        {
            'stringValue': '2014-05-09 04:34:33.0'
        }
    ],
    [
        {
            'longValue': 1
        },
        {
            'stringValue': 'STILES'
        },
        {
            'stringValue': 'JOHN'
```

```
        },
        {
            'stringValue': '2017-09-20 04:34:33.0'
        }
    ]
]
```

Ausführen einer DML SQL-Anweisung

Sie können eine Data Manipulation Language (DML)-Anweisung ausführen, um in Ihrer Datenbank Daten einzufügen, zu aktualisieren oder zu löschen. Sie können in DML-Anweisungen auch Parameter verwenden.

> **Important**
>
> Wenn ein Aufruf kein Teil einer Transaktion ist, da er den Parameter `transactionID` nicht enthält, werden Änderungen, die sich aus dem Aufruf ergeben, automatisch übergeben.

Im folgenden Beispiel werden eine SQL Insert-Anweisung ausgeführt und Parameter verwendet.

```
import boto3

cluster_arn = 'arn:aws:rds:us-east-1:123456789012:cluster:mydbcluster'
secret_arn = 'arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret'

rdsData = boto3.client('rds-data')


param1 = {'name':'firstname', 'value':{'stringValue': 'JACKSON'}}
param2 = {'name':'lastname', 'value':{'stringValue': 'MATEO'}}
paramSet = [param1, param2]

response2 = rdsData.execute_statement(resourceArn=cluster_arn,
                                      secretArn=secret_arn,
                                      database='mydb',
                                      sql='insert into employees(first_name, last_name)
 VALUES(:firstname, :lastname)',
                                      parameters = paramSet)

print (response2["numberOfRecordsUpdated"])
```

Ausführen einer SQL-Transaktion

Sie können eine SQL-Transaktion starten, eine oder mehrere SQL-Anweisungen ausführen und anschließend die Änderungen mit einer Python-Anwendung übergeben.

> **Important**
>
> Bei einer Transaktion kommt es zu einer Zeitüberschreitung, wenn es innerhalb von drei Minuten keine Aufrufe gibt, die ihre Transaktions-ID verwenden. Wenn es zu einer Zeitüberschreitung kommt, bevor die Transaktion festgeschrieben wird, wird die Transaktion automatisch zurückgesetzt.
> Wenn Sie keine Transaktions-ID angeben, werden Änderungen, die sich durch den Aufruf ergeben, automatisch übergeben.

Im folgenden Beispiel wird eine SQL-Transaktion ausgeführt, die eine Zeile in eine Tabelle einfügt.

```
import boto3

rdsData = boto3.client('rds-data')

cluster_arn = 'arn:aws:rds:us-east-1:123456789012:cluster:mydbcluster'
secret_arn = 'arn:aws:secretsmanager:us-east-1:123456789012:secret:mysecret'

tr = rdsData.begin_transaction(
     resourceArn = cluster_arn,
     secretArn = secret_arn,
     database = 'mydb')

response3 = rdsData.execute_statement(
     resourceArn = cluster_arn,
     secretArn = secret_arn,
     database = 'mydb',
     sql = 'insert into employees(first_name, last_name) values('XIULAN', 'WANG')',
     transactionId = tr['transactionId'])

cr = rdsData.commit_transaction(
     resourceArn = cluster_arn,
     secretArn = secret_arn,
     transactionId = tr['transactionId'])

cr['transactionStatus']
```

```
'Transaction Committed'

response3['numberOfRecordsUpdated']
1
```

> **Note**
>
> Wenn Sie eine DDL-Anweisung ausführen, sollten Sie die Anweisung auch nach Ablauf des Aufrufs weiter ausführen. Wenn eine DDL-Anweisung vor Ende der Ausführung beendet wird, kann dies zu Fehlern und möglicherweise beschädigten Datenstrukturen führen. Um eine Anweisung weiter auszuführen, nachdem ein Aufruf das RDS-Daten-API-Timeout-Intervall von 45 Sekunden überschritten hat, setzen Sie den `continueAfterTimeout` Parameter auf`true`.

RDS-Daten-API von einer Java-Anwendung aus aufrufen

Sie können die RDS-Daten-API (Daten-API) von einer Java-Anwendung aus aufrufen.

Die folgenden Beispiele verwenden das AWS SDK for Java. Weitere Informationen finden Sie im AWS SDK for Java -Entwicklerhandbuch.

Ersetzen Sie in jedem Beispiel den Amazon Resource Name (ARN) des DB-Clusters durch den ARN für Ihren Aurora-DB-Cluster. Ersetzen Sie außerdem den geheimen ARN durch den ARN des geheimen Schlüssels in Secrets Manager, der den Zugriff auf den DB-Cluster ermöglicht.

Themen

- Ausführen einer SQL-Abfrage
- Ausführen einer SQL-Transaktion
- Ausführen einer Stapel-SQL-Operation

Ausführen einer SQL-Abfrage

Sie können eine `SELECT`-Anweisung ausführen und die Ergebnisse mit einer Java-Anwendung abrufen.

Im folgenden Beispiel wird eine SQL-Abfrage ausgeführt.

```
package com.amazonaws.rdsdata.examples;

import com.amazonaws.services.rdsdata.AWSRDSData;
import com.amazonaws.services.rdsdata.AWSRDSDataClient;
import com.amazonaws.services.rdsdata.model.ExecuteStatementRequest;
import com.amazonaws.services.rdsdata.model.ExecuteStatementResult;
import com.amazonaws.services.rdsdata.model.Field;

import java.util.List;

public class FetchResultsExample {
  public static final String RESOURCE_ARN = "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster";
  public static final String SECRET_ARN = "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret";

  public static void main(String[] args) {
    AWSRDSData rdsData = AWSRDSDataClient.builder().build();

    ExecuteStatementRequest request = new ExecuteStatementRequest()
            .withResourceArn(RESOURCE_ARN)
            .withSecretArn(SECRET_ARN)
            .withDatabase("mydb")
            .withSql("select * from mytable");

    ExecuteStatementResult result = rdsData.executeStatement(request);

    for (List<Field> fields: result.getRecords()) {
      String stringValue = fields.get(0).getStringValue();
      long numberValue = fields.get(1).getLongValue();

      System.out.println(String.format("Fetched row: string = %s, number = %d",
 stringValue, numberValue));
    }
  }
}
```

Ausführen einer SQL-Transaktion

Sie können eine SQL-Transaktion starten, eine oder mehrere SQL-Anweisungen ausführen und anschließend die Änderungen mit einer Java-Anwendung übergeben.

> **Important**
>
> Bei einer Transaktion kommt es zu einer Zeitüberschreitung, wenn es innerhalb von drei Minuten keine Aufrufe gibt, die ihre Transaktions-ID verwenden. Wenn es zu einer Zeitüberschreitung kommt, bevor die Transaktion festgeschrieben wird, wird die Transaktion automatisch zurückgesetzt.
>
> Wenn Sie keine Transaktions-ID angeben, werden Änderungen, die sich durch den Aufruf ergeben, automatisch übergeben.

Im folgenden Beispiel wird eine SQL-Transaktion ausgeführt.

```
package com.amazonaws.rdsdata.examples;

import com.amazonaws.services.rdsdata.AWSRDSData;
import com.amazonaws.services.rdsdata.AWSRDSDataClient;
import com.amazonaws.services.rdsdata.model.BeginTransactionRequest;
import com.amazonaws.services.rdsdata.model.BeginTransactionResult;
import com.amazonaws.services.rdsdata.model.CommitTransactionRequest;
import com.amazonaws.services.rdsdata.model.ExecuteStatementRequest;

public class TransactionExample {
  public static final String RESOURCE_ARN = "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster";
  public static final String SECRET_ARN = "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret";

  public static void main(String[] args) {
    AWSRDSData rdsData = AWSRDSDataClient.builder().build();

    BeginTransactionRequest beginTransactionRequest = new BeginTransactionRequest()
            .withResourceArn(RESOURCE_ARN)
            .withSecretArn(SECRET_ARN)
            .withDatabase("mydb");
    BeginTransactionResult beginTransactionResult =
 rdsData.beginTransaction(beginTransactionRequest);
    String transactionId = beginTransactionResult.getTransactionId();

    ExecuteStatementRequest executeStatementRequest = new ExecuteStatementRequest()
            .withTransactionId(transactionId)
            .withResourceArn(RESOURCE_ARN)
            .withSecretArn(SECRET_ARN)
```

```
            .withSql("INSERT INTO test_table VALUES ('hello world!')");
    rdsData.executeStatement(executeStatementRequest);

    CommitTransactionRequest commitTransactionRequest = new CommitTransactionRequest()
            .withTransactionId(transactionId)
            .withResourceArn(RESOURCE_ARN)
            .withSecretArn(SECRET_ARN);
    rdsData.commitTransaction(commitTransactionRequest);
  }
}
```

> **Note**
>
> Wenn Sie eine DDL-Anweisung ausführen, sollten Sie die Anweisung auch nach Ablauf des Aufrufs weiter ausführen. Wenn eine DDL-Anweisung vor Ende der Ausführung beendet wird, kann dies zu Fehlern und möglicherweise beschädigten Datenstrukturen führen. Um eine Anweisung weiter auszuführen, nachdem ein Aufruf das RDS-Daten-API-Timeout-Intervall von 45 Sekunden überschritten hat, setzen Sie den `continueAfterTimeout` Parameter auf`true`.

Ausführen einer Stapel-SQL-Operation

Sie können mit einer Java-Anwendung Operationen für Masseneinfügungen und -aktualisierungen für ein Daten-Array ausführen. Sie können eine DML-Anweisung mit einem Array von Parametersätzen ausführen.

> **Important**
>
> Wenn Sie keine Transaktions-ID angeben, werden Änderungen, die sich durch den Aufruf ergeben, automatisch übergeben.

Im folgenden Beispiel wird eine Batch-Einfügungs-Operation ausgeführt.

```
package com.amazonaws.rdsdata.examples;

import com.amazonaws.services.rdsdata.AWSRDSData;
import com.amazonaws.services.rdsdata.AWSRDSDataClient;
import com.amazonaws.services.rdsdata.model.BatchExecuteStatementRequest;
```

```
import com.amazonaws.services.rdsdata.model.Field;
import com.amazonaws.services.rdsdata.model.SqlParameter;

import java.util.Arrays;

public class BatchExecuteExample {
  public static final String RESOURCE_ARN = "arn:aws:rds:us-
east-1:123456789012:cluster:mydbcluster";
  public static final String SECRET_ARN = "arn:aws:secretsmanager:us-
east-1:123456789012:secret:mysecret";

  public static void main(String[] args) {
      AWSRDSData rdsData = AWSRDSDataClient.builder().build();

    BatchExecuteStatementRequest request = new BatchExecuteStatementRequest()
            .withDatabase("test")
            .withResourceArn(RESOURCE_ARN)
            .withSecretArn(SECRET_ARN)
            .withSql("INSERT INTO test_table2 VALUES (:string, :number)")
            .withParameterSets(Arrays.asList(
                    Arrays.asList(
                            new SqlParameter().withName("string").withValue(new
 Field().withStringValue("Hello")),
                            new SqlParameter().withName("number").withValue(new
 Field().withLongValue(1L))
                    ),
                    Arrays.asList(
                            new SqlParameter().withName("string").withValue(new
 Field().withStringValue("World")),
                            new SqlParameter().withName("number").withValue(new
 Field().withLongValue(2L))
                    )
            ));

    rdsData.batchExecuteStatement(request);
  }
}
```

Steuern des Timeout-Verhaltens der Daten-API

Alle Aufrufe der Daten-API erfolgen synchron. Angenommen, Sie führen eine Daten-API-Operation durch, die eine SQL-Anweisung wie `INSERT` oder `CREATE TABLE` ausführt. Wenn der Daten-API-Aufruf erfolgreich zurückkehrt, ist die SQL-Verarbeitung abgeschlossen, wenn der Aufruf zurückkehrt.

Standardmäßig bricht die Daten-API einen Vorgang ab und gibt einen Timeout-Fehler zurück, wenn die Verarbeitung nicht innerhalb von 45 Sekunden abgeschlossen wird. In diesem Fall werden die Daten nicht eingefügt, die Tabelle nicht erstellt usw.

Sie können die Daten-API verwenden, um lang andauernde Operationen auszuführen, die nicht innerhalb von 45 Sekunden abgeschlossen werden können. Wenn Sie davon ausgehen, dass ein Vorgang, z. B. ein Bulk `INSERT` - oder DDL-Vorgang, an einer großen Tabelle länger als 45 Sekunden dauert, können Sie den `continueAfterTimeout` Parameter für den `ExecuteStatement` Vorgang angeben. Ihre Anwendung erhält immer noch den Timeout-Fehler. Der Vorgang wird jedoch weiterhin ausgeführt und nicht abgebrochen. Ein Beispiel finden Sie unter Ausführen einer SQL-Transaktion.

Wenn das AWS SDK für Ihre Programmiersprache einen eigenen Timeout-Zeitraum für API-Aufrufe oder HTTP-Socket-Verbindungen hat, stellen Sie sicher, dass alle diese Timeout-Perioden mehr als 45 Sekunden betragen. Bei einigen SDKs beträgt der Timeout-Zeitraum standardmäßig weniger als 45 Sekunden. Wir empfehlen, alle SDK-spezifischen oder clientspezifischen Timeout-Zeiträume auf mindestens eine Minute festzulegen. Dadurch wird die Möglichkeit vermieden, dass Ihre Anwendung einen Timeout-Fehler erhält, während der Daten-API-Vorgang weiterhin erfolgreich abgeschlossen wird. Auf diese Weise können Sie sicher sein, ob Sie den Vorgang wiederholen möchten oder nicht.

Nehmen wir beispielsweise an, dass das SDK einen Timeout-Fehler an Ihre Anwendung zurückgibt, der Daten-API-Vorgang aber trotzdem innerhalb des Daten-API-Timeout-Intervalls abgeschlossen wird. In diesem Fall könnte ein erneuter Versuch des Vorgangs doppelte Daten einfügen oder auf andere Weise zu falschen Ergebnissen führen. Das SDK wiederholt den Vorgang möglicherweise automatisch, wodurch falsche Daten entstehen, ohne dass Ihre Anwendung etwas dagegen unternommen hat.

Das Timeout-Intervall ist besonders wichtig für das Java 2 SDK. In diesem SDK betragen das API-Aufruf-Timeout und das HTTP-Socket-Timeout standardmäßig beide 30 Sekunden. Hier ist ein Beispiel für das Setzen dieser Timeouts auf einen höheren Wert:

```
public RdsDataClient createRdsDataClient() {
    return RdsDataClient.builder()
        .region(Region.US_EAST_1) // Change this to your desired Region
        .overrideConfiguration(createOverrideConfiguration())
        .httpClientBuilder(createHttpClientBuilder())
        .credentialsProvider(defaultCredentialsProvider()) // Change this to your
 desired credentials provider
        .build();
```

```
}

private static ClientOverrideConfiguration createOverrideConfiguration() {
    return ClientOverrideConfiguration.builder()
        .apiCallTimeout(Duration.ofSeconds(60))
        .build();
}

private HttpClientBuilder createHttpClientBuilder() {
    return ApacheHttpClient.builder() // Change this to your desired HttpClient
        .socketTimeout(Duration.ofSeconds(60));
}
```

Hier ist ein äquivalentes Beispiel für die Verwendung des asynchronen Datenclients:

```
public static RdsDataAsyncClient createRdsDataAsyncClient() {
    return RdsDataAsyncClient.builder()
        .region(Region.US_EAST_1) // Change this to your desired Region
        .overrideConfiguration(createOverrideConfiguration())
        .credentialsProvider(defaultCredentialsProvider())  // Change this to your
 desired credentials provider
        .build();
}

private static ClientOverrideConfiguration createOverrideConfiguration() {
    return ClientOverrideConfiguration.builder()
        .apiCallAttemptTimeout(Duration.ofSeconds(60))
        .build();
}

private HttpClientBuilder createHttpClientBuilder() {
    return NettyNioAsyncHttpClient.builder() // Change this to your desired
 AsyncHttpClient
        .readTimeout(Duration.ofSeconds(60));
}
```

Verwendung der Java-Clientbibliothek für die RDS-Daten-API

Sie können eine Java-Clientbibliothek für die RDS Data API (Data API) herunterladen und verwenden. Diese Java-Clientbibliothek bietet eine alternative Möglichkeit zur Verwendung der Daten-API. Mithilfe dieser Bibliothek können Sie Ihre clientseitigen Klassen Daten-API-Anfragen und

-Antworten zuordnen. Dieser Mapping-Support kann die Integration mit einigen bestimmten Java-Typen wie etwa `Date`, `Time` und `BigDecimal` erleichtern.

Herunterladen der Java Client-Bibliothek für die Daten-API

Die Data API-Java-Clientbibliothek ist GitHub am folgenden Speicherort als Open Source verfügbar:

https://github.com/awslabs/rds-data-api-client-library-java

Sie können die Bibliothek manuell aus den Quelldateien aufbauen, die bewährte Methode ist jedoch, die Bibliothek unter Verwendung der Apache Maven-Dependenzverwaltung zu nutzen. Fügen Sie die folgende Abhängigkeit zu Ihrer Maven-POM-Datei hinzu.

Verwenden Sie für Version 2.x, die mit AWS SDK 2.x kompatibel ist, Folgendes:

```
<dependency>
   <groupId>software.amazon.rdsdata</groupId>
   <artifactId>rds-data-api-client-library-java</artifactId>
   <version>2.0.0</version>
</dependency>
```

Verwenden Sie für Version 1.x, die mit AWS SDK 1.x kompatibel ist, Folgendes:

```
<dependency>
    <groupId>software.amazon.rdsdata</groupId>
    <artifactId>rds-data-api-client-library-java</artifactId>
    <version>1.0.8</version>
</dependency>
```

Java Client-Bibliothek-Beispiele

Nachfolgend finden Sie einige typische Beispiele für die Verwendung der Daten-API-Java-Client-Bibliothek. Diese Beispiele gehen davon aus, dass Sie eine Tabelle `accounts` mit zwei Spalten haben: `accountId` und `name`. Weiterhin haben Sie das folgende Datentransferobjekt (DTO):

```
public class Account {
    int accountId;
    String name;
    // getters and setters omitted
}
```

Die Client-Bibliothek ermöglicht die Übergabe von DTOs als Eingabeparameter. Das folgende Beispiel zeigt, wie Kunden-DTOs Eingabeparametersätzen zugeordnet werden.

```
var account1 = new Account(1, "John");
var account2 = new Account(2, "Mary");
client.forSql("INSERT INTO accounts(accountId, name) VALUES(:accountId, :name)")
         .withParamSets(account1, account2)
         .execute();
```

In manchen Fällen ist es einfacher, mit einfachen Werten als Eingabeparametern zu arbeiten. Verwenden Sie dazu die folgende Syntax.

```
client.forSql("INSERT INTO accounts(accountId, name) VALUES(:accountId, :name)")
         .withParameter("accountId", 3)
         .withParameter("name", "Zhang")
         .execute();
```

Es folgt ein weiteres Beispiel, das mit einfachen Werten als Eingabeparametern arbeitet.

```

client.forSql("INSERT INTO accounts(accountId, name) VALUES(?, ?)", 4, "Carlos")
         .execute();

```

Die Client-Bibliothek bietet das automatische Mapping zu DTOs, wenn ein Ergebnis zurückgegeben wird. Die folgenden Beispiele zeigen, wie das Ergebnis Ihren DTOs zugeordnet wird.

```
List<Account> result = client.forSql("SELECT * FROM accounts")
          .execute()
          .mapToList(Account.class);

Account result = client.forSql("SELECT * FROM accounts WHERE account_id = 1")
          .execute()
          .mapToSingle(Account.class);
```

In vielen Fällen enthält die Datenbank-Ergebnismenge einen einzigen Wert. Um das Abrufen solcher Ergebnisse zu vereinfachen, bietet die Kundenbibliothek die folgende API an:

```
int numberOfAccounts = client.forSql("SELECT COUNT(*) FROM accounts")
          .execute()
```

```
            .singleValue(Integer.class);
```

> **Note**
>
> Die `mapToList`-Funktion konvertiert einen SQL-Ergebnissatz in eine benutzerdefinierte Objektliste. Wir unterstützen die Verwendung der `.withFormatRecordsAs(RecordsFormatType.JSON)`-Anweisung in einem `ExecuteStatement`-Anruf für die Java-Clientbibliothek nicht, weil sie dem gleichen Zweck dient. Weitere Informationen finden Sie unter Verarbeitung der Ergebnisse der RDS-Daten-API-Abfrage im JSON-Format.

Verarbeitung der Ergebnisse der RDS-Daten-API-Abfrage im JSON-Format

Wenn Sie die `ExecuteStatement`-Operation aufrufen, können Sie auswählen, ob die Abfrageergebnisse als Zeichenfolge im JSON-Format zurückgegeben werden sollen. Auf diese Weise können Sie die JSON-Parsing-Funktionen Ihrer Programmiersprache verwenden, um die Ergebnismenge zu interpretieren und neu zu formatieren. Dies kann dazu beitragen, zu vermeiden, zusätzlichen Code zu schreiben, um die Ergebnismenge zu durchlaufen und jeden Spaltenwert zu interpretieren.

Zum Anfordern der Ergebnismenge im JSON-Format übergeben Sie den optionalen `formatRecordsAs`-Parameter mit dem Wert `JSON`. Die JSON-formatierte Ergebnismenge wird im Feld `formattedRecords` der `ExecuteStatementResponse`-Struktur zurückgegeben.

Die `BatchExecuteStatement`-Aktion gibt keine Ergebnismenge zurück. Daher gilt die JSON-Option nicht für diese Aktion.

Wenn Sie die Schlüssel in der JSON-Hash-Struktur anpassen möchten, definieren Sie Spaltenaliasnamen in der Ergebnismenge. Verwenden Sie dazu die `AS`-Klausel in der Spaltenliste Ihrer SQL-Abfrage.

Sie können die JSON-Funktion verwenden, um die Ergebnismenge besser lesbar zu machen und den Inhalt sprachspezifischen Frameworks zuzuordnen. Da das Volume der ASCII-kodierten Ergebnismenge größer als die Standarddarstellung ist, können Sie die Standarddarstellung für Abfragen auswählen, die eine große Anzahl von Zeilen oder große Spaltenwerte zurückgeben, die mehr Speicher belegen, als für Ihre Anwendung verfügbar ist.

Themen

Abrufen von Abfrageergebnissen im JSON-Format

Um die Ergebnismenge als JSON-Zeichenfolge zu erhalten, fügen Sie sie `.withFormatRecordsAs(RecordsFormatType.JSON)` in den `ExecuteStatement` Aufruf ein. Der Rückgabewert wird im Feld `formattedRecords` als JSON-Zeichenfolge angezeigt. In diesem Fall hat `columnMetadata` den Wert `null`. Die Spaltenbeschriftungen sind die Schlüssel des Objekts, das jede Zeile darstellt. Diese Spaltennamen werden für jede Zeile in der Ergebnismenge wiederholt. Die Spaltenwerte sind in Anführungszeichen gesetzte Zeichenfolgen, numerische Werte oder Sonderwerte, die `true`, `false` oder `null` darstellen. Spaltenmetadaten wie Längenbeschränkungen und der genaue Typ für Zahlen und Zeichenfolgen werden in der JSON-Antwort nicht beibehalten.

Wenn Sie den `.withFormatRecordsAs()`-Aufruf weglassen oder einen Parameter `NONE` angeben, wird die Ergebnismenge im Binärformat unter Verwendung der Felder `Records` und `columnMetadata` zurückgegeben.

Datentypenzuordnung

Die SQL-Werte in der Ergebnismenge werden einem kleineren Satz von JSON-Typen zugeordnet. Die Werte werden in JSON als Zeichenfolgen, Zahlen und einige spezielle Konstanten wie `true`, `false` und `null` dargestellt. Sie können diese Werte in Variablen in Ihrer Anwendung umwandeln, indem Sie eine starke oder schwache Eingabe verwenden, die für Ihre Programmiersprache geeignet ist.

JDBC-Datentyp	JSON-Datentyp
`INTEGER`, `TINYINT`, `SMALLINT`, `BIGINT`	Die Standardeinstellung ist Zahl. Zeichenfolge, wenn die Option `LongReturnType` auf `STRING` eingestellt ist.

JDBC-Datentyp	JSON-Datentyp
FLOAT, REAL, DOUBLE	Zahl
DECIMAL	Die Standardeinstellung ist Zeichenfolge. Zahl, wenn die Option DecimalReturnType auf DOUBLE_OR_LONG eingestellt ist.
STRING	String
BOOLEAN, BIT	Boolesch
BLOB, BINARY, VARBINARY , LONGVARBINARY	Zeichenfolge in Base64-Kodierung.
CLOB	String
ARRAY	Array
NULL	null
Andere Typen (einschließlich datums- und zeitbezogener Typen)	String

Fehlerbehebung

Die JSON-Antwort ist auf 10 Megabyte begrenzt. Wenn die Antwort größer als dieses Limit ist, erhält Ihr Programm einen BadRequestException-Fehler. In diesem Fall können Sie den Fehler mit einer der folgenden Methoden beheben:

- Reduzieren Sie die Anzahl der Zeilen in der Ergebnismenge. Fügen Sie dazu eine LIMIT-Klausel hinzu. Sie können eine große Ergebnismenge in mehrere kleinere aufteilen, indem Sie mehrere Abfragen mit den Klauseln LIMIT und OFFSET senden.

  Wenn die Ergebnismenge Zeilen enthält, die durch die Anwendungslogik herausgefiltert werden, können Sie diese Zeilen aus der Ergebnismenge entfernen, indem Sie der WHERE-Klausel weitere Bedingungen hinzufügen.
- Reduzieren Sie die Anzahl der Spalten in der Ergebnismenge. Entfernen Sie dazu Elemente aus der Auswahlliste der Abfrage.

- Verkürzen Sie die Spaltenbeschriftungen, indem Sie Spaltenaliasnamen in der Abfrage verwenden. Jeder Spaltenname wird in der JSON-Zeichenfolge für jede Zeile der Ergebnismenge wiederholt. Daher könnte ein Abfrageergebnis mit langen Spaltennamen und vielen Zeilen die Größenbeschränkung überschreiten. Verwenden Sie insbesondere Spaltenaliasnamen für komplizierte Ausdrücke, um zu vermeiden, dass der gesamte Ausdruck in der JSON-Zeichenfolge wiederholt wird.
- Während Sie mit SQL Spaltenaliasnamen verwenden können, um eine Ergebnismenge mit mehr als einer Spalte mit demselben Namen zu erzeugen, sind doppelte Schlüsselnamen in JSON nicht zulässig. Die RDS-Daten-API gibt einen Fehler zurück, wenn Sie die Ergebnismenge im JSON-Format anfordern und mehr als eine Spalte denselben Namen hat. Stellen Sie daher sicher, dass alle Spaltenbeschriftungen eindeutige Namen haben.

Beispiele

Die folgenden Java-Beispiele zeigen, wie Sie `ExecuteStatement` mit der Antwort als JSON-formatierte Zeichenfolge aufrufen und dann die Ergebnismenge interpretieren. Ersetzen Sie die Parameter *`DatabaseName`*, *`secret StoreArn`* und *`clusterArn`* durch die entsprechenden Werte.

Das folgende Java-Beispiel veranschaulicht eine Abfrage, die einen numerischen Dezimalwert in der Ergebnismenge zurückgibt. `assertThat`-Aufrufe testen anhand der Regeln für JSON-Ergebnismengen, ob die Felder der Antwort die erwarteten Eigenschaften haben.

Dieses Beispiel funktioniert mit dem folgenden Schema und den folgenden Beispieldaten:

```
create table test_simplified_json (a float);
insert into test_simplified_json values(10.0);
```

```
public void JSON_result_set_demo() {
    var sql = "select * from test_simplified_json";
    var request = new ExecuteStatementRequest()
      .withDatabase(databaseName)
      .withSecretArn(secretStoreArn)
      .withResourceArn(clusterArn)
      .withSql(sql)
      .withFormatRecordsAs(RecordsFormatType.JSON);
    var result = rdsdataClient.executeStatement(request);
}
```

Der Wert des Felds `formattedRecords` aus dem vorhergehenden Programm lautet:

```
[{"a":10.0}]
```

Die Felder `Records` und `ColumnMetadata` in der Antwort sind aufgrund des Vorhandenseins der JSON-Ergebnismenge beide null.

Das folgende Java-Beispiel veranschaulicht eine Abfrage, die einen numerischen Ganzzahlwert in der Ergebnismenge zurückgibt. Das Beispiel ruft `getFormattedRecords` auf, um nur die JSON-formatierte Zeichenfolge zurückzugeben und die anderen Antwortfelder zu ignorieren, die leer oder null sind. Im Beispiel wird das Ergebnis in eine Struktur deserialisiert, die eine Liste von Datensätzen darstellt. Jeder Datensatz enthält Felder, deren Namen den Spaltenaliasnamen aus der Ergebnismenge entsprechen. Diese Methode vereinfacht den Code, der die Ergebnismenge analysiert. Ihre Anwendung muss nicht die Zeilen und Spalten der Ergebnismenge durchlaufen und jeden Wert in den entsprechenden Typ konvertieren.

Dieses Beispiel funktioniert mit dem folgenden Schema und den folgenden Beispieldaten:

```
create table test_simplified_json (a int);
insert into test_simplified_json values(17);
```

```
public void JSON_deserialization_demo() {
    var sql = "select * from test_simplified_json";
    var request = new ExecuteStatementRequest()
      .withDatabase(databaseName)
      .withSecretArn(secretStoreArn)
      .withResourceArn(clusterArn)
      .withSql(sql)
      .withFormatRecordsAs(RecordsFormatType.JSON);
    var result = rdsdataClient.executeStatement(request)
      .getFormattedRecords();

/* Turn the result set into a Java object, a list of records.
   Each record has a field 'a' corresponding to the column
   labelled 'a' in the result set. */
    private static class Record { public int a; }
    var recordsList = new ObjectMapper().readValue(
        response, new TypeReference<List<Record>>() {
        });
}
```

Der Wert des Felds `formattedRecords` aus dem vorhergehenden Programm lautet:

```
[{"a":17}]
```

Zum Abrufen der Spalte a der Ergebniszeile 0 würde sich die Anwendung auf `recordsList.get(0).a` beziehen.

Im Gegensatz dazu zeigt das folgende Java-Beispiel die Art von Code, der zum Erstellen einer Datenstruktur erforderlich ist, die die Ergebnismenge enthält, wenn Sie das JSON-Format nicht verwenden. In diesem Fall enthält jede Zeile der Ergebnismenge Felder mit Informationen über einen einzelnen Benutzer. Das Erstellen einer Datenstruktur zur Darstellung der Ergebnismenge erfordert das Durchlaufen der Zeilen. Für jede Zeile ruft der Code den Wert jedes Felds ab, führt eine entsprechende Typkonvertierung durch und weist das Ergebnis dem entsprechenden Feld im Objekt zu, das die Zeile darstellt. Dann fügt der Code das Objekt, das jeden Benutzer repräsentiert, der Datenstruktur hinzu, die die gesamte Ergebnismenge darstellt. Wenn die Abfrage geändert wurde, um Felder in der Ergebnismenge neu anzuordnen, hinzuzufügen oder zu entfernen, müsste sich der Anwendungscode ebenfalls ändern.

```
/* Verbose result-parsing code that doesn't use the JSON result set format */
for (var row: response.getRecords()) {
    var user = User.builder()
      .userId(row.get(0).getLongValue())
      .firstName(row.get(1).getStringValue())
      .lastName(row.get(2).getStringValue())
      .dob(Instant.parse(row.get(3).getStringValue()))
      .build();
    result.add(user);
  }
```

Die folgenden Beispielwerte zeigen die Werte des Felds `formattedRecords` für Ergebnismengen mit unterschiedlicher Anzahl von Spalten, Spaltenaliasnamen und Spaltendatentypen.

Wenn die Ergebnismenge mehrere Zeilen enthält, wird jede Zeile als Objekt dargestellt, das ein Array-Element ist. Jede Spalte in der Ergebnismenge wird zu einem Schlüssel im Objekt. Die Schlüssel werden für jede Zeile in der Ergebnismenge wiederholt. Daher müssen Sie für Ergebnismengen, die aus vielen Zeilen und Spalten bestehen, möglicherweise kurze Spaltenaliasnamen definieren, um zu vermeiden, dass das Längenlimit für die gesamte Antwort überschritten wird.

Dieses Beispiel funktioniert mit dem folgenden Schema und den folgenden Beispieldaten:

```
create table sample_names (id int, name varchar(128));
```

```
insert into sample_names values (0, "Jane"), (1, "Mohan"), (2, "Maria"), (3, "Bruce"),
 (4, "Jasmine");
```

```
[{"id":0,"name":"Jane"},{"id":1,"name":"Mohan"},
{"id":2,"name":"Maria"},{"id":3,"name":"Bruce"},{"id":4,"name":"Jasmine"}]
```

Wenn eine Spalte in der Ergebnismenge als Ausdruck definiert ist, wird der Text des Ausdrucks zum JSON-Schlüssel. Daher ist es normalerweise praktisch, einen beschreibenden Spaltenalias für jeden Ausdruck in der Auswahlliste der Abfrage zu definieren. Die folgende Abfrage enthält beispielsweise Ausdrücke wie Funktionsaufrufe und arithmetische Operationen in ihrer Auswahlliste.

```
select count(*), max(id), 4+7 from sample_names;
```

Diese Ausdrücke werden als Schlüssel an die JSON-Ergebnismenge übergeben.

```
[{"count(*)":5,"max(id)":4,"4+7":11}]
```

Wenn Sie AS-Spalten mit beschreibenden Beschriftungen hinzufügen, können die Schlüssel in der JSON-Ergebnismenge einfacher interpretiert werden.

```
select count(*) as rows, max(id) as largest_id, 4+7 as addition_result from
 sample_names;
```

Bei der überarbeiteten SQL-Abfrage werden die Spaltenbeschriftungen, die durch die AS-Klauseln definiert werden, als Schlüsselnamen verwendet.

```
[{"rows":5,"largest_id":4,"addition_result":11}]
```

Der Wert für jedes Schlüssel-Wert-Paar in der JSON-Zeichenfolge kann eine Zeichenfolge in Anführungszeichen sein. Die Zeichenfolge enthält möglicherweise Unicode-Zeichen. Wenn die Zeichenfolge Escape-Sequenzen oder die Zeichen " oder \ enthält, wird diesen Zeichen ein Escape-Zeichen mit umgekehrtem Schrägstrich vorangestellt. Die folgenden Beispiele für JSON-Zeichenfolgen veranschaulichen diese Möglichkeiten. Das Ergebnis `string_with_escape_sequences` enthält z. B. die Sonderzeichen Rücktaste, Zeilenumbruch, Wagenrücklauf, Tabulator, Seitenvorschub und \.

```
[{"quoted_string":"hello"}]
```

```
[{"unicode_string":"####"}]
[{"string_with_escape_sequences":"\b \n \r \t \f \\ '"}]
```

Der Wert für jedes Schlüssel-Wert-Paar in der JSON-Zeichenfolge kann auch eine Zahl darstellen. Die Zahl kann eine Ganzzahl, ein Gleitkommawert, ein negativer Wert oder ein Wert sein, der in Exponentialschreibweise dargestellt wird. Die folgenden Beispiele für JSON-Zeichenfolgen veranschaulichen diese Möglichkeiten.

```
[{"integer_value":17}]
[{"float_value":10.0}]
[{"negative_value":-9223372036854775808,"positive_value":9223372036854775807}]
[{"very_small_floating_point_value":4.9E-324,"very_large_floating_point_value":1.79769313486231
```

Boolesche und Nullwerte werden mit den Sonderschlüsselwörtern `true`, `false` und `null` ohne Anführungszeichen dargestellt. Die folgenden Beispiele für JSON-Zeichenfolgen veranschaulichen diese Möglichkeiten.

```
[{"boolean_value_1":true,"boolean_value_2":false}]
[{"unknown_value":null}]
```

Wenn Sie einen Wert eines BLOB-Typs auswählen, wird das Ergebnis in der JSON-Zeichenfolge als Base64-kodierter Wert dargestellt. Wenn Sie den Wert wieder in seine ursprüngliche Darstellung umwandeln möchten, können Sie die entsprechende Dekodierungsfunktion in der Sprache Ihrer Anwendung verwenden. In Java rufen Sie beispielsweise die Funktion `Base64.getDecoder().decode()` auf. Die folgende Beispielausgabe zeigt das Ergebnis der Auswahl des BLOB-Werts `hello world` und gibt die Ergebnismenge als JSON-Zeichenfolge zurück.

```
[{"blob_column":"aGVsbG8gd29ybGQ="}]
```

Das folgende Python-Beispiel zeigt, wie Sie auf die Werte aus dem Ergebnis eines Aufrufs der Python-Funktion `execute_statement` zugreifen. Die Ergebnismenge ist ein Zeichenfolgenwert im Feld `response['formattedRecords']`. Der Code verwandelt die JSON-Zeichenfolge durch Aufrufen der Funktion `json.loads` in eine Datenstruktur. Dann ist jede Zeile der Ergebnismenge ein Listenelement innerhalb der Datenstruktur und innerhalb jeder Zeile können Sie auf jedes Feld der Ergebnismenge nach Namen verweisen.

```
import json
```

```
result = json.loads(response['formattedRecords'])
print (result[0]["id"])
```

Das folgende JavaScript Beispiel zeigt, wie auf die Werte aus dem Ergebnis eines Funktionsaufrufs zugegriffen wird. JavaScript `executeStatement` Die Ergebnismenge ist ein Zeichenfolgenwert im Feld `response.formattedRecords`. Der Code verwandelt die JSON-Zeichenfolge durch Aufrufen der Funktion `JSON.parse` in eine Datenstruktur. Dann ist jede Zeile der Ergebnismenge ein Array-Element innerhalb der Datenstruktur und innerhalb jeder Zeile können Sie auf jedes Feld der Ergebnismenge nach Namen verweisen.

```
<script>
    const result = JSON.parse(response.formattedRecords);
    document.getElementById("display").innerHTML = result[0].id;
</script>
```

Behebung von Problemen mit der RDS-Daten-API

Verwenden Sie die folgenden Abschnitte mit den häufigsten Fehlermeldungen, um Probleme mit der RDS Data API (Daten-API) zu beheben.

Themen

Transaction <transaction_ID> Is Not Found (Transaktion nicht gefunden)

In diesem Fall wurde die in einem Data-API-Aufruf angegebene Transaktions-ID nicht gefunden. Die Ursache für dieses Problem wird an die Fehlermeldung angehängt und ist eine der folgenden:

- Die Transaktion ist möglicherweise abgelaufen.

  Stellen Sie sicher, dass jeder Transaktionsaufruf innerhalb von drei Minuten nach dem letzten ausgeführt wird.

Es ist auch möglich, dass die angegebene Transaktions-ID nicht durch einen BeginTransactionAufruf erstellt wurde. Stellen Sie sicher, dass Ihr Aufruf eine gültige Transaktions-ID hat.

- Ein vorheriger Aufruf führte zu einer Beendigung Ihrer Transaktion.

  Die Transaktion wurde bereits von Ihrem `CommitTransaction`- oder `RollbackTransaction`-Aufruf beendet.
- Die Transaktion wurde aufgrund eines Fehlers eines früheren Aufrufs abgebrochen.

  Prüfen Sie, ob Ihre vorherigen Aufrufe Ausnahmen ausgelöst haben.

Informationen zum Ausführen von Transaktionen finden Sie unter Aufrufen der RDS-Daten-API.

Packet for Query Is Too Large (Paket für Abfrage zu groß)

In diesem Fall war die zurückgegebene Ergebnismenge für eine Zeile zu groß. Die Größenbegrenzung der Data-API beträgt 64 KB pro Zeile in der von der Datenbank zurückgegebenen Ergebnismenge.

Um dieses Problem zu beheben, stellen Sie sicher, dass jede Zeile in einem Ergebnissatz höchstens 64 KB groß ist.

Database Response Exceeded Size Limit Datenbankantwort überschreitet Größenlimit)

In diesem Fall war die Größe der von der Datenbank zurückgegebenen Ergebnismenge zu groß. Das Data-API-Limit beträgt 1 MiB für die von der Datenbank zurückgegebene Ergebnismenge.

Um dieses Problem zu lösen, stellen Sie sicher, dass Aufrufe der Daten-API 1 MiB Daten oder weniger zurückgeben. Wenn Sie mehr als 1 MiB zurückgeben müssen, können Sie mit der `LIMIT`-Klausel in Ihrer Abfrage mehrere `ExecuteStatement`-Aufrufe verwenden.

Weitere Informationen über die `LIMIT`-Klausel finden Sie unter SELECT-Syntax in der MySQL-Dokumentation.

HttpEndpointist nicht für Cluster aktiviert <cluster_ID>

Überprüfen Sie die folgenden möglichen Ursachen für dieses Problem:

- Der Aurora-DB-Cluster unterstützt keine Daten-API. Für Aurora MySQL können Sie beispielsweise die Daten-API nur mit verwendenAurora Serverless v1. Informationen zu den Typen von DB-Clustern, die die RDS Data API unterstützt, finden Sie unterthe section called “Verfügbarkeit von Regionen und Versionen”.
- Die Daten-API ist für den Aurora-DB-Cluster nicht aktiviert. Um die Daten-API mit einem Aurora-DB-Cluster zu verwenden, muss die Daten-API für den DB-Cluster aktiviert sein. Informationen zur Aktivierung der Daten-API finden Sie unterRDS-Daten-API aktivieren.
- Der DB-Cluster wurde umbenannt, nachdem die Daten-API für ihn aktiviert wurde. Schalten Sie in diesem Fall die Daten-API für diesen Cluster aus und aktivieren Sie ihn dann erneut.
- Der von Ihnen angegebene ARN stimmt nicht genau mit dem ARN des Clusters überein. Stellen Sie sicher, dass der von einer anderen Quelle zurückgegebene oder durch Programmlogik erstellte ARN genau mit dem ARN des Clusters übereinstimmt. Stellen Sie beispielsweise sicher, dass der von Ihnen verwendete ARN die richtigen Groß-/Kleinschreibung für alle alphabetischen Zeichen aufweist.

Protokollieren von RDS-Daten-API-Aufrufen mit AWS CloudTrail

Die RDS-Daten-API (Daten-API) ist in integriert, einem Service AWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines - AWS Services in der Daten-API aufzeichnet. CloudTrail erfasst alle API-Aufrufe für die Daten-API als Ereignisse, einschließlich Aufrufen von der Amazon-RDS-Konsole und von Code-Aufrufen an Daten-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für die Daten-API. Anhand der von CloudTrailgesammelten Daten können Sie viele Informationen ermitteln. Diese Informationen umfassen die Anforderung an Data API, die IP-Adresse, von der die Anforderung gestellt wurde, wer die Anforderung gestellt hat, wann sie gestellt wurde, und zusätzliche Details.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

Arbeiten mit Data API-Informationen in CloudTrail

CloudTrail wird beim Erstellen des AWS Kontos in Ihrem Konto aktiviert. Wenn die unterstützte Aktivität (Verwaltungsereignisse) in der Daten-API auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen - AWS Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können aktuelle Verwaltungsereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail Ereignisverlauf im AWS CloudTrail -Benutzerhandbuch.

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich Ereignissen für die Daten-API, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen AWS Regionen in der - AWS Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3-Bucket bereit. Darüber hinaus können Sie andere - AWS Services konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail -Benutzerhandbuch:

- Übersicht zum Erstellen eines Trails
- CloudTrail Von unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle Daten-API-Operationen werden von protokolliert CloudTrail und in der Amazon-RDS-Datenservice-API-Referenz dokumentiert. Aufrufe der `ExecuteStatement` Operationen `BatchExecuteStatement`, `CommitTransaction`, und erzeugen beispielsweise Einträge in den `BeginTransaction` CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Root- oder -Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung von einem anderen - AWS Service gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Ein- und Ausschließen von Daten-API-Ereignissen aus einem - AWS CloudTrail Trail

Die meisten Daten-API-Benutzer verlassen sich auf die Ereignisse in einem - AWS CloudTrail Trail, um eine Aufzeichnung der Daten-API-Operationen bereitzustellen. Ereignisdaten geben

den Datenbanknamen, den Schemanamen oder die SQL-Anweisungen in Anforderungen an die Daten-API nicht preis. Wenn Sie jedoch wissen, welcher Benutzer zu einem bestimmten Zeitpunkt eine Art von Aufruf gegen einen bestimmten DB-Cluster getätigt hat, kann dies dazu beitragen, ungewöhnliche Zugriffsmuster zu erkennen.

Einschließen von Daten-API-Ereignissen in einen - AWS CloudTrail Trail

Für Aurora PostgreSQL Serverless v2 und bereitgestellte Datenbanken werden die folgenden Daten-API-Operationen in AWS CloudTrail als Datenereignisse protokolliert. Datenereignisse sind API-Operationen auf Datenebene mit hohem Volumen, die CloudTrail standardmäßig nicht protokolliert werden. Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zu CloudTrail Preisen finden Sie unter -AWS CloudTrail Preise.

- BatchExecuteStatement
- BeginTransaction
- CommitTransaction
- ExecuteStatement
- RollbackTransaction

Sie können die - CloudTrail Konsole oder CloudTrail -API-Operationen verwendenAWS CLI, um diese Daten-API-Operationen zu protokollieren. Wählen Sie in der CloudTrail Konsole RDS Data API – DB Cluster als Datenereignistyp aus. Weitere Informationen finden Sie unter Protokollieren von Datenereignissen mit AWS Management Console im AWS CloudTrail -Benutzerhandbuch.

Führen Sie mithilfe der den `aws cloudtrail put-event-selectors` Befehl aus AWS CLI, um diese Daten-API-Operationen für Ihren Trail zu protokollieren. Um alle Daten-API-Ereignisse in -DB-Clustern zu protokollieren, geben Sie `AWS::RDS::DBCluster` für den Ressourcentyp an. Im folgenden Beispiel werden alle Daten-API-Ereignisse auf -DB-Clustern protokolliert. Weitere Informationen finden Sie unter Protokollieren von Datenereignissen mit AWS Command Line Interface im AWS CloudTrail -Benutzerhandbuch.

```
aws cloudtrail put-event-selectors --trail-name trail_name --advanced-event-selectors \
'{
   "Name": "RDS Data API Selector",
   "FieldSelectors": [
      {
         "Field": "eventCategory",
         "Equals": [
```

```
            "Data"
         ]
      },
      {
         "Field": "resources.type",
         "Equals": [
            "AWS::RDS::DBCluster"
         ]
      }
   ]
}'
```

Sie können erweiterte Ereignisselektoren konfigurieren, um zusätzlich nach den `resources.ARN` Feldern `readOnly`, `eventName,` und zu filtern. Weitere Informationen zu diesen Feldern finden Sie unter AdvancedFieldSelector.

Ausschließen von Daten-API-Ereignissen aus einem - AWS CloudTrail Trail (Aurora Serverless v1nur)

Für sind Aurora Serverless v1Daten-API-Ereignisse Verwaltungsereignisse. Standardmäßig sind alle Daten-API-Ereignisse in einem - AWS CloudTrail Trail enthalten. Da die Daten-API jedoch eine große Anzahl von Ereignissen generieren kann, möchten Sie diese Ereignisse möglicherweise aus Ihrem CloudTrail Trail ausschließen. Die Einstellung Amazon-RDS-Daten-API-Ereignisse ausschließen schließt alle Daten-API-Ereignisse aus dem Trail aus. Sie können bestimmte Daten-API-Ereignisse nicht ausschließen.

Zum Ausschließen von Daten-API-Ereignissen aus einem Trail führen Sie die folgenden Schritte aus:

- Wählen Sie in der CloudTrail Konsole die Einstellung Amazon-RDS-Daten-API-Ereignisse ausschließen, wenn Sie einen Trail erstellen oder einen Trail aktualisieren.
- Verwenden Sie in der CloudTrail API die -PutEventSelectorsOperation. Wenn Sie erweiterte Ereignisselektoren verwenden, können Sie Daten-API-Ereignisse ausschließen, indem Sie das `eventSource` Feld nicht auf setzen`rdsdata.amazonaws.com`. Wenn Sie grundlegende Ereignisselektoren verwenden, können Sie Daten-API-Ereignisse ausschließen, indem Sie den Wert des Attributs `ExcludeManagementEventSources` auf setzen`rdsdata.amazonaws.com`. Weitere Informationen finden Sie unter Protokollieren von Ereignissen mit AWS Command Line Interface im AWS CloudTrail -Benutzerhandbuch.

> **Warning**
>
> Das Ausschließen von Daten-API-Ereignissen aus einem CloudTrail Protokoll kann Daten-API-Aktionen verdecken. Seien Sie vorsichtig, wenn Sie Prinzipalen die `cloudtrail:PutEventSelectors`-Berechtigung erteilen, die zum Ausführen dieses Vorgangs erforderlich ist.

Sie können diesen Ausschluss jederzeit deaktivieren, indem Sie die Konsoleneinstellung oder die Ereignisselektoren für einen Trail ändern. Der Trail beginnt dann mit der Aufzeichnung von Daten-API-Ereignissen. Er kann jedoch keine Daten-API-Ereignisse wiederherstellen, die aufgetreten sind, während der Ausschluss wirksam war.

Wenn Sie Daten-API-Ereignisse mithilfe der Konsole oder API ausschließen, wird der resultierende CloudTrail `PutEventSelectors` API-Vorgang auch in Ihren CloudTrail Protokollen protokolliert. Wenn Daten-API-Ereignisse nicht in Ihren CloudTrail Protokollen angezeigt werden, suchen Sie nach einem `PutEventSelectors` Ereignis, bei dem das `ExcludeManagementEventSources` Attribut auf gesetzt ist`rdsdata.amazonaws.com`.

Weitere Informationen finden Sie unter Protokollieren von Managementereignissen für Trails im AWS CloudTrail -Benutzerhandbuch.

Grundlegendes zu Data API-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Aurora PostgreSQL Serverless v2 und bereitgestellt

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die -`ExecuteStatement`Operation für Aurora PostgreSQL Serverless v2 und bereitgestellte Datenbanken demonstriert. Für diese Datenbanken sind alle Daten-API-Ereignisse Datenereignisse, bei denen die Ereignisquelle rdsdataapi.amazonaws.com und der Ereignistyp Rds Data Service ist.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/johndoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "johndoe"
    },
    "eventTime": "2019-12-18T00:49:34Z",
    "eventSource": "rdsdataapi.amazonaws.com",
    "eventName": "ExecuteStatement",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.16.102 Python/3.7.2 Windows/10 botocore/1.12.92",
    "requestParameters": {
        "continueAfterTimeout": false,
        "database": "**********",
        "includeResultMetadata": false,
        "parameters": [],
        "resourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:my-database-1",
        "schema": "**********",
        "secretArn": "arn:aws:secretsmanager:us-
east-1:123456789012:secret:dataapisecret-ABC123",
        "sql": "**********"
    },
    "responseElements": null,
    "requestID": "6ba9a36e-b3aa-4ca8-9a2e-15a9eada988e",
    "eventID": "a2c7a357-ee8e-4755-a0d0-aed11ed4253a",
    "eventType": "Rds Data Service",
    "recipientAccountId": "123456789012"
}
```


Aurora Serverless v1

Das folgende Beispiel zeigt, wie der vorherige CloudTrail Beispielprotokolleintrag für angezeigt wirdAurora Serverless v1. Für sind alle Ereignisse VerwaltungsereignisseAurora Serverless v1, bei denen die Ereignisquelle rdsdata.amazonaws.com und der Ereignistyp istAwsApiCall.


```
{
    "eventVersion": "1.05",
```

```
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/johndoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "johndoe"
    },
    "eventTime": "2019-12-18T00:49:34Z",
    "eventSource": "rdsdata.amazonaws.com",
    "eventName": "ExecuteStatement",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.16.102 Python/3.7.2 Windows/10 botocore/1.12.92",
    "requestParameters": {
        "continueAfterTimeout": false,
        "database": "**********",
        "includeResultMetadata": false,
        "parameters": [],
        "resourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:my-database-1",
        "schema": "**********",
        "secretArn": "arn:aws:secretsmanager:us-
east-1:123456789012:secret:dataapisecret-ABC123",
        "sql": "**********"
    },
    "responseElements": null,
    "requestID": "6ba9a36e-b3aa-4ca8-9a2e-15a9eada988e",
    "eventID": "a2c7a357-ee8e-4755-a0d0-aed11ed4253a",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Verwenden des Aurora-Abfrage-Editors

Mit dem Aurora-Abfrage-Editor können Sie SQL-Anweisungen auf Ihrem Aurora-DB-Cluster über den ausführen AWS Management Console. Sie können SQL-Abfragen, Datenmanipulationsanweisungen (DML) und Datendefinitionsanweisungen (DDL) ausführen. Mithilfe der Konsolenschnittstelle können Sie Datenbankwartung durchführen, Berichte erstellen und SQL-Experimente durchführen. Sie können vermeiden, die Netzwerkkonfiguration so einzurichten, dass Sie von einem separaten Clientsystem wie einer EC2-Instance oder einem Laptop aus eine Verbindung zu Ihrem DB-Cluster herstellen.

Für den Abfrage-Editor ist ein Aurora-DB-Cluster mit aktivierter RDS-Daten-API (Daten-API) erforderlich. Informationen zu DB-Clustern, die die Daten-API unterstützen, und zu deren Aktivierung finden Sie unterVerwenden der RDS-Daten-API. Das SQL, das Sie ausführen können, unterliegt den Einschränkungen der Daten-API. Weitere Informationen finden Sie unter the section called “Einschränkungen”.

Verfügbarkeit des Abfrage-Editors

Der Abfrage-Editor ist für Aurora-DB-Cluster verfügbar, die Aurora MySQL- und Aurora PostgreSQL-Engine-Versionen verwenden, die Data API unterstützen, und dort, AWS-Regionen wo Data API verfügbar ist. Weitere Informationen finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für die RDS-Daten-API.

Autorisieren des Zugriffs auf den Abfrage-Editor

Ein Benutzer muss zum Ausführen von Abfragen im Abfrage-Editor autorisiert sein. Sie können einen Benutzer autorisieren, Abfragen im Abfrage-Editor auszuführen, indem Sie diesem Benutzer die `AmazonRDSDataFullAccess` Richtlinie, eine vordefinierte Richtlinie AWS Identity and Access Management (IAM), hinzufügen.

> **Note**
>
> Stellen Sie sicher, dass Sie beim Erstellen des IAM-Benutzers denselben Benutzernamen und dasselbe Kennwort verwenden wie für den Datenbankbenutzer, z. B. den Administratorbenutzernamen und das Kennwort. Weitere Informationen zum Hinzufügen

von Benutzern finden Sie unter Erstellen eines IAM-Benutzers in Ihrem AWS-Konto im AWS Identity and Access Management -Benutzerhandbuch.

Sie können auch eine IAM-Richtlinie erstellen die Zugriff auf den Abfrage-Editor gewährt. Nach dem Erstellen der Richtlinie können Sie diese jedem Benutzer hinzufügen, der Zugriff auf den Abfrage-Editor benötigt.

Die folgende Richtlinie bietet die mindestens erforderlichen Berechtigungen für einen Benutzer, um auf den Abfrage-Editor zuzugreifen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "QueryEditor0",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:PutResourcePolicy",
                "secretsmanager:PutSecretValue",
                "secretsmanager:DeleteSecret",
                "secretsmanager:DescribeSecret",
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
        },
        {
            "Sid": "QueryEditor1",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword",
                "tag:GetResources",
                "secretsmanager:CreateSecret",
                "secretsmanager:ListSecrets",
                "dbqms:CreateFavoriteQuery",
                "dbqms:DescribeFavoriteQueries",
                "dbqms:UpdateFavoriteQuery",
                "dbqms:DeleteFavoriteQueries",
                "dbqms:GetQueryString",
                "dbqms:CreateQueryHistory",
```

```
                "dbqms:UpdateQueryHistory",
                "dbqms:DeleteQueryHistory",
                "dbqms:DescribeQueryHistory",
                "rds-data:BatchExecuteStatement",
                "rds-data:BeginTransaction",
                "rds-data:CommitTransaction",
                "rds-data:ExecuteStatement",
                "rds-data:RollbackTransaction"
            ],
            "Resource": "*"
        }
    ]
}
```

Informationen zum Erstellen einer IAM-Richtlinie finden Sie unter Erstellen von IAM-Richtlinien im AWS Identity and Access Management -Benutzerhandbuch.

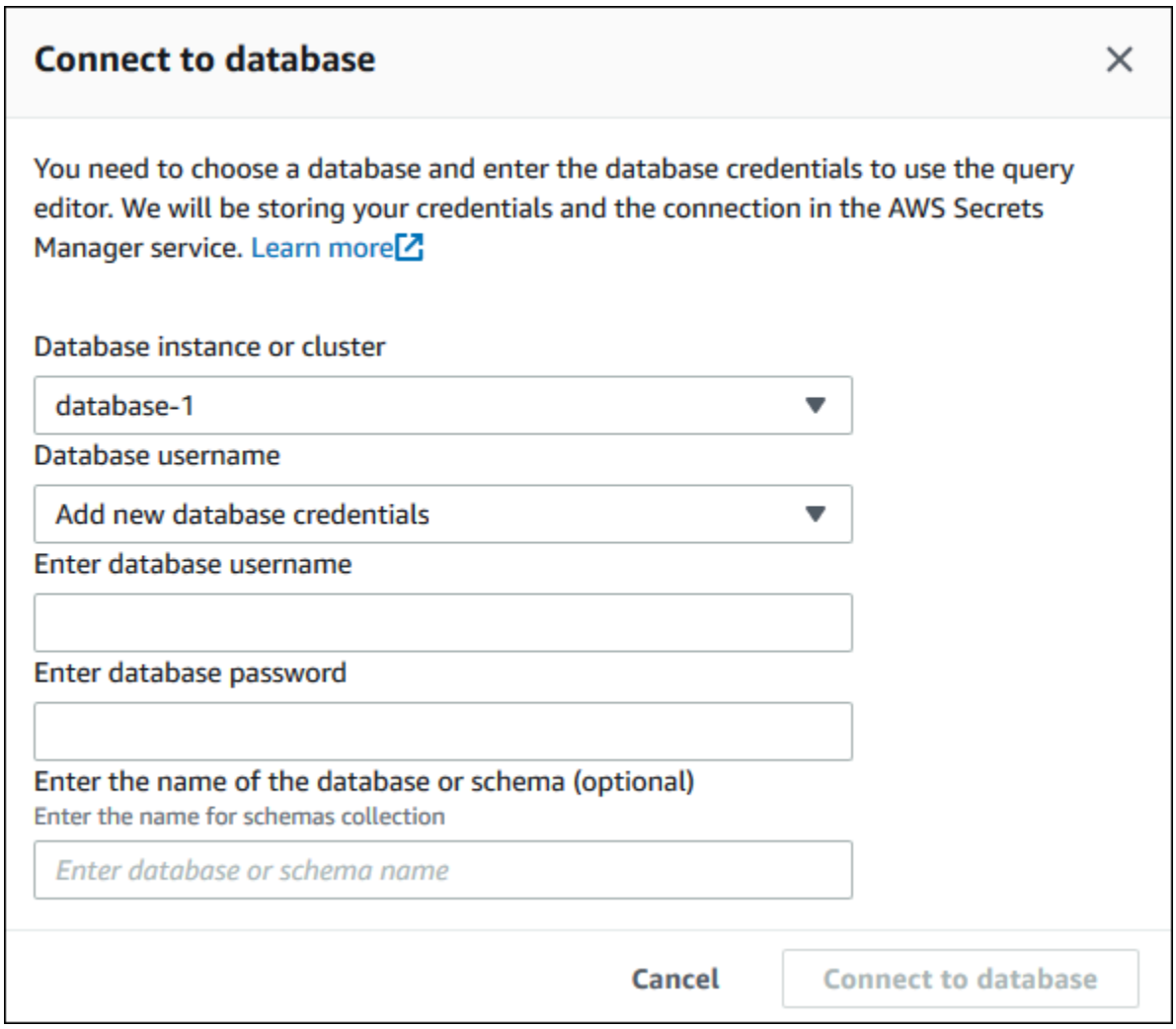
Informationen zum Hinzufügen einer IAM-Richtlinie zu einem Benutzer finden Sie im Abschnitt Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im AWS Identity and Access Management -Benutzerhandbuch.

Ausführen von Abfragen im Abfrage-Editor

Sie können SQL-Anweisungen auf einem Aurora-DB-Cluster im Abfrage-Editor ausführen. Das SQL, das Sie ausführen können, unterliegt den Einschränkungen der Daten-API. Weitere Informationen finden Sie unter the section called “Einschränkungen”.

So führen Sie eine Abfrage im Abfrage-Editor aus

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der oberen rechten Ecke des den aus AWS Management Console, AWS-Region in dem Sie die Aurora-DB-Cluster erstellt haben, die Sie abfragen möchten.
3. Wählen Sie im Navigationsbereich Datenbanken aus.
4. Wählen Sie den Aurora-DB-Cluster aus, auf dem Sie SQL-Abfragen ausführen möchten.
5. Wählen Sie für Aktionen die Option Abfrage aus. Falls Sie noch keine Verbindung zur Datenbank hergestellt haben, wird die Seite Connect to database (Verbindung zur Datenbank herstellen) geöffnet.



6. Geben Sie die folgenden Informationen ein:

   a. Wählen Sie für Datenbank-Instance oder -Cluster den Aurora-DB-Cluster aus, auf dem Sie SQL-Abfragen ausführen möchten.

   b. Wählen Sie in Database username (Datenbank-Benutzername) den Benutzernamen des Benutzers der Datenbank aus, mit der Sie eine Verbindung herstellen möchten, oder wählen Sie Add new database credentials (Neue Datenbankanmeldeinformationen hinzufügen) aus. Wenn Sie Add new database credentials (Neue Datenbankanmeldeinformationen) auswählen, geben Sie den Benutzernamen für die neuen Datenbankanmeldeinformationen in Enter database username (Datenbank-Benutzername eingeben) ein.

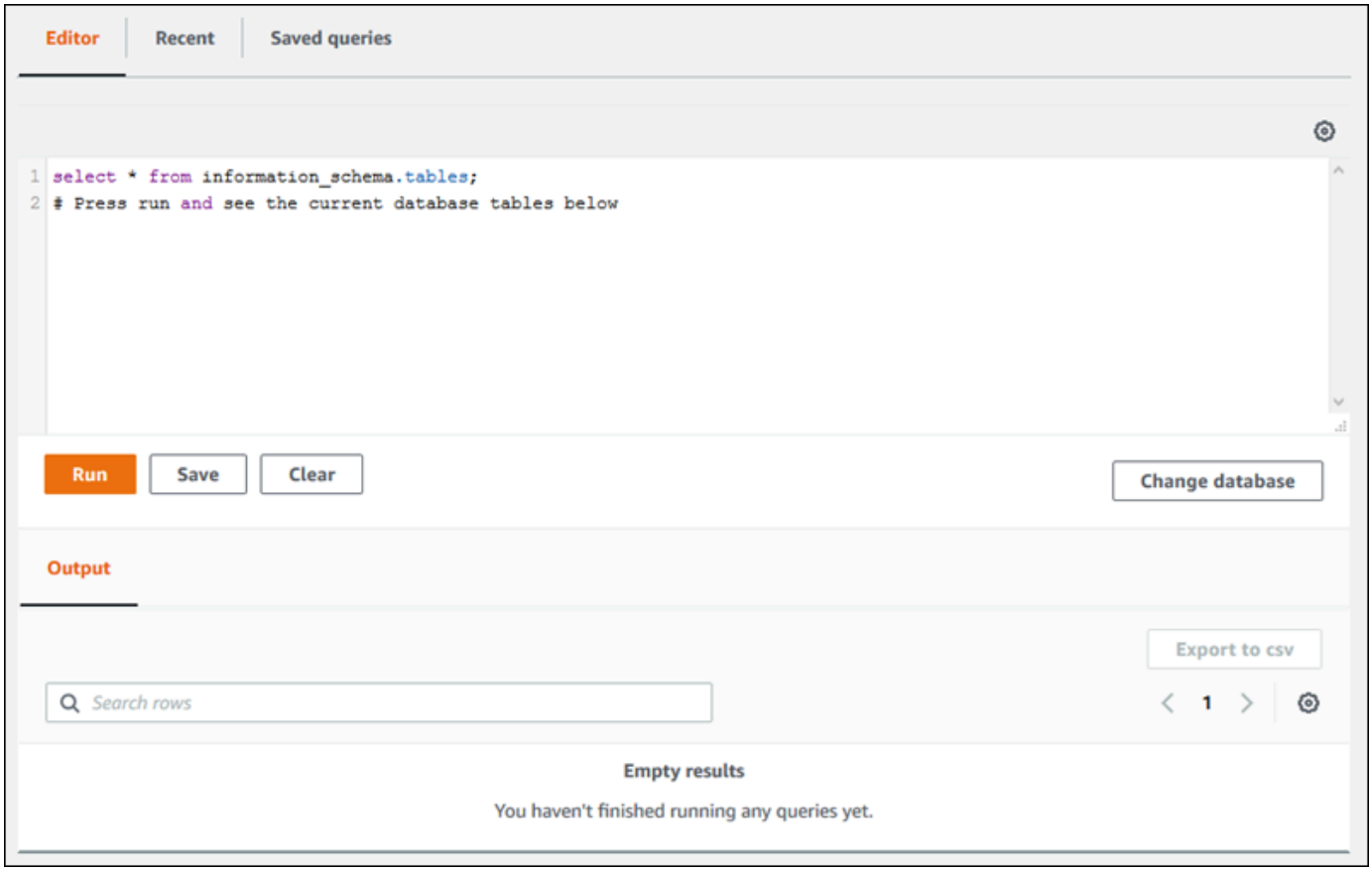
   c. Geben Sie in Enter database password (Datenbankpasswort eingeben) das Passwort für den von Ihnen ausgewählten Datenbankbenutzer ein.

   d. Geben Sie in das letzte Feld den Namen der Datenbank oder des Schemas ein, die bzw. das Sie für das Aurora-DB-Cluster verwenden möchten.

e. Wählen Sie Connect to database (Verbindung zur Datenbank herstellen).

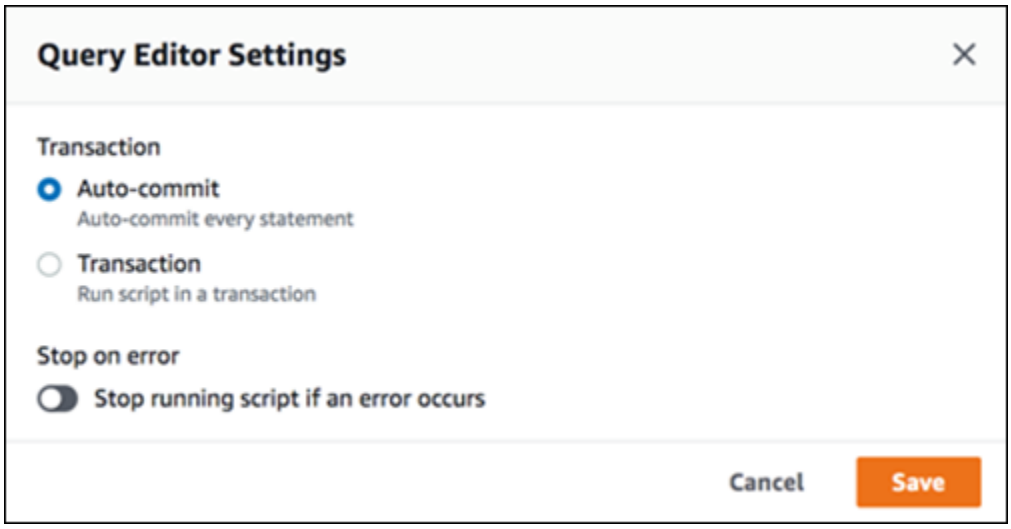
> **Note**
>
> Wenn Ihre Verbindung erfolgreich ist, werden Ihre Verbindungs- und Authentifizierungsinformationen in gespeicher AWS Secrets Manager. Sie müssen die Verbindungsinformationen nicht noch einmal eingeben.

7. Geben Sie im Abfrage-Editor die SQL-Abfrage ein, die Sie für die Datenbank ausführen möchten.



Jede SQL-Anweisung kann automatisch übergeben werden. Alternativ können Sie SQL-Anweisungen in einem Skript als Teil einer Transaktion ausführen. Um dieses Verhalten zu steuern, wählen Sie das Zahnradsymbol oberhalb des Abfragefensters aus.

Das Fenster Query Editor Settings (Einstellungen des Abfrage-Editors) wird angezeigt.



Wenn Sie Auto-commit (Automatisch übergeben) wählen, wird jede SQL-Anweisung automatisch übergeben. Wenn Sie Transaktion wählen, können Sie eine Gruppe von Anweisungen in einem Skript ausführen. Anweisungen werden automatisch am Ende des Skripts festgeschrieben, es sei denn, vorher wurde explizit festgeschrieben oder zurückgesetzt. Sie können ein Skript, das ausgeführt wird, bei Auftreten eines Fehlers auch anhalten, indem Sie Stop on error (Bei Fehler anhalten) aktivieren.

> **Note**
>
> In einer Gruppe von Anweisungen können Data Definition Language (DDL)-Anweisungen dazu führen, dass frühere Data Manipulation Language (DML)-Anweisungen übergeben werden. Sie können in einer Gruppe von Anweisungen in einem Skript auch `COMMIT`- und `ROLLBACK`-Anweisungen einfügen.

Wählen Sie nach Festlegen der Optionen im Fenster Query Editor Settings (Einstellungen des Abfrage-Editors) Save (Speichern) aus.

8. Wählen Sie Run (Ausführen) oder drücken Sie STRG+Eingabetaste. Der Abfrage-Editor zeigt dann die Ergebnisse Ihrer Abfrage an.

   Speichern Sie nach dem Ausführen der Abfrage diese in Saved Queries (Gespeicherte Abfragen) durch Auswahl von Save (Speichern).

   Sie können die Abfrageergebnisse durch Auswahl von Export to csv (Zu CSV exportieren) in ein Tabellenformat exportieren.

Sie können frühere Abfragen suchen, bearbeiten und erneut ausführen. Hierzu wählen Sie die Registerkarte Recent (Zuletzt) oder Saved queries (Gespeicherte Abfragen), den Abfragetext und anschließend Run (Ausführen) aus.

Um die Datenbank zu ändern, wählen Sie Change database (Datenbank ändern).

API-Referenz für Database Query Metadata Service (DBQMS)

Der Database Query Metadata Service (`dbqms`) ist ein reiner Dienst für interne Daten. Er stellt Ihre aktuellen und gespeicherten Abfragen für den Abfrage-Editor auf AWS Management Console für mehrere AWS-Services bereit, einschließlich Amazon RDS.

Die folgenden DBQMS-Aktionen werden unterstützt:

Themen

- CreateFavoriteQuery
- CreateQueryHistory
- CreateTab

CreateFavoriteQuery

Speichern Sie eine neue bevorzugte Abfrage. Jeder -Benutzer kann bis zu 1000 gespeicherte Abfragen erstellen. Dieses Limit kann in Zukunft geändert werden.

CreateQueryHistory

Dient zum Speichern eines neuen Abfrageverlaufseintrags.

CreateTab

Speichern Sie eine neue Abfrage-Registerkarte. Jeder -Benutzer kann bis zu 10 Abfrage-Registerkarten erstellen.

DeleteFavoriteQueries

Löschen Sie eine oder mehrere gespeicherte Abfragen.

DeleteQueryHistory

Dient zum Löschen von Abfrageverlaufseinträgen.

DeleteTab

Löschen Sie Einträge der Abfrage-Registerkarte

DescribeFavoriteQueries

Listet gespeicherte Abfragen auf, die von einem Benutzer in einem bestimmten Konto erstellt wurden.

DescribeQueryHistory

Listet Abfrageverlaufseinträge auf.

DescribeTabs

Listet Abfrage-Registerkarten auf, die von einem Benutzer in einem bestimmten Konto erstellt wurden.

GetQueryString

Dient zum Abruf des vollständigen Abfragetexts über eine Abfrage-ID.

UpdateFavoriteQuery

Ermöglicht die Aktualisierung der Abfragezeichenfolge, der Beschreibung, des Namens oder des Ablaufdatums.

UpdateQueryHistory

Dient zum Aktualisieren des Status des Abfrageverlaufs.

UpdateTab

Aktualisieren Sie den Namen der Abfrage-Registerkarte und die Abfragezeichenfolge.

Verwenden von Amazon Aurora Machine Learning

Durch die Verwendung von Amazon Aurora Machine Learning können Sie Ihren Aurora-DB-Cluster je nach Bedarf in einen der folgenden AWS Machine-Learning-Services integrieren. Sie unterstützen jeweils bestimmte Anwendungsfälle für Machine Learning.

Amazon Bedrock

Amazon Bedrock ist ein vollständig verwalteter Service, der führende Grundlagenmodelle von KI-Unternehmen über eine API zur Verfügung stellt, zusammen mit Entwicklertools, um die Entwicklung und Skalierung generativer KI-Anwendungen zu unterstützen. Bei Amazon Bedrock zahlen Sie für das Bilden von Inferenzen in allen Basismodellen von Drittanbietern. Die Preisgestaltung richtet sich nach der Menge der Ein- und Ausgabetoken und danach, ob Sie bereitgestellten Durchsatz für das Modell erworben haben. Weitere Informationen finden Sie unter Was ist Amazon Bedrock? im Amazon Bedrock-Benutzerhandbuch.

Amazon Comprehend

Amazon Comprehend ist ein verwalteter Dienst für die natürliche Sprachverarbeitung (NLP), der verwendet wird, um Informationen aus Dokumenten zu extrahieren. Mit Amazon Comprehend können Sie anhand des Inhalts von Dokumenten Stimmungen ableiten, indem Entitäten, Schlüsselphrasen, Sprache und andere Merkmale analysiert werden. Weitere Informationen finden Sie unter Was ist Amazon Comprehend? im Entwicklerhandbuch für Amazon Comprehend.

SageMaker

Amazon SageMaker ist ein vollständig verwalteter Machine-Learning-Service. Datenwissenschaftler und Entwickler verwenden Amazon, SageMaker um Machine-Learning-Modelle für eine Vielzahl von Inferenzaufgaben wie Betrugserkennung und Produktempfehlungen zu erstellen, zu trainieren und zu testen. Wenn ein Machine-Learning-Modell für die Verwendung in der Produktion bereit ist, kann es in der von Amazon SageMaker gehosteten Umgebung bereitgestellt werden. Weitere Informationen finden Sie unter Was ist Amazon SageMaker? im Amazon- SageMaker Entwicklerhandbuch.

Die Verwendung von Amazon Comprehend mit Ihrem Aurora-DB-Cluster hat eine weniger vorbereitende Einrichtung als die Verwendung von SageMaker. Wenn Sie noch nicht mit AWS Machine Learning vertraut sind, empfehlen wir Ihnen, zunächst Amazon Comprehend zu erkunden.

Themen

Verwendung von Amazon Aurora Machine Learning mit Aurora MySQL

Wenn Sie Amazon Aurora Machine Learning mit Ihrem Aurora MySQL-DB-Cluster verwenden, können Sie je nach Bedarf Amazon Bedrock, Amazon Comprehend oder Amazon SageMaker verwenden. Sie unterstützen jeweils unterschiedliche Anwendungsfälle für maschinelles Lernen.

Inhalt

  - Abfrage-Cache
  - Batch-Optimierung für Aurora-Machine-Learning-Funktionsaufrufe
- Überwachung von Aurora Machine Learning

Voraussetzungen für die Verwendung von Aurora Machine Learning mit Aurora MySQL

AWS Dienste für maschinelles Lernen sind verwaltete Dienste, die in ihren eigenen Produktionsumgebungen eingerichtet und ausgeführt werden. Aurora Machine Learning unterstützt die Integration mit Amazon Bedrock, Amazon Comprehend und. SageMaker Bevor Sie versuchen, Ihren DB-Cluster von Aurora MySQL für die Verwendung von Aurora Machine Learning einzurichten, stellen Sie sicher, dass Sie die folgenden Anforderungen und Voraussetzungen verstehen.

- Die Machine-Learning-Dienste müssen im selben System AWS-Region wie Ihr Aurora MySQL-DB-Cluster laufen. Sie können keine Machine-Learning-Dienste von einem Aurora MySQL-DB-Cluster in einer anderen Region verwenden.
- Wenn sich Ihr Aurora MySQL-DB-Cluster in einer anderen Virtual Public Cloud (VPC) als Ihr Amazon Bedrock, Amazon Comprehend oder SageMaker Service befindet, muss die Sicherheitsgruppe der VPC ausgehende Verbindungen zum Aurora-Zielservice für maschinelles Lernen zulassen. Weitere Informationen finden Sie unter Steuern des Datenverkehrs zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen im Amazon VPC-Benutzerhandbuch.
- Sie können einen Aurora-Cluster, auf dem eine niedrigere Version von Aurora MySQL ausgeführt wird, auf eine unterstützte höhere Version aktualisieren, wenn Sie Aurora Machine Learning mit diesem Cluster verwenden möchten. Weitere Informationen finden Sie unter Datenbank-Engine-Updates für Amazon Aurora MySQL.
- Ihr Aurora MySQL-DB-Cluster muss eine benutzerdefinierte DB-Cluster-Parametergruppe verwenden. Am Ende des Einrichtungsvorgangs für jeden Aurora-Service für Machine Learning, den Sie verwenden möchten, fügen Sie den Amazon-Ressourcennamen (ARN) der zugehörigen IAM-Rolle hinzu, die für den Service erstellt wurde. Wir empfehlen Ihnen, vorab eine benutzerdefinierte DB-Cluster-Parametergruppe für Aurora MySQL zu erstellen und Ihren DB-Cluster von Aurora MySQL für ihre Verwendung zu konfigurieren, damit sie am Ende des Einrichtungsvorgangs von Ihnen geändert werden kann.
- Für SageMaker:
  - Die Komponenten für maschinelles Lernen, die Sie für Inferenzen verwenden möchten, müssen eingerichtet und einsatzbereit sein. Stellen Sie während des Konfigurationsprozesses für Ihren

Aurora MySQL-DB-Cluster sicher, dass der ARN des SageMaker Endpunkts verfügbar ist. Die Datenwissenschaftler in Ihrem Team sind wahrscheinlich am besten in der Lage SageMaker , die Modelle vorzubereiten und die anderen Aufgaben dieser Art zu erledigen. Informationen zu den ersten Schritten mit Amazon SageMaker finden Sie unter Erste Schritte mit Amazon SageMaker. Weitere Informationen zu Rückschlüssen und Endpunkten finden Sie unter Echtzeit-Inferenz.

- Für die Verwendung SageMaker mit Ihren eigenen Trainingsdaten müssen Sie einen Amazon S3 S3-Bucket als Teil Ihrer Aurora MySQL-Konfiguration für Aurora Machine Learning einrichten. Dazu folgen Sie demselben allgemeinen Prozess wie beim Einrichten der SageMaker Integration. Eine Zusammenfassung dieses optionalen Einrichtungsprozesses finden Sie unter Einrichtung Ihres Aurora MySQL-DB-Clusters für die Verwendung von Amazon S3 SageMaker (optional).

- Für globale Aurora-Datenbanken richten Sie die Aurora-Dienste für maschinelles Lernen ein, die Sie in allen Bereichen AWS-Regionen Ihrer globalen Aurora-Datenbank verwenden möchten. Wenn Sie beispielsweise Aurora Machine Learning mit für Ihre globale Aurora-Datenbank verwenden möchten, gehen Sie SageMaker für jeden Aurora MySQL-DB-Cluster in jedem wie folgt vor AWS-Region:
  - Richten Sie die SageMaker Amazon-Services mit denselben SageMaker Schulungsmodellen und Endpunkten ein. Diese müssen auch dieselben Namen tragen.
  - Erstellen Sie die IAM-Rollen wie unter Einrichten Ihres DB-Clusters von Aurora MySQL zur Verwendung von Aurora Machine Learning beschrieben.
  - Fügen Sie den ARN der IAM-Rolle der benutzerdefinierten DB-Cluster-Parametergruppe für jeden DB-Cluster von Aurora MySQL in jeder AWS-Region hinzu.

  Diese Aufgaben setzen voraus, dass Aurora Machine Learning für Ihre Version von Aurora MySQL in allen Bereichen AWS-Regionen Ihrer globalen Aurora-Datenbank verfügbar ist.

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Aurora-Datenbank-Engines und in allen AWS-Regionen.

- Informationen zur Version und regionalen Verfügbarkeit für Amazon Comprehend und Amazon SageMaker with Aurora MySQL finden Sie unter. Aurora Machine Learning mit Aurora MySQL
- Amazon Bedrock wird nur auf Aurora MySQL Version 3.06 und höher unterstützt.

Informationen zur regionalen Verfügbarkeit von Amazon Bedrock finden Sie unter Unterstützte Modelle in Amazon Bedrock im Amazon Bedrock-Benutzerhandbuch.

Unterstützte Funktionen und Einschränkungen von Aurora Machine Learning mit Aurora MySQL

Bei der Verwendung von Aurora MySQL mit Aurora Machine Learning gelten die folgenden Einschränkungen:

- Die Aurora-Erweiterung für maschinelles Lernen unterstützt keine Vektorschnittstellen.
- Aurora-Integrationen für maschinelles Lernen werden nicht unterstützt, wenn sie in einem Trigger verwendet werden.
- Aurora-Funktionen für maschinelles Lernen sind nicht mit der Replikation von Binärprotokollierung (Binlog) kompatibel.
  - Die Einstellung `--binlog-format=STATEMENT` führt beim Aufrufen von Aurora Machine Learning-Funktionen zu einer Ausnahme.
  - Aurora-Funktionen für Machine Learning sind nichtdeterministisch und nichtdeterministische gespeicherte Funktionen sind mit diesem Binlog-Format nicht kompatibel.

  Weitere Informationen finden Sie unter Binary Logging Formats in der MySQL-Dokumentation.
- Gespeicherte Funktionen, die Tabellen mit „Generated-always“-Spalten aufrufen, werden nicht unterstützt. Dies gilt für jede gespeicherte Aurora-MySQL-Funktion. Weitere Informationen zu diesem Spaltentyp finden Sie unter CREATE TABLE und „Generated“-Spalten in der MySQL-Dokumentation.
- Die Funktionen von Amazon Bedrock werden nicht unterstütztRETURNS `JSON`. Sie können `CONVERT` oder verwendenCAST, um bei `JSON` Bedarf von `TEXT` zu konvertieren.
- Amazon Bedrock unterstützt keine Batch-Anfragen.
- Aurora MySQL unterstützt jeden SageMaker Endpunkt, der das CSV-Format (Comma-Separated Value) liest und schreibt, und zwar über ein `ContentType` of. `text/csv` Dieses Format wird von den folgenden integrierten SageMaker Algorithmen akzeptiert:
  - Lineares Lernen
  - Random Cut Forest
  - XGBoost

Weitere Informationen zu diesen Algorithmen finden Sie unter Choose an Algorithm im Amazon SageMaker Developer Guide.

Einrichten Ihres DB-Clusters von Aurora MySQL zur Verwendung von Aurora Machine Learning

In den folgenden Themen finden Sie separate Einrichtungsverfahren für jeden dieser Aurora-Dienste für Machine Learning.

Themen

Einrichtung Ihres Aurora MySQL-DB-Clusters für die Verwendung von Amazon Bedrock

Aurora Machine Learning stützt sich auf AWS Identity and Access Management (IAM-) Rollen und Richtlinien, damit Ihr Aurora MySQL-DB-Cluster auf die Amazon Bedrock-Services zugreifen und diese nutzen kann. Die folgenden Verfahren erstellen eine IAM-Berechtigungsrichtlinie und -rolle, sodass Ihr DB-Cluster in Amazon Bedrock integriert werden kann.

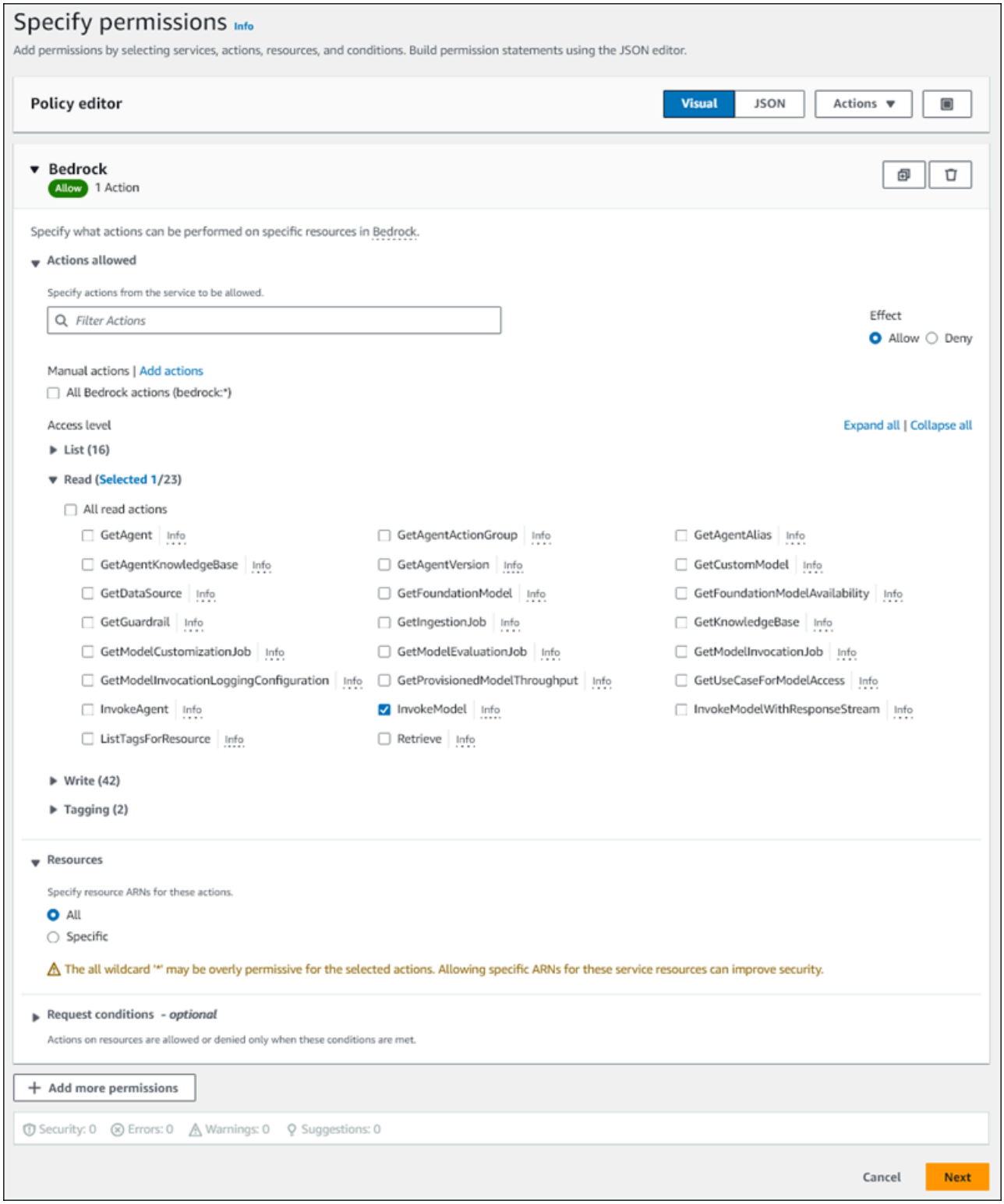
So erstellen Sie die -IAM-Richtlinie

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien aus.
3. Klicken Sie auf Create a policy (Richtlinie erstellen).

4. Wählen Sie auf der Seite „Berechtigungen angeben“ für Dienst auswählen die Option Bedrock aus.

   Die Amazon Bedrock-Berechtigungen werden angezeigt.
5. Erweitern Sie Lesen und wählen Sie dann aus InvokeModel.
6. Wählen Sie für Ressourcen die Option Alle aus.

   Die Seite „Berechtigungen angeben“ sollte der folgenden Abbildung ähneln.



7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Überprüfen und erstellen beispielsweise einen Namen für Ihre Richtlinie ein. **`BedrockInvokeModel`**

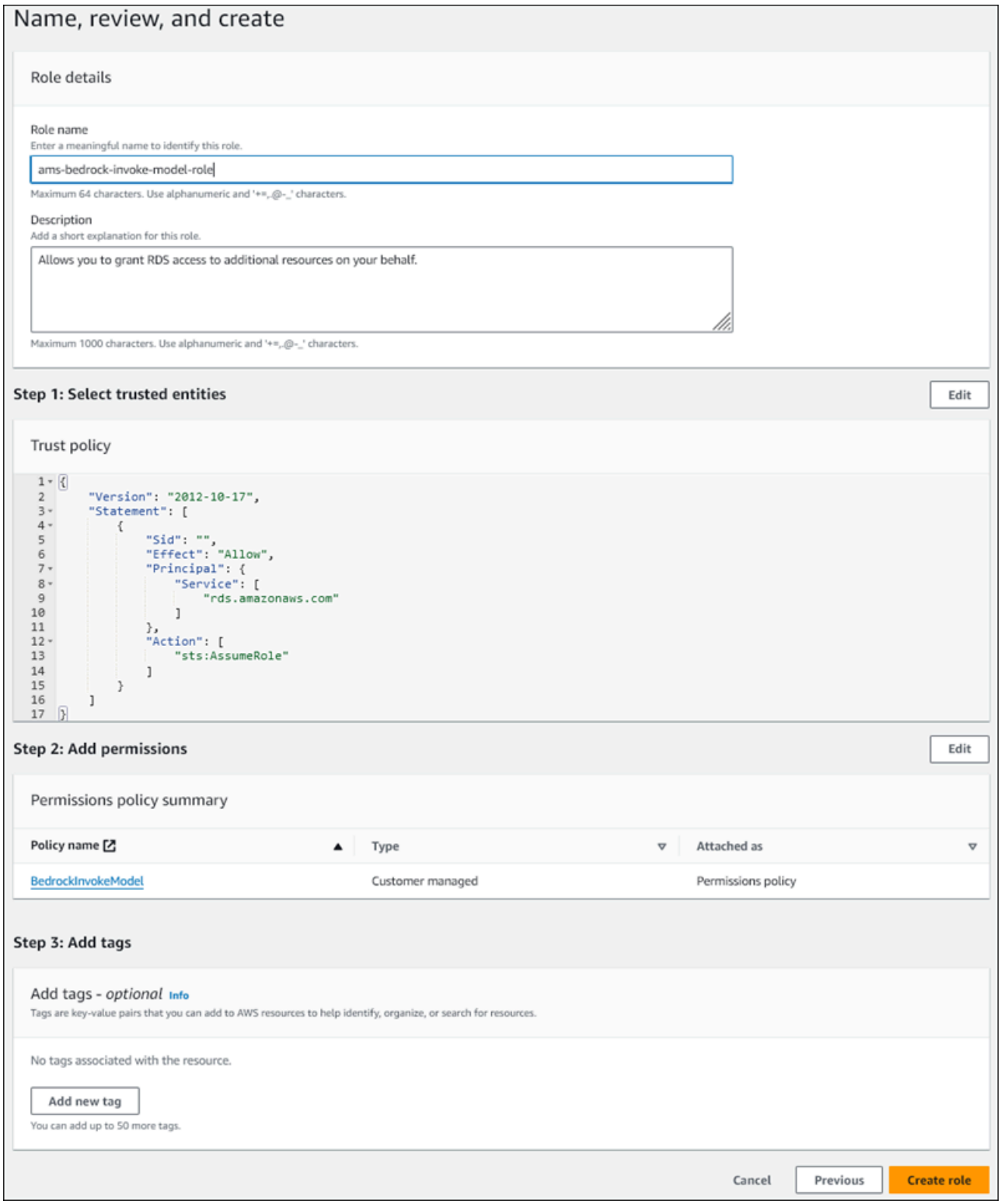
9. Überprüfen Sie Ihre Richtlinie und wählen Sie dann Richtlinie erstellen aus.

Als Nächstes erstellen Sie die IAM-Rolle, die die Amazon Bedrock-Berechtigungsrichtlinie verwendet.

So erstellen Sie die IAM-Rolle

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rollen) aus.
3. Wählen Sie Rolle erstellen aus.
4. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen für Anwendungsfall die Option RDS aus.
5. Wählen Sie RDS — Rolle zur Datenbank hinzufügen und dann Weiter aus.
6. Wählen Sie auf der Seite „Berechtigungen hinzufügen“ für Berechtigungsrichtlinien die IAM-Richtlinie aus, die Sie erstellt haben, und klicken Sie dann auf Weiter.
7. Geben Sie auf der Seite Name, Überprüfung und Erstellung beispielsweise **`ams-bedrock-invoke-model-role`** einen Namen für Ihre Rolle ein.

   Die Rolle sollte der folgenden Abbildung ähneln.



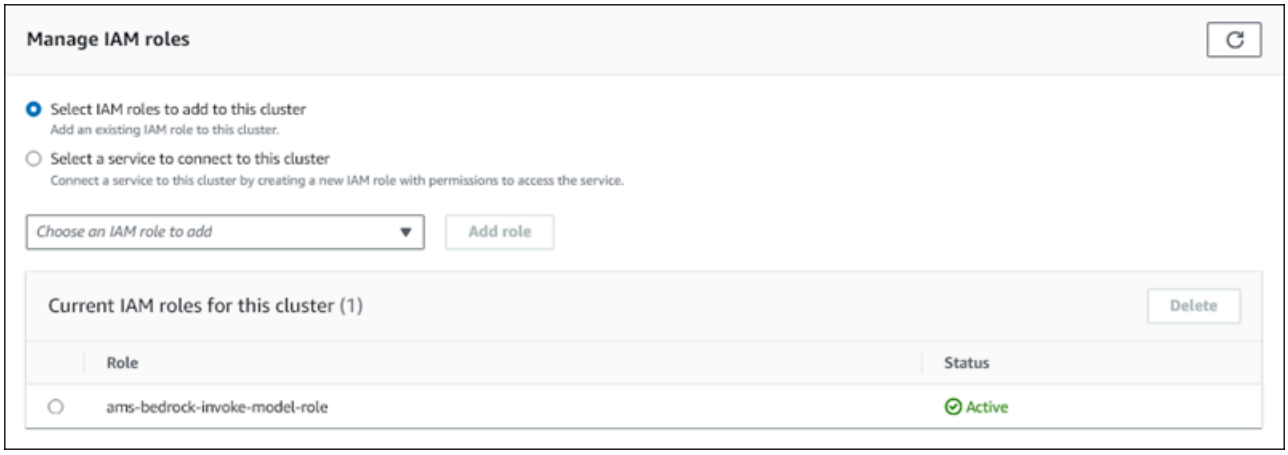
8. Überprüfen Sie Ihre Rolle und wählen Sie dann Rolle erstellen aus.

Als Nächstes verknüpfen Sie die Amazon Bedrock IAM-Rolle mit Ihrem DB-Cluster.

Um die IAM-Rolle Ihrem DB-Cluster zuzuordnen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie aus dem Navigationsbereich Datenbanken aus.
3. Wählen Sie den Aurora MySQL-DB-Cluster aus, den Sie mit den Amazon Bedrock-Services verbinden möchten.
4. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit).
5. Wählen Sie im Abschnitt „IAM-Rollen verwalten“ die Option IAM auswählen, um es diesem Cluster hinzuzufügen.
6. Wählen Sie das IAM aus, das Sie erstellt haben, und klicken Sie dann auf Rolle hinzufügen.

   Die IAM-Rolle ist Ihrem DB-Cluster zugeordnet, zunächst mit dem Status Ausstehend, dann mit dem Status Aktiv. Wenn der Vorgang abgeschlossen ist, wird die Rolle in der Liste Current IAM roles for this cluster (Aktuelle IAM-Rollen für diesen Cluster) angezeigt.



Sie müssen den ARN dieser IAM-Rolle dem Parameter der benutzerdefinierten `aws_default_bedrock_role` DB-Cluster-Parametergruppe hinzufügen, die Ihrem Aurora MySQL-DB-Cluster zugeordnet ist. Wenn Ihr DB-Cluster von Aurora MySQL keine benutzerdefinierte DB-Cluster-Parametergruppe verwendet, müssen Sie eine erstellen, die Sie mit Ihrem DB-Cluster von Aurora MySQL nutzen können, um die Integration abzuschließen. Weitere Informationen finden Sie unter Arbeiten mit DB-Cluster-Parametergruppen.

Um den DB-Cluster-Parameter zu konfigurieren

1. Öffnen Sie in der Amazon-RDS-Konsole die Registerkarte Configuration (Konfiguration) Ihres DB-Clusters von Aurora MySQL.

2. Suchen Sie die für Ihren Cluster konfigurierte DB-Cluster-Parametergruppe. Wählen Sie den Link, um Ihre benutzerdefinierte DB-Cluster-Parametergruppe zu öffnen, und klicken Sie dann auf Bearbeiten.
3. Suchen Sie den `aws_default_bedrock_role`-Parameter in Ihrer benutzerdefinierten DB-Cluster-Parametergruppe.
4. Geben Sie im Feld Wert den ARN der IAM-Rolle ein.
5. Wählen Sie zum Speichern der Einstellung Save Changes (Änderungen speichern) aus.
6. Starten Sie die primäre Instance Ihres DB-Clusters von Aurora MySQL neu, damit diese Parametereinstellung wirksam wird.

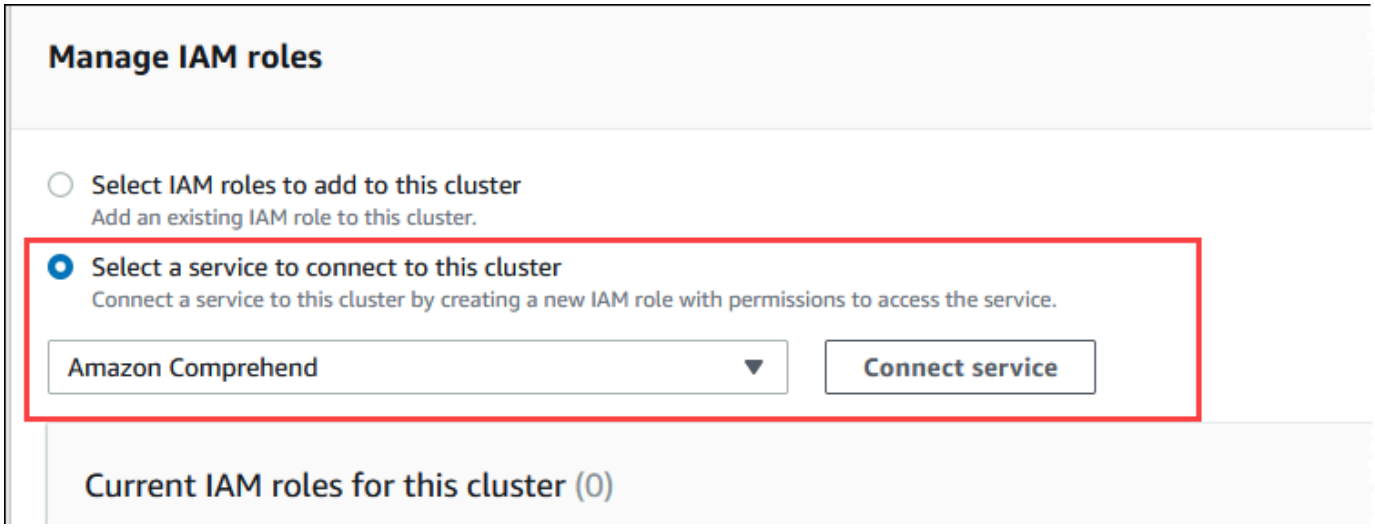
Die IAM-Integration für Amazon Bedrock ist abgeschlossen. Fahren Sie mit der Einrichtung Ihres Aurora MySQL-DB-Clusters für die Zusammenarbeit mit Amazon Bedrock by Erteilen des Zugriffs auf Aurora Machine Learning für Datenbankbenutzer fort.

Einrichten Ihres DB-Clusters von Aurora MySQL zur Verwendung von Amazon Comprehend

Aurora Machine Learning stützt sich auf AWS Identity and Access Management Rollen und Richtlinien, damit Ihr Aurora MySQL-DB-Cluster auf die Amazon Comprehend-Services zugreifen und diese nutzen kann. Mit dem folgenden Verfahren werden automatisch eine IAM-Rolle und -Richtlinie für Ihren Cluster erstellt, sodass dieser Amazon Comprehend verwenden kann.

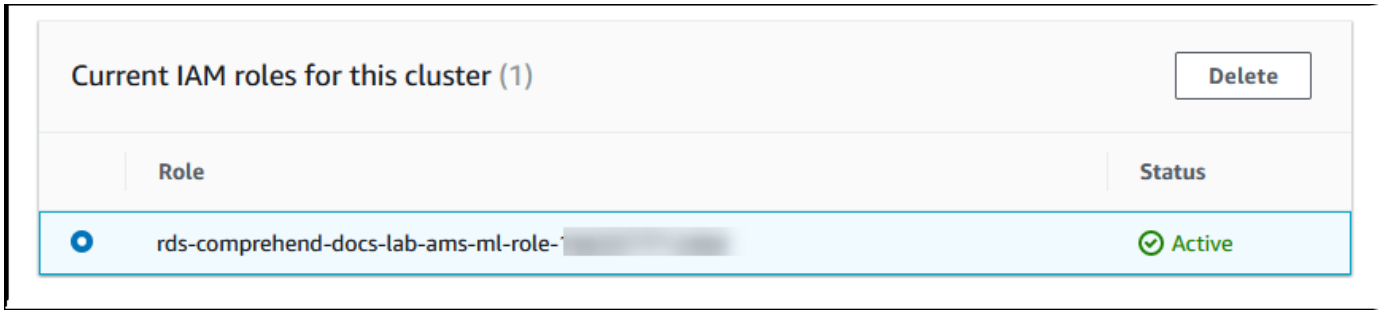
So richten Sie Ihren DB-Cluster von Aurora MySQL zur Verwendung von Amazon Comprehend ein

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie aus dem Navigationsbereich Datenbanken aus.
3. Wählen Sie den Aurora MySQL-DB-Cluster aus, den Sie mit Amazon Comprehend Services verbinden möchten.
4. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit).
5. Wählen Sie im Abschnitt „IAM-Rollen verwalten“ die Option Wählen Sie einen Service aus, um eine Verbindung zu diesem Cluster herzustellen.
6. Wählen Sie Amazon Comprehend aus dem Menü und wählen Sie dann Connect Service.



7. Für das Dialogfeld Connect cluster to Amazon Comprehend (Cluster mit Amazon Comprehend verbinden) sind keine zusätzlichen Informationen erforderlich. Möglicherweise wird jedoch eine Meldung mit dem Hinweis angezeigt, dass sich die Integration von Aurora und Amazon Comprehend derzeit in der Vorschau befindet. Lesen Sie die Nachricht unbedingt, bevor Sie fortfahren. Sie können Abbrechen wählen, wenn Sie nicht fortfahren möchten.
8. Wählen Sie Connect service (Service verbinden) aus, um den Integrationsvorgang abzuschließen.

   Aurora erstellt die IAM-Rolle. Es erstellt auch die Richtlinie, die es dem Aurora MySQL-DB-Cluster ermöglicht, Amazon Comprehend Services zu nutzen, und fügt die Richtlinie der Rolle hinzu. Wenn der Vorgang abgeschlossen ist, wird die Rolle in der Liste Current IAM roles for this cluster (Aktuelle IAM-Rollen für diesen Cluster) angezeigt, wie in der folgenden Abbildung dargestellt.



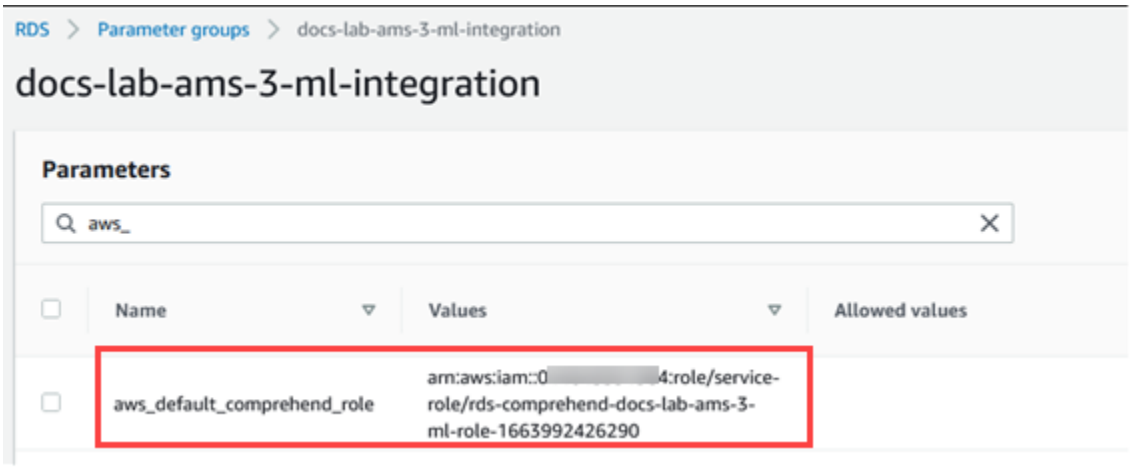
   Sie müssen den ARN dieser IAM-Rolle dem Parameter der benutzerdefinierten `aws_default_comprehend_role` DB-Cluster-Parametergruppe hinzufügen, die Ihrem Aurora MySQL-DB-Cluster zugeordnet ist. Wenn Ihr DB-Cluster von Aurora MySQL keine benutzerdefinierte DB-Cluster-Parametergruppe verwendet, müssen Sie eine erstellen, die Sie

mit Ihrem DB-Cluster von Aurora MySQL nutzen können, um die Integration abzuschließen. Weitere Informationen finden Sie unter Arbeiten mit DB-Cluster-Parametergruppen.

Nachdem Sie Ihre benutzerdefinierte DB-Cluster-Parametergruppe erstellt und mit Ihrem DB-Cluster von Aurora MySQL verknüpft haben, können Sie mit den folgenden Schritten fortfahren.

Wenn Ihr Cluster eine benutzerdefinierte DB-Cluster-Parametergruppe verwendet, gehen Sie wie folgt vor.

a. Öffnen Sie in der Amazon-RDS-Konsole die Registerkarte Configuration (Konfiguration) Ihres DB-Clusters von Aurora MySQL.
b. Suchen Sie die für Ihren Cluster konfigurierte DB-Cluster-Parametergruppe. Wählen Sie den Link, um Ihre benutzerdefinierte DB-Cluster-Parametergruppe zu öffnen, und klicken Sie dann auf Bearbeiten.
c. Suchen Sie den `aws_default_comprehend_role`-Parameter in Ihrer benutzerdefinierten DB-Cluster-Parametergruppe.
d. Geben Sie im Feld Wert den ARN der IAM-Rolle ein.
e. Wählen Sie zum Speichern der Einstellung Save Changes (Änderungen speichern) aus. Die folgende Abbildung zeigt ein Beispiel.

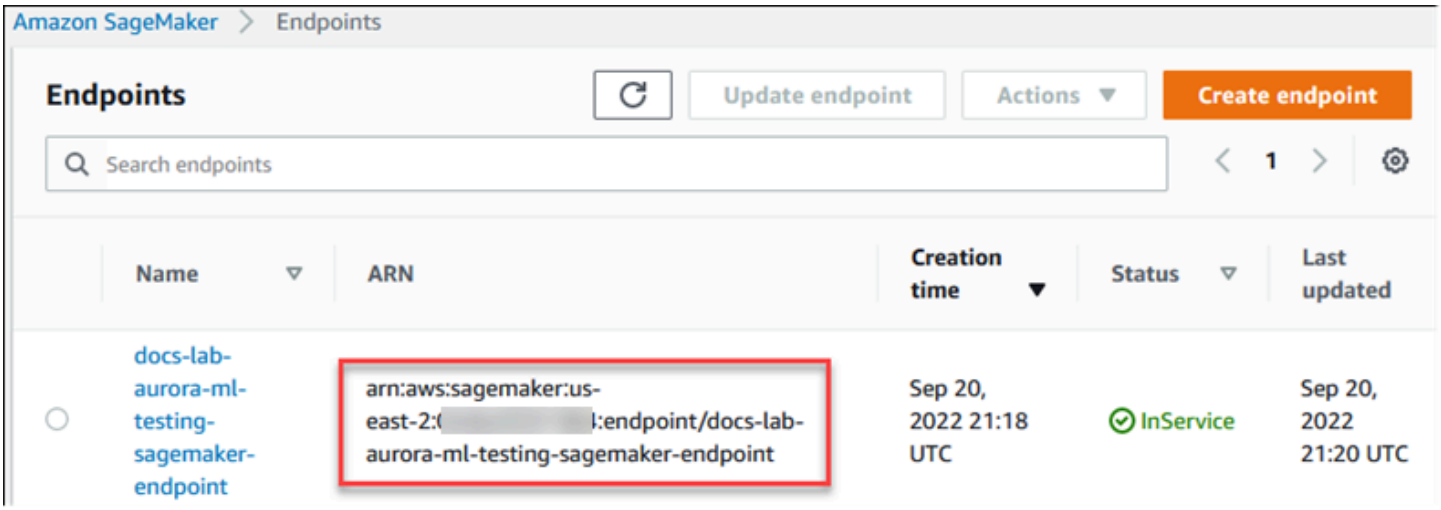


Starten Sie die primäre Instance Ihres DB-Clusters von Aurora MySQL neu, damit diese Parametereinstellung wirksam wird.

Die IAM-Integration für Amazon Comprehend ist abgeschlossen. Fahren Sie mit der Einrichtung Ihres DB-Clusters von Aurora MySQL zur Zusammenarbeit mit Amazon Comprehend fort, indem Sie den entsprechenden Datenbankbenutzern Zugriff gewähren.

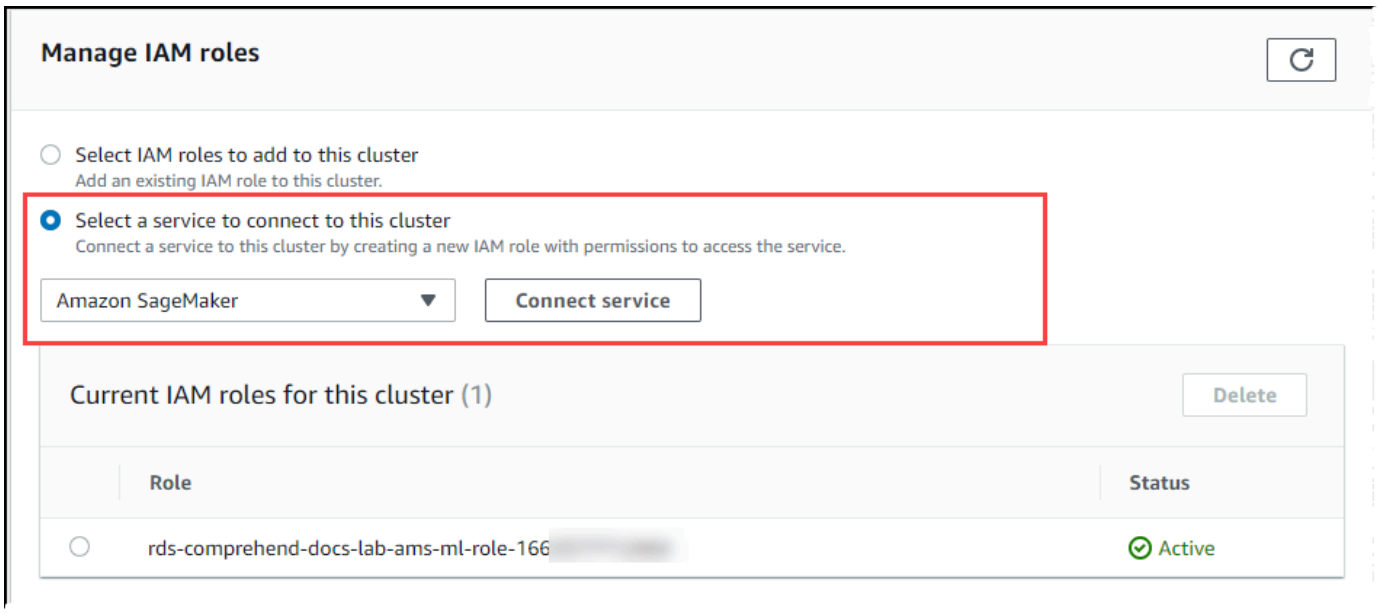
Einrichtung Ihres Aurora MySQL-DB-Clusters zur Verwendung SageMaker

Das folgende Verfahren erstellt automatisch die IAM-Rolle und -Richtlinie für Ihren Aurora MySQL-DB-Cluster, sodass er sie verwenden SageMaker kann. Bevor Sie versuchen, dieses Verfahren zu befolgen, stellen Sie sicher, dass Sie den SageMaker Endpunkt verfügbar haben, damit Sie ihn bei Bedarf eingeben können. In der Regel ist es Aufgabe der Datenwissenschaftler in Ihrem Team, einen Endpunkt zu erstellen, den Sie von Ihrem DB-Cluster von Aurora MySQL aus verwenden können. Sie finden solche Endpunkte in der SageMaker Konsole. Öffnen Sie im Navigationsbereich das Menü Inference (Inferenz) und wählen Sie Endpoints (Endpunkte) aus. Die folgende Abbildung zeigt ein Beispiel.

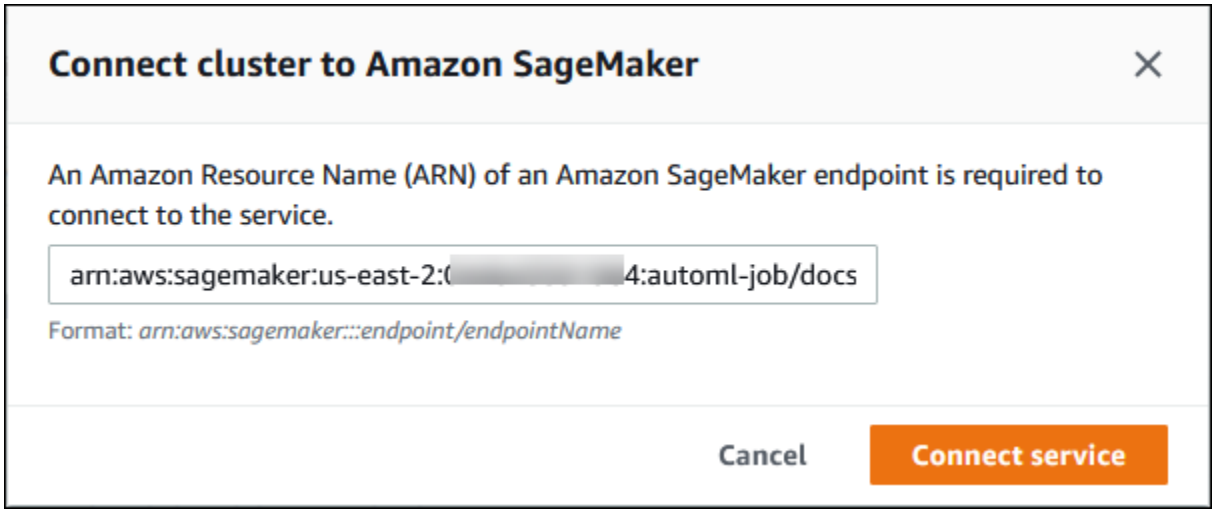


So richten Sie Ihren Aurora MySQL-DB-Cluster zur Verwendung ein SageMaker

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie Datenbanken aus dem Amazon RDS-Navigationsmenü und wählen Sie dann den Aurora MySQL-DB-Cluster aus, den Sie mit SageMaker Services verbinden möchten.
3. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit).
4. Wählen Sie Select a service to connect to this cluster (Auswahl eines Services zur Verbindung mit diesem Cluster) im Abschnitt Manage IAM roles (IAM-Rollen verwalten) aus. Wählen Sie SageMakeraus dem Selektor.



5. Wählen Sie Connect Service (Service verbinden).
6. Geben Sie im SageMaker Dialogfeld Cluster verbinden mit den ARN des SageMaker Endpunkts ein.



7. Aurora erstellt die IAM-Rolle. Es erstellt auch die Richtlinie, die es dem Aurora MySQL-DB-Cluster ermöglicht, SageMaker Dienste zu nutzen, und fügt die Richtlinie der Rolle hinzu. Wenn der Vorgang abgeschlossen ist, wird die Rolle in der Liste Current IAM roles for this cluster (Aktuelle IAM-Rollen für diesen Cluster) angezeigt.
8. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
9. Wählen Sie Roles (Rollen) aus dem Abschnitt „Access management“ (Zugriffsverwaltung) des Navigationsmenüs von AWS Identity and Access Management aus.
10. Suchen Sie die Rolle in der Liste. Der Name verwendet das folgende Format.

```
rds-sagemaker-your-cluster-name-role-auto-generated-digits
```

11. Öffnen Sie die Seite „Summary“ (Zusammenfassung) der Rolle und suchen Sie den ARN. Notieren Sie sich den ARN oder kopieren Sie ihn mit dem Widget „Copy“ (Kopieren).
12. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
13. Wählen Sie Ihren DB-Cluster von Aurora MySQL und dann die Registerkarte Configuration (Konfiguration) aus.
14. Suchen Sie die DB-Cluster-Parametergruppe und wählen Sie den Link zum Öffnen Ihrer benutzerdefinierten DB-Cluster-Parametergruppe aus. Suchen Sie den `aws_default_sagemaker_role`-Parameter und geben Sie den ARN der IAM-Rolle in das Feld „Value“ (Wert) ein. Speichern Sie die Einstellung mit „Save“ (Speichern).
15. Starten Sie die primäre Instance Ihres DB-Clusters von Aurora MySQL neu, damit diese Parametereinstellung wirksam wird.

Die IAM-Einrichtung ist damit abgeschlossen. Setzen Sie die Einrichtung Ihres Aurora MySQL-DB-Clusters fort, mit dem Sie arbeiten können, SageMaker indem Sie den entsprechenden Datenbankbenutzern Zugriff gewähren.

Wenn Sie Ihre SageMaker Modelle für Schulungen verwenden möchten, anstatt vorgefertigte SageMaker Komponenten zu verwenden, müssen Sie auch den Amazon S3 S3-Bucket zu Ihrem Aurora MySQL-DB-Cluster hinzufügen, wie im Einrichtung Ihres Aurora MySQL-DB-Clusters für die Verwendung von Amazon S3 SageMaker (optional) Folgenden beschrieben.

Einrichtung Ihres Aurora MySQL-DB-Clusters für die Verwendung von Amazon S3 SageMaker (optional)

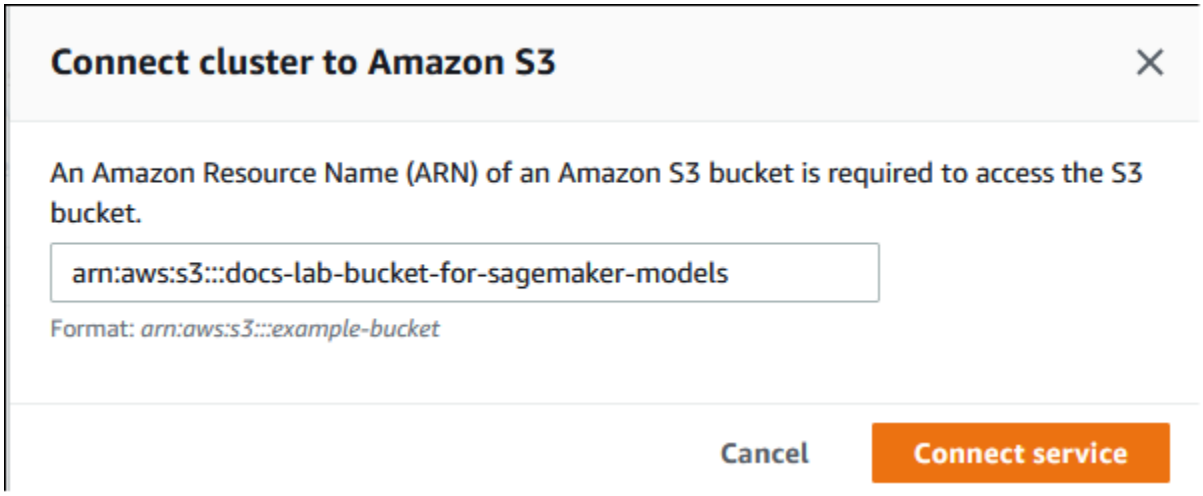
Für die Verwendung SageMaker mit Ihren eigenen Modellen, anstatt die von bereitgestellten vorgefertigten Komponenten zu verwenden SageMaker, müssen Sie einen Amazon S3 S3-Bucket einrichten, den der Aurora MySQL-DB-Cluster verwenden kann. Weitere Informationen zum Erstellen eines Amazon-S3-Buckets finden Sie unter Erstellen von Buckets im Handbuch für Amazon Simple Storage Service.

So richten Sie Ihren Aurora MySQL-DB-Cluster für die Verwendung eines Amazon S3 S3-Buckets ein SageMaker

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.

2. Wählen Sie Datenbanken aus dem Amazon RDS-Navigationsmenü und wählen Sie dann den Aurora MySQL-DB-Cluster aus, den Sie mit SageMaker Services verbinden möchten.
3. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit).
4. Wählen Sie Select a service to connect to this cluster (Auswahl eines Services zur Verbindung mit diesem Cluster) im Abschnitt Manage IAM roles (IAM-Rollen verwalten) aus. Wählen Sie Amazon S3 in der Auswahl aus.

5. Wählen Sie Connect Service (Service verbinden).
6. Geben Sie im Dialogfeld Cluster mit Amazon S3 verbinden den ARN des Amazon S3 S3-Buckets ein, wie in der folgenden Abbildung gezeigt.



7. Wählen Sie Connect service (Service verbinden) aus, um den Integrationsvorgang abzuschließen.

Weitere Informationen zur Verwendung von Amazon S3 S3-Buckets mit SageMaker finden Sie unter Spezifizieren eines Amazon S3 S3-Buckets zum Hochladen von Trainingsdatensätzen und Speichern von Ausgabedaten im Amazon SageMaker Developer Guide. Weitere Informationen zur Arbeit mit SageMaker finden Sie unter Erste Schritte mit Amazon SageMaker Notebook-Instances im Amazon SageMaker Developer Guide.

Erteilen des Zugriffs auf Aurora Machine Learning für Datenbankbenutzer

Datenbankbenutzern muss die Erlaubnis erteilt werden, Aurora-Funktionen für maschinelles Lernen aufzurufen. Wie Sie Berechtigungen erteilen, hängt von der MySQL-Version ab, die Sie für Ihren DB-Cluster von Aurora MySQL verwenden, wie im Folgenden beschrieben. Wie Sie diesen Vorgang ausführen, hängt von der MySQL-Version ab, die Ihr DB-Cluster von Aurora MySQL verwendet.

- Für Aurora MySQL Version 3 (MySQL 8.0-kompatibel) muss Datenbankbenutzern die entsprechende Datenbankrolle zugewiesen werden. Weitere Informationen finden Sie unter Rollen verwenden im MySQL 8.0-Referenzhandbuch.
- Für Aurora MySQL Version 2 (MySQL 5.7-kompatibel) werden Datenbankbenutzern Rechte gewährt. Weitere Informationen finden Sie unter Zugriffskontrolle und Kontoverwaltung im MySQL 5.7-Referenzhandbuch.

Die folgende Tabelle zeigt die Rollen und Rechte, die Datenbankbenutzer benötigen, um mit Funktionen für maschinelles Lernen zu arbeiten.

Aurora MySQL Version 3 (Rolle)	Aurora MySQL Version 2 (Privileg)
AWS_BEDROCK_ACCESS	–
AWS_COMPREHEND_ACCESS	INVOKE COMPREHEND
AWS_SAGEMAKER_ACCESS	INVOKE SAGEMAKER

Zugriff auf Amazon Bedrock-Funktionen gewähren

Verwenden Sie die folgende SQL-Anweisung, um Datenbankbenutzern Zugriff auf Amazon Bedrock-Funktionen zu gewähren:

```
GRANT AWS_BEDROCK_ACCESS TO user@domain-or-ip-address;
```

Datenbankbenutzern müssen auch `EXECUTE` Berechtigungen für die Funktionen erteilt werden, die Sie für die Arbeit mit Amazon Bedrock erstellen:

```
GRANT EXECUTE ON FUNCTION database_name.function_name TO user@domain-or-ip-address;
```

Schließlich müssen die Rollen der Datenbankbenutzer wie folgt festgelegt sein`AWS_BEDROCK_ACCESS`:

```
SET ROLE AWS_BEDROCK_ACCESS;
```

Die Funktionen von Amazon Bedrock können jetzt verwendet werden.

Erteilen des Zugriffs auf Amazon-Comprehend-Funktionen

Wenn Sie Datenbankbenutzern Zugriff auf Amazon-Comprehend-Funktionen erteilen möchten, verwenden Sie die entsprechende Anweisung für Ihre Aurora-MySQL-Version.

- Aurora-MySQL-Version 3 (mit MySQL 8.0 kompatibel)

```
GRANT AWS_COMPREHEND_ACCESS TO user@domain-or-ip-address;
```

- Aurora-MySQL-Version 2 (mit MySQL 5.7 kompatibel)

```
GRANT INVOKE COMPREHEND ON *.* TO user@domain-or-ip-address;
```

Die Amazon-Comprehend-Funktionen sind jetzt verfügbar. Anwendungsbeispiele finden Sie unter Verwenden von Amazon Comprehend mit Ihrem DB-Cluster von Aurora MySQL.

Zugriff auf Funktionen gewähren SageMaker

Um Datenbankbenutzern Zugriff auf SageMaker Funktionen zu gewähren, verwenden Sie die entsprechende Anweisung für Ihre Aurora MySQL-Version.

- Aurora-MySQL-Version 3 (mit MySQL 8.0 kompatibel)

```
GRANT AWS_SAGEMAKER_ACCESS TO user@domain-or-ip-address;
```

- Aurora-MySQL-Version 2 (mit MySQL 5.7 kompatibel)

```
GRANT INVOKE SAGEMAKER ON *.* TO user@domain-or-ip-address;
```

Datenbankbenutzern müssen außerdem EXECUTE Berechtigungen für die Funktionen erteilt werden, die Sie für die Arbeit mit ihnen erstellen SageMaker. Angenommen, Sie haben zwei Funktionen erstellt, `db1.anomoly_score` und`db2.company_forecasts`, um die Dienste Ihres SageMaker Endpunkts aufzurufen. Sie gewähren Ausführungsrechte, wie im folgenden Beispiel gezeigt.

```
GRANT EXECUTE ON FUNCTION db1.anomaly_score TO user1@domain-or-ip-address1;
GRANT EXECUTE ON FUNCTION db2.company_forecasts TO user2@domain-or-ip-address2;
```

Die SageMaker Funktionen können jetzt verwendet werden. Anwendungsbeispiele finden Sie unter Verwendung SageMaker mit Ihrem Aurora MySQL-DB-Cluster.

Amazon Bedrock mit Ihrem Aurora MySQL-DB-Cluster verwenden

Um Amazon Bedrock zu verwenden, erstellen Sie eine benutzerdefinierte Funktion (UDF) in Ihrer Aurora MySQL-Datenbank, die ein Modell aufruft. Weitere Informationen finden Sie unter Unterstützte Modelle in Amazon Bedrock im Amazon Bedrock-Benutzerhandbuch.

Eine UDF verwendet die folgende Syntax:

```
CREATE FUNCTION function_name (argument type)
        [DEFINER = user]
    RETURNS mysql_data_type
    [SQL SECURITY {DEFINER | INVOKER}]
    ALIAS AWS_BEDROCK_INVOKE_MODEL
    MODEL ID 'model_id'
    [CONTENT_TYPE 'content_type']
    [ACCEPT 'content_type']
    [TIMEOUT_MS timeout_in_milliseconds];
```

- Die Funktionen von Amazon Bedrock werden nicht unterstütztRETURNS JSON. Sie können CONVERT oder verwendenCAST, um bei JSON Bedarf von TEXT zu konvertieren.
- Wenn Sie CONTENT_TYPE oder nicht angebenACCEPT, ist die Standardeinstellungapplication/json.
- Wenn Sie nichts angebenTIMEOUT_MS, aurora_ml_inference_timeout wird der Wert für verwendet.

Die folgende UDF ruft beispielsweise das Amazon Titan Text Express-Modell auf:

```
CREATE FUNCTION invoke_titan (request_body TEXT)
    RETURNS TEXT
    ALIAS AWS_BEDROCK_INVOKE_MODEL
    MODEL ID 'amazon.titan-text-express-v1'
    CONTENT_TYPE 'application/json'
    ACCEPT 'application/json';
```

Verwenden Sie den folgenden SQL-Befehl, um einem DB-Benutzer die Verwendung dieser Funktion zu ermöglichen:

```
GRANT EXECUTE ON FUNCTION database_name.invoke_titan TO user@domain-or-ip-address;
```

Dann kann der Benutzer `invoke_titan` wie jede andere Funktion aufrufen, wie im folgenden Beispiel gezeigt. Achten Sie darauf, den Text der Anfrage gemäß den Textmodellen von Amazon Titan zu formatieren.

```
CREATE TABLE prompts (request varchar(1024));
INSERT INTO prompts VALUES (
'{
    "inputText": "Generate synthetic data for daily product sales in various categories
 - include row number, product name, category, date of sale and price. Produce output
 in JSON format. Count records and ensure there are no more than 5.",
    "textGenerationConfig": {
        "maxTokenCount": 1024,
        "stopSequences": [],
        "temperature":0,
        "topP":1
    }
}');

SELECT invoke_titan(request) FROM prompts;

{"inputTextTokenCount":44,"results":[{"tokenCount":296,"outputText":"
```tabular-data-json
{
    "rows": [
        {
            "Row Number": "1",
            "Product Name": "T-Shirt",
            "Category": "Clothing",
            "Date of Sale": "2024-01-01",
            "Price": "$20"
        },
        {
            "Row Number": "2",
            "Product Name": "Jeans",
            "Category": "Clothing",
            "Date of Sale": "2024-01-02",
            "Price": "$30"
        },
        {
            "Row Number": "3",
            "Product Name": "Hat",
            "Category": "Accessories",
            "Date of Sale": "2024-01-03",
```
```

```
            "Price": "$15"
        },
        {
            "Row Number": "4",
            "Product Name": "Watch",
            "Category": "Accessories",
            "Date of Sale": "2024-01-04",
            "Price": "$40"
        },
        {
            "Row Number": "5",
            "Product Name": "Phone Case",
            "Category": "Accessories",
            "Date of Sale": "2024-01-05",
            "Price": "$25"
        }
    ]
}
```","completionReason":"FINISH"}]}

Achten Sie bei anderen Modellen, die Sie verwenden, darauf, den Anfragetext entsprechend zu formatieren. Weitere Informationen finden Sie unter Inferenzparameter für Fundamentmodelle im Amazon Bedrock-Benutzerhandbuch.

Verwenden von Amazon Comprehend mit Ihrem DB-Cluster von Aurora MySQL

Für Aurora MySQL bietet Aurora Machine Learning die folgenden zwei integrierten Funktionen für die Arbeit mit Amazon Comprehend und Ihren Textdaten. Sie geben den zu analysierenden Text (`input_data`) und die Sprache (`language_code`) an.

aws_comprehend_detect_sentiment

Diese Funktion erkennt, dass der Text eine positive, negative, neutrale oder gemischte emotionale Haltung hat. Die Referenzdokumentation dieser Funktion lautet wie folgt.

```
aws_comprehend_detect_sentiment(
  input_text,
  language_code
  [,max_batch_size]
)
```

Weitere Informationen finden Sie unter Stimmung im Entwicklerhandbuch für Amazon Comprehend.

aws_comprehend_detect_sentiment_confidence

Diese Funktion misst den Wahrscheinlichkeitsgrad der für einen bestimmten Text erkannten Stimmung. Sie gibt einen Wert (Typ, `double`) zurück, der die Wahrscheinlichkeit der Stimmung angibt, die dem Text von der aws_comprehend_detect_sentiment-Funktion zugewiesen wurde. Die Wahrscheinlichkeit ist eine statistische Metrik zwischen 0 und 1. Je höher der Wahrscheinlichkeitsgrad ist, desto stärker können Sie das Ergebnis gewichten. Eine Zusammenfassung der Dokumentation der Funktion lautet wie folgt.

```
aws_comprehend_detect_sentiment_confidence(
  input_text,
  language_code
  [,max_batch_size]
)
```

In beiden Funktionen (aws_comprehend_detect_sentiment_confidence, aws_comprehend_detect_sentiment) verwendet `max_batch_size` den Standardwert 25, wenn kein Wert angegeben ist. Die Batch-Größe sollte immer größer als 0 sein. Sie können `max_batch_size` zur Optimierung der Leistung der Amazon-Comprehend-Funktionsaufrufe verwenden. Große Stapel bieten schnellere Leistung bei gleichzeitig höherer Speichernutzung auf dem DB-Cluster von Aurora MySQL. Weitere Informationen finden Sie unter Leistungsaspekte zur Verwendung von Aurora Machine Learning mit Aurora MySQL.

Weitere Informationen zu Parametern und Rückgabetypen für die Stimmungserkennungsfunktionen in Amazon Comprehend finden Sie unter DetectSentiment

Example Beispiel: Eine einfache Abfrage mit Amazon-Comprehend-Funktionen

Hier ist ein Beispiel für eine einfache Abfrage, die diese beiden Funktionen aufruft, um festzustellen, wie zufrieden Ihre Kunden mit Ihrem Support-Team sind. Angenommen, Sie haben eine Datenbanktabelle (`support`), in der Kundenfeedback nach jeder Supportanfrage gespeichert wird. Diese Beispielabfrage wendet beide integrierten Funktionen auf den Text in der `feedback`-Spalte der Tabelle an und gibt die Ergebnisse aus. Die von der Funktion zurückgegebenen Wahrscheinlichkeitswerte sind Doppelwerte zwischen 0,0 und 1,0. Für eine besser lesbare Ausgabe rundet diese Abfrage die Ergebnisse auf 6 Dezimalstellen auf. Diese Abfrage sortiert außerdem

die Ergebnisse in absteigender Reihenfolge, angefangen mit dem Ergebnis mit dem höchsten Wahrscheinlichkeitsgrad, um Vergleiche einfacher zu gestalten.

```
SELECT feedback AS 'Customer feedback',
    aws_comprehend_detect_sentiment(feedback, 'en') AS Sentiment,
    ROUND(aws_comprehend_detect_sentiment_confidence(feedback, 'en'), 6)
    AS Confidence FROM support
    ORDER BY Confidence DESC;
+-----------------------------------------------------------+-----------+------------+
| Customer feedback                                         | Sentiment | Confidence |
+-----------------------------------------------------------+-----------+------------+
| Thank you for the excellent customer support!             | POSITIVE  |   0.999771 |
| The latest version of this product stinks!                | NEGATIVE  |   0.999184 |
| Your support team is just awesome! I am blown away.       | POSITIVE  |   0.997774 |
| Your product is too complex, but your support is great.   | MIXED     |   0.957958 |
| Your support tech helped me in fifteen minutes.           | POSITIVE  |   0.949491 |
| My problem was never resolved!                            | NEGATIVE  |   0.920644 |
| When will the new version of this product be released?    | NEUTRAL   |   0.902706 |
| I cannot stand that chatbot.                              | NEGATIVE  |   0.895219 |
| Your support tech talked down to me.                      | NEGATIVE  |   0.868598 |
| It took me way too long to get a real person.             | NEGATIVE  |   0.481805 |
+-----------------------------------------------------------+-----------+------------+
 10 rows in set (0.1898 sec)
```

Example Beispiel: Ermitteln der durchschnittlichen Stimmung für Text oberhalb eines bestimmten Wahrscheinlichkeitsgrads

Eine typische Amazon Comprehend-Abfrage sucht nach Zeilen, auf denen die Stimmung einen bestimmten Wert hat, mit einem Zuverlässigkeitsniveau, das über einem bestimmten numerischen Wert liegt. Beispielsweise zeigt die folgende Abfrage, wie Sie die durchschnittliche Stimmung in Dokumenten in Ihrer Datenbank feststellen können. Die Abfrage berücksichtigt nur Dokumente mit einer Feststellungszuverlässigkeit von mindestens 80 %.

```
SELECT AVG(CASE aws_comprehend_detect_sentiment(productTable.document, 'en')
  WHEN 'POSITIVE' THEN 1.0
  WHEN 'NEGATIVE' THEN -1.0
  ELSE 0.0 END) AS avg_sentiment, COUNT(*) AS total
FROM productTable
WHERE productTable.productCode = 1302 AND
    aws_comprehend_detect_sentiment_confidence(productTable.document, 'en') >= 0.80;
```

Verwendung SageMaker mit Ihrem Aurora MySQL-DB-Cluster

Um SageMaker Funktionen aus Ihrem Aurora MySQL-DB-Cluster nutzen zu können, müssen Sie gespeicherte Funktionen erstellen, die Ihre Aufrufe an den SageMaker Endpunkt und seine Inferenzfunktionen einbetten. Verwenden Sie dazu `CREATE FUNCTION` von MySQL im Prinzip auf die gleiche Weise wie für andere Verarbeitungsaufgaben auf Ihrem DB-Cluster von Aurora MySQL.

Um Modelle zu verwenden, die SageMaker für Inferenz bereitgestellt werden, erstellen Sie benutzerdefinierte Funktionen mithilfe von MySQL Data Definition Language (DDL) -Anweisungen für gespeicherte Funktionen. Jede gespeicherte Funktion stellt den SageMaker Endpunkt dar, der das Modell hostet. Wenn Sie eine solche Funktion definieren, geben Sie die Eingabeparameter für das Modell, den spezifischen SageMaker Endpunkt, der aufgerufen werden soll, und den Rückgabetyp an. Die Funktion gibt die vom SageMaker Endpunkt berechnete Inferenz zurück, nachdem das Modell auf die Eingabeparameter angewendet wurde.

Alle gespeicherten Aurora Machine Learning-Funktionen geben numerische Typen oder zurüc `VARCHAR`. Sie können alle numerischen Typen außer verwende `BIT`. Andere Typen wie etwa `JSON`, `BLOB`, `TEXT` oder `DATE` sind nicht zulässig.

Das folgende Beispiel zeigt die `CREATE FUNCTION` Syntax für die Arbeit mit. SageMaker

```
CREATE FUNCTION function_name (
     arg1 type1,
     arg2 type2, ...)
     [DEFINER = user]
  RETURNS mysql_type
  [SQL SECURITY { DEFINER | INVOKER } ]
  ALIAS AWS_SAGEMAKER_INVOKE_ENDPOINT
  ENDPOINT NAME 'endpoint_name'
  [MAX_BATCH_SIZE max_batch_size];
```

Dies ist eine Erweiterung der regulären `CREATE FUNCTION`-DDL-Anweisung. In der `CREATE FUNCTION` Anweisung, die die SageMaker Funktion definiert, geben Sie keinen Funktionskörper an. Stattdessen geben Sie das Schlüsselwort `ALIAS` dort an, wo normalerweise der Funktionstext steht. Derzeit unterstützt Aurora Machine Learning nur `aws_sagemaker_invoke_endpoint` für diese erweiterte Syntax. Sie müssen den Parameter `endpoint_name` angeben. Ein SageMaker Endpunkt kann für jedes Modell unterschiedliche Eigenschaften haben.

> **Note**
>
> Weitere Informationen zu `CREATE FUNCTION` finden Sie unter CREATE PROCEDURE- und CREATE FUNCTION-Anweisungen im MySQL-8.0-Referenzhandbuch.

Der Parameter `max_batch_size` ist optional. Standardmäßig beträgt die maximale Stapelgröße 10 000. Sie können diesen Parameter in Ihrer Funktion verwenden, um die maximale Anzahl der in einer Batch-Anfrage verarbeiteten Eingaben auf zu SageMaker beschränken. Der `max_batch_size` Parameter kann dazu beitragen, Fehler zu vermeiden, die durch zu große Eingaben verursacht werden, oder dazu, dass schneller eine Antwort SageMaker zurückgegeben wird. Dieser Parameter beeinflusst die Größe eines internen Puffers, der für die SageMaker Anforderungsverarbeitung verwendet wird. Die Angabe eines zu großen Werts für `max_batch_size` kann zu erheblicher Speicherüberlastung auf Ihrer DB-Instance führen.

Wir empfehlen Ihnen, für die Einstellung `MANIFEST` den Standardwert `OFF` zu belassen. Sie können die `MANIFEST ON` Option zwar verwenden, aber einige SageMaker Funktionen können die mit dieser Option exportierte CSV nicht direkt verwenden. Das Manifestformat ist nicht kompatibel mit dem erwarteten Manifestformat von SageMaker.

Sie erstellen für jedes Ihrer SageMaker Modelle eine separate gespeicherte Funktion. Dieses Mapping von Funktionen zu Modellen ist erforderlich, da ein Endpunkt mit einem spezifischen Modell verbunden ist und jedes Modell unterschiedliche Parameter akzeptiert. Die Verwendung von SQL-Typen für die Modelleingaben und den Modellausgabetyp trägt dazu bei, Typkonvertierungsfehler bei der Übertragung von Daten zwischen den AWS Diensten zu vermeiden. Sie können steuern, wer das Modell anwenden kann. Sie können auch die Laufzeiteigenschaften steuern, indem Sie einen Parameter angeben, der für die maximale Stapelgröße steht.

Derzeit haben alle Aurora Machine Learning-Funktionen die `NOT DETERMINISTIC`-Eigenschaft. Wenn Sie diese Eigenschaft nicht explizit angeben, richtet Aurora `NOT DETERMINISTIC` automatisch ein. Diese Anforderung besteht darin, dass das SageMaker Modell ohne Benachrichtigung an die Datenbank geändert werden kann. Wenn dies geschieht, führen Aufrufe an eine Aurora Machine Learning-Funktion möglicherweise zu unterschiedlichen Ergebnissen für gleiche Eingaben innerhalb einer einzigen Transaktion.

Sie können die Merkmale `CONTAINS SQL`, `NO SQL`, `READS SQL DATA` oder `MODIFIES SQL DATA` in Ihrer `CREATE FUNCTION`-Anweisung nicht verwenden.

Im Folgenden finden Sie ein Beispiel für die Verwendung des Aufrufs eines SageMaker Endpunkts zur Erkennung von Anomalien. Es gibt einen Endpunkt. SageMaker `random-cut-forest-model` Das entsprechende Modell wurde bereits durch den `random-cut-forest`-Algorithmus trainiert. Für jede Eingabe gibt das Modell einen Anomaliewert aus. Dieses Beispiel zeigt die Datenpunkte, deren Wert über 3 Standardabweichungen (etwa das 99,9-te Perzentil) vom Durchschnittsergebnis liegt.

```
CREATE FUNCTION anomaly_score(value real) returns real
  alias aws_sagemaker_invoke_endpoint endpoint name 'random-cut-forest-model-demo';

set @score_cutoff = (select avg(anomaly_score(value)) + 3 * std(anomaly_score(value))
 from nyc_taxi);

select *, anomaly_detection(value) score from nyc_taxi
  where anomaly_detection(value) > @score_cutoff;
```

Zeichensatzanforderung für SageMaker Funktionen, die Zeichenketten zurückgeben

Wir empfehlen, einen Zeichensatz von `utf8mb4` als Rückgabetyp für Ihre SageMaker Funktionen anzugeben, die Zeichenkettenwerte zurückgeben. Wenn dies nicht sinnvoll ist, verwenden Sie eine ausreichende Zeichenfolgenlänge, damit der Rückgabetyp einen im `utf8mb4`-Zeichensatz ausgedrückten Wert aufnehmen kann. Das folgende Beispiel illustriert die Angabe des `utf8mb4`-Zeichensatzes für Ihre Funktion.

```
CREATE FUNCTION my_ml_func(...) RETURNS VARCHAR(5) CHARSET utf8mb4 ALIAS ...
```

Derzeit verwendet jede SageMaker Funktion, die eine Zeichenfolge zurückgibt, den Zeichensatz `utf8mb4` als Rückgabewert. Der Rückgabewert verwendet diesen Zeichensatz, auch wenn Ihre SageMaker Funktion implizit oder explizit einen anderen Zeichensatz für ihren Rückgabetyp deklariert. Wenn Ihre SageMaker Funktion einen anderen Zeichensatz für den Rückgabewert deklariert, werden die zurückgegebenen Daten möglicherweise automatisch gekürzt, wenn Sie sie in einer Tabellenspalte speichern, die nicht lang genug ist. Beispielsweise erstellt eine Abfrage mit einer `DISTINCT`-Klausel eine temporäre Tabelle. Daher kann das SageMaker Funktionsergebnis aufgrund der Art und Weise, wie Zeichenketten während einer Abfrage intern behandelt werden, gekürzt werden.

Exportieren von Daten nach Amazon S3 für SageMaker Modelltraining (Fortgeschritten)

Wir empfehlen Ihnen, mit Aurora Machine Learning zu beginnen und SageMaker einige der bereitgestellten Algorithmen zu verwenden und dass die Datenwissenschaftler in Ihrem Team Ihnen die SageMaker Endpunkte zur Verfügung stellen, die Sie mit Ihrem SQL-Code verwenden können. Im Folgenden finden Sie minimale Informationen zur Verwendung Ihres eigenen Amazon S3 S3-Buckets mit Ihren eigenen SageMaker Modellen und Ihrem Aurora MySQL-DB-Cluster.

Machine Learning besteht aus zwei Hauptschritten: Training und Inferenz. Um SageMaker Modelle zu trainieren, exportieren Sie Daten in einen Amazon S3 S3-Bucket. Der Amazon S3 S3-Bucket wird von einer SageMaker Jupyter-Notebook-Instance verwendet, um Ihr Modell vor der Bereitstellung zu trainieren. Sie können die Anweisung `SELECT INTO OUTFILE S3` verwenden, um Daten aus einem Aurora MySQL-DB-Cluster abzufragen und sie direkt in Textdateien in einem Amazon S3-Bucket zu speichern. Anschließend verwendet die Notebook-Instance die Daten aus dem Amazon S3-Bucket für das Training.

Aurora Machine Learning erweitert die bestehende `SELECT INTO OUTFILE`-Syntax in Aurora MySQL zum Export von Daten im CSV-Format. Die generierte CSV-Datei kann direkt von Modellen verwendet werden, die dieses Format für Trainingszwecke benötigen.

```
SELECT * INTO OUTFILE S3 's3_uri' [FORMAT {CSV|TEXT} [HEADER]] FROM table_name;
```

Die Erweiterung unterstützt das Standard-CSV-Format.

- Format `TEXT` ist identisch mit dem bestehenden MySQL-Exportformat. Dies ist das Standardformat.
- Format `CSV` ist ein neu eingeführtes Format, das der Spezifikation in RFC-4180 folgt.
- Wenn Sie das optionale Schlüsselwort `HEADER` angeben, enthält die Ausgabedatei eine Kopfzeile. Die Beschriftungen in der Kopfzeile entsprechen den Spaltennamen aus der `SELECT`-Anweisung.
- Sie können die Schlüsselwörter `CSV` und `HEADER` weiterhin als Kennungen verwenden.

Die erweiterte Syntax und Grammatik von `SELECT INTO` sind jetzt wie folgt.

```
INTO OUTFILE S3 's3_uri'
[CHARACTER SET charset_name]
[FORMAT {CSV|TEXT} [HEADER]]
[{FIELDS | COLUMNS}
```

```
  [TERMINATED BY 'string']
  [[OPTIONALLY] ENCLOSED BY 'char']
  [ESCAPED BY 'char']
]
[LINES
  [STARTING BY 'string']
  [TERMINATED BY 'string']
]
```

Leistungsaspekte zur Verwendung von Aurora Machine Learning mit Aurora MySQL

Amazon Bedrock, Amazon Comprehend und die SageMaker Dienste erledigen den Großteil der Arbeit, wenn sie von einer Aurora-Funktion für maschinelles Lernen aufgerufen werden. Das bedeutet, dass Sie diese Ressourcen nach Bedarf unabhängig voneinander skalieren können. Für Ihren DB-Cluster von Aurora MySQL können Sie Ihre Funktionsaufrufe so effizient wie möglich gestalten. Im Folgenden finden Sie einige Leistungsaspekte, die Sie bei der Arbeit mit Aurora Machine Learning beachten sollten.

Modell und Aufforderung

Die Leistung bei der Verwendung von Amazon Bedrock hängt stark vom Modell und der verwendeten Eingabeaufforderung ab. Wählen Sie ein Modell und eine Aufforderung, die für Ihren Anwendungsfall optimal sind.

Abfrage-Cache

Der Abfrage-Cache von Aurora MySQL funktioniert nicht für Aurora-Funktionen für Machine Learning. Aurora MySQL speichert keine Abfrageergebnisse im Abfrage-Cache für SQL-Anweisungen, die Aurora-Funktionen für Machine Learning aufrufen.

Batch-Optimierung für Aurora-Machine-Learning-Funktionsaufrufe

Der wichtigste Aurora Machine Learning-Performanceaspekt, den Sie von Ihrem Aurora-Cluster aus beeinflussen können, ist die Batch-Moduseinstellung für Aufrufe der gespeicherten Aurora-Machine-Learning-Funktion. Machine-Learning-Funktionen erfordern in der Regel einen erheblichen Overhead, was es unpraktisch macht, einen externen Service für jede Zeile separat aufzurufen. Aurora Machine Learning kann diesen Overhead minimieren, indem die Aufrufe des externen Aurora-Machine-Learning-Services für viele Zeilen in einem einzigen Batch zusammengefasst werden. Aurora Machine Learning empfängt die Antworten für alle Eingabezeilen und liefert die Antworten

Zeile für Zeile an die Abfrage, während sie ausgeführt wird. Diese Optimierung verbessert den Durchsatz und die Latenz für Ihre Aurora-Abfragen ohne Änderungen bei den Ergebnissen.

Wenn Sie eine gespeicherte Aurora-Funktion erstellen, die mit einem SageMaker Endpunkt verbunden ist, definieren Sie den Batchgröße-Parameter. Dieser Parameter beeinflusst, wie viele Zeilen für jeden zugrunde liegenden Aufruf an übertragen werden SageMaker. Bei Abfragen, die eine große Anzahl von Zeilen verarbeiten, kann der Aufwand, für jede Zeile einen separaten SageMaker Aufruf durchzuführen, erheblich sein. Je größer der von der gespeicherten Prozedur verarbeitete Datensatz ist, umso größer kann die Stapelgröße gewählt werden.

Ob die Optimierung im Batchmodus auf eine SageMaker Funktion angewendet werden kann, können Sie anhand des durch die `EXPLAIN PLAN` Anweisung erstellten Abfrageplans feststellen. In diesem Fall enthält die `extra`-Spalte in dem Ausführungsplan `Batched machine learning`. Das folgende Beispiel zeigt den Aufruf einer SageMaker Funktion, die den Batch-Modus verwendet.

```
mysql> CREATE FUNCTION anomaly_score(val real) returns real alias
 aws_sagemaker_invoke_endpoint endpoint name 'my-rcf-model-20191126';
Query OK, 0 rows affected (0.01 sec)

mysql> explain select timestamp, value, anomaly_score(value) from nyc_taxi;
+----+-------------+----------+------------+------+---------------+------+---------
+------+------+----------+-------------------------+
| id | select_type | table    | partitions | type | possible_keys | key  | key_len |
 ref  | rows | filtered | Extra                   |
+----+-------------+----------+------------+------+---------------+------+---------
+------+------+----------+-------------------------+
|  1 | SIMPLE      | nyc_taxi | NULL       | ALL  | NULL          | NULL | NULL    |
 NULL |   48 |   100.00 | Batched machine learning |
+----+-------------+----------+------------+------+---------------+------+---------
+------+------+----------+-------------------------+
1 row in set, 1 warning (0.01 sec)
```

Wenn Sie eine der integrierten Amazon Comprehend-Funktionen aufrufen, können Sie die Stapelgröße steuern, indem Sie den optionalen `max_batch_size`-Parameter angeben. Dieser Parameter schränkt die maximale Anzahl der in jedem Stapel verarbeiteten `input_text`-Werte ein. Wenn mehrere Elemente gleichzeitig gesendet werden, reduziert dies die Anzahl der Wiederholungen zwischen Aurora und Amazon Comprehend. Die Begrenzung der Stapelgröße ist in verschiedenen Situationen sinnvoll, etwa bei einer Abfrage mit einer `LIMIT`-Klausel. Durch die Verwendung eines kleineren Wertes für `max_batch_size` vermeiden Sie, dass Amazon Comprehend häufiger aufgerufen wird als Eingabetexte vorhanden sind.

Die Batchoptimierung für die Evaluierung von Aurora-Machine-Learning-Funktionen gilt in den folgenden Fällen:

- Funktionsaufrufen innerhalb der Auswahlliste oder der `WHERE` `SELECT` Anweisungsklausel
- Funktionsaufrufe in der `VALUES` Liste der `INSERT` `REPLACE` AND-Anweisungen
- SageMaker Funktionen in `SET` Werten in `UPDATE` Anweisungen:

```
INSERT INTO MY_TABLE (col1, col2, col3) VALUES
  (ML_FUNC(1), ML_FUNC(2), ML_FUNC(3)),
  (ML_FUNC(4), ML_FUNC(5), ML_FUNC(6));
UPDATE MY_TABLE SET col1 = ML_FUNC(col2), SET col3 = ML_FUNC(col4) WHERE ...;
```

Überwachung von Aurora Machine Learning

Sie können die Batchoperationen für maschinelles Lernen in Aurora überwachen, indem Sie mehrere globale Variablen abfragen, wie im folgenden Beispiel gezeigt.

```
show status like 'Aurora_ml%';
```

Sie können die Statusvariablen mit einer `FLUSH STATUS`-Anweisung zurücksetzen. So stehen alle Zahlen für Gesamtwerte, Durchschnittswerte usw. seit der letzten Zurücksetzung der Variablen.

`Aurora_ml_logical_request_cnt`

Die Anzahl der logischen Anfragen, die die DB-Instance seit dem letzten Status-Reset zum Senden an die Aurora-Machine-Learning-Services ausgewertet hat. Je nachdem, ob Stapelverarbeitung verwendet wurde, kann dieser Wert höher sein als `Aurora_ml_actual_request_cnt`.

`Aurora_ml_logical_response_cnt`

Die aggregierte Zahl der Antworten, die Aurora MySQL von den Machine-Learning-Services von Aurora über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg erhält.

`Aurora_ml_actual_request_cnt`

Die aggregierte Zahl der Anfragen, die Aurora MySQL an die Machine-Learning-Services von Aurora über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg stellt.

`Aurora_ml_actual_response_cnt`

Die aggregierte Zahl der Antworten, die Aurora MySQL von den Machine-Learning-Services von Aurora über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg erhält.

`Aurora_ml_cache_hit_cnt`

Die aggregierte Zahl der internen Cache-Treffer, die Aurora MySQL von den Machine-Learning-Services von Aurora über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg erhält.

`Aurora_ml_retry_request_cnt`

Die Anzahl der wiederholten Anfragen, die die DB-Instance seit dem letzten Status-Reset an die Aurora-Machine-Learning-Services gesendet hat.

`Aurora_ml_single_request_cnt`

Die aggregierte Zahl der Machine-Learning-Funktionen von Aurora, die im Nicht-Batch-Modus über alle von Benutzern der DB-Instance durchgeführten Abfragen hinweg evaluiert werden.

Informationen zur Überwachung der Leistung von SageMaker Vorgängen, die von Aurora-Funktionen für maschinelles Lernen aufgerufen werden, finden Sie unter Amazon überwachen SageMaker.

Verwendung von Amazon Aurora Machine Learning mit Aurora PostgreSQL

Wenn Sie Amazon Aurora Machine Learning mit Ihrem Aurora PostgreSQL-DB-Cluster verwenden, können Sie je nach Bedarf Amazon Comprehend oder Amazon SageMaker oder Amazon Bedrock verwenden. Diese Services unterstützen jeweils spezifische Anwendungsfälle für maschinelles Lernen.

Aurora Machine Learning wird nur in bestimmten AWS-Regionen und für bestimmte Versionen von Aurora PostgreSQL unterstützt. Bevor Sie versuchen, Aurora Machine Learning einzurichten, überprüfen Sie die Verfügbarkeit Ihrer Aurora-PostgreSQL-Version und Ihrer Region. Details hierzu finden Sie unter Aurora Machine Learning mit Aurora PostgreSQL.

Themen

- Unterstützte Funktionen und Einschränkungen von Aurora Machine Learning mit Aurora PostgreSQL
- Einrichten Ihres DB-Clusters von Aurora PostgreSQL zur Verwendung von Aurora Machine Learning
- Verwenden von Amazon Bedrock mit Ihrem Aurora PostgreSQL-DB-Cluster
- Verwenden von Amazon Comprehend mit Ihrem DB-Cluster von Aurora PostgreSQL
- Verwendung SageMaker mit Ihrem Aurora PostgreSQL-DB-Cluster
- Exportieren von Daten nach Amazon S3 für SageMaker Modelltraining (Fortgeschritten)
- Leistungsaspekte zur Verwendung von Aurora Machine Learning mit Aurora PostgreSQL
- Überwachung von Aurora Machine Learning

Voraussetzungen für die Verwendung von Aurora Machine Learning mit Aurora PostgreSQL

AWS Dienste für maschinelles Lernen sind verwaltete Dienste, die in ihren eigenen Produktionsumgebungen eingerichtet und ausgeführt werden. Aurora Machine Learning unterstützt die Integration mit Amazon Comprehend und Amazon SageMaker Bedrock. Bevor Sie versuchen, Ihren DB-Cluster von Aurora PostgreSQL für die Verwendung von Aurora Machine Learning einzurichten, stellen Sie sicher, dass Sie die folgenden Anforderungen und Voraussetzungen verstehen.

- Die Amazon Comprehend- und Amazon Bedrock-Services müssen im selben System AWS-Region wie Ihr Aurora PostgreSQL-DB-Cluster ausgeführt werden. SageMaker Sie können Amazon Comprehend- SageMaker oder Amazon Bedrock-Services nicht von einem Aurora PostgreSQL-DB-Cluster in einer anderen Region aus verwenden.
- Wenn sich Ihr Aurora PostgreSQL-DB-Cluster in einer anderen Virtual Public Cloud (VPC) befindet, die auf dem Amazon VPC-Service basiert, als Ihr Amazon Comprehend und Ihre SageMaker Services, muss die Sicherheitsgruppe der VPC ausgehende Verbindungen zum Aurora-Zielservice für maschinelles Lernen zulassen. Weitere Informationen finden Sie unter Aktivieren der Netzwerkkommunikation von Amazon Aurora MySQL zu anderen AWS-Services.
- Denn die Komponenten des maschinellen Lernens SageMaker, die Sie für Inferenzen verwenden möchten, müssen eingerichtet und einsatzbereit sein. Während des Konfigurationsprozesses für Ihren Aurora PostgreSQL-DB-Cluster muss der Amazon-Ressourcenname (ARN) des SageMaker Endpunkts verfügbar sein. Die Datenwissenschaftler in Ihrem Team sind wahrscheinlich am

besten in der Lage, die Modelle vorzubereiten und die anderen Aufgaben dieser Art SageMaker zu erledigen. Informationen zu den ersten Schritten mit Amazon SageMaker finden Sie unter Erste Schritte mit Amazon SageMaker. Weitere Informationen zu Rückschlüssen und Endpunkten finden Sie unter Echtzeit-Inferenz.

- Für Amazon Bedrock müssen Sie die Modell-ID der Bedrock-Modelle, die Sie für Inferenzen verwenden möchten, während des Konfigurationsprozesses Ihres Aurora PostgreSQL-DB-Clusters zur Verfügung haben. Die Datenwissenschaftler in Ihrem Team sind wahrscheinlich am besten in der Lage, mit Bedrock zusammenzuarbeiten, um zu entscheiden, welche Modelle verwendet werden sollen, sie bei Bedarf zu verfeinern und andere solche Aufgaben zu erledigen. Informationen zu den ersten Schritten mit Amazon Bedrock finden Sie unter So richten Sie Bedrock ein.
- Amazon-Bedrock-Benutzer müssen den Zugriff auf Modelle anfordern, bevor sie verwendet werden können. Wenn Sie zusätzliche Modelle für die Text-, Chat- und Bildgenerierung hinzufügen möchten, müssen Sie den Zugriff auf Modelle in Amazon Bedrock anfordern. Weitere Informationen finden Sie unter Modellzugriff.

Unterstützte Funktionen und Einschränkungen von Aurora Machine Learning mit Aurora PostgreSQL

Aurora Machine Learning unterstützt jeden SageMaker Endpunkt, der das CSV-Format (Comma-Separated Value) lesen und schreiben kann, und zwar mit einem `ContentType` Wert von. `text/csv` Die integrierten SageMaker Algorithmen, die dieses Format derzeit akzeptieren, sind die folgenden.

- Lineares Lernen
- Random Cut Forest
- XGBoost

  Weitere Informationen zu diesen Algorithmen finden Sie unter Choose an Algorithm im Amazon SageMaker Developer Guide.

Bei der Verwendung von Amazon Bedrock mit Aurora Machine Learning gelten die folgenden Einschränkungen:

- Die benutzerdefinierten Funktionen (UDFs) bieten eine native Möglichkeit, mit Amazon Bedrock zu interagieren. Die UDFs haben keine spezifischen Anforderungen an Anfragen oder Antworten, sodass sie jedes Modell verwenden können.
- Sie können UDFs verwenden, um jeden gewünschten Workflow zu erstellen. Sie können beispielsweise Basis-Primitive kombinieren, `pg_cron` um beispielsweise eine Abfrage auszuführen, Daten abzurufen, Schlussfolgerungen zu generieren und in Tabellen zu schreiben, um Abfragen direkt zu bearbeiten.
- UDFs unterstützen keine gestapelten oder parallel Aufrufe.
- Die Aurora Machine Learning Learning-Erweiterung unterstützt keine Vektorschnittstellen. Als Teil der Erweiterung ist eine Funktion verfügbar, mit der die Einbettungen der Modellantwort in dem `float8[]` Format ausgegeben werden können, in dem diese Einbettungen in Aurora gespeichert werden. Weitere Informationen zur Verwendung von finden Sie unter. `float8[]` Verwenden von Amazon Bedrock mit Ihrem Aurora PostgreSQL-DB-Cluster

Einrichten Ihres DB-Clusters von Aurora PostgreSQL zur Verwendung von Aurora Machine Learning

Damit Aurora Machine Learning mit Ihrem Aurora PostgreSQL-DB-Cluster funktioniert, müssen Sie für jeden der Dienste, die Sie verwenden möchten, eine AWS Identity and Access Management (IAM-) Rolle erstellen. Die IAM-Rolle ermöglicht es Ihrem DB-Cluster von Aurora PostgreSQL, den Aurora-Dienst für Machine Learning im Namen des Clusters zu verwenden. Sie müssen auch die Aurora-Erweiterung für Machine Learning installieren. In den folgenden Themen finden Sie Einrichtungsverfahren für jeden dieser Aurora-Dienste für Machine Learning.

Themen

- Aurora PostgreSQL für die Verwendung von Amazon Bedrock einrichten
- Einrichten von Aurora PostgreSQL für die Verwendung von Amazon Comprehend
- Aurora PostgreSQL für die Nutzung von Amazon einrichten SageMaker
  - Aurora PostgreSQL für die Verwendung von Amazon S3 einrichten SageMaker (Fortgeschritten)
- Installieren der Aurora-Erweiterung für Machine Learning

Aurora PostgreSQL für die Verwendung von Amazon Bedrock einrichten

Im folgenden Verfahren erstellen Sie zunächst die IAM-Rolle und -Richtlinie, die Ihrem Aurora PostgreSQL die Erlaubnis geben, Amazon Bedrock im Namen des Clusters zu verwenden.

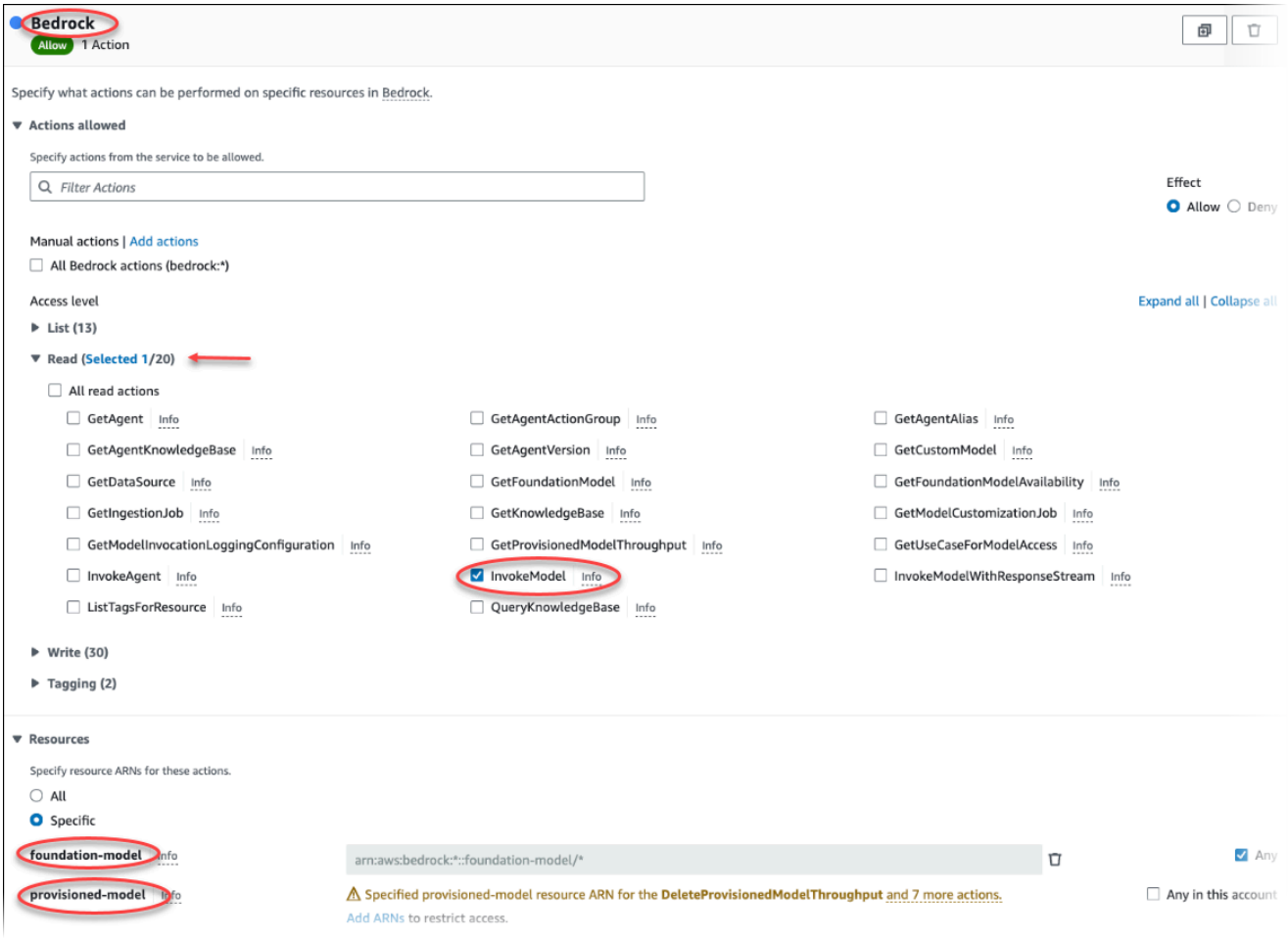
Anschließend fügen Sie die Richtlinie einer IAM-Rolle hinzu, die Ihr Aurora PostgreSQL-DB-Cluster für die Zusammenarbeit mit Amazon Bedrock verwendet. Der Einfachheit halber verwendet dieses Verfahren die, um alle Aufgaben AWS Management Console zu erledigen.

So richten Sie Ihren Aurora PostgreSQL-DB-Cluster für die Verwendung von Amazon Bedrock ein

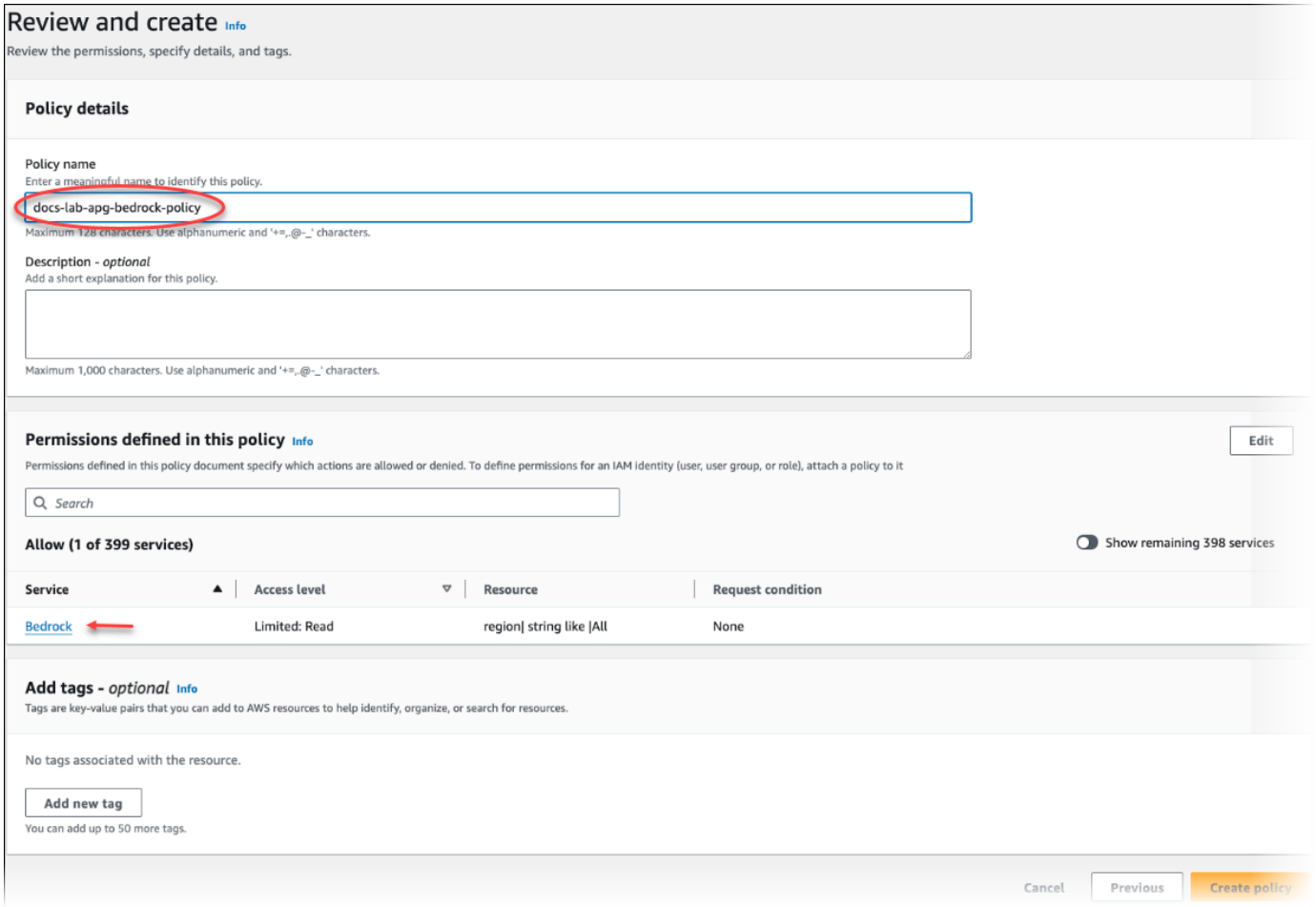
1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
3. Wählen Sie im Konsolenmenü (IAM) die Option Richtlinien AWS Identity and Access Management (unter Zugriffsverwaltung) aus.

    a. Wählen Sie Richtlinie erstellen aus. Wählen Sie auf der Visual Editor-Seite Service aus und geben Sie dann Bedrock in das Feld Service auswählen ein. Erweitern Sie die Lesezugriffsebene. Wählen Sie InvokeModelaus den Amazon Bedrock-Leseeinstellungen.

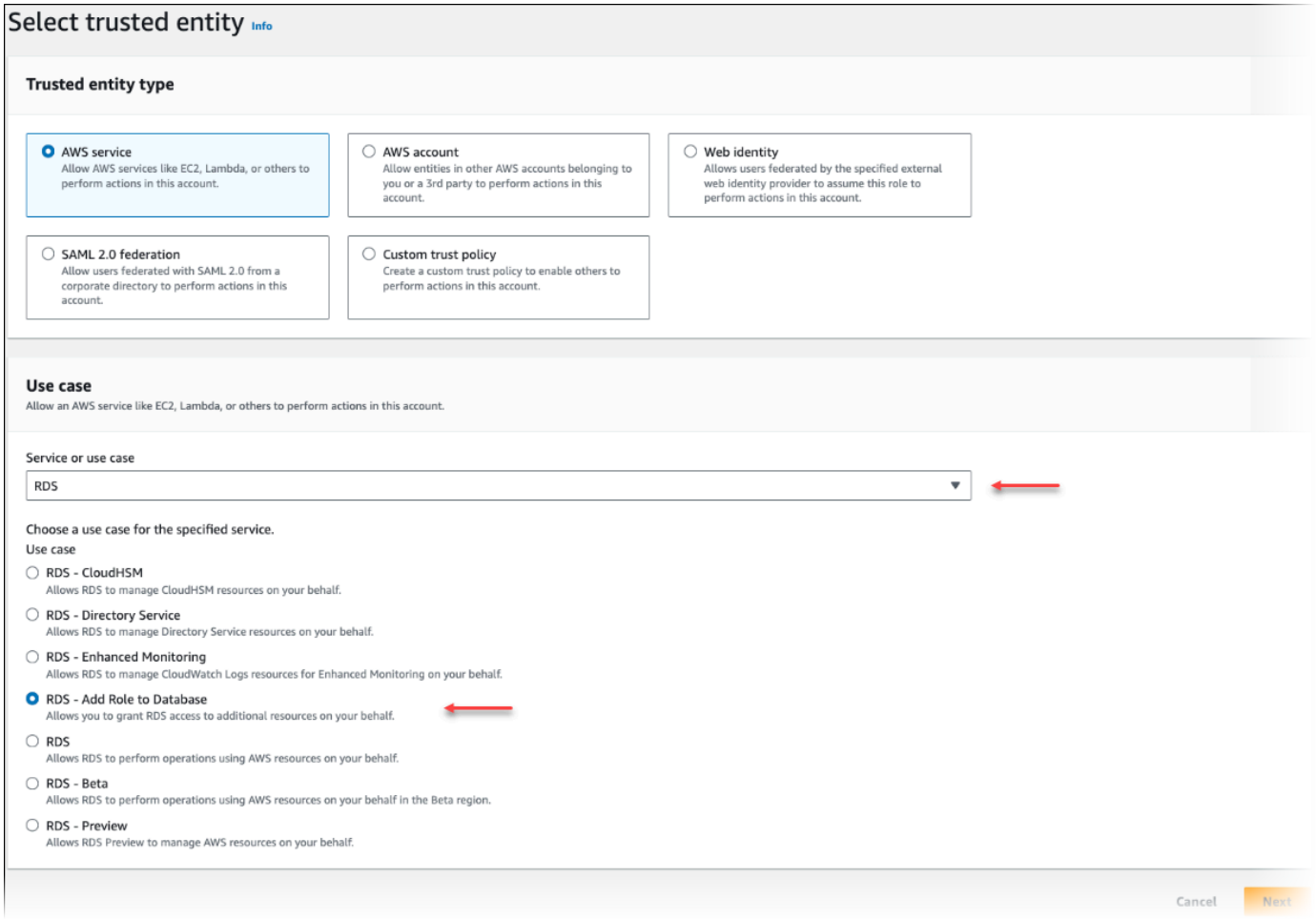
    b. Wählen Sie das Foundation/Provisioned-Modell aus, dem Sie über die Richtlinie Lesezugriff gewähren möchten.



4. Wählen Sie Next: Tags (Weiter: Tags) aus und definieren Sie Tags (dies ist optional). Wählen Sie Weiter: Prüfen aus. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein, wie in der Abbildung gezeigt.

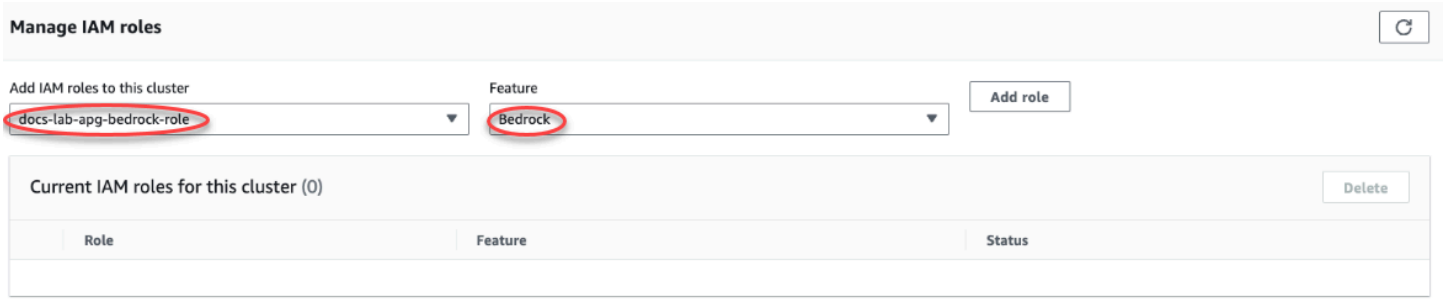


5. Wählen Sie Richtlinie erstellen aus. Die Konsole zeigt eine Warnung an, wenn die Richtlinie gespeichert wurde. Sie finden sie in der Liste der Richtlinien.
6. Wählen Sie in der IAM-Konsole die Option Roles (Rollen) (unter „Access management“ (Zugriffsverwaltung)) aus.
7. Wählen Sie Rolle erstellen aus.
8. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen die AWS Service-Kachel und dann RDS aus, um den Selektor zu öffnen.
9. Wählen Sie RDS – Add Role to Database (RDS – Rolle zu Datenbank hinzufügen) aus.



10. Wählen Sie Weiter aus. Suchen Sie auf der Seite „Add permissions“ (Berechtigungen hinzufügen) nach der im vorherigen Schritt erstellten Richtlinie und wählen Sie sie aus den aufgelisteten Richtlinien aus. Wählen Sie Weiter aus.
11. Next: Review (Weiter: Überprüfung). Geben Sie einen Namen und eine Beschreibung für die IAM-Rolle ein.
12. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
13. Navigieren Sie zu dem AWS-Region Ort, an dem sich Ihr Aurora PostgreSQL-DB-Cluster befindet.
14. Wählen Sie im Navigationsbereich Datenbanken und dann den Aurora PostgreSQL-DB-Cluster aus, den Sie mit Bedrock verwenden möchten.
15. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit) aus und scrollen Sie zum Abschnitt Manage IAM roles (IAM-Rollen verwalten) auf der Seite. Wählen Sie in der Auswahl Add IAM roles to this cluster (Diesem Cluster IAM-Rollen hinzufügen) die Rolle aus, die Sie in den vorherigen Schritten erstellt haben. Wählen Sie in der Funktionsauswahl Bedrock und dann Rolle hinzufügen aus.

Die Rolle ist (mit ihrer Richtlinie) dem DB-Cluster von Aurora PostgreSQL zugeordnet. Wenn der Vorgang abgeschlossen ist, wird die Rolle in der Liste „Current IAM roles for this cluster“ (Aktuelle IAM-Rollen für diesen Cluster) angezeigt, wie in der folgenden Abbildung dargestellt.



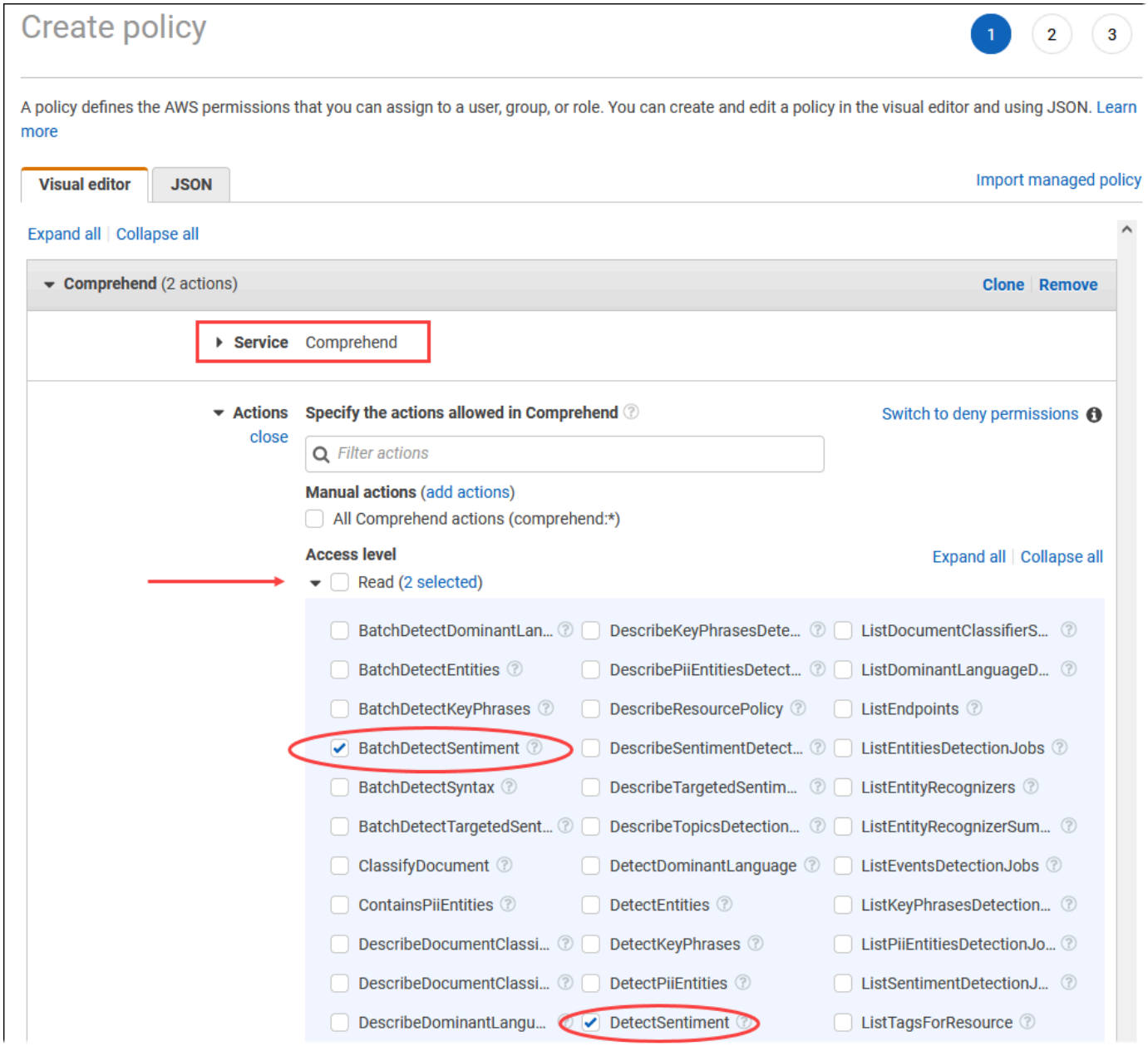
Das IAM-Setup für Amazon Bedrock ist abgeschlossen. Fahren Sie mit der Einrichtung von Aurora PostgreSQL für Aurora Machine Learning fort, indem Sie die Erweiterung wie unter Installieren der Aurora-Erweiterung für Machine Learning beschrieben installieren.

Einrichten von Aurora PostgreSQL für die Verwendung von Amazon Comprehend

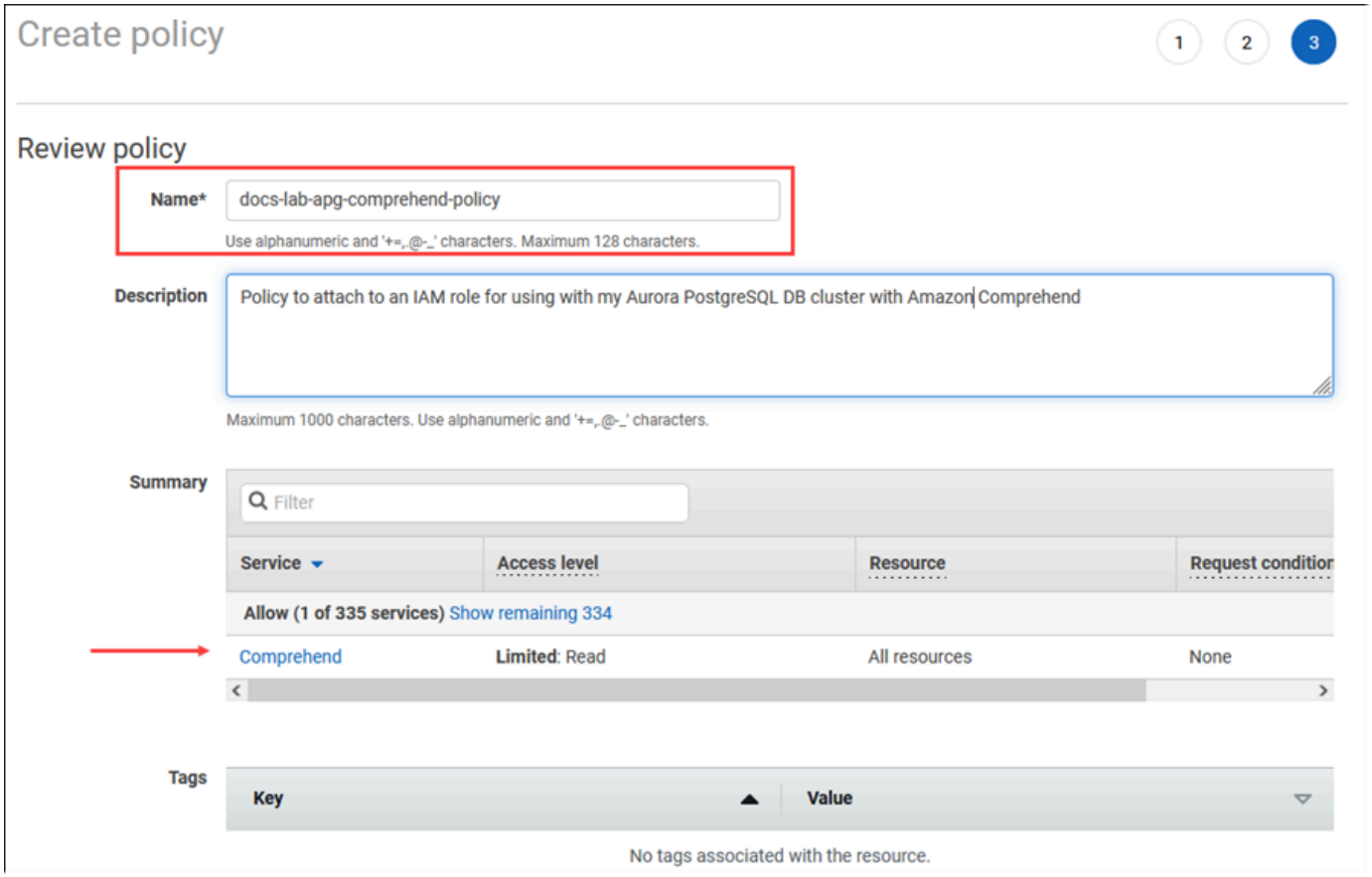
Im folgenden Verfahren erstellen Sie zunächst die IAM-Rolle und -Richtlinie, die Aurora PostgreSQL die Berechtigung erteilt, Amazon Comprehend im Namen des Clusters zu verwenden. Anschließend fügen Sie die Richtlinie einer IAM-Rolle an, die Ihr DB-Cluster von Aurora PostgreSQL für die Arbeit mit Amazon Comprehend verwendet. Der Einfachheit halber nutzt dieses Verfahren die AWS Management Console , um alle Aufgaben abzuschließen.

So richten Sie Ihren DB-Cluster von Aurora PostgreSQL zur Verwendung von Amazon Comprehend ein

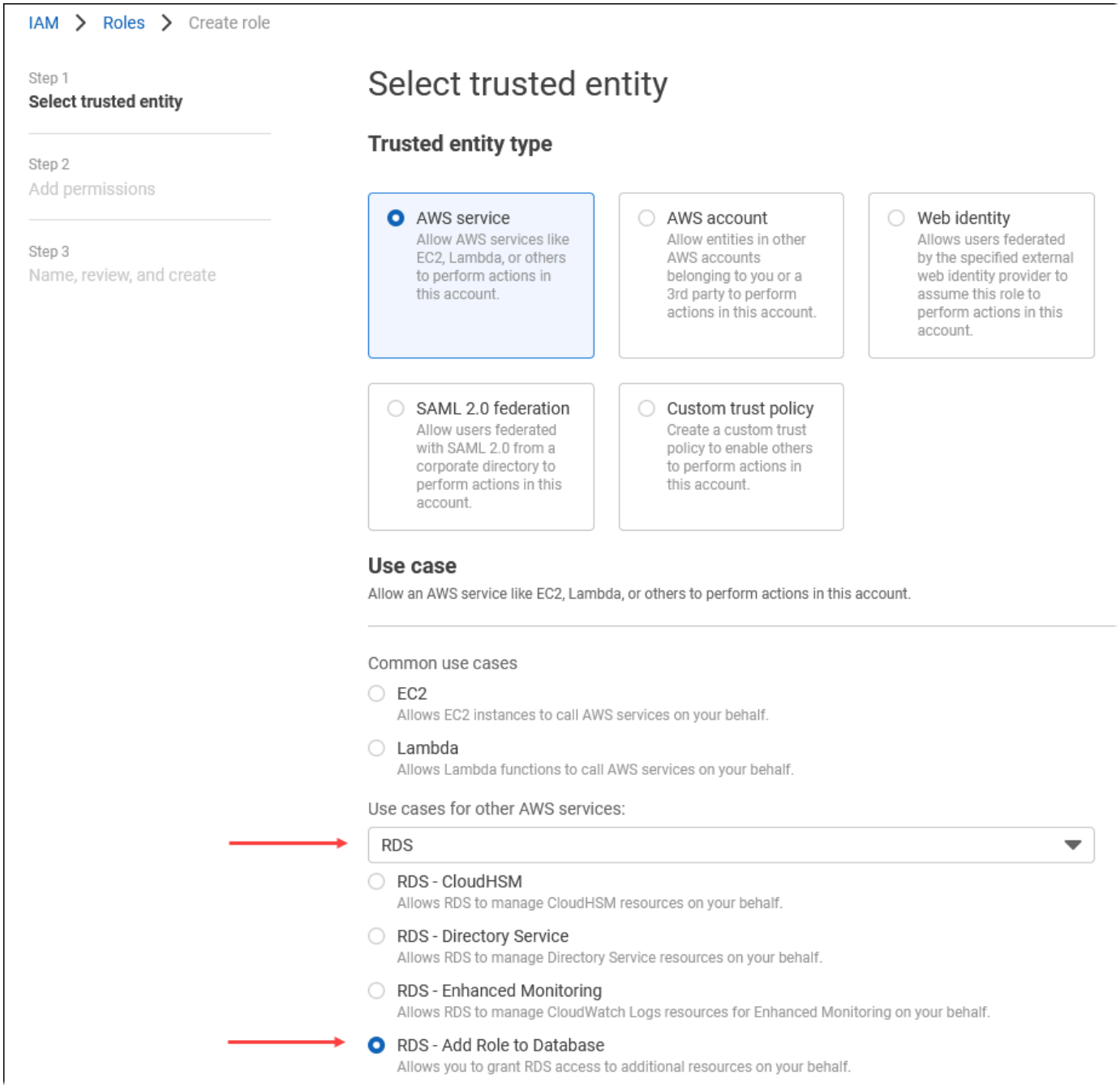
1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
3. Wählen Sie im Konsolenmenü (IAM) die Option Richtlinien AWS Identity and Access Management (unter Zugriffsverwaltung) aus.



4. Wählen Sie Richtlinie erstellen aus. Wählen Sie auf der Seite „Visual editor“ (Visueller Editor) die Option Service (Service) aus und geben Sie dann im Feld „Select a service“ (Service auswählen) Comprehend ein. Erweitern Sie die Lesezugriffsebene. Wählen Sie BatchDetectSentimentund DetectSentimentaus den Amazon Comprehend Leseeinstellungen.
5. Wählen Sie Next: Tags (Weiter: Tags) aus und definieren Sie Tags (dies ist optional). Wählen Sie Weiter: Prüfen aus. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein, wie in der Abbildung gezeigt.



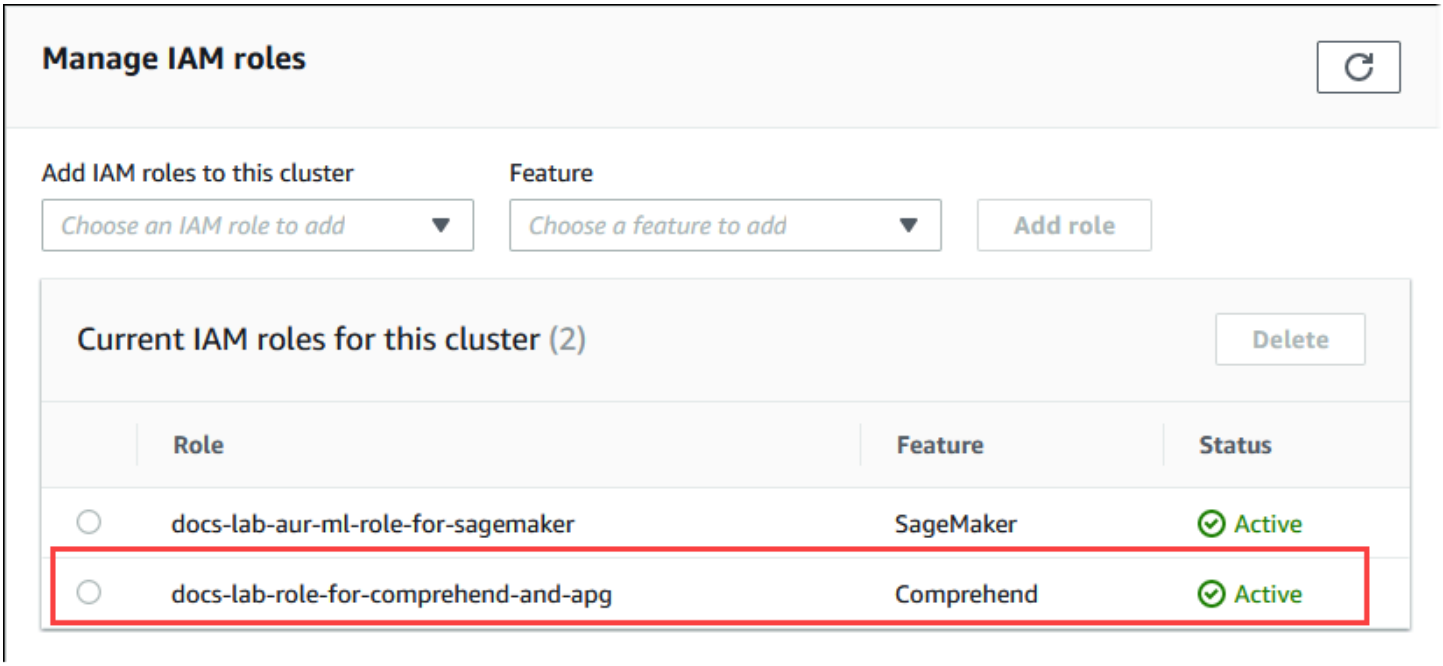
6. Wählen Sie Richtlinie erstellen aus. Die Konsole zeigt eine Warnung an, wenn die Richtlinie gespeichert wurde. Sie finden sie in der Liste der Richtlinien.
7. Wählen Sie in der IAM-Konsole die Option Roles (Rollen) (unter „Access management“ (Zugriffsverwaltung)) aus.
8. Wählen Sie Rolle erstellen aus.
9. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen die AWS Service-Kachel und dann RDS aus, um den Selektor zu öffnen.
10. Wählen Sie RDS – Add Role to Database (RDS – Rolle zu Datenbank hinzufügen) aus.



11. Wählen Sie Weiter aus. Suchen Sie auf der Seite „Add permissions“ (Berechtigungen hinzufügen) nach der im vorherigen Schritt erstellten Richtlinie und wählen Sie sie aus den aufgelisteten Richtlinien aus. Wählen Sie Next (Weiter) aus.
12. Next: Review (Weiter: Überprüfung). Geben Sie einen Namen und eine Beschreibung für die IAM-Rolle ein.
13. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

14. Navigieren Sie zu dem AWS-Region Ort, an dem sich Ihr Aurora PostgreSQL-DB-Cluster befindet.
15. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann den DB-Cluster von Aurora PostgreSQL aus, den Sie mit Amazon Comprehend verwenden möchten.
16. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit) aus und scrollen Sie zum Abschnitt Manage IAM roles (IAM-Rollen verwalten) auf der Seite. Wählen Sie in der Auswahl Add IAM roles to this cluster (Diesem Cluster IAM-Rollen hinzufügen) die Rolle aus, die Sie in den vorherigen Schritten erstellt haben. Wählen Sie in der Funktionsauswahl die Option Comprehend und dann Add role aus.

Die Rolle ist (mit ihrer Richtlinie) dem DB-Cluster von Aurora PostgreSQL zugeordnet. Wenn der Vorgang abgeschlossen ist, wird die Rolle in der Liste „Current IAM roles for this cluster“ (Aktuelle IAM-Rollen für diesen Cluster) angezeigt, wie in der folgenden Abbildung dargestellt.



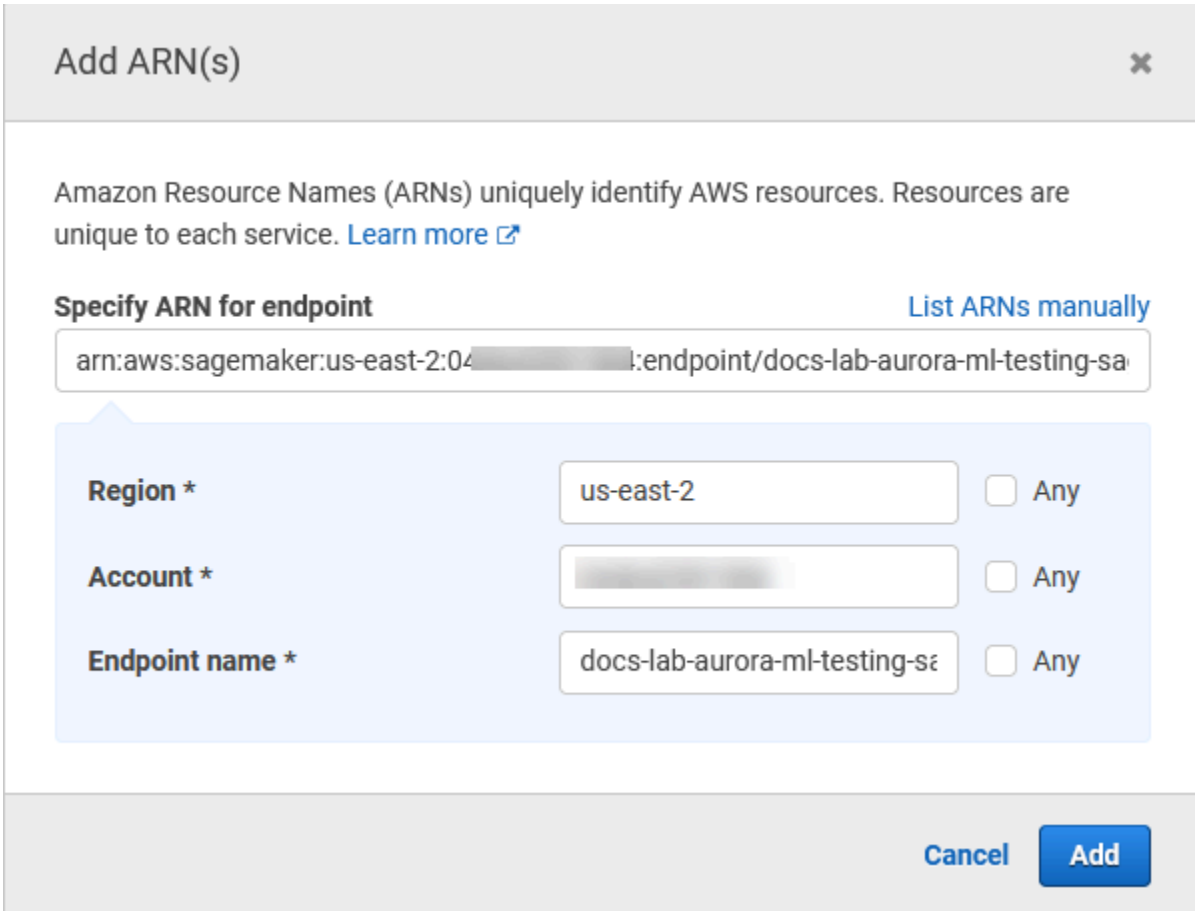
Die IAM-Einrichtung für Amazon Comprehend ist abgeschlossen. Fahren Sie mit der Einrichtung von Aurora PostgreSQL für Aurora Machine Learning fort, indem Sie die Erweiterung wie unter Installieren der Aurora-Erweiterung für Machine Learning beschrieben installieren.

Aurora PostgreSQL für die Nutzung von Amazon einrichten SageMaker

Bevor Sie die IAM-Richtlinie und -Rolle für Ihren Aurora PostgreSQL-DB-Cluster erstellen können, müssen Sie Ihr SageMaker Modell-Setup und Ihren Endpunkt verfügbar haben.

So richten Sie Ihren Aurora PostgreSQL-DB-Cluster zur Verwendung ein SageMaker

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Konsolenmenü (IAM) die Option Richtlinien AWS Identity and Access Management (unter Zugriffsverwaltung) und wählen Sie dann Richtlinie erstellen aus. Wählen Sie im Visual Editor SageMakerden Service aus. Öffnen Sie für Aktionen den Auswahlbereich Lesen (unter Zugriffsebene) und wählen Sie InvokeEndpoint. Daraufhin wird ein Warnsymbol angezeigt.
3. Öffnen Sie die Ressourcenauswahl und wählen Sie unter Endpunktressourcen-ARN angeben für die InvokeEndpoint Aktion den Link ARN hinzufügen, um den Zugriff einzuschränken.
4. Geben Sie Ihre SageMaker Ressourcen und den Namen Ihres Endpunkts ein. AWS-Region Ihr AWS Konto ist vorausgefüllt.



5. Wählen Sie zum Speichern Add (Hinzufügen) aus. Wählen Sie Next: Tags (Weiter: Tags) und Next: Review (Weiter: Überprüfen) aus, um zur letzten Seite des Richtlinienerstellungsprozesses zu gelangen.

6. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein und wählen Sie dann Create policy (Richtlinie erstellen) aus. Die Richtlinie wird erstellt und der Liste „Policies“ (Richtlinien) hinzugefügt. Dabei wird in der Konsole eine Warnung angezeigt.
7. Wählen Sie in der IAM-Konsole Roles (Rollen) aus.
8. Wählen Sie Rolle erstellen aus.
9. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen die AWS Dienstkachel und dann RDS aus, um den Selektor zu öffnen.
10. Wählen Sie RDS – Add Role to Database (RDS – Rolle zu Datenbank hinzufügen) aus.
11. Wählen Sie Weiter aus. Suchen Sie auf der Seite „Add permissions“ (Berechtigungen hinzufügen) nach der im vorherigen Schritt erstellten Richtlinie und wählen Sie sie aus den aufgelisteten Richtlinien aus. Wählen Sie Next (Weiter) aus.
12. Next: Review (Weiter: Überprüfung). Geben Sie einen Namen und eine Beschreibung für die IAM-Rolle ein.
13. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
14. Navigieren Sie zu dem AWS-Region Ort, an dem sich Ihr Aurora PostgreSQL-DB-Cluster befindet.
15. Wählen Sie im Navigationsbereich Datenbanken und dann den Aurora PostgreSQL-DB-Cluster aus, mit dem Sie es verwenden möchten. SageMaker
16. Wählen Sie die Registerkarte Connectivity & security (Konnektivität und Sicherheit) aus und scrollen Sie zum Abschnitt Manage IAM roles (IAM-Rollen verwalten) auf der Seite. Wählen Sie in der Auswahl Add IAM roles to this cluster (Diesem Cluster IAM-Rollen hinzufügen) die Rolle aus, die Sie in den vorherigen Schritten erstellt haben. Wählen Sie in der Funktionsauswahl die Option und SageMaker anschließend Rolle hinzufügen aus.

Die Rolle ist (mit ihrer Richtlinie) dem DB-Cluster von Aurora PostgreSQL zugeordnet. Wenn der Vorgang abgeschlossen ist, wird die Rolle in der Liste „Current IAM roles for this cluster“ (Aktuelle IAM-Rollen für diesen Cluster) angezeigt.

Das IAM-Setup für SageMaker ist abgeschlossen. Fahren Sie mit der Einrichtung von Aurora PostgreSQL für Aurora Machine Learning fort, indem Sie die Erweiterung wie unter Installieren der Aurora-Erweiterung für Machine Learning beschrieben installieren.

Aurora PostgreSQL für die Verwendung von Amazon S3 einrichten SageMaker (Fortgeschritten)

Für die Verwendung SageMaker mit Ihren eigenen Modellen, anstatt die von bereitgestellten vorgefertigten Komponenten zu verwenden SageMaker, müssen Sie einen Amazon Simple Storage

Service (Amazon S3) -Bucket einrichten, den der Aurora PostgreSQL-DB-Cluster verwenden kann. Dies ist ein Thema für Fortgeschrittene und wird in diesem Benutzerhandbuch für Amazon Aurora nicht vollständig dokumentiert. Der allgemeine Prozess ist derselbe wie bei der Integration der Unterstützung für SageMaker, und zwar wie folgt.

1. Erstellen Sie die IAM-Richtlinie und -Rolle für Amazon S3.
2. Fügen Sie die IAM-Rolle und den Amazon-S3-Import oder -Export als Funktion auf der Registerkarte „Connectivity & security“ (Konnektivität und Sicherheit) Ihres DB-Clusters von Aurora PostgreSQL hinzu.
3. Fügen Sie den ARN der Rolle der benutzerdefinierten DB-Cluster-Parametergruppe für jeden Aurora-DB-Cluster hinzu.

Grundlegende Informationen zur Nutzung finden Sie unter Exportieren von Daten nach Amazon S3 für SageMaker Modelltraining (Fortgeschritten).

Installieren der Aurora-Erweiterung für Machine Learning

Die Aurora-Erweiterungen `aws_ml 1.0` für maschinelles Lernen bieten zwei Funktionen, mit denen Sie Amazon Comprehend SageMaker Comprehend-Dienste aufrufen können, sowie `aws_ml 2.0` zwei zusätzliche Funktionen, mit denen Sie Amazon Bedrock-Dienste aufrufen können. Durch die Installation dieser Erweiterungen auf Ihrem Aurora PostgreSQL-DB-Cluster wird auch eine Administratorrolle für die Funktion erstellt.

> **Note**
>
> Die Verwendung dieser Funktionen hängt davon ab, ob die IAM-Einrichtung für den Aurora-Service für maschinelles Lernen (Amazon Comprehend SageMaker, Amazon Bedrock) abgeschlossen ist, wie unter beschrieben. Einrichten Ihres DB-Clusters von Aurora PostgreSQL zur Verwendung von Aurora Machine Learning

- aws_comprehend.detect_sentiment – Sie verwenden diese Funktion, um Stimmungsanalysen auf Text anzuwenden, der in der Datenbank Ihres DB-Clusters von Aurora PostgreSQL gespeichert ist.
- aws_sagemaker.invoke_endpoint — Sie verwenden diese Funktion in Ihrem SQL-Code, um von Ihrem Cluster aus mit dem Endpunkt zu kommunizieren. SageMaker
- aws_bedrock.invoke_model — Sie verwenden diese Funktion in Ihrem SQL-Code, um mit den Bedrock-Modellen aus Ihrem Cluster zu kommunizieren. Die Antwort dieser Funktion erfolgt im

Format eines TEXTS. Wenn also ein Modell im Format eines JSON-Hauptteils antwortet, wird die Ausgabe dieser Funktion im Format einer Zeichenfolge an den Endbenutzer weitergeleitet.

- aws_bedrock.invoke_model_get_embeddings — Sie verwenden diese Funktion in Ihrem SQL-Code, um Bedrock-Modelle aufzurufen, die Ausgabeeinbettungen innerhalb einer JSON-Antwort zurückgeben. Dies kann genutzt werden, wenn Sie die direkt mit dem JSON-Key verknüpften Einbettungen extrahieren möchten, um die Antwort mit selbstverwalteten Workflows zu optimieren.

So richten Sie die Aurora-Erweiterung für Machine Learning in Ihrem DB-Cluster von Aurora PostgreSQL ein

- Verwenden Sie `psql`, um eine Verbindung mit der Writer-Instance Ihres DB-Clusters von Aurora PostgreSQL herzustellen. Stellen Sie eine Verbindung mit der entsprechenden Datenbank her, in der die `aws_ml`-Erweiterung installiert werden soll.

  ```
  psql --host=cluster-instance-1.111122223333.aws-region.rds.amazonaws.com --
  port=5432 --username=postgres --password --dbname=labdb
  ```

```
labdb=> CREATE EXTENSION IF NOT EXISTS aws_ml CASCADE;
NOTICE:  installing required extension "aws_commons"
CREATE EXTENSION
labdb=>
```

Durch die Installation der `aws_ml` Erweiterungen werden auch die `aws_ml` Administratorrolle und zwei neue Schemas wie folgt erstellt.

- `aws_comprehend` – Schema für den Amazon-Comprehend-Service und die Quelle der `detect_sentiment`-Funktion (`aws_comprehend.detect_sentiment`).
- `aws_sagemaker`— Schema für den SageMaker Dienst und die Quelle der `invoke_endpoint` Funktion (`aws_sagemaker.invoke_endpoint`).
- `aws_bedrock`— Schema für den Amazon Bedrock-Service und Quelle der `invoke_model(aws_bedrock.invoke_model)` `invoke_model_get_embeddings(aws_bedrock.invoke_model_get_embeddings)` Funktionen.

Der `rds_superuser`-Rolle wird die administrative `aws_ml`-Rolle zugewiesen und wird damit zum `OWNER` dieser beiden Aurora-Schemata für Machine Learning. Damit andere Datenbankbenutzer

auf die Aurora-Funktionen für Machine Learning zugreifen können, muss der `rds_superuser` `EXECUTE`-Berechtigungen für die Aurora-Funktionen für Machine Learning erteilen. Standardmäßig werden `EXECUTE`-Berechtigungen von `PUBLIC` für die Funktionen in den beiden Aurora-Schemata für Machine Learning widerrufen.

In einer Datenbankkonfiguration mit mehreren Mandanten können Sie verhindern, dass Mandanten auf Aurora-Funktionen für Machine Learning zugreifen, indem Sie `REVOKE USAGE` für das spezifische Aurora-Schema für Machine Learning verwenden, das Sie schützen möchten.

Verwenden von Amazon Bedrock mit Ihrem Aurora PostgreSQL-DB-Cluster

Für Aurora PostgreSQL bietet Aurora Machine Learning die folgende Amazon Bedrock-Funktion für die Arbeit mit Ihren Textdaten. Diese Funktion ist erst verfügbar, nachdem Sie die `aws_ml` 2.0-Erweiterung installiert und alle Einrichtungsverfahren abgeschlossen haben. Weitere Informationen finden Sie unter Einrichten Ihres DB-Clusters von Aurora PostgreSQL zur Verwendung von Aurora Machine Learning.

aws_bedrock.invoke_model

Diese Funktion verwendet in JSON formatierten Text als Eingabe und verarbeitet ihn für eine Vielzahl von Modellen, die auf Amazon Bedrock gehostet werden, und ruft die JSON-Textantwort vom Modell zurück. Diese Antwort kann Text, Bild oder Einbettungen enthalten. Eine Zusammenfassung der Dokumentation der Funktion lautet wie folgt.

```
aws_bedrock.invoke_model(
   IN model_id      varchar,
   IN content_type  text,
   IN accept_type   text,
   IN model_input   text,
   OUT model_output varchar)
```

Die Ein- und Ausgaben dieser Funktion sind wie folgt.

- `model_id`— Kennung des Modells.
- `content_type`— Der Typ der Anfrage an das Bedrock-Modell.
- `accept_type`— Die Art der Antwort, die von Bedrocks Modell zu erwarten ist. Normalerweise application/JSON für die meisten Modelle.

- `model_input`— Eingabeaufforderungen; ein bestimmter Satz von Eingaben für das Modell in dem von content_type angegebenen Format. Weitere Informationen zum Anforderungsformat/zur Struktur, die das Modell akzeptiert, finden Sie unter Inferenzparameter für Fundamentmodelle.
- `model_output`— Die Ausgabe des Bedrock-Modells als Text.

Das folgende Beispiel zeigt, wie mit invoke_model ein Anthropic Claude 2-Modell für Bedrock aufgerufen wird.

Example Beispiel: Eine einfache Abfrage mit Amazon Bedrock-Funktionen

```
SELECT aws_bedrock.invoke_model (
    model_id    := 'anthropic.claude-v2',
    content_type:= 'application/json',
    accept_type := 'application/json',
    model_input := '{"prompt": "\n\nHuman: You are a helpful assistant that answers
 questions directly and only using the information provided in the context below.
\nDescribe the answer
    in detail.\n\nContext: %s \n\nQuestion: %s \n
\nAssistant:","max_tokens_to_sample":4096,"temperature":0.5,"top_k":250,"top_p":0.5,"stop_seque
[]}'
);
```

aws_bedrock.invoke_model_get_embeddings

Die Modellausgabe kann in einigen Fällen auf Vektoreinbettungen verweisen. Da die Antwort je nach Modell unterschiedlich ist, kann eine weitere Funktion namens invoke_model_get_embeddings genutzt werden, die genau wie invoke_model funktioniert, aber die Einbettungen durch Angabe des entsprechenden JSON-Schlüssels ausgibt.

```
aws_bedrock.invoke_model_get_embeddings(
   IN model_id      varchar,
   IN content_type  text,
   IN json_key      text,
   IN model_input   text,
   OUT model_output float8[])
```

Die Ein- und Ausgaben dieser Funktion sind wie folgt.

- `model_id`— Bezeichner des Modells.

- `content_type`— Der Typ der Anfrage an das Bedrock-Modell. Hier ist accept_type auf den Standardwert gesetzt. `application/json`
- `model_input`— Eingabeaufforderungen; ein bestimmter Satz von Eingaben für das Modell in dem von content_type angegebenen Format. Weitere Informationen zum Anforderungsformat/zur Struktur, die das Modell akzeptiert, finden Sie unter Inferenzparameter für Fundamentmodelle.
- `json_key`— Verweis auf das Feld, aus dem die Einbettung extrahiert werden soll. Dies kann variieren, wenn sich das Einbettungsmodell ändert.
- `model_output`— Die Ausgabe des Bedrock-Modells als Array von Einbettungen mit 16-Bit-Dezimalzahlen.

Das folgende Beispiel zeigt, wie eine Einbettung mit dem Modell Titan Embeddings G1 — Text Embedding für den Ausdruck PostgreSQL I/O monitoring views generiert wird.

Example Beispiel: Eine einfache Abfrage mit Amazon Bedrock-Funktionen

```
SELECT aws_bedrock.invoke_model_get_embeddings(
   model_id      := 'amazon.titan-embed-text-v1',
   content_type  := 'application/json',
   json_key      := 'embedding',
   model_input   := '{ "inputText": "PostgreSQL I/O monitoring views"}') AS embedding;
```

Verwenden von Amazon Comprehend mit Ihrem DB-Cluster von Aurora PostgreSQL

Für Aurora PostgreSQL bietet Aurora Machine Learning die folgende Amazon-Comprehend-Funktion für die Arbeit mit Ihren Textdaten. Diese Funktion ist erst verfügbar, nachdem Sie die `aws_ml`-Erweiterung installiert und alle Einrichtungsvorgänge abgeschlossen haben. Weitere Informationen finden Sie unter Einrichten Ihres DB-Clusters von Aurora PostgreSQL zur Verwendung von Aurora Machine Learning.

aws_comprehend.detect_sentiment

Diese Funktion nimmt Text als Eingabe und wertet aus, ob der Text eine positive, negative, neutrale oder gemischte emotionale Haltung hat. Sie gibt diese Stimmung zusammen mit einem Wahrscheinlichkeitsgrad für ihre Bewertung aus. Eine Zusammenfassung der Dokumentation der Funktion lautet wie folgt.

```
aws_comprehend.detect_sentiment(
```

```
    IN input_text varchar,
    IN language_code varchar,
    IN max_rows_per_batch int,
    OUT sentiment varchar,
    OUT confidence real)
```

Die Ein- und Ausgaben dieser Funktion sind wie folgt.

- `input_text` – Der Text zur Bewertung und Zuordnung der Stimmung (negativ, positiv, neutral, gemischt).
- `language_code` – Die Sprache des identifizierten `input_text` unter Verwendung der aus zwei Buchstaben bestehenden ISO-639-1-Kennung mit regionalem Untertag (nach Bedarf) bzw. dem aus drei Buchstaben bestehenden ISO-639-2-Code. Zum Beispiel ist `en` der Code für Englisch, `zh` der Code für vereinfachtes Chinesisch. Weitere Informationen finden Sie unter Unterstützte Sprachen im Amazon-Comprehend-Entwicklerhandbuch.
- `max_rows_per_batch` – Die maximale Anzahl von Zeilen pro Batch für die Verarbeitung im Batch-Modus. Weitere Informationen finden Sie unter Grundlagen zum Batch-Modus und zu den Aurora-Funktionen für Machine Learning.
- `sentiment` – Die Stimmung des Eingabetexts, die als POSITIV, NEGATIV, NEUTRAL oder GEMISCHT identifiziert wird.
- `confidence` – Der Grad der Wahrscheinlichkeit für die Genauigkeit der angegebenen `sentiment`. Die Werte können zwischen 0,0 und 1,0 liegen.

Nachstehend finden Sie Beispiele zur Verwendung dieser Funktion.

Example Beispiel: Eine einfache Abfrage mit Amazon-Comprehend-Funktionen

Hier ist ein Beispiel für eine einfache Abfrage, die diese Funktion aufruft, um die Kundenzufriedenheit mit Ihrem Support-Team zu bewerten. Angenommen, Sie haben eine Datenbanktabelle (`support`), in der Kundenfeedback nach jeder Supportanfrage gespeichert wird. Diese Beispielabfrage wendet die `aws_comprehend.detect_sentiment`-Funktion auf den Text in der `feedback`-Spalte der Tabelle an und gibt die Stimmung und den Wahrscheinlichkeitsgrad für diese Stimmung aus. Diese Abfrage gibt Ergebnisse außerdem in absteigender Reihenfolge aus.

```
SELECT feedback, s.sentiment,s.confidence
    FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
    ORDER BY s.confidence DESC;
```

```
feedback                          | sentiment | confidence
----------------------------------------------------------+-----------+------------
Thank you for the excellent customer support!             | POSITIVE  |   0.999771
The latest version of this product stinks!                | NEGATIVE  |   0.999184
Your support team is just awesome! I am blown away.       | POSITIVE  |   0.997774
Your product is too complex, but your support is great.   | MIXED     |   0.957958
Your support tech helped me in fifteen minutes.           | POSITIVE  |   0.949491
My problem was never resolved!                            | NEGATIVE  |   0.920644
When will the new version of this product be released?    | NEUTRAL   |   0.902706
I cannot stand that chatbot.                              | NEGATIVE  |   0.895219
Your support tech talked down to me.                      | NEGATIVE  |   0.868598
It took me way too long to get a real person.             | NEGATIVE  |   0.481805

(10 rows)
```

Damit vermieden wird, dass Sie für die Stimmungserkennung mehr als einmal pro Tabellenzeile belastet werden, können Sie die Ergebnisse materialisieren. Tun Sie dies in den relevanten Zeilen. Beispielsweise werden die Notizen des Klinikers aktualisiert, sodass nur Personen auf Französisch (`fr`) die Stimmungserkennungsfunktion verwenden.

```
UPDATE clinician_notes
SET sentiment = (aws_comprehend.detect_sentiment (french_notes, 'fr')).sentiment,
    confidence = (aws_comprehend.detect_sentiment (french_notes, 'fr')).confidence
WHERE
    clinician_notes.french_notes IS NOT NULL AND
    LENGTH(TRIM(clinician_notes.french_notes)) > 0 AND
    clinician_notes.sentiment IS NULL;
```

Weitere Informationen zur Optimierung Ihrer Funktionsaufrufe finden Sie unter Leistungsaspekte zur Verwendung von Aurora Machine Learning mit Aurora PostgreSQL.

Verwendung SageMaker mit Ihrem Aurora PostgreSQL-DB-Cluster

Nachdem Sie Ihre SageMaker Umgebung eingerichtet und wie unter beschrieben in Aurora PostgreSQL integriert habenAurora PostgreSQL für die Nutzung von Amazon einrichten SageMaker , können Sie mithilfe der Funktion Operationen aufrufen. `aws_sagemaker.invoke_endpoint` Die `aws_sagemaker.invoke_endpoint`-Funktion stellt nur eine Verbindung mit einem Modellendpunkt in derselben AWS-Region her. Wenn Ihre Datenbank-Instance über mehrere Replikate verfügt, stellen Sie AWS-Regionen sicher, dass Sie jedes Modell einrichten und für jedes SageMaker Modell bereitstellen. AWS-Region

Aufrufe von `aws_sagemaker.invoke_endpoint` werden mithilfe der IAM-Rolle authentifiziert, die Sie eingerichtet haben, um Ihren Aurora PostgreSQL-DB-Cluster mit dem SageMaker Service und dem Endpunkt zu verknüpfen, den Sie während des Einrichtungsvorgangs angegeben haben. SageMaker Modellendpunkte sind auf ein einzelnes Konto beschränkt und nicht öffentlich. Die `endpoint_name` URL enthält nicht die Konto-ID. SageMaker bestimmt die Konto-ID anhand des Authentifizierungstoken, das von der SageMaker IAM-Rolle der Datenbankinstanz bereitgestellt wird.

aws_sagemaker.invoke_endpoint

Diese Funktion verwendet den SageMaker Endpunkt als Eingabe und die Anzahl der Zeilen, die als Batch verarbeitet werden sollen. Sie verwendet auch die verschiedenen Parameter, die vom SageMaker Modellendpunkt erwartet werden, als Eingabe. Die Referenzdokumentation dieser Funktion lautet wie folgt.

```
aws_sagemaker.invoke_endpoint(
  IN endpoint_name varchar,
  IN max_rows_per_batch int,
  VARIADIC model_input "any",
  OUT model_output varchar
  )
```

Die Ein- und Ausgaben dieser Funktion sind wie folgt.

- `endpoint_name`— Eine Endpunkt-URL, die AWS-Region—unabhängig ist.
- `max_rows_per_batch` – Die maximale Anzahl von Zeilen pro Batch für die Verarbeitung im Batch-Modus. Weitere Informationen finden Sie unter Grundlagen zum Batch-Modus und zu den Aurora-Funktionen für Machine Learning.
- `model_input` – Ein oder mehrere Eingabeparameter für das Modell. Dabei kann es sich um jeden Datentyp handeln, den das SageMaker Modell benötigt. Mit PostgreSQL können Sie bis zu 100 Eingabeparameter für eine Funktion angeben. Array-Datentypen müssen eindimensional sein, können aber so viele Elemente enthalten, wie vom SageMaker Modell erwartet werden. Die Anzahl der Eingaben in ein SageMaker Modell ist nur durch die Nachrichtengrößenbeschränkung von SageMaker 6 MB begrenzt.
- `model_output`— Die Ausgabe des SageMaker Modells als Text.

Erstellen einer benutzerdefinierten Funktion zum Aufrufen eines Modells SageMaker

Erstellen Sie eine separate benutzerdefinierte Funktion, die `aws_sagemaker.invoke_endpoint` für jedes Ihrer Modelle aufgerufen wird. SageMaker Ihre benutzerdefinierte Funktion stellt den SageMaker Endpunkt dar, auf dem das Modell gehostet wird. Die `aws_sagemaker.invoke_endpoint`-Funktion wird innerhalb der benutzerdefinierten Funktion ausgeführt. Benutzerdefinierte Funktionen bieten viele Vorteile:

- Sie können Ihrem SageMaker Modell einen eigenen Namen geben, anstatt nur alle Ihre SageMaker Modelle aufzurufen`aws_sagemaker.invoke_endpoint`.
- Sie können die Modellendpunkt-URL an nur einer Stelle im SQL-Anwendungscode angeben.
- Sie können `EXECUTE`-Berechtigungen für jede Aurora-Funktion für Machine Learning unabhängig steuern.
- Sie können die Modellein- und Ausgabetypen mit SQL-Typen deklarieren. SQL erzwingt die Anzahl und den Typ der an Ihr SageMaker Modell übergebenen Argumente und führt bei Bedarf eine Typkonvertierung durch. Die Verwendung von SQL-Typen führt auch `SQL NULL` zu dem entsprechenden Standardwert, der von Ihrem SageMaker Modell erwartet wird.
- Sie können die maximale Stapelgröße reduzieren, wenn Sie die ersten paar Zeilen etwas schneller zurückgeben möchten.

Um eine benutzerdefinierte Funktion anzugeben, verwenden Sie die SQL Data Definition Language (DDL)-Anweisung `CREATE FUNCTION`. Beim Definieren der Funktion geben Sie Folgendes an:

- Die Eingabeparameter für das Modell.
- Der spezifische SageMaker Endpunkt, der aufgerufen werden soll.
- Den Rückgabetyp.

Die benutzerdefinierte Funktion gibt die vom SageMaker Endpunkt berechnete Inferenz zurück, nachdem das Modell mit den Eingabeparametern ausgeführt wurde. Im folgenden Beispiel wird eine benutzerdefinierte Funktion für ein SageMaker Modell mit zwei Eingabeparametern erstellt.

```
CREATE FUNCTION classify_event (IN arg1 INT, IN arg2 DATE, OUT category INT)
AS $$
    SELECT aws_sagemaker.invoke_endpoint (
        'sagemaker_model_endpoint_name', NULL,
        arg1, arg2                       -- model inputs are separate arguments
```

```
        )::INT                              -- cast the output to INT
$$ LANGUAGE SQL PARALLEL SAFE COST 5000;
```

Beachten Sie Folgendes:

- Die `aws_sagemaker.invoke_endpoint`-Funktionseingabe kann ein oder mehrere Parameter eines beliebigen Datentyps sein.
- In diesem Beispiel wird ein INT-Ausgabetyp verwendet. Wenn Sie die Ausgabe von einem `varchar`-Typ in einen anderen Typ umwandeln, muss sie in einen von PostgreSQL eingebauten skalaren Typ wie `INTEGER`, `REAL`, `FLOAT` oder `NUMERIC` umgewandelt werden. Weitere Informationen zu diesen Typen finden Sie unter Datentypen in der PostgreSQL-Dokumentation.
- Geben Sie `PARALLEL SAFE` an, um die parallele Abfrageausführung zu aktivieren. Weitere Informationen finden Sie unter Verbessern von Antwortzeiten durch parallele Abfrageverarbeitung.
- Geben Sie `COST 5000` an, um die Kosten für die Ausführung der Funktion zu schätzen. Verwenden Sie eine positive Zahl, welche die geschätzten Ausführungskosten für die Funktion in -Einheiten angib `cpu_operator_cost`.

Übergabe eines Arrays als Eingabe an ein Modell SageMaker

Die `aws_sagemaker.invoke_endpoint`-Funktion kann bis zu 100 Eingabeparameter haben, was die Grenze für PostgreSQL-Funktionen ist. Wenn das SageMaker Modell mehr als 100 Parameter desselben Typs benötigt, übergeben Sie die Modellparameter als Array.

Das folgende Beispiel definiert eine Funktion, die ein Array als Eingabe an das SageMaker Regressionsmodell übergibt. Die Ausgabe wird in einen `REAL`-Wert umgewandelt.

```
CREATE FUNCTION regression_model (params REAL[], OUT estimate REAL)
AS $$
    SELECT aws_sagemaker.invoke_endpoint (
      'sagemaker_model_endpoint_name',
      NULL,
      params
      )::REAL
$$ LANGUAGE SQL PARALLEL SAFE COST 5000;
```

Angabe der Batchgröße beim Aufrufen eines Modells SageMaker

Im folgenden Beispiel wird eine benutzerdefinierte Funktion für ein SageMaker Modell erstellt, die den Standardwert für die Batchgröße auf NULL setzt. Mit der Funktion können Sie auch eine andere Stapelgröße angeben, wenn Sie sie aufrufen.

```
CREATE FUNCTION classify_event (
    IN event_type INT, IN event_day DATE, IN amount REAL, -- model inputs
    max_rows_per_batch INT DEFAULT NULL,  -- optional batch size limit
    OUT category INT)                     -- model output
AS $$
    SELECT aws_sagemaker.invoke_endpoint (
        'sagemaker_model_endpoint_name', max_rows_per_batch,
        event_type, event_day, COALESCE(amount, 0.0)
        )::INT              -- casts output to type INT
$$ LANGUAGE SQL PARALLEL SAFE COST 5000;
```

Beachten Sie Folgendes:

- Verwenden Sie den optionalen `max_rows_per_batch`-Parameter, um die Anzahl der Zeilen für einen Stapelmodus-Funktionsaufruf zu steuern. Wenn Sie den Wert NULL verwenden, wählt der Abfrageoptimierer automatisch die maximale Stapelgröße aus. Weitere Informationen finden Sie unter Grundlagen zum Batch-Modus und zu den Aurora-Funktionen für Machine Learning.
- Standardmäßig wird die Übergabe von NULL als Parameterwert vor der Übergabe an in eine leere Zeichenfolge übersetzt. SageMaker Für dieses Beispiel haben die Eingaben unterschiedliche Typen.
- Wenn Sie über eine Nicht-Texteingabe oder eine Texteingabe verfügen, die standardmäßig auf einen anderen Wert als eine leere Zeichenfolge gesetzt werden muss, verwenden Sie die `COALESCE`-Anweisung. Verwenden Sie `COALESCE`, um NULL in den gewünschten Nullersetzungswert im Aufruf von `aws_sagemaker.invoke_endpoint` zu übersetzen. Für den `amount`-Parameter in diesem Beispiel wird ein NULL-Wert in 0,0 konvertiert.

Aufrufen eines SageMaker Modells mit mehreren Ausgaben

Im folgenden Beispiel wird eine benutzerdefinierte Funktion für ein SageMaker Modell erstellt, das mehrere Ausgaben zurückgibt. Ihre Funktion muss die Ausgabe der `aws_sagemaker.invoke_endpoint`-Funktion in einen entsprechenden Datentyp umwandeln.

Beispielsweise können Sie den integrierten PostgreSQL-Punkttyp für (x,y)-Paare oder einen benutzerdefinierten zusammengesetzten Typ verwenden.

Diese benutzerdefinierte Funktion gibt Werte aus einem Modell zurück, das mehrere Ausgaben zurückgibt, indem ein zusammengesetzter Typ für die Ausgaben verwendet wird.

```
CREATE TYPE company_forecasts AS (
    six_month_estimated_return real,
    one_year_bankruptcy_probability float);
CREATE FUNCTION analyze_company (
    IN free_cash_flow NUMERIC(18, 6),
    IN debt NUMERIC(18,6),
    IN max_rows_per_batch INT DEFAULT NULL,
    OUT prediction company_forecasts)
AS $$
    SELECT (aws_sagemaker.invoke_endpoint('endpt_name',
       max_rows_per_batch,free_cash_flow, debt))::company_forecasts;


$$ LANGUAGE SQL PARALLEL SAFE COST 5000;
```

Verwenden Sie für den zusammengesetzten Typ Felder in der gleichen Reihenfolge wie sie in der Modellausgabe angezeigt werden und wandeln Sie die Ausgabe von `aws_sagemaker.invoke_endpoint` in den zusammengesetzten Typ um. Der Aufrufer kann die einzelnen Felder entweder nach Namen oder mit der PostgreSQL-".*"-Notation extrahieren.

Exportieren von Daten nach Amazon S3 für SageMaker Modelltraining (Fortgeschritten)

Wir empfehlen Ihnen, sich mit Aurora Machine Learning vertraut zu machen und SageMaker die bereitgestellten Algorithmen und Beispiele zu verwenden, anstatt zu versuchen, Ihre eigenen Modelle zu trainieren. Weitere Informationen finden Sie unter Erste Schritte mit Amazon SageMaker

Um SageMaker Modelle zu trainieren, exportieren Sie Daten in einen Amazon S3 S3-Bucket. Der Amazon S3 S3-Bucket wird verwendet SageMaker, um Ihr Modell vor der Bereitstellung zu trainieren. Sie können Daten aus einem Aurora PostgreSQL-DB-Cluster abfragen und direkt in Textdateien speichern, die in einem Amazon S3-Bucket gespeichert sind. SageMaker Nutzt dann die Daten aus dem Amazon S3 S3-Bucket für das Training. Weitere Informationen zum SageMaker Modelltraining finden Sie unter Modeltraining mit Amazon SageMaker.

> **Note**
>
> Wenn Sie einen Amazon S3 S3-Bucket für SageMaker Modelltraining oder Batch-Scoring erstellen, verwenden Sie `sagemaker` den Namen des Amazon S3 S3-Buckets. Weitere Informationen finden Sie unter Spezifizieren eines Amazon S3 S3-Buckets zum Hochladen von Trainingsdatensätzen und Speichern von Ausgabedaten im Amazon SageMaker Developer Guide.

Weitere Informationen zum Exportieren der Daten finden Sie unter Exportieren von Daten aus einem/einer Aurora PostgreSQL-DB-Cluster zu Amazon S3.

Leistungsaspekte zur Verwendung von Aurora Machine Learning mit Aurora PostgreSQL

Amazon Comprehend und die SageMaker Dienste erledigen die meiste Arbeit, wenn sie von einer Aurora-Funktion für maschinelles Lernen aufgerufen werden. Das bedeutet, dass Sie diese Ressourcen nach Bedarf unabhängig voneinander skalieren können. Für Ihren DB-Cluster von Aurora PostgreSQL können Sie Ihre Funktionsaufrufe so effizient wie möglich gestalten. Im Folgenden finden Sie einige Leistungsaspekte, die Sie bei der Arbeit mit Aurora Machine Learning und Aurora PostgreSQL beachten sollten.

Themen

- Grundlagen zum Batch-Modus und zu den Aurora-Funktionen für Machine Learning
- Verbessern von Antwortzeiten durch parallele Abfrageverarbeitung
- Verwenden von materialisierten Ansichten und materialisierten Spalten

Grundlagen zum Batch-Modus und zu den Aurora-Funktionen für Machine Learning

Normalerweise führt PostgreSQL Funktionen zeilenweise aus. Aurora Machine Learning kann diesen Overhead reduzieren, indem die Aufrufe an den externen Aurora-Service für Machine Learning für viele Zeilen in Batches mit einem Ansatz kombiniert werden, der als Ausführung im Batch-Modus bezeichnet wird. Im Batch-Modus empfängt Aurora Machine Learning die Antworten für einen Batch von Eingabezeilen und sendet dann die Antworten eine Zeile nach der anderen an die laufende Abfrage zurück. Diese Optimierung verbessert den Durchsatz Ihrer Aurora-Abfragen, ohne den PostgreSQL-Abfrageoptimierer zu beschränken.

Aurora verwendet automatisch den Stapelmodus, wenn die Funktion aus der SELECT-Liste, einer WHERE-Klausel oder einer HAVING-Klausel referenziert wird. Beachten Sie, dass einfache CASE-Ausdrücke der obersten Ebene für die Ausführung im Stapelmodus geeignet sind. Gesuchte CASE-Ausdrücke der obersten Ebene sind auch für die Ausführung im Stapelmodus berechtigt, vorausgesetzt, die erste WHEN-Klausel ist ein einfaches Prädikat mit einem Stapelmodus-Funktionsaufruf.

Ihre benutzerdefinierte Funktion muss eine LANGUAGE SQL-Funktion sein und sollte PARALLEL SAFE und COST 5000 angeben.

Funktionsmigration von der SELECT-Anweisung zur FROM-Klausel

Normalerweise wird eine aws_ml-Funktion, die für die Ausführung im Stapelmodus berechtigt ist, automatisch von Aurora in die FROM-Klausel migriert.

Die Migration berechtigter Funktionen im Stapelmodus in die FROM-Klausel kann manuell auf Abfrageebene untersucht werden. Dazu verwenden Sie EXPLAIN-Anweisungen (und ANALYZE und VERBOSE) und finden unter jedem im Stapelmodus die "Stapelverarbeitungs"-Informatione Function Scan. Sie können EXPLAIN (mit VERBOSE) auch verwenden, ohne die Abfrage auszuführen. Sie beobachten dann, ob die Aufrufe der Funktion als Function Scan unter einem eingebetteten Loop-Join erscheinen, der nicht in der ursprünglichen Anweisung angegeben wurde.

Im folgenden Beispiel zeigt der eingebettete Loop-Join-Operator im Plan, dass Aurora die anomaly_score-Funktion migriert hat. Sie migrierte diese Funktion von der SELECT-Liste in die FROM-Klausel, wo sie für die Ausführung im Stapelmodus berechtigt ist.

```
EXPLAIN (VERBOSE, COSTS false)
SELECT anomaly_score(ts.R.description) from ts.R;
                         QUERY PLAN
-------------------------------------------------------------
 Nested Loop
   Output: anomaly_score((r.description)::text)
   ->  Seq Scan on ts.r
         Output: r.id, r.description, r.score
   ->  Function Scan on public.anomaly_score
         Output: anomaly_score.anomaly_score
         Function Call: anomaly_score((r.description)::text)
```

Um die Ausführung im Stapelmodus zu deaktivieren, setzen Sie den apg_enable_function_migration-Parameter auf false. Dies verhindert die Migration von

aws_ml-Funktionen von der SELECT in die FROM-Klausel. Nachfolgend wird gezeigt, wie Sie dies tun.

```
SET apg_enable_function_migration = false;
```

Der apg_enable_function_migration-Parameter ist ein GUC-Parameter (Grand Unified Configuration), der von der Aurora PostgreSQL apg_plan_mgmt-Erweiterung für die Abfrageplanverwaltung erkannt wird. Um die Funktionsmigration in einer Sitzung zu deaktivieren, speichern Sie den resultierenden Plan mithilfe der Abfrageplanverwaltung als approved-Plan. Zur Laufzeit erzwingt die Abfrageplanverwaltung den approved-Plan mit seiner apg_enable_function_migration-Einstellung. Diese Erzwingung erfolgt unabhängig von der Einstellung des apg_enable_function_migration-GUC-Parameters. Weitere Informationen finden Sie unter Verwalten von Abfrageausführungsplänen für Aurora PostgreSQL.

Verwenden des max_rows_per_batch-Parameters

Sowohl die aws_comprehend.detect_sentiment- als auch die aws_sagemaker.invoke_endpoint-Funktion verfügen über einen max_rows_per_batch-Parameter. Dieser Parameter gibt die Anzahl der Zeilen an, die an den Aurora-Service für Machine Learning gesendet werden können. Je größer der von Ihrer Funktion verarbeitete Datensatz ist, umso größer kann die Batch-Größe gewählt werden.

Funktionen im Batch-Modus verbessern die Effizienz, indem sie Batches von Zeilen erstellen, welche die Kosten der Aurora Machine Learning-Funktionsaufrufe über eine große Anzahl von Zeilen verteilen. Wenn jedoch eine SELECT-Anweisung aufgrund einer LIMIT-Klausel früh beendet wird, kann der Stapel über mehr Zeilen konstruiert werden, als die Abfrage verwendet. Dieser Ansatz kann zu zusätzlichen Gebühren für Ihr Konto führen. AWS Um die Vorteile der Ausführung im Stapelmodus zu nutzen, aber das Erstellen zu großer Stapel zu vermeiden, verwenden Sie einen kleineren Wert für den max_rows_per_batch-Parameter in Ihren Funktionsaufrufen.

Wenn Sie eine EXPLAIN (VERBOSE, ANALYZE) einer Abfrage ausführen, welche die Ausführung im Stapelmodus verwendet, sehen Sie einen FunctionScan-Operator, der unterhalb eines eingebetteten Loop-Joins ist. Die Anzahl der von EXPLAIN gemeldeten Schleifen entspricht der Angabe, wie oft eine Zeile vom FunctionScan-Operator abgerufen wurde. Wenn eine Anweisung eine LIMIT-Klausel verwendet, ist die Anzahl der Abrufe konsistent. Um die Größe des Stapels zu optimieren, setzen Sie den max_rows_per_batch-Parameter auf diesen Wert. Wenn jedoch die Funktion im Stapelmodus in einem Prädikat in der WHERE-Klausel oder HAVING-Klausel referenziert wird, können Sie die Anzahl der Abrufe wahrscheinlich nicht im Voraus kennen. Verwenden Sie in

diesem Fall die Schleifen als Richtlinie und experimentieren Sie mit `max_rows_per_batch`, um eine Einstellung zu finden, welche die Leistung optimiert.

Überprüfen der Ausführung im Stapelmodus

Um festzustellen, ob eine Funktion im Batch-Modus ausgeführt wurde, verwenden Sie `EXPLAIN ANALYZE`. Wenn die Ausführung im Stapelmodus verwendet wurde, enthält der Abfrageplan die Informationen in einem Abschnitt "Stapelverarbeitung".

```
EXPLAIN ANALYZE SELECT user-defined-function();
 Batch Processing: num batches=1 avg/min/max batch size=3333.000/3333.000/3333.000
                                 avg/min/max batch call time=146.273/146.273/146.273
```

In diesem Beispiel gab es 1 Stapel, der 3.333 Zeilen enthielt, deren Verarbeitung 146,273 ms dauerte. Der Abschnitt "Stapelverarbeitung" zeigt Folgendes:

- Wie viele Stapel es für diese Scan-Operation der Funktion gab
- Die durchschnittliche, minimale und maximale Stapelgröße
- Die durchschnittliche, minimale und maximale Stapel-Ausführungszeit

In der Regel ist der letzte Stapel kleiner als der Rest, was häufig zu einer minimalen Stapelgröße führt, die viel kleiner als der Durchschnitt ist.

Um die ersten Zeilen schneller zurückzugeben, setzen Sie den `max_rows_per_batch`-Parameter auf einen kleineren Wert.

Um die Anzahl der Aufrufe im Stapelmodus an den ML-Service zu reduzieren, wenn Sie ein `LIMIT` in Ihrer benutzerdefinierten Funktion verwenden, setzen Sie den `max_rows_per_batch`-Parameter auf einen kleineren Wert.

Verbessern von Antwortzeiten durch parallele Abfrageverarbeitung

Damit Sie möglichst schnell Ergebnisse aus einer großen Anzahl von Zeilen erhalten, können Sie die parallele Abfrageverarbeitung mit der Verarbeitung im Batch-Modus kombinieren. Sie können die parallele Abfrageverarbeitung für `SELECT`-, `CREATE TABLE AS SELECT`- und `CREATE MATERIALIZED VIEW`-Anweisungen verwenden.

> **Note**
>
> PostgreSQL unterstützt noch keine parallele Abfrage für DML-Anweisungen (Data Manipulation Language).

Die parallele Abfrageverarbeitung erfolgt sowohl innerhalb der Datenbank als auch innerhalb des ML-Services. Die Anzahl der Kerne in der Instance-Klasse der Datenbank begrenzt den Parallelitätsgrad, der während der Abfrageausführung verwendet werden kann. Der Datenbankserver kann einen Ausführungsplan für parallele Abfragen erstellen, der die Aufgabe unter einer Gruppe von parallelen Workern partitioniert. Dann kann jeder dieser Worker Stapelanforderungen erstellen, die Zehntausende von Zeilen enthalten (oder so viele, wie es von jedem Service erlaubt ist).

Die gebündelten Anfragen von allen parallel Workern werden an den SageMaker Endpunkt gesendet. Der Grad der Parallelität, den der Endpunkt unterstützen kann, hängt von der Anzahl und Art der Instances ab, die ihn unterstützen. Für K Grade der Parallelität benötigen Sie eine Datenbank-Instance-Klasse mit mindestens K Kernen. Außerdem müssen Sie den SageMaker Endpunkt für Ihr Modell so konfigurieren, dass er über K Anfangsinstanzen einer ausreichend leistungsstarken Instanzklasse verfügt.

Zur Nutzung der parallelen Abfrageverarbeitung können Sie den `parallel_workers`-Speicherparameter der Tabelle festlegen, welche die Daten enthält, die Sie übergeben möchten. Sie setzen `parallel_workers` auf eine Funktion im Stapelmodus wie `aws_comprehend.detect_sentiment`. Wenn der Optimierer einen parallelen Abfrageplan wählt, können die AWS ML-Dienste sowohl im Batch als auch parallel aufgerufen werden.

Sie können die folgenden Parameter mit der `aws_comprehend.detect_sentiment`-Funktion verwenden, um einen Plan mit 4-Wege-Parallelität zu erhalten. Wenn Sie einen der beiden folgenden Parameter ändern, müssen Sie die Datenbank-Instance neu starten, damit die Änderungen wirksam werden.

```
-- SET max_worker_processes to 8;  -- default value is 8
-- SET max_parallel_workers to 8;  -- not greater than max_worker_processes
SET max_parallel_workers_per_gather to 4;  -- not greater than max_parallel_workers

-- You can set the parallel_workers storage parameter on the table that the data
-- for the Aurora machine learning function is coming from in order to manually
 override the degree of
-- parallelism that would otherwise be chosen by the query optimizer
```

```
--
ALTER TABLE yourTable SET (parallel_workers = 4);

-- Example query to exploit both batch-mode execution and parallel query
EXPLAIN (verbose, analyze, buffers, hashes)
SELECT aws_comprehend.detect_sentiment(description, 'en')).*
FROM yourTable
WHERE id < 100;
```

Weitere Informationen zum Steuern paralleler Abfragen finden Sie unter Parallele Pläne in der PostgreSQL-Dokumentation.

Verwenden von materialisierten Ansichten und materialisierten Spalten

Wenn Sie einen AWS Service wie SageMaker Amazon Comprehend aus Ihrer Datenbank aufrufen, wird Ihr Konto gemäß der Preispolitik dieses Dienstes belastet. Um die Gebühren für Ihr Konto zu minimieren, können Sie das Ergebnis des Aufrufs des AWS Service in einer materialisierten Spalte materialisieren, sodass der AWS Service nicht mehr als einmal pro Eingabezeile aufgerufen wird. Wenn gewünscht, können Sie eine `materializedAt`-Zeitstempelspalte hinzufügen, um die Zeit aufzuzeichnen, zu der die Spalten materialisiert wurden.

Die Latenz einer gewöhnlichen einzeiligen `INSERT`-Anweisung ist in der Regel viel geringer als die Latenz beim Aufrufen einer Funktion im Stapelmodus. Daher können Sie möglicherweise die Latenzanforderungen Ihrer Anwendung nicht erfüllen, wenn Sie die Funktion im Stapelmodus für jede einzeilige `INSERT` aufrufen, die Ihre Anwendung ausführt. Um das Ergebnis des Aufrufs eines AWS Dienstes in einer materialisierten Spalte zu materialisieren, müssen Hochleistungsanwendungen in der Regel die materialisierten Spalten auffüllen. Dazu geben sie regelmäßig eine `UPDATE`-Anweisung aus, die gleichzeitig für einen großen Stapel von Zeilen ausgeführt wird.

`UPDATE` führt eine Sperre auf Zeilenebene durch, die sich auf eine laufende Anwendung auswirken kann. Sie müssen also möglicherweise `SELECT ... FOR UPDATE SKIP LOCKED` oder `MATERIALIZED VIEW` verwenden.

Analyseabfragen, die mit einer großen Anzahl von Zeilen in Echtzeit arbeiten, können die Materialisierung im Batch-Modus mit der Echtzeitverarbeitung kombinieren. Dazu fügen diese Abfragen eine `UNION ALL` der vormaterialisierten Ergebnisse mit einer Abfrage über die Zeilen zusammen, die noch keine materialisierten Ergebnisse haben. In einigen Fällen wird eine solche `UNION ALL` an mehreren Stellen benötigt oder die Abfrage wird von einer Drittanbieteranwendung generiert. Wenn ja, können Sie eine `VIEW` erstellen, um die `UNION ALL`-Operation zu kapseln, damit dieses Detail nicht für den Rest der SQL-Anwendung verfügbar gemacht wird.

Sie können eine materialisierte Ansicht verwenden, um die Ergebnisse einer beliebigen SELECT-Anweisung rechtzeitig zu einem Snapshot zu materialisieren. Sie können sie auch verwenden, um die materialisierte Ansicht jederzeit in der Zukunft zu aktualisieren. Derzeit unterstützt PostgreSQL keine inkrementelle Aktualisierung, so dass jedes Mal, wenn die materialisierte Ansicht aktualisiert wird, die materialisierte Ansicht vollständig neu berechnet wird.

Sie können materialisierte Ansichten mit der CONCURRENTLY-Option aktualisieren, die den Inhalt der materialisierten Ansicht aktualisiert, ohne eine exklusive Sperre durchzuführen. Dadurch kann eine SQL-Anwendung aus der materialisierten Ansicht lesen, während sie aktualisiert wird.

Überwachung von Aurora Machine Learning

Sie können die aws_ml-Funktionen überwachen, indem Sie den track_functions-Parameter in Ihrer benutzerdefinierten DB-Cluster-Parametergruppe auf all festlegen. Standardmäßig ist dieser Parameter auf pl eingestellt, was bedeutet, dass nur „procedure-language“-Funktionen verfolgt werden. Wenn Sie diese Einstellung in all ändern, werden auch die aws_ml-Funktionen verfolgt. Weitere Informationen finden Sie unter Laufzeitstatistik in der PostgreSQL-Dokumentation.

Informationen zur Überwachung der Leistung von SageMaker Vorgängen, die von Aurora-Funktionen für maschinelles Lernen aufgerufen werden, finden Sie unter Monitor Amazon SageMaker im Amazon SageMaker Developer Guide.

Wenn track_functions auf all festgelegt ist, können Sie die pg_stat_user_functions-Ansicht abfragen, um Statistiken über die Funktionen zu erhalten, die Sie definieren und zum Aufrufen von Aurora-Services für Machine Learning verwenden. Die Ansicht gibt die Anzahl der calls, total_time und self_time für jede Funktion an.

Wenn Sie die Statistiken für die aws_sagemaker.invoke_endpoint- und aws_comprehend.detect_sentiment-Funktionen anzeigen möchten, können Sie die Ergebnisse mit der folgenden Abfrage nach Schemanamen filtern.

```
SELECT * FROM pg_stat_user_functions
    WHERE schemaname
    LIKE 'aws_%';
```

Gehen Sie wie folgt vor, um die Statistiken zu löschen.

```
SELECT pg_stat_reset();
```

Sie können die Namen Ihrer SQL-Funktionen, die die `aws_sagemaker.invoke_endpoint`-Funktion aufrufen, abrufen, indem Sie den `pg_proc`-Systemkatalog von PostgreSQL abfragen. Dieser Katalog speichert Informationen zu Funktionen, Prozeduren und mehr. Weitere Informationen finden Sie unter pg_proc in der PostgreSQL-Dokumentation. Das folgende Beispiel veranschaulicht das Abfragen der Tabelle, um die Namen von Funktionen (`proname`) zu erhalten, deren Quelle (`prosrc`) den Text invoke_endpoint enthält.

```
SELECT proname FROM pg_proc WHERE prosrc LIKE '%invoke_endpoint%';
```

Codebeispiele für Aurora mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Aurora mit einem AWS Software Development Kit (SDK) verwendet wird.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Servicefunktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien und serviceübergreifenden Beispiele sehen.

Szenarien sind Codebeispiele, die Ihnen zeigen, wie Sie eine bestimmte Aufgabe ausführen können, indem Sie mehrere Funktionen innerhalb desselben Services aufrufen.

Serviceübergreifende Beispiele sind Beispielanwendungen, die über mehrere AWS-Services hinweg arbeiten.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erste Schritte

Hello Aurora

Die folgenden Codebeispiele veranschaulichen die ersten Schritte mit Aurora.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
using Amazon.RDS;
using Amazon.RDS.Model;
```

```
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

namespace AuroraActions;

public static class HelloAurora
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the
        // Amazon Relational Database Service (Amazon RDS).
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRDS>()
            ).Build();

        // Now the client is available for injection. Fetching it directly here
 for example purposes only.
        var rdsClient = host.Services.GetRequiredService<IAmazonRDS>();

        // You can use await and any of the async methods to get a response.
        var response = await rdsClient.DescribeDBClustersAsync(new
 DescribeDBClustersRequest { IncludeShared = true });
        Console.WriteLine($"Hello Amazon RDS Aurora! Let's list some clusters in
 this account:");
        foreach (var cluster in response.DBClusters)
        {
            Console.WriteLine($"\tCluster: database: {cluster.DatabaseName}
 identifier: {cluster.DBClusterIdentifier}.");
        }
    }
}
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zu AWS SDK for .NET .

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Code für die C MakeLists .txt-CMake-Datei.

```
# Set the minimum required version of CMake for this project.
cmake_minimum_required(VERSION 3.13)

# Set the AWS service components used by this project.
set(SERVICE_COMPONENTS rds)

# Set this project's name.
project("hello_aurora")

# Set the C++ standard to use to build this target.
# At least C++ 11 is required for the AWS SDK for C++.
set(CMAKE_CXX_STANDARD 11)

# Use the MSVC variable to determine if this is a Windows build.
set(WINDOWS_BUILD ${MSVC})

if (WINDOWS_BUILD) # Set the location where CMake can find the installed
 libraries for the AWS SDK.
    string(REPLACE ";" "/aws-cpp-sdk-all;" SYSTEM_MODULE_PATH
 "${CMAKE_SYSTEM_PREFIX_PATH}/aws-cpp-sdk-all")
    list(APPEND CMAKE_PREFIX_PATH ${SYSTEM_MODULE_PATH})
endif ()

# Find the AWS SDK for C++ package.
find_package(AWSSDK REQUIRED COMPONENTS ${SERVICE_COMPONENTS})

if (WINDOWS_BUILD AND AWSSDK_INSTALL_AS_SHARED_LIBS)
     # Copy relevant AWS SDK for C++ libraries into the current binary directory
 for running and debugging.
```

```
    # set(BIN_SUB_DIR "/Debug") # If you are building from the command line, you
 may need to uncomment this
                                    # and set the proper subdirectory to the
 executables' location.

    AWSSDK_CPY_DYN_LIBS(SERVICE_COMPONENTS ""
 ${CMAKE_CURRENT_BINARY_DIR}${BIN_SUB_DIR})
endif ()

add_executable(${PROJECT_NAME}
        hello_aurora.cpp)

target_link_libraries(${PROJECT_NAME}
        ${AWSSDK_LINK_LIBRARIES})
```

Code für die Quelldatei „hello_aurora.cpp“.

```
#include <aws/core/Aws.h>
#include <aws/rds/RDSClient.h>
#include <aws/rds/model/DescribeDBClustersRequest.h>
#include <iostream>

/*
 *  A "Hello Aurora" starter application which initializes an Amazon Relational
 Database Service (Amazon RDS) client
 *  and describes the Amazon Aurora (Aurora) clusters.
 *
 *  main function
 *
 *  Usage: 'hello_aurora'
 *
 */
int main(int argc, char **argv) {
    Aws::SDKOptions options;
    // Optionally change the log level for debugging.
//   options.loggingOptions.logLevel = Utils::Logging::LogLevel::Debug;
    Aws::InitAPI(options); // Should only be called once.
    int result = 0;
    {
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";
```

```
        Aws::RDS::RDSClient rdsClient(clientConfig);

        Aws::String marker; // Used for pagination.
        std::vector<Aws::String> clusterIds;
        do {
            Aws::RDS::Model::DescribeDBClustersRequest request;

            Aws::RDS::Model::DescribeDBClustersOutcome outcome =
                    rdsClient.DescribeDBClusters(request);

            if (outcome.IsSuccess()) {
                for (auto &cluster: outcome.GetResult().GetDBClusters()) {
                    clusterIds.push_back(cluster.GetDBClusterIdentifier());
                }
                marker = outcome.GetResult().GetMarker();
            } else {
                result = 1;
                std::cerr << "Error with Aurora::GDescribeDBClusters. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                break;
            }
        } while (!marker.empty());

        std::cout << clusterIds.size() << " Aurora clusters found." << std::endl;
        for (auto &clusterId: clusterIds) {
            std::cout << "  clusterId " << clusterId << std::endl;
        }
    }

    Aws::ShutdownAPI(options); // Should only be called once.
    return 0;
}
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zu AWS SDK for C++ .

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/rds"
)

// main uses the AWS SDK for Go V2 to create an Amazon Aurora client and list up
 to 20
// DB clusters in your account.
// This example uses the default settings specified in your shared credentials
// and config files.
func main() {
 sdkConfig, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  fmt.Println("Couldn't load default configuration. Have you set up your AWS
 account?")
  fmt.Println(err)
  return
 }
 auroraClient := rds.NewFromConfig(sdkConfig)
 const maxClusters = 20
 fmt.Printf("Let's list up to %v DB clusters.\n", maxClusters)
 output, err := auroraClient.DescribeDBClusters(context.TODO(),
  &rds.DescribeDBClustersInput{MaxRecords: aws.Int32(maxClusters)})
 if err != nil {
  fmt.Printf("Couldn't list DB clusters: %v\n", err)
```

```
  return
 }
 if len(output.DBClusters) == 0 {
  fmt.Println("No DB clusters found.")
 } else {
  for _, cluster := range output.DBClusters {
   fmt.Printf("DB cluster %v has database %v.\n", *cluster.DBClusterIdentifier,
    *cluster.DatabaseName)
  }
 }
}
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zu AWS SDK for Go .

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
import software.amazon.awssdk.services.rds.paginators.DescribeDBClustersIterable;

public class DescribeDbClusters {
    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        describeClusters(rdsClient);
        rdsClient.close();
    }
```

```
    public static void describeClusters(RdsClient rdsClient) {
        DescribeDBClustersIterable clustersIterable =
 rdsClient.describeDBClustersPaginator();
        clustersIterable.stream()
                .flatMap(r -> r.dbClusters().stream())
                .forEach(cluster -> System.out
                        .println("Database name: " + cluster.databaseName() + "
 Arn = " + cluster.dbClusterArn()));
    }
}
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zu AWS SDK for Java 2.x .

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_sdk_rds::Client;

#[derive(Debug)]
struct Error(String);
impl std::fmt::Display for Error {
    fn fmt(&self, f: &mut std::fmt::Formatter<'_>) -> std::fmt::Result {
        write!(f, "{}", self.0)
    }
}
impl std::error::Error for Error {}

#[tokio::main]
async fn main() -> Result<(), Error> {
```

```
    tracing_subscriber::fmt::init();
    let sdk_config = aws_config::from_env().load().await;
    let client = Client::new(&sdk_config);

    let describe_db_clusters_output = client
        .describe_db_clusters()
        .send()
        .await
        .map_err(|e| Error(e.to_string()))?;
    println!(
        "Found {} clusters:",
        describe_db_clusters_output.db_clusters().len()
    );
    for cluster in describe_db_clusters_output.db_clusters() {
        let name = cluster.database_name().unwrap_or("Unknown");
        let engine = cluster.engine().unwrap_or("Unknown");
        let id = cluster.db_cluster_identifier().unwrap_or("Unknown");
        let class = cluster.db_cluster_instance_class().unwrap_or("Unknown");
        println!("\tDatabase: {name}",);
        println!("\t  Engine: {engine}",);
        println!("\t      ID: {id}",);
        println!("\tInstance: {class}",);
    }

    Ok(())
}
```

- Informationen zu APIs finden Sie unter DescribeDBClusters in der API-Referenz zum AWS -SDK für Rust.

Codebeispiele

- Aktionen für Aurora mithilfe von AWS SDKs
  - Verwendung CreateDBCluster mit einem AWS SDK oder CLI
  - Verwendung CreateDBClusterParameterGroup mit einem AWS SDK oder CLI
  - Verwendung CreateDBClusterSnapshot mit einem AWS SDK oder CLI
  - Verwendung CreateDBInstance mit einem AWS SDK oder CLI
  - Verwendung DeleteDBCluster mit einem AWS SDK oder CLI
  - Verwendung DeleteDBClusterParameterGroup mit einem AWS SDK oder CLI

Aktionen für Aurora mithilfe von AWS SDKs

Die folgenden Codebeispiele zeigen, wie einzelne Aurora-Aktionen mit AWS SDKs durchgeführt werden. Diese Auszüge rufen die Aurora-API auf und sind Codeauszüge aus größeren Programmen, die im Kontext ausgeführt werden müssen. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden können.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der Amazon-Aurora-API-Referenz.

Beispiele

- Verwendung CreateDBCluster mit einem AWS SDK oder CLI
- Verwendung CreateDBClusterParameterGroup mit einem AWS SDK oder CLI
- Verwendung CreateDBClusterSnapshot mit einem AWS SDK oder CLI
- Verwendung CreateDBInstance mit einem AWS SDK oder CLI
- Verwendung DeleteDBCluster mit einem AWS SDK oder CLI
- Verwendung DeleteDBClusterParameterGroup mit einem AWS SDK oder CLI
- Verwendung DeleteDBInstance mit einem AWS SDK oder CLI

- Verwendung DescribeDBClusterParameterGroups mit einem AWS SDK oder CLI
- Verwendung DescribeDBClusterParameters mit einem AWS SDK oder CLI
- Verwendung DescribeDBClusterSnapshots mit einem AWS SDK oder CLI
- Verwendung DescribeDBClusters mit einem AWS SDK oder CLI
- Verwendung DescribeDBEngineVersions mit einem AWS SDK oder CLI
- Verwendung DescribeDBInstances mit einem AWS SDK oder CLI
- Verwendung DescribeOrderableDBInstanceOptions mit einem AWS SDK oder CLI
- Verwendung ModifyDBClusterParameterGroup mit einem AWS SDK oder CLI

Verwendung **`CreateDBCluster`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`CreateDBCluster`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/// <summary>
/// Create a new cluster and database.
/// </summary>
/// <param name="dbName">The name of the new database.</param>
/// <param name="clusterIdentifier">The identifier of the cluster.</param>
/// <param name="parameterGroupName">The name of the parameter group.</param>
/// <param name="dbEngine">The engine to use for the new cluster.</param>
/// <param name="dbEngineVersion">The version of the engine to use.</param>
/// <param name="adminName">The admin username.</param>
```

```
    /// <param name="adminPassword">The primary admin password.</param>
    /// <returns>The cluster object.</returns>
    public async Task<DBCluster> CreateDBClusterWithAdminAsync(
        string dbName,
        string clusterIdentifier,
        string parameterGroupName,
        string dbEngine,
        string dbEngineVersion,
        string adminName,
        string adminPassword)
    {
        var request = new CreateDBClusterRequest
        {
            DatabaseName = dbName,
            DBClusterIdentifier = clusterIdentifier,
            DBClusterParameterGroupName = parameterGroupName,
            Engine = dbEngine,
            EngineVersion = dbEngineVersion,
            MasterUsername = adminName,
            MasterUserPassword = adminPassword,
        };

        var response = await _amazonRDS.CreateDBClusterAsync(request);
        return response.DBCluster;
    }
```

- Weitere API-Informationen finden Sie unter CreateDBCluster in der API-Referenz zu AWS SDK for .NET .

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
```

```
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::CreateDBClusterRequest request;
        request.SetDBClusterIdentifier(DB_CLUSTER_IDENTIFIER);
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);
        request.SetEngine(engineName);
        request.SetEngineVersion(engineVersionName);
        request.SetMasterUsername(administratorName);
        request.SetMasterUserPassword(administratorPassword);

        Aws::RDS::Model::CreateDBClusterOutcome outcome =
                client.CreateDBCluster(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB cluster creation has started."
                      << std::endl;
        }
        else {
            std::cerr << "Error with Aurora::CreateDBCluster. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, "", "", client);
            return false;
        }
```

- Weitere API-Informationen finden Sie unter CreateDBCluster in der API-Referenz zu AWS SDK for C++ .

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// CreateDbCluster creates a DB cluster that is configured to use the specified
 parameter group.
// The newly created DB cluster contains a database that uses the specified
 engine and
// engine version.
func (clusters *DbClusters) CreateDbCluster(clusterName string,
 parameterGroupName string,
 dbName string, dbEngine string, dbEngineVersion string, adminName string,
 adminPassword string) (
 *types.DBCluster, error) {

 output, err := clusters.AuroraClient.CreateDBCluster(context.TODO(),
 &rds.CreateDBClusterInput{
  DBClusterIdentifier:         aws.String(clusterName),
  Engine:                      aws.String(dbEngine),
  DBClusterParameterGroupName: aws.String(parameterGroupName),
  DatabaseName:                aws.String(dbName),
  EngineVersion:               aws.String(dbEngineVersion),
  MasterUserPassword:          aws.String(adminPassword),
  MasterUsername:              aws.String(adminName),
 })
 if err != nil {
  log.Printf("Couldn't create DB cluster %v: %v\n", clusterName, err)
  return nil, err
 } else {
  return output.DBCluster, err
 }
}
```

- Weitere API-Informationen finden Sie unter CreateDBCluster in der API-Referenz zu AWS SDK for Go .

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static String createDBCluster(RdsClient rdsClient, String
dbParameterGroupFamily, String dbName,
           String dbClusterIdentifier, String userName, String password) {
       try {
           CreateDbClusterRequest clusterRequest =
CreateDbClusterRequest.builder()
                   .databaseName(dbName)
                   .dbClusterIdentifier(dbClusterIdentifier)
                   .dbClusterParameterGroupName(dbParameterGroupFamily)
                   .engine("aurora-mysql")
                   .masterUsername(userName)
                   .masterUserPassword(password)
                   .build();

           CreateDbClusterResponse response =
rdsClient.createDBCluster(clusterRequest);
           return response.dbCluster().dbClusterArn();

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Weitere API-Informationen finden Sie unter CreateDBCluster in der API-Referenz zu AWS SDK for Java 2.x .

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun createDBCluster(
    dbParameterGroupFamilyVal: String?,
    dbName: String?,
    dbClusterIdentifierVal: String?,
    userName: String?,
    password: String?,
): String? {
    val clusterRequest =
        CreateDbClusterRequest {
            databaseName = dbName
            dbClusterIdentifier = dbClusterIdentifierVal
            dbClusterParameterGroupName = dbParameterGroupFamilyVal
            engine = "aurora-mysql"
            masterUsername = userName
            masterUserPassword = password
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbCluster(clusterRequest)
        return response.dbCluster?.dbClusterArn
    }
}
```

- Weitere API-Informationen finden Sie unter CreateDBCluster in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def create_db_cluster(
        self,
        cluster_name,
        parameter_group_name,
        db_name,
        db_engine,
        db_engine_version,
        admin_name,
        admin_password,
    ):
        """
        Creates a DB cluster that is configured to use the specified parameter
 group.
```

```
        The newly created DB cluster contains a database that uses the specified
engine and
        engine version.

        :param cluster_name: The name of the DB cluster to create.
        :param parameter_group_name: The name of the parameter group to associate
with
                                     the DB cluster.
        :param db_name: The name of the database to create.
        :param db_engine: The database engine of the database that is created,
such as MySql.
        :param db_engine_version: The version of the database engine.
        :param admin_name: The user name of the database administrator.
        :param admin_password: The password of the database administrator.
        :return: The newly created DB cluster.
        """
        try:
            response = self.rds_client.create_db_cluster(
                DatabaseName=db_name,
                DBClusterIdentifier=cluster_name,
                DBClusterParameterGroupName=parameter_group_name,
                Engine=db_engine,
                EngineVersion=db_engine_version,
                MasterUsername=admin_name,
                MasterUserPassword=admin_password,
            )
            cluster = response["DBCluster"]
        except ClientError as err:
            logger.error(
                "Couldn't create database %s. Here's why: %s: %s",
                db_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return cluster
```

- Weitere API-Informationen finden Sie unter CreateDBCluster in der API-Referenz zum AWS SDK für Python (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   // Get a list of allowed engine versions.
rds.DescribeDbEngineVersions(Engine='aurora-mysql', DBParameterGroupFamily=<the
family used to create your parameter group in step 2>)
   // Create an Aurora DB cluster database cluster that contains a MySql
database and uses the parameter group you created.
   // Wait for DB cluster to be ready. Call rds.DescribeDBClusters and check for
Status == 'available'.
   // Get a list of instance classes available for the selected engine
and engine version. rds.DescribeOrderableDbInstanceOptions(Engine='mysql',
EngineVersion=).

   // Create a database instance in the cluster.
   // Wait for DB instance to be ready. Call rds.DescribeDbInstances and check
for DBInstanceStatus == 'available'.
   pub async fn start_cluster_and_instance(&mut self) -> Result<(),
ScenarioError> {
       if self.password.is_none() {
           return Err(ScenarioError::with(
               "Must set Secret Password before starting a cluster",
           ));
       }
       let create_db_cluster = self
           .rds
           .create_db_cluster(
               DB_CLUSTER_IDENTIFIER,
               DB_CLUSTER_PARAMETER_GROUP_NAME,
               DB_ENGINE,
               self.engine_version.as_deref().expect("engine version"),
               self.username.as_deref().expect("username"),
               self.password
                   .replace(SecretString::new("".to_string()))
                   .expect("password"),
```

```
            )
            .await;
        if let Err(err) = create_db_cluster {
            return Err(ScenarioError::new(
                "Failed to create DB Cluster with cluster group",
                &err,
            ));
        }

        self.db_cluster_identifier = create_db_cluster
            .unwrap()
            .db_cluster
            .and_then(|c| c.db_cluster_identifier);

        if self.db_cluster_identifier.is_none() {
            return Err(ScenarioError::with("Created DB Cluster missing
Identifier"));
        }

        info!(
            "Started a db cluster: {}",
            self.db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing ARN")
        );

        let create_db_instance = self
            .rds
            .create_db_instance(
                self.db_cluster_identifier.as_deref().expect("cluster name"),
                DB_INSTANCE_IDENTIFIER,
                self.instance_class.as_deref().expect("instance class"),
                DB_ENGINE,
            )
            .await;
        if let Err(err) = create_db_instance {
            return Err(ScenarioError::new(
                "Failed to create Instance in DB Cluster",
                &err,
            ));
        }

        self.db_instance_identifier = create_db_instance
            .unwrap()
```

```
            .db_instance
            .and_then(|i| i.db_instance_identifier);

        // Cluster creation can take up to 20 minutes to become available
        let cluster_max_wait = Duration::from_secs(20 * 60);
        let waiter = Waiter::builder().max(cluster_max_wait).build();
        while waiter.sleep().await.is_ok() {
            let cluster = self
                .rds
                .describe_db_clusters(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = cluster {
                warn!(?err, "Failed to describe cluster while waiting for
ready");
                continue;
            }

            let instance = self
                .rds
                .describe_db_instance(
                    self.db_instance_identifier
                        .as_deref()
                        .expect("instance identifier"),
                )
                .await;
            if let Err(err) = instance {
                return Err(ScenarioError::new(
                    "Failed to find instance for cluster",
                    &err,
                ));
            }

            let instances_available = instance
                .unwrap()
                .db_instances()
                .iter()
                .all(|instance| instance.db_instance_status() ==
Some("Available"));
```

```
            let endpoints = self
                .rds
                .describe_db_cluster_endpoints(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = endpoints {
                return Err(ScenarioError::new(
                    "Failed to find endpoint for cluster",
                    &err,
                ));
            }

            let endpoints_available = endpoints
                .unwrap()
                .db_cluster_endpoints()
                .iter()
                .all(|endpoint| endpoint.status() == Some("available"));

            if instances_available && endpoints_available {
                return Ok(());
            }
        }

        Err(ScenarioError::with("timed out waiting for cluster"))
    }

    pub async fn create_db_cluster(
        &self,
        name: &str,
        parameter_group: &str,
        engine: &str,
        version: &str,
        username: &str,
        password: SecretString,
    ) -> Result<CreateDbClusterOutput, SdkError<CreateDBClusterError>> {
        self.inner
            .create_db_cluster()
            .db_cluster_identifier(name)
            .db_cluster_parameter_group_name(parameter_group)
            .engine(engine)
```

```
            .engine_version(version)
            .master_username(username)
            .master_user_password(password.expose_secret())
            .send()
            .await
    }

#[tokio::test]
async fn test_start_cluster_and_instance() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
```

```
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_describe_db_instance()
        .with(eq("RustSDKCodeExamplesDBInstance"))
        .return_once(|name| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_instance_identifier(name)
                        .db_instance_status("Available")
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()

.db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
```

```
    scenario.password = Some(SecretString::new("test password".into()));

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
        assert!(scenario
            .password
            .replace(SecretString::new("BAD SECRET".into()))
            .unwrap()
            .expose_secret()
            .is_empty());
        assert_eq!(
            scenario.db_cluster_identifier,
            Some("RustSDKCodeExamplesDBCluster".into())
        );
    });
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Err(SdkError::service_error(
                CreateDBClusterError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db cluster error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));
```

```
    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _}) if message
 == "Failed to create DB Cluster with cluster group")
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_missing_id() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()
                .db_cluster(DbCluster::builder().build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context:_ }) if message
 == "Created DB Cluster missing Identifier");
}

#[tokio::test]
async fn test_start_cluster_and_instance_instance_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
```

```
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .return_once(|_, _, _, _| {
            Err(SdkError::service_error(
                CreateDBInstanceError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db instance error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _ }) if message
 == "Failed to create Instance in DB Cluster")
}

#[tokio::test]
async fn test_start_cluster_and_instance_wait_hiccup() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
```

```
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

.db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe cluster error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        })
```

```
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds.expect_describe_db_instance().return_once(|name| {
        Ok(DescribeDbInstancesOutput::builder()
            .db_instances(
                DbInstance::builder()
                    .db_instance_identifier(name)
                    .db_instance_status("Available")
                    .build(),
            )
            .build())
    });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()

.db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
```

```
    let _ = assertions.await;
}
```

- Informationen zu APIs finden Sie unter CreateDBCluster in der API-Referenz zum AWS -SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`CreateDBClusterParameterGroup`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`CreateDBClusterParameterGroup`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Create a custom cluster parameter group.
    /// </summary>
    /// <param name="parameterGroupFamily">The family of the parameter group.</
param>
    /// <param name="groupName">The name for the new parameter group.</param>
    /// <param name="description">A description for the new parameter group.</
param>
```

```
    /// <returns>The new parameter group object.</returns>
    public async Task<DBClusterParameterGroup>
CreateCustomClusterParameterGroupAsync(
        string parameterGroupFamily,
        string groupName,
        string description)
    {
        var request = new CreateDBClusterParameterGroupRequest
        {
            DBParameterGroupFamily = parameterGroupFamily,
            DBClusterParameterGroupName = groupName,
            Description = description,
        };

        var response = await
_amazonRDS.CreateDBClusterParameterGroupAsync(request);
        return response.DBClusterParameterGroup;
    }
```

- Einzelheiten zur API finden Sie unter ClusterParameterCreateDB-Gruppe in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::CreateDBClusterParameterGroupRequest request;
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);
```

```
        request.SetDBParameterGroupFamily(dbParameterGroupFamily);
        request.SetDescription("Example cluster parameter group.");

        Aws::RDS::Model::CreateDBClusterParameterGroupOutcome outcome =
                client.CreateDBClusterParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB cluster parameter group was successfully
 created."
                      << std::endl;
        }
        else {
            std::cerr << "Error with Aurora::CreateDBClusterParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
```

- Einzelheiten zur API finden Sie unter ClusterParameterCreateDB-Gruppe in der AWS SDK for C++ API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// CreateParameterGroup creates a DB cluster parameter group that is based on the
 specified
```

```
// parameter group family.
func (clusters *DbClusters) CreateParameterGroup(
 parameterGroupName string, parameterGroupFamily string, description string) (
 *types.DBClusterParameterGroup, error) {

 output, err :=
 clusters.AuroraClient.CreateDBClusterParameterGroup(context.TODO(),
  &rds.CreateDBClusterParameterGroupInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
   DBParameterGroupFamily:      aws.String(parameterGroupFamily),
   Description:                 aws.String(description),
  })
 if err != nil {
  log.Printf("Couldn't create parameter group %v: %v\n", parameterGroupName, err)
  return nil, err
 } else {
  return output.DBClusterParameterGroup, err
 }
}
```

- Einzelheiten zur API finden Sie unter ClusterParameterCreateDB-Gruppe in der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void createDBClusterParameterGroup(RdsClient rdsClient, String
dbClusterGroupName,
           String dbParameterGroupFamily) {
       try {
           CreateDbClusterParameterGroupRequest groupRequest =
CreateDbClusterParameterGroupRequest.builder()
```

```
                    .dbClusterParameterGroupName(dbClusterGroupName)
                    .dbParameterGroupFamily(dbParameterGroupFamily)
                    .description("Created by using the AWS SDK for Java")
                    .build();

            CreateDbClusterParameterGroupResponse response =
 rdsClient.createDBClusterParameterGroup(groupRequest);
            System.out.println("The group name is " +
 response.dbClusterParameterGroup().dbClusterParameterGroupName());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie unter ClusterParameterCreateDB-Gruppe in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun createDBClusterParameterGroup(
    dbClusterGroupNameVal: String?,
    dbParameterGroupFamilyVal: String?,
) {
    val groupRequest =
        CreateDbClusterParameterGroupRequest {
            dbClusterParameterGroupName = dbClusterGroupNameVal
            dbParameterGroupFamily = dbParameterGroupFamilyVal
            description = "Created by using the AWS SDK for Kotlin"
        }
```

```
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbClusterParameterGroup(groupRequest)
        println("The group name is
 ${response.dbClusterParameterGroup?.dbClusterParameterGroupName}")
    }
}
```

- API-Details finden Sie unter CreateDB ClusterParameter Group in der AWS SDK for Kotlin API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def create_parameter_group(
```

```
        self, parameter_group_name, parameter_group_family, description
    ):
        """
        Creates a DB cluster parameter group that is based on the specified
parameter group
        family.

        :param parameter_group_name: The name of the newly created parameter
group.
        :param parameter_group_family: The family that is used as the basis of
the new
                                       parameter group.
        :param description: A description given to the parameter group.
        :return: Data about the newly created parameter group.
        """
        try:
            response = self.rds_client.create_db_cluster_parameter_group(
                DBClusterParameterGroupName=parameter_group_name,
                DBParameterGroupFamily=parameter_group_family,
                Description=description,
            )
        except ClientError as err:
            logger.error(
                "Couldn't create parameter group %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- API-Details finden Sie unter ClusterParameterCreateDB-Gruppe in der API-Referenz für AWS SDK for Python (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   // Select an engine family and create a custom DB cluster parameter group.
rds.CreateDbClusterParameterGroup(DBParameterGroupFamily='aurora-mysql8.0')
   pub async fn set_engine(&mut self, engine: &str, version: &str) -> Result<(),
ScenarioError> {
       self.engine_family = Some(engine.to_string());
       self.engine_version = Some(version.to_string());
       let create_db_cluster_parameter_group = self
           .rds
           .create_db_cluster_parameter_group(
               DB_CLUSTER_PARAMETER_GROUP_NAME,
               DB_CLUSTER_PARAMETER_GROUP_DESCRIPTION,
               engine,
           )
           .await;

       match create_db_cluster_parameter_group {
           Ok(CreateDbClusterParameterGroupOutput {
               db_cluster_parameter_group: None,
               ..
           }) => {
               return Err(ScenarioError::with(
                   "CreateDBClusterParameterGroup had empty response",
               ));
           }
           Err(error) => {
               if error.code() == Some("DBParameterGroupAlreadyExists") {
                   info!("Cluster Parameter Group already exists, nothing to
do");
               } else {
                   return Err(ScenarioError::new(
                       "Could not create Cluster Parameter Group",
                       &error,
```

```
                    ));
                }
            }
            _ => {
                info!("Created Cluster Parameter Group");
            }
        }

        Ok(())
    }

    pub async fn create_db_cluster_parameter_group(
        &self,
        name: &str,
        description: &str,
        family: &str,
    ) -> Result<CreateDbClusterParameterGroupOutput,
 SdkError<CreateDBClusterParameterGroupError>>
    {
        self.inner
            .create_db_cluster_parameter_group()
            .db_cluster_parameter_group_name(name)
            .description(description)
            .db_parameter_group_family(family)
            .send()
            .await
    }

#[tokio::test]
async fn test_scenario_set_engine() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .with(
            eq("RustSDKCodeExamplesDBParameterGroup"),
            eq("Parameter Group created by Rust SDK Code Example"),
            eq("aurora-mysql"),
        )
        .return_once(|_, _, _| {
            Ok(CreateDbClusterParameterGroupOutput::builder()

 .db_cluster_parameter_group(DbClusterParameterGroup::builder().build())
                .build())
```

```
        });

    let mut scenario = AuroraScenario::new(mock_rds);

    let set_engine = scenario.set_engine("aurora-mysql", "aurora-
mysql8.0").await;

    assert_eq!(set_engine, Ok(()));
    assert_eq!(Some("aurora-mysql"), scenario.engine_family.as_deref());
    assert_eq!(Some("aurora-mysql8.0"), scenario.engine_version.as_deref());
}

#[tokio::test]
async fn test_scenario_set_engine_not_create() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .with(
            eq("RustSDKCodeExamplesDBParameterGroup"),
            eq("Parameter Group created by Rust SDK Code Example"),
            eq("aurora-mysql"),
        )
        .return_once(|_, _, _|
 Ok(CreateDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);

    let set_engine = scenario.set_engine("aurora-mysql", "aurora-
mysql8.0").await;

    assert!(set_engine.is_err());
}

#[tokio::test]
async fn test_scenario_set_engine_param_group_exists() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .withf(|_, _, _| true)
        .return_once(|_, _, _| {
            Err(SdkError::service_error(
```

```
 CreateDBClusterParameterGroupError::DbParameterGroupAlreadyExistsFault(
                    DbParameterGroupAlreadyExistsFault::builder().build(),
                ),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);

    let set_engine = scenario.set_engine("aurora-mysql", "aurora-
mysql8.0").await;

    assert!(set_engine.is_err());
}
```

- Einzelheiten zur API finden Sie unter CreateDB ClusterParameter Group in der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`CreateDBClusterSnapshot`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`CreateDBClusterSnapshot`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Create a snapshot of a cluster.
    /// </summary>
    /// <param name="dbClusterIdentifier">DB cluster identifier.</param>
    /// <param name="snapshotIdentifier">Identifier for the snapshot.</param>
    /// <returns>DB snapshot object.</returns>
    public async Task<DBClusterSnapshot>
CreateClusterSnapshotByIdentifierAsync(string dbClusterIdentifier, string
snapshotIdentifier)
    {
        var response = await _amazonRDS.CreateDBClusterSnapshotAsync(
            new CreateDBClusterSnapshotRequest()
            {
                DBClusterIdentifier = dbClusterIdentifier,
                DBClusterSnapshotIdentifier = snapshotIdentifier,
            });

        return response.DBClusterSnapshot;
    }
```

- Einzelheiten zur API finden Sie unter CreateDB ClusterSnapshot in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

            Aws::RDS::Model::CreateDBClusterSnapshotRequest request;
            request.SetDBClusterIdentifier(DB_CLUSTER_IDENTIFIER);
            request.SetDBClusterSnapshotIdentifier(snapshotID);

            Aws::RDS::Model::CreateDBClusterSnapshotOutcome outcome =
                    client.CreateDBClusterSnapshot(request);

            if (outcome.IsSuccess()) {
                std::cout << "Snapshot creation has started."
                          << std::endl;
            }
            else {
                std::cerr << "Error with Aurora::CreateDBClusterSnapshot. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
                                 DB_CLUSTER_IDENTIFIER, DB_INSTANCE_IDENTIFIER,
client);
                return false;
            }
```

- Einzelheiten zur API finden Sie unter CreateDB ClusterSnapshot in der AWS SDK for C++ API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// CreateClusterSnapshot creates a snapshot of a DB cluster.
func (clusters *DbClusters) CreateClusterSnapshot(clusterName string,
 snapshotName string) (
 *types.DBClusterSnapshot, error) {
 output, err := clusters.AuroraClient.CreateDBClusterSnapshot(context.TODO(),
 &rds.CreateDBClusterSnapshotInput{
  DBClusterIdentifier:         aws.String(clusterName),
  DBClusterSnapshotIdentifier: aws.String(snapshotName),
 })
 if err != nil {
  log.Printf("Couldn't create snapshot %v: %v\n", snapshotName, err)
  return nil, err
 } else {
  return output.DBClusterSnapshot, nil
 }
}
```

- Einzelheiten zur API finden Sie unter CreateDB ClusterSnapshot in der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void createDBClusterSnapshot(RdsClient rdsClient, String
dbInstanceClusterIdentifier,
           String dbSnapshotIdentifier) {
       try {
           CreateDbClusterSnapshotRequest snapshotRequest =
CreateDbClusterSnapshotRequest.builder()
                   .dbClusterIdentifier(dbInstanceClusterIdentifier)
                   .dbClusterSnapshotIdentifier(dbSnapshotIdentifier)
                   .build();

           CreateDbClusterSnapshotResponse response =
rdsClient.createDBClusterSnapshot(snapshotRequest);
           System.out.println("The Snapshot ARN is " +
response.dbClusterSnapshot().dbClusterSnapshotArn());

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Einzelheiten zur API finden Sie unter CreateDB ClusterSnapshot in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun createDBClusterSnapshot(
    dbInstanceClusterIdentifier: String?,
    dbSnapshotIdentifier: String?,
) {
    val snapshotRequest =
        CreateDbClusterSnapshotRequest {
            dbClusterIdentifier = dbInstanceClusterIdentifier
            dbClusterSnapshotIdentifier = dbSnapshotIdentifier
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbClusterSnapshot(snapshotRequest)
        println("The Snapshot ARN is
 ${response.dbClusterSnapshot?.dbClusterSnapshotArn}")
    }
}
```

- API-Details finden Sie unter CreateDB ClusterSnapshot in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def create_cluster_snapshot(self, snapshot_id, cluster_id):
        """
        Creates a snapshot of a DB cluster.

        :param snapshot_id: The ID to give the created snapshot.
        :param cluster_id: The DB cluster to snapshot.
        :return: Data about the newly created snapshot.
        """
        try:
            response = self.rds_client.create_db_cluster_snapshot(
                DBClusterSnapshotIdentifier=snapshot_id,
 DBClusterIdentifier=cluster_id
            )
            snapshot = response["DBClusterSnapshot"]
        except ClientError as err:
            logger.error(
                "Couldn't create snapshot of %s. Here's why: %s: %s",
                cluster_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return snapshot
```

- API-Details finden Sie unter CreateDB ClusterSnapshot in AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   // Get a list of allowed engine versions.
rds.DescribeDbEngineVersions(Engine='aurora-mysql', DBParameterGroupFamily=<the
family used to create your parameter group in step 2>)
   // Create an Aurora DB cluster database cluster that contains a MySql
database and uses the parameter group you created.
   // Wait for DB cluster to be ready. Call rds.DescribeDBClusters and check for
Status == 'available'.
   // Get a list of instance classes available for the selected engine
and engine version. rds.DescribeOrderableDbInstanceOptions(Engine='mysql',
EngineVersion=).

   // Create a database instance in the cluster.
   // Wait for DB instance to be ready. Call rds.DescribeDbInstances and check
for DBInstanceStatus == 'available'.
   pub async fn start_cluster_and_instance(&mut self) -> Result<(),
ScenarioError> {
       if self.password.is_none() {
           return Err(ScenarioError::with(
               "Must set Secret Password before starting a cluster",
           ));
       }
       let create_db_cluster = self
           .rds
           .create_db_cluster(
               DB_CLUSTER_IDENTIFIER,
```

```
                DB_CLUSTER_PARAMETER_GROUP_NAME,
                DB_ENGINE,
                self.engine_version.as_deref().expect("engine version"),
                self.username.as_deref().expect("username"),
                self.password
                    .replace(SecretString::new("".to_string()))
                    .expect("password"),
            )
            .await;
        if let Err(err) = create_db_cluster {
            return Err(ScenarioError::new(
                "Failed to create DB Cluster with cluster group",
                &err,
            ));
        }

        self.db_cluster_identifier = create_db_cluster
            .unwrap()
            .db_cluster
            .and_then(|c| c.db_cluster_identifier);

        if self.db_cluster_identifier.is_none() {
            return Err(ScenarioError::with("Created DB Cluster missing
Identifier"));
        }

        info!(
            "Started a db cluster: {}",
            self.db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing ARN")
        );

        let create_db_instance = self
            .rds
            .create_db_instance(
                self.db_cluster_identifier.as_deref().expect("cluster name"),
                DB_INSTANCE_IDENTIFIER,
                self.instance_class.as_deref().expect("instance class"),
                DB_ENGINE,
            )
            .await;
        if let Err(err) = create_db_instance {
            return Err(ScenarioError::new(
```

```
                "Failed to create Instance in DB Cluster",
                &err,
            ));
        }

        self.db_instance_identifier = create_db_instance
            .unwrap()
            .db_instance
            .and_then(|i| i.db_instance_identifier);

        // Cluster creation can take up to 20 minutes to become available
        let cluster_max_wait = Duration::from_secs(20 * 60);
        let waiter = Waiter::builder().max(cluster_max_wait).build();
        while waiter.sleep().await.is_ok() {
            let cluster = self
                .rds
                .describe_db_clusters(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = cluster {
                warn!(?err, "Failed to describe cluster while waiting for
ready");
                continue;
            }

            let instance = self
                .rds
                .describe_db_instance(
                    self.db_instance_identifier
                        .as_deref()
                        .expect("instance identifier"),
                )
                .await;
            if let Err(err) = instance {
                return Err(ScenarioError::new(
                    "Failed to find instance for cluster",
                    &err,
                ));
            }
```

```
            let instances_available = instance
                .unwrap()
                .db_instances()
                .iter()
                .all(|instance| instance.db_instance_status() ==
Some("Available"));

            let endpoints = self
                .rds
                .describe_db_cluster_endpoints(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = endpoints {
                return Err(ScenarioError::new(
                    "Failed to find endpoint for cluster",
                    &err,
                ));
            }

            let endpoints_available = endpoints
                .unwrap()
                .db_cluster_endpoints()
                .iter()
                .all(|endpoint| endpoint.status() == Some("available"));

            if instances_available && endpoints_available {
                return Ok(());
            }
        }

        Err(ScenarioError::with("timed out waiting for cluster"))
    }

    pub async fn snapshot_cluster(
        &self,
        db_cluster_identifier: &str,
        snapshot_name: &str,
    ) -> Result<CreateDbClusterSnapshotOutput,
SdkError<CreateDBClusterSnapshotError>> {
        self.inner
```

```
            .create_db_cluster_snapshot()
            .db_cluster_identifier(db_cluster_identifier)
            .db_cluster_snapshot_identifier(snapshot_name)
            .send()
            .await
    }

#[tokio::test]
async fn test_start_cluster_and_instance() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
```

```
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_describe_db_instance()
        .with(eq("RustSDKCodeExamplesDBInstance"))
        .return_once(|name| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_instance_identifier(name)
                        .db_instance_status("Available")
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()

.db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
```

```
    scenario.password = Some(SecretString::new("test password".into()));

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
        assert!(scenario
            .password
            .replace(SecretString::new("BAD SECRET".into()))
            .unwrap()
            .expose_secret()
            .is_empty());
        assert_eq!(
            scenario.db_cluster_identifier,
            Some("RustSDKCodeExamplesDBCluster".into())
        );
    });
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Err(SdkError::service_error(
                CreateDBClusterError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db cluster error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));
```

```
    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _}) if message
 == "Failed to create DB Cluster with cluster group")
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_missing_id() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()
                .db_cluster(DbCluster::builder().build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context:_ }) if message
 == "Created DB Cluster missing Identifier");
}

#[tokio::test]
async fn test_start_cluster_and_instance_instance_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
```

```
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .return_once(|_, _, _, _| {
            Err(SdkError::service_error(
                CreateDBInstanceError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db instance error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _ }) if message
 == "Failed to create Instance in DB Cluster")
}

#[tokio::test]
async fn test_start_cluster_and_instance_wait_hiccup() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
```

```
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

.db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe cluster error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        })
```

```
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds.expect_describe_db_instance().return_once(|name| {
        Ok(DescribeDbInstancesOutput::builder()
            .db_instances(
                DbInstance::builder()
                    .db_instance_identifier(name)
                    .db_instance_status("Available")
                    .build(),
            )
            .build())
    });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()

.db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
```

```
    let _ = assertions.await;
}
```

- Einzelheiten zur API finden Sie unter CreateDB ClusterSnapshot in der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`CreateDBInstance`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`CreateDBInstance`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   /// <summary>
   /// Create an Amazon Relational Database Service (Amazon RDS) DB instance
   /// with a particular set of properties. Use the action
DescribeDBInstancesAsync
   /// to determine when the DB instance is ready to use.
   /// </summary>
   /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
   /// <param name="dbClusterIdentifier">DB cluster identifier.</param>
   /// <param name="dbEngine">The engine for the DB instance.</param>
   /// <param name="dbEngineVersion">Version for the DB instance.</param>
```

```
    /// <param name="instanceClass">Class for the DB instance.</param>
    /// <returns>DB instance object.</returns>
    public async Task<DBInstance> CreateDBInstanceInClusterAsync(
        string dbClusterIdentifier,
        string dbInstanceIdentifier,
        string dbEngine,
        string dbEngineVersion,
        string instanceClass)
    {
        // When creating the instance within a cluster, do not specify the name
or size.
        var response = await _amazonRDS.CreateDBInstanceAsync(
            new CreateDBInstanceRequest()
            {
                DBClusterIdentifier = dbClusterIdentifier,
                DBInstanceIdentifier = dbInstanceIdentifier,
                Engine = dbEngine,
                EngineVersion = dbEngineVersion,
                DBInstanceClass = instanceClass
            });

        return response.DBInstance;
    }
```

- Weitere API-Informationen finden Sie unter CreateDBInstance in der AWS SDK for .NET - API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";
```

```
    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::CreateDBInstanceRequest request;
        request.SetDBInstanceIdentifier(DB_INSTANCE_IDENTIFIER);
        request.SetDBClusterIdentifier(DB_CLUSTER_IDENTIFIER);
        request.SetEngine(engineName);
        request.SetDBInstanceClass(dbInstanceClass);

        Aws::RDS::Model::CreateDBInstanceOutcome outcome =
                client.CreateDBInstance(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB instance creation has started."
                      << std::endl;
        }
        else {
            std::cerr << "Error with RDS::CreateDBInstance. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, DB_CLUSTER_IDENTIFIER,
"",
                             client);
            return false;
        }
```

- Weitere API-Informationen finden Sie unter CreateDBInstance in der AWS SDK for C++ - API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// CreateInstanceInCluster creates a database instance in an existing DB cluster.
 The first database that is
// created defaults to a read-write DB instance.
func (clusters *DbClusters) CreateInstanceInCluster(clusterName string,
 instanceName string,
 dbEngine string, dbInstanceClass string) (*types.DBInstance, error) {
 output, err := clusters.AuroraClient.CreateDBInstance(context.TODO(),
 &rds.CreateDBInstanceInput{
  DBInstanceIdentifier: aws.String(instanceName),
  DBClusterIdentifier:  aws.String(clusterName),
  Engine:               aws.String(dbEngine),
  DBInstanceClass:      aws.String(dbInstanceClass),
 })
 if err != nil {
  log.Printf("Couldn't create instance %v: %v\n", instanceName, err)
  return nil, err
 } else {
  return output.DBInstance, nil
 }
}
```

- Weitere API-Informationen finden Sie unter CreateDBInstance in der AWS SDK for Go -API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public static String createDBInstanceCluster(RdsClient rdsClient,
            String dbInstanceIdentifier,
            String dbInstanceClusterIdentifier,
            String instanceClass) {
        try {
            CreateDbInstanceRequest instanceRequest =
CreateDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .dbClusterIdentifier(dbInstanceClusterIdentifier)
                    .engine("aurora-mysql")
                    .dbInstanceClass(instanceClass)
                    .build();

            CreateDbInstanceResponse response =
rdsClient.createDBInstance(instanceRequest);
            System.out.print("The status is " +
response.dbInstance().dbInstanceStatus());
            return response.dbInstance().dbInstanceArn();

        } catch (RdsException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }
```

- Weitere API-Informationen finden Sie unter CreateDBInstance in der AWS SDK for Java 2.x -API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun createDBInstanceCluster(
```

```
    dbInstanceIdentifierVal: String?,
    dbInstanceClusterIdentifierVal: String?,
    instanceClassVal: String?,
): String? {
    val instanceRequest =
        CreateDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            dbClusterIdentifier = dbInstanceClusterIdentifierVal
            engine = "aurora-mysql"
            dbInstanceClass = instanceClassVal
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbInstance(instanceRequest)
        print("The status is ${response.dbInstance?.dbInstanceStatus}")
        return response.dbInstance?.dbInstanceArn
    }
}
```

- Weitere API-Informationen finden Sie unter CreateDBInstance in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
```

```
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def create_instance_in_cluster(
        self, instance_id, cluster_id, db_engine, instance_class
    ):
        """
        Creates a database instance in an existing DB cluster. The first database
that is
        created defaults to a read-write DB instance.

        :param instance_id: The ID to give the newly created DB instance.
        :param cluster_id: The ID of the DB cluster where the DB instance is
created.
        :param db_engine: The database engine of a database to create in the DB
instance.
                          This must be compatible with the configured parameter
group
                          of the DB cluster.
        :param instance_class: The DB instance class for the newly created DB
instance.
        :return: Data about the newly created DB instance.
        """
        try:
            response = self.rds_client.create_db_instance(
                DBInstanceIdentifier=instance_id,
                DBClusterIdentifier=cluster_id,
                Engine=db_engine,
                DBInstanceClass=instance_class,
            )
            db_inst = response["DBInstance"]
        except ClientError as err:
            logger.error(
                "Couldn't create DB instance %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
```

```
                err.response["Error"]["Message"],
            )
            raise
        else:
            return db_inst
```

- Weitere API-Informationen finden Sie unter CreateDBInstance in der API-Referenz zum AWS SDK für Python (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   // Get a list of allowed engine versions.
rds.DescribeDbEngineVersions(Engine='aurora-mysql', DBParameterGroupFamily=<the
family used to create your parameter group in step 2>)
   // Create an Aurora DB cluster database cluster that contains a MySql
database and uses the parameter group you created.
   // Wait for DB cluster to be ready. Call rds.DescribeDBClusters and check for
Status == 'available'.
   // Get a list of instance classes available for the selected engine
and engine version. rds.DescribeOrderableDbInstanceOptions(Engine='mysql',
EngineVersion=).

   // Create a database instance in the cluster.
   // Wait for DB instance to be ready. Call rds.DescribeDbInstances and check
for DBInstanceStatus == 'available'.
   pub async fn start_cluster_and_instance(&mut self) -> Result<(),
ScenarioError> {
       if self.password.is_none() {
           return Err(ScenarioError::with(
               "Must set Secret Password before starting a cluster",
           ));
```

```
        }
        let create_db_cluster = self
            .rds
            .create_db_cluster(
                DB_CLUSTER_IDENTIFIER,
                DB_CLUSTER_PARAMETER_GROUP_NAME,
                DB_ENGINE,
                self.engine_version.as_deref().expect("engine version"),
                self.username.as_deref().expect("username"),
                self.password
                    .replace(SecretString::new("".to_string()))
                    .expect("password"),
            )
            .await;
        if let Err(err) = create_db_cluster {
            return Err(ScenarioError::new(
                "Failed to create DB Cluster with cluster group",
                &err,
            ));
        }

        self.db_cluster_identifier = create_db_cluster
            .unwrap()
            .db_cluster
            .and_then(|c| c.db_cluster_identifier);

        if self.db_cluster_identifier.is_none() {
            return Err(ScenarioError::with("Created DB Cluster missing
Identifier"));
        }

        info!(
            "Started a db cluster: {}",
            self.db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing ARN")
        );

        let create_db_instance = self
            .rds
            .create_db_instance(
                self.db_cluster_identifier.as_deref().expect("cluster name"),
                DB_INSTANCE_IDENTIFIER,
                self.instance_class.as_deref().expect("instance class"),
```

```
                DB_ENGINE,
            )
            .await;
        if let Err(err) = create_db_instance {
            return Err(ScenarioError::new(
                "Failed to create Instance in DB Cluster",
                &err,
            ));
        }

        self.db_instance_identifier = create_db_instance
            .unwrap()
            .db_instance
            .and_then(|i| i.db_instance_identifier);

        // Cluster creation can take up to 20 minutes to become available
        let cluster_max_wait = Duration::from_secs(20 * 60);
        let waiter = Waiter::builder().max(cluster_max_wait).build();
        while waiter.sleep().await.is_ok() {
            let cluster = self
                .rds
                .describe_db_clusters(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = cluster {
                warn!(?err, "Failed to describe cluster while waiting for
ready");
                continue;
            }

            let instance = self
                .rds
                .describe_db_instance(
                    self.db_instance_identifier
                        .as_deref()
                        .expect("instance identifier"),
                )
                .await;
            if let Err(err) = instance {
                return Err(ScenarioError::new(
```

```
                    "Failed to find instance for cluster",
                    &err,
                ));
            }

            let instances_available = instance
                .unwrap()
                .db_instances()
                .iter()
                .all(|instance| instance.db_instance_status() ==
Some("Available"));

            let endpoints = self
                .rds
                .describe_db_cluster_endpoints(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = endpoints {
                return Err(ScenarioError::new(
                    "Failed to find endpoint for cluster",
                    &err,
                ));
            }

            let endpoints_available = endpoints
                .unwrap()
                .db_cluster_endpoints()
                .iter()
                .all(|endpoint| endpoint.status() == Some("available"));

            if instances_available && endpoints_available {
                return Ok(());
            }
        }

        Err(ScenarioError::with("timed out waiting for cluster"))
    }

    pub async fn create_db_instance(
        &self,
```

```
        cluster_name: &str,
        instance_name: &str,
        instance_class: &str,
        engine: &str,
    ) -> Result<CreateDbInstanceOutput, SdkError<CreateDBInstanceError>> {
        self.inner
            .create_db_instance()
            .db_cluster_identifier(cluster_name)
            .db_instance_identifier(instance_name)
            .db_instance_class(instance_class)
            .engine(engine)
            .send()
            .await
    }

#[tokio::test]
async fn test_start_cluster_and_instance() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
```

```
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_describe_db_instance()
        .with(eq("RustSDKCodeExamplesDBInstance"))
        .return_once(|name| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_instance_identifier(name)
                        .db_instance_status("Available")
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()
```

```
 .db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
        assert!(scenario
            .password
            .replace(SecretString::new("BAD SECRET".into()))
            .unwrap()
            .expose_secret()
            .is_empty());
        assert_eq!(
            scenario.db_cluster_identifier,
            Some("RustSDKCodeExamplesDBCluster".into())
        );
    });
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Err(SdkError::service_error(
                CreateDBClusterError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db cluster error",
                ))),
```

```
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _}) if message
 == "Failed to create DB Cluster with cluster group")
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_missing_id() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()
                .db_cluster(DbCluster::builder().build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context:_ }) if message
 == "Created DB Cluster missing Identifier");
}

#[tokio::test]
async fn test_start_cluster_and_instance_instance_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
```

```
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .return_once(|_, _, _, _| {
            Err(SdkError::service_error(
                CreateDBInstanceError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db instance error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _ }) if message
 == "Failed to create Instance in DB Cluster")
}

#[tokio::test]
async fn test_start_cluster_and_instance_wait_hiccup() {
    let mut mock_rds = MockRdsImpl::default();
```

```
    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

.db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
```

```
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe cluster error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        })
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds.expect_describe_db_instance().return_once(|name| {
        Ok(DescribeDbInstancesOutput::builder()
            .db_instances(
                DbInstance::builder()
                    .db_instance_identifier(name)
                    .db_instance_status("Available")
                    .build(),
            )
            .build())
    });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()

.db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));
```

```
    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
    let _ = assertions.await;
}
```

- Informationen zu APIs finden Sie unter CreateDBInstance in der API-Referenz zum AWS -SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DeleteDBCluster`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DeleteDBCluster`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Delete a particular DB cluster.
    /// </summary>
    /// <param name="dbClusterIdentifier">DB cluster identifier.</param>
    /// <returns>DB cluster object.</returns>
    public async Task<DBCluster> DeleteDBClusterByIdentifierAsync(string
dbClusterIdentifier)
    {
        var response = await _amazonRDS.DeleteDBClusterAsync(
            new DeleteDBClusterRequest()
            {
                DBClusterIdentifier = dbClusterIdentifier,
                SkipFinalSnapshot = true
            });

        return response.DBCluster;
    }
```

- Weitere API-Informationen finden Sie unter DeleteDBCluster in der API-Referenz zu AWS SDK for .NET .

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

            Aws::RDS::Model::DeleteDBClusterRequest request;
            request.SetDBClusterIdentifier(dbClusterIdentifier);
            request.SetSkipFinalSnapshot(true);
```

```
            Aws::RDS::Model::DeleteDBClusterOutcome outcome =
                    client.DeleteDBCluster(request);

            if (outcome.IsSuccess()) {
                std::cout << "DB cluster deletion has started."
                          << std::endl;
                clusterDeleting = true;
                std::cout
                        << "Waiting for DB cluster to delete before deleting the
 parameter group."
                        << std::endl;
                std::cout << "This may take a while." << std::endl;
            }
            else {
                std::cerr << "Error with Aurora::DeleteDBCluster. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                result = false;
            }
```

- Weitere API-Informationen finden Sie unter DeleteDBCluster in der API-Referenz zu AWS SDK for C++ .

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}
```

```
// DeleteDbCluster deletes a DB cluster without keeping a final snapshot.
func (clusters *DbClusters) DeleteDbCluster(clusterName string) error {
 _, err := clusters.AuroraClient.DeleteDBCluster(context.TODO(),
 &rds.DeleteDBClusterInput{
  DBClusterIdentifier: aws.String(clusterName),
  SkipFinalSnapshot:   true,
 })
 if err != nil {
  log.Printf("Couldn't delete DB cluster %v: %v\n", clusterName, err)
  return err
 } else {
  return nil
 }
}
```

- Weitere API-Informationen finden Sie unter DeleteDBCluster in der API-Referenz zu AWS SDK for Go .

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void deleteCluster(RdsClient rdsClient, String
dbInstanceClusterIdentifier) {
       try {
           DeleteDbClusterRequest deleteDbClusterRequest =
DeleteDbClusterRequest.builder()
                   .dbClusterIdentifier(dbInstanceClusterIdentifier)
                   .skipFinalSnapshot(true)
                   .build();

           rdsClient.deleteDBCluster(deleteDbClusterRequest);
```

```
            System.out.println(dbInstanceClusterIdentifier + " was deleted!");

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Weitere API-Informationen finden Sie unter DeleteDBCluster in der API-Referenz zu AWS SDK for Java 2.x .

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun deleteCluster(dbInstanceClusterIdentifier: String) {
    val deleteDbClusterRequest =
        DeleteDbClusterRequest {
            dbClusterIdentifier = dbInstanceClusterIdentifier
            skipFinalSnapshot = true
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        rdsClient.deleteDbCluster(deleteDbClusterRequest)
        println("$dbInstanceClusterIdentifier was deleted!")
    }
}
```

- Weitere API-Informationen finden Sie unter DeleteDBCluster in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def delete_db_cluster(self, cluster_name):
        """
        Deletes a DB cluster.

        :param cluster_name: The name of the DB cluster to delete.
        """
        try:
            self.rds_client.delete_db_cluster(
                DBClusterIdentifier=cluster_name, SkipFinalSnapshot=True
            )
            logger.info("Deleted DB cluster %s.", cluster_name)
        except ClientError:
            logger.exception("Couldn't delete DB cluster %s.", cluster_name)
```

```
            raise
```

- Weitere API-Informationen finden Sie unter DeleteDBCluster in der API-Referenz zum AWS SDK für Python (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    pub async fn clean_up(self) -> Result<(), Vec<ScenarioError>> {
        let mut clean_up_errors: Vec<ScenarioError> = vec![];

        // Delete the instance. rds.DeleteDbInstance.
        let delete_db_instance = self
            .rds
            .delete_db_instance(
                self.db_instance_identifier
                    .as_deref()
                    .expect("instance identifier"),
            )
            .await;
        if let Err(err) = delete_db_instance {
            let identifier = self
                .db_instance_identifier
                .as_deref()
                .unwrap_or("Missing Instance Identifier");
            let message = format!("failed to delete db instance {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance to delete
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
```

```
                let describe_db_instances =
self.rds.describe_db_instances().await;
                if let Err(err) = describe_db_instances {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check instance state during deletion",
                        &err,
                    ));
                    break;
                }
                let db_instances = describe_db_instances
                    .unwrap()
                    .db_instances()
                    .iter()
                    .filter(|instance| instance.db_cluster_identifier ==
self.db_cluster_identifier)
                    .cloned()
                    .collect::<Vec<DbInstance>>();

                if db_instances.is_empty() {
                    trace!("Delete Instance waited and no instances were found");
                    break;
                }
                match db_instances.first().unwrap().db_instance_status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but instances is in
{status}");
                        continue;
                    }
                    None => {
                        warn!("No status for DB instance");
                        break;
                    }
                }
            }
        }

        // Delete the DB cluster. rds.DeleteDbCluster.
        let delete_db_cluster = self
            .rds
            .delete_db_cluster(
                self.db_cluster_identifier
                    .as_deref()
                    .expect("cluster identifier"),
```

```
            )
            .await;

        if let Err(err) = delete_db_cluster {
            let identifier = self
                .db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing DB Cluster Identifier");
            let message = format!("failed to delete db cluster {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance and cluster to fully delete.
rds.DescribeDbInstances and rds.DescribeDbClusters until both are not found.
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
                let describe_db_clusters = self
                    .rds
                    .describe_db_clusters(
                        self.db_cluster_identifier
                            .as_deref()
                            .expect("cluster identifier"),
                    )
                    .await;
                if let Err(err) = describe_db_clusters {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check cluster state during deletion",
                        &err,
                    ));
                    break;
                }
                let describe_db_clusters = describe_db_clusters.unwrap();
                let db_clusters = describe_db_clusters.db_clusters();
                if db_clusters.is_empty() {
                    trace!("Delete cluster waited and no clusters were found");
                    break;
                }
                match db_clusters.first().unwrap().status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but clusters is in
{status}");
                        continue;
                    }
                    None => {
```

```
                        warn!("No status for DB cluster");
                        break;
                    }
                }
            }
        }

        // Delete the DB cluster parameter group.
rds.DeleteDbClusterParameterGroup.
        let delete_db_cluster_parameter_group = self
            .rds
            .delete_db_cluster_parameter_group(
                self.db_cluster_parameter_group
                    .map(|g| {
                        g.db_cluster_parameter_group_name
                            .unwrap_or_else(||
DB_CLUSTER_PARAMETER_GROUP_NAME.to_string())
                    })
                    .as_deref()
                    .expect("cluster parameter group name"),
            )
            .await;
        if let Err(error) = delete_db_cluster_parameter_group {
            clean_up_errors.push(ScenarioError::new(
                "Failed to delete the db cluster parameter group",
                &error,
            ))
        }

        if clean_up_errors.is_empty() {
            Ok(())
        } else {
            Err(clean_up_errors)
        }
    }

    pub async fn delete_db_cluster(
        &self,
        cluster_identifier: &str,
    ) -> Result<DeleteDbClusterOutput, SdkError<DeleteDBClusterError>> {
        self.inner
            .delete_db_cluster()
            .db_cluster_identifier(cluster_identifier)
            .skip_final_snapshot(true)
```

```
            .send()
            .await
    }

#[tokio::test]
async fn test_scenario_clean_up() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| Ok(DescribeDbInstancesOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
```

```
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| Ok(DescribeDbClustersOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
 Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
```

```
async fn test_scenario_clean_up_errors() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| {
            Err(SdkError::service_error(
                DescribeDBInstancesError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db instances error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
```

```
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db clusters error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_err());
        let errs = clean_up.unwrap_err();
        assert_eq!(errs.len(), 2);
```

```
        assert_matches!(errs.get(0), Some(ScenarioError {message, context: _}) if
 message == "Failed to check instance state during deletion");
        assert_matches!(errs.get(1), Some(ScenarioError {message, context: _}) if
 message == "Failed to check cluster state during deletion");
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}
```

- Informationen zu APIs finden Sie unter DeleteDBCluster in der API-Referenz zum AWS - SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DeleteDBClusterParameterGroup`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DeleteDBClusterParameterGroup`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Delete a particular parameter group by name.
    /// </summary>
    /// <param name="groupName">The name of the parameter group.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteClusterParameterGroupByNameAsync(string
groupName)
    {
        var request = new DeleteDBClusterParameterGroupRequest
        {
            DBClusterParameterGroupName = groupName,
        };

        var response = await
_amazonRDS.DeleteDBClusterParameterGroupAsync(request);
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }
```

- Einzelheiten zur API finden Sie unter ClusterParameterDeleteDB-Gruppe in AWS SDK for .NET der API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::DeleteDBClusterParameterGroupRequest request;
        request.SetDBClusterParameterGroupName(parameterGroupName);

        Aws::RDS::Model::DeleteDBClusterParameterGroupOutcome outcome =
                client.DeleteDBClusterParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB parameter group was successfully deleted."
                      << std::endl;
        }
        else {
            std::cerr << "Error with Aurora::DeleteDBClusterParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            result = false;
        }
```

- Einzelheiten zur API finden Sie unter ClusterParameterDeleteDB-Gruppe in AWS SDK for C ++ der API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}
```

```
// DeleteParameterGroup deletes the named DB cluster parameter group.
func (clusters *DbClusters) DeleteParameterGroup(parameterGroupName string) error
 {
 _, err := clusters.AuroraClient.DeleteDBClusterParameterGroup(context.TODO(),
  &rds.DeleteDBClusterParameterGroupInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
  })
 if err != nil {
  log.Printf("Couldn't delete parameter group %v: %v\n", parameterGroupName, err)
  return err
 } else {
  return nil
 }
}
```

- Einzelheiten zur API finden Sie unter ClusterParameterDeleteDB-Gruppe in AWS SDK for Go der API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void deleteDBClusterGroup(RdsClient rdsClient, String
dbClusterGroupName, String clusterDBARN)
           throws InterruptedException {
       try {
           boolean isDataDel = false;
           boolean didFind;
           String instanceARN;
```

```
            // Make sure that the database has been deleted.
            while (!isDataDel) {
                DescribeDbInstancesResponse response =
rdsClient.describeDBInstances();
                List<DBInstance> instanceList = response.dbInstances();
                int listSize = instanceList.size();
                didFind = false;
                int index = 1;
                for (DBInstance instance : instanceList) {
                    instanceARN = instance.dbInstanceArn();
                    if (instanceARN.compareTo(clusterDBARN) == 0) {
                        System.out.println(clusterDBARN + " still exists");
                        didFind = true;
                    }
                    if ((index == listSize) && (!didFind)) {
                        // Went through the entire list and did not find the
database ARN.
                        isDataDel = true;
                    }
                    Thread.sleep(sleepTime * 1000);
                    index++;
                }
            }

            DeleteDbClusterParameterGroupRequest clusterParameterGroupRequest =
DeleteDbClusterParameterGroupRequest
                    .builder()
                    .dbClusterParameterGroupName(dbClusterGroupName)
                    .build();


rdsClient.deleteDBClusterParameterGroup(clusterParameterGroupRequest);
            System.out.println(dbClusterGroupName + " was deleted.");

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie unter ClusterParameterDeleteDB-Gruppe in AWS SDK for Java 2.x der API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
@Throws(InterruptedException::class)
suspend fun deleteDBClusterGroup(
    dbClusterGroupName: String,
    clusterDBARN: String,
) {
    var isDataDel = false
    var didFind: Boolean
    var instanceARN: String

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        // Make sure that the database has been deleted.
        while (!isDataDel) {
            val response = rdsClient.describeDbInstances()
            val instanceList = response.dbInstances
            val listSize = instanceList?.size
            isDataDel = false
            didFind = false
            var index = 1
            if (instanceList != null) {
                for (instance in instanceList) {
                    instanceARN = instance.dbInstanceArn.toString()
                    if (instanceARN.compareTo(clusterDBARN) == 0) {
                        println("$clusterDBARN still exists")
                        didFind = true
                    }
                    if (index == listSize && !didFind) {
                        // Went through the entire list and did not find the
 database ARN.
                        isDataDel = true
                    }
                    delay(slTime * 1000)
                    index++
```

```
                }
            }
        }
        val clusterParameterGroupRequest =
            DeleteDbClusterParameterGroupRequest {
                dbClusterParameterGroupName = dbClusterGroupName
            }

        rdsClient.deleteDbClusterParameterGroup(clusterParameterGroupRequest)
        println("$dbClusterGroupName was deleted.")
    }
}
```

- API-Details finden Sie unter DeleteDB ClusterParameter Group in der AWS SDK for Kotlin API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
```

```
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def delete_parameter_group(self, parameter_group_name):
        """
        Deletes a DB cluster parameter group.

        :param parameter_group_name: The name of the parameter group to delete.
        :return: Data about the parameter group.
        """
        try:
            response = self.rds_client.delete_db_cluster_parameter_group(
                DBClusterParameterGroupName=parameter_group_name
            )
        except ClientError as err:
            logger.error(
                "Couldn't delete parameter group %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- API-Details finden Sie unter ClusterParameterDeleteDB-Gruppe in der API-Referenz für AWS SDK for Python (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    pub async fn clean_up(self) -> Result<(), Vec<ScenarioError>> {
        let mut clean_up_errors: Vec<ScenarioError> = vec![];

        // Delete the instance. rds.DeleteDbInstance.
        let delete_db_instance = self
            .rds
            .delete_db_instance(
                self.db_instance_identifier
                    .as_deref()
                    .expect("instance identifier"),
            )
            .await;
        if let Err(err) = delete_db_instance {
            let identifier = self
                .db_instance_identifier
                .as_deref()
                .unwrap_or("Missing Instance Identifier");
            let message = format!("failed to delete db instance {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance to delete
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
                let describe_db_instances =
self.rds.describe_db_instances().await;
                if let Err(err) = describe_db_instances {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check instance state during deletion",
                        &err,
                    ));
                    break;
                }
                let db_instances = describe_db_instances
                    .unwrap()
                    .db_instances()
                    .iter()
                    .filter(|instance| instance.db_cluster_identifier ==
self.db_cluster_identifier)
                    .cloned()
                    .collect::<Vec<DbInstance>>();

                if db_instances.is_empty() {
                    trace!("Delete Instance waited and no instances were found");
```

```
                    break;
                }
                match db_instances.first().unwrap().db_instance_status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but instances is in
{status}");
                        continue;
                    }
                    None => {
                        warn!("No status for DB instance");
                        break;
                    }
                }
            }
        }

        // Delete the DB cluster. rds.DeleteDbCluster.
        let delete_db_cluster = self
            .rds
            .delete_db_cluster(
                self.db_cluster_identifier
                    .as_deref()
                    .expect("cluster identifier"),
            )
            .await;

        if let Err(err) = delete_db_cluster {
            let identifier = self
                .db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing DB Cluster Identifier");
            let message = format!("failed to delete db cluster {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance and cluster to fully delete.
rds.DescribeDbInstances and rds.DescribeDbClusters until both are not found.
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
                let describe_db_clusters = self
                    .rds
                    .describe_db_clusters(
                        self.db_cluster_identifier
                            .as_deref()
```

```
                            .expect("cluster identifier"),
                    )
                    .await;
                if let Err(err) = describe_db_clusters {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check cluster state during deletion",
                        &err,
                    ));
                    break;
                }
                let describe_db_clusters = describe_db_clusters.unwrap();
                let db_clusters = describe_db_clusters.db_clusters();
                if db_clusters.is_empty() {
                    trace!("Delete cluster waited and no clusters were found");
                    break;
                }
                match db_clusters.first().unwrap().status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but clusters is in
{status}");
                        continue;
                    }
                    None => {
                        warn!("No status for DB cluster");
                        break;
                    }
                }
            }
        }

        // Delete the DB cluster parameter group.
rds.DeleteDbClusterParameterGroup.
        let delete_db_cluster_parameter_group = self
            .rds
            .delete_db_cluster_parameter_group(
                self.db_cluster_parameter_group
                    .map(|g| {
                        g.db_cluster_parameter_group_name
                            .unwrap_or_else(||
DB_CLUSTER_PARAMETER_GROUP_NAME.to_string())
                    })
                    .as_deref()
                    .expect("cluster parameter group name"),
```

```
            )
            .await;
        if let Err(error) = delete_db_cluster_parameter_group {
            clean_up_errors.push(ScenarioError::new(
                "Failed to delete the db cluster parameter group",
                &error,
            ))
        }

        if clean_up_errors.is_empty() {
            Ok(())
        } else {
            Err(clean_up_errors)
        }
    }

    pub async fn delete_db_cluster_parameter_group(
        &self,
        name: &str,
    ) -> Result<DeleteDbClusterParameterGroupOutput,
 SdkError<DeleteDBClusterParameterGroupError>>
    {
        self.inner
            .delete_db_cluster_parameter_group()
            .db_cluster_parameter_group_name(name)
            .send()
            .await
    }

#[tokio::test]
async fn test_scenario_clean_up() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
```

```
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| Ok(DescribeDbInstancesOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| Ok(DescribeDbClustersOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
```

```
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_scenario_clean_up_errors() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
```

```
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| {
            Err(SdkError::service_error(
                DescribeDBInstancesError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db instances error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db clusters error",
                ))),
```

```
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
 Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_err());
        let errs = clean_up.unwrap_err();
        assert_eq!(errs.len(), 2);
        assert_matches!(errs.get(0), Some(ScenarioError {message, context: _}) if
 message == "Failed to check instance state during deletion");
        assert_matches!(errs.get(1), Some(ScenarioError {message, context: _}) if
 message == "Failed to check cluster state during deletion");
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}
```

- Einzelheiten zur API finden Sie unter DeleteDB ClusterParameter Group in der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DeleteDBInstance`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DeleteDBInstance`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   /// <summary>
   /// Delete a particular DB instance.
   /// </summary>
   /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
   /// <returns>DB instance object.</returns>
   public async Task<DBInstance> DeleteDBInstanceByIdentifierAsync(string
dbInstanceIdentifier)
   {
       var response = await _amazonRDS.DeleteDBInstanceAsync(
           new DeleteDBInstanceRequest()
           {
```

```
                DBInstanceIdentifier = dbInstanceIdentifier,
                SkipFinalSnapshot = true,
                DeleteAutomatedBackups = true
            });

        return response.DBInstance;
    }
```

- Weitere API-Informationen finden Sie unter DeleteDBInstance in der API-Referenz zu AWS SDK for .NET .

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

            Aws::RDS::Model::DeleteDBInstanceRequest request;
            request.SetDBInstanceIdentifier(dbInstanceIdentifier);
            request.SetSkipFinalSnapshot(true);
            request.SetDeleteAutomatedBackups(true);

            Aws::RDS::Model::DeleteDBInstanceOutcome outcome =
                    client.DeleteDBInstance(request);

            if (outcome.IsSuccess()) {
                std::cout << "DB instance deletion has started."
                          << std::endl;
                instanceDeleting = true;
                std::cout
```

```
                        << "Waiting for DB instance to delete before deleting the
 parameter group."
                        << std::endl;
            }
            else {
                std::cerr << "Error with Aurora::DeleteDBInstance. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                result = false;
            }
```

- Weitere API-Informationen finden Sie unter DeleteDBInstance in der API-Referenz zu AWS SDK for C++ .

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// DeleteInstance deletes a DB instance.
func (clusters *DbClusters) DeleteInstance(instanceName string) error {
 _, err := clusters.AuroraClient.DeleteDBInstance(context.TODO(),
 &rds.DeleteDBInstanceInput{
  DBInstanceIdentifier:   aws.String(instanceName),
  SkipFinalSnapshot:      true,
  DeleteAutomatedBackups: aws.Bool(true),
 })
 if err != nil {
```

```
  log.Printf("Couldn't delete instance %v: %v\n", instanceName, err)
  return err
 } else {
  return nil
 }
}
```

- Weitere API-Informationen finden Sie unter DeleteDBInstance in der API-Referenz zu AWS SDK for Go .

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void deleteDatabaseInstance(RdsClient rdsClient, String
dbInstanceIdentifier) {
       try {
           DeleteDbInstanceRequest deleteDbInstanceRequest =
DeleteDbInstanceRequest.builder()
                   .dbInstanceIdentifier(dbInstanceIdentifier)
                   .deleteAutomatedBackups(true)
                   .skipFinalSnapshot(true)
                   .build();

           DeleteDbInstanceResponse response =
rdsClient.deleteDBInstance(deleteDbInstanceRequest);
           System.out.println("The status of the database is " +
response.dbInstance().dbInstanceStatus());

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
```

```
    }
```

- Weitere API-Informationen finden Sie unter DeleteDBInstance in der API-Referenz zu AWS SDK for Java 2.x .

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun deleteDBInstance(dbInstanceIdentifierVal: String) {
    val deleteDbInstanceRequest =
        DeleteDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            deleteAutomatedBackups = true
            skipFinalSnapshot = true
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.deleteDbInstance(deleteDbInstanceRequest)
        print("The status of the database is
 ${response.dbInstance?.dbInstanceStatus}")
    }
}
```

- Weitere API-Informationen finden Sie unter DeleteDBInstance in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def delete_db_instance(self, instance_id):
        """
        Deletes a DB instance.

        :param instance_id: The ID of the DB instance to delete.
        :return: Data about the deleted DB instance.
        """
        try:
            response = self.rds_client.delete_db_instance(
                DBInstanceIdentifier=instance_id,
                SkipFinalSnapshot=True,
                DeleteAutomatedBackups=True,
            )
```

```
            db_inst = response["DBInstance"]
        except ClientError as err:
            logger.error(
                "Couldn't delete DB instance %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return db_inst
```

- Weitere API-Informationen finden Sie unter DeleteDBInstance in der API-Referenz zum AWS SDK für Python (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    pub async fn clean_up(self) -> Result<(), Vec<ScenarioError>> {
        let mut clean_up_errors: Vec<ScenarioError> = vec![];

        // Delete the instance. rds.DeleteDbInstance.
        let delete_db_instance = self
            .rds
            .delete_db_instance(
                self.db_instance_identifier
                    .as_deref()
                    .expect("instance identifier"),
            )
            .await;
        if let Err(err) = delete_db_instance {
            let identifier = self
```

```
                .db_instance_identifier
                .as_deref()
                .unwrap_or("Missing Instance Identifier");
            let message = format!("failed to delete db instance {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance to delete
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
                let describe_db_instances =
self.rds.describe_db_instances().await;
                if let Err(err) = describe_db_instances {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check instance state during deletion",
                        &err,
                    ));
                    break;
                }
                let db_instances = describe_db_instances
                    .unwrap()
                    .db_instances()
                    .iter()
                    .filter(|instance| instance.db_cluster_identifier ==
self.db_cluster_identifier)
                    .cloned()
                    .collect::<Vec<DbInstance>>();

                if db_instances.is_empty() {
                    trace!("Delete Instance waited and no instances were found");
                    break;
                }
                match db_instances.first().unwrap().db_instance_status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but instances is in
{status}");
                        continue;
                    }
                    None => {
                        warn!("No status for DB instance");
                        break;
                    }
                }
            }
```

```
        }

        // Delete the DB cluster. rds.DeleteDbCluster.
        let delete_db_cluster = self
            .rds
            .delete_db_cluster(
                self.db_cluster_identifier
                    .as_deref()
                    .expect("cluster identifier"),
            )
            .await;

        if let Err(err) = delete_db_cluster {
            let identifier = self
                .db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing DB Cluster Identifier");
            let message = format!("failed to delete db cluster {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance and cluster to fully delete.
rds.DescribeDbInstances and rds.DescribeDbClusters until both are not found.
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
                let describe_db_clusters = self
                    .rds
                    .describe_db_clusters(
                        self.db_cluster_identifier
                            .as_deref()
                            .expect("cluster identifier"),
                    )
                    .await;
                if let Err(err) = describe_db_clusters {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check cluster state during deletion",
                        &err,
                    ));
                    break;
                }
                let describe_db_clusters = describe_db_clusters.unwrap();
                let db_clusters = describe_db_clusters.db_clusters();
                if db_clusters.is_empty() {
                    trace!("Delete cluster waited and no clusters were found");
                    break;
```

```
                }
                match db_clusters.first().unwrap().status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but clusters is in
{status}");
                        continue;
                    }
                    None => {
                        warn!("No status for DB cluster");
                        break;
                    }
                }
            }
        }

        // Delete the DB cluster parameter group.
rds.DeleteDbClusterParameterGroup.
        let delete_db_cluster_parameter_group = self
            .rds
            .delete_db_cluster_parameter_group(
                self.db_cluster_parameter_group
                    .map(|g| {
                        g.db_cluster_parameter_group_name
                            .unwrap_or_else(||
DB_CLUSTER_PARAMETER_GROUP_NAME.to_string())
                    })
                    .as_deref()
                    .expect("cluster parameter group name"),
            )
            .await;
        if let Err(error) = delete_db_cluster_parameter_group {
            clean_up_errors.push(ScenarioError::new(
                "Failed to delete the db cluster parameter group",
                &error,
            ))
        }

        if clean_up_errors.is_empty() {
            Ok(())
        } else {
            Err(clean_up_errors)
        }
    }
```

```
    pub async fn delete_db_instance(
        &self,
        instance_identifier: &str,
    ) -> Result<DeleteDbInstanceOutput, SdkError<DeleteDBInstanceError>> {
        self.inner
            .delete_db_instance()
            .db_instance_identifier(instance_identifier)
            .skip_final_snapshot(true)
            .send()
            .await
    }

#[tokio::test]
async fn test_scenario_clean_up() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| Ok(DescribeDbInstancesOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));
```

```
    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| Ok(DescribeDbClustersOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
Describe Instances
```

```
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_scenario_clean_up_errors() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| {
            Err(SdkError::service_error(
                DescribeDBInstancesError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db instances error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });
```

```
    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db clusters error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
```

```
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_err());
        let errs = clean_up.unwrap_err();
        assert_eq!(errs.len(), 2);
        assert_matches!(errs.get(0), Some(ScenarioError {message, context: _}) if
 message == "Failed to check instance state during deletion");
        assert_matches!(errs.get(1), Some(ScenarioError {message, context: _}) if
 message == "Failed to check cluster state during deletion");
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}
```

- Informationen zu APIs finden Sie unter DeleteDBInstance in der API-Referenz zum AWS -SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeDBClusterParameterGroups`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeDBClusterParameterGroups`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Get the description of a DB cluster parameter group by name.
    /// </summary>
    /// <param name="name">The name of the DB parameter group to describe.</
param>
    /// <returns>The parameter group description.</returns>
    public async Task<DBClusterParameterGroup?>
 DescribeCustomDBClusterParameterGroupAsync(string name)
    {
        var response = await _amazonRDS.DescribeDBClusterParameterGroupsAsync(
            new DescribeDBClusterParameterGroupsRequest()
            {
                DBClusterParameterGroupName = name
            });
        return response.DBClusterParameterGroups.FirstOrDefault();
    }
```

- Einzelheiten zur API finden Sie unter ClusterParameterDescribeDB-Gruppen in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::DescribeDBClusterParameterGroupsRequest request;
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);

        Aws::RDS::Model::DescribeDBClusterParameterGroupsOutcome outcome =
                client.DescribeDBClusterParameterGroups(request);

        if (outcome.IsSuccess()) {
            std::cout << "DB cluster parameter group named '" <<
                      CLUSTER_PARAMETER_GROUP_NAME << "' already exists." <<
 std::endl;
            dbParameterGroupFamily =
 outcome.GetResult().GetDBClusterParameterGroups()
[0].GetDBParameterGroupFamily();
        }

        else {
            std::cerr << "Error with Aurora::DescribeDBClusterParameterGroups. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
```

- Einzelheiten zur API finden Sie unter ClusterParameterDescribeDB-Gruppen in der AWS SDK for C++ API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// GetParameterGroup gets a DB cluster parameter group by name.
func (clusters *DbClusters) GetParameterGroup(parameterGroupName string) (
 *types.DBClusterParameterGroup, error) {
 output, err := clusters.AuroraClient.DescribeDBClusterParameterGroups(
  context.TODO(), &rds.DescribeDBClusterParameterGroupsInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
  })
 if err != nil {
  var notFoundError *types.DBParameterGroupNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("Parameter group %v does not exist.\n", parameterGroupName)
   err = nil
  } else {
   log.Printf("Error getting parameter group %v: %v\n", parameterGroupName, err)
  }
  return nil, err
 } else {
  return &output.DBClusterParameterGroups[0], err
 }
}
```

- Einzelheiten zur API finden Sie unter ClusterParameterDescribeDB-Gruppen in der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void describeDbClusterParameterGroups(RdsClient rdsClient,
String dbClusterGroupName) {
       try {
           DescribeDbClusterParameterGroupsRequest groupsRequest =
DescribeDbClusterParameterGroupsRequest.builder()
                   .dbClusterParameterGroupName(dbClusterGroupName)
                   .maxRecords(20)
                   .build();

           List<DBClusterParameterGroup> groups =
rdsClient.describeDBClusterParameterGroups(groupsRequest)
                   .dbClusterParameterGroups();
           for (DBClusterParameterGroup group : groups) {
               System.out.println("The group name is " +
group.dbClusterParameterGroupName());
               System.out.println("The group ARN is " +
group.dbClusterParameterGroupArn());
           }

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Einzelheiten zur API finden Sie unter ClusterParameterDescribeDB-Gruppen in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun describeDbClusterParameterGroups(dbClusterGroupName: String?) {
    val groupsRequest =
        DescribeDbClusterParameterGroupsRequest {
            dbClusterParameterGroupName = dbClusterGroupName
            maxRecords = 20
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbClusterParameterGroups(groupsRequest)
        response.dbClusterParameterGroups?.forEach { group ->
            println("The group name is ${group.dbClusterParameterGroupName}")
            println("The group ARN is ${group.dbClusterParameterGroupArn}")
        }
    }
}
```

- API-Details finden Sie unter ClusterParameterDescribeDB-Gruppen im AWS SDK für die Kotlin-API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_parameter_group(self, parameter_group_name):
        """
        Gets a DB cluster parameter group.

        :param parameter_group_name: The name of the parameter group to retrieve.
        :return: The requested parameter group.
        """
        try:
            response = self.rds_client.describe_db_cluster_parameter_groups(
                DBClusterParameterGroupName=parameter_group_name
            )
            parameter_group = response["DBClusterParameterGroups"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBParameterGroupNotFound":
                logger.info("Parameter group %s does not exist.",
 parameter_group_name)
            else:
                logger.error(
                    "Couldn't get parameter group %s. Here's why: %s: %s",
                    parameter_group_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

```
        else:
            return parameter_group
```

- API-Details finden Sie unter ClusterParameterDescribeDB-Gruppen in der API-Referenz zum AWS SDK for Python (Boto3).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeDBClusterParameters`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeDBClusterParameters`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/// <summary>
/// Describe the cluster parameters in a parameter group.
/// </summary>
/// <param name="groupName">The name of the parameter group.</param>
/// <param name="source">The optional name of the source filter.</param>
/// <returns>The collection of parameters.</returns>
```

```
    public async Task<List<Parameter>>
DescribeDBClusterParametersInGroupAsync(string groupName, string? source = null)
    {
        var paramList = new List<Parameter>();

        DescribeDBClusterParametersResponse response;
        var request = new DescribeDBClusterParametersRequest
        {
            DBClusterParameterGroupName = groupName,
            Source = source,
        };

        // Get the full list if there are multiple pages.
        do
        {
            response = await
_amazonRDS.DescribeDBClusterParametersAsync(request);
            paramList.AddRange(response.Parameters);

            request.Marker = response.Marker;
        }
        while (response.Marker is not null);

        return paramList;
    }
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterParameters in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
```

```
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);


//! Routine which gets DB parameters using the 'DescribeDBClusterParameters' api.
/*!
 \sa getDBCLusterParameters()
 \param parameterGroupName: The name of the cluster parameter group.
 \param namePrefix: Prefix string to filter results by parameter name.
 \param source: A source such as 'user', ignored if empty.
 \param parametersResult: Vector of 'Parameter' objects returned by the routine.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::getDBCLusterParameters(const Aws::String
 &parameterGroupName,
                                             const Aws::String &namePrefix,
                                             const Aws::String &source,

 Aws::Vector<Aws::RDS::Model::Parameter> &parametersResult,
                                             const Aws::RDS::RDSClient &client) {
    Aws::String marker; // The marker is used for pagination.
    do {
        Aws::RDS::Model::DescribeDBClusterParametersRequest request;
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);
        if (!marker.empty()) {
            request.SetMarker(marker);
        }
        if (!source.empty()) {
            request.SetSource(source);
        }

        Aws::RDS::Model::DescribeDBClusterParametersOutcome outcome =
                client.DescribeDBClusterParameters(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::Parameter> &parameters =
                    outcome.GetResult().GetParameters();
            for (const Aws::RDS::Model::Parameter &parameter: parameters) {
                if (!namePrefix.empty()) {
                    if (parameter.GetParameterName().find(namePrefix) == 0) {
                        parametersResult.push_back(parameter);
```

```
                    }
                }
                else {
                    parametersResult.push_back(parameter);
                }
            }

            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with Aurora::DescribeDBClusterParameters. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!marker.empty());

    return true;
}
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterParameters in der AWS SDK for C ++ API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}
```

```
// GetParameters gets the parameters that are contained in a DB cluster parameter
 group.
func (clusters *DbClusters) GetParameters(parameterGroupName string, source
 string) (
 []types.Parameter, error) {

 var output *rds.DescribeDBClusterParametersOutput
 var params []types.Parameter
 var err error
 parameterPaginator :=
 rds.NewDescribeDBClusterParametersPaginator(clusters.AuroraClient,
  &rds.DescribeDBClusterParametersInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
   Source:                      aws.String(source),
  })
 for parameterPaginator.HasMorePages() {
  output, err = parameterPaginator.NextPage(context.TODO())
  if err != nil {
   log.Printf("Couldn't get paramaeters for %v: %v\n", parameterGroupName, err)
   break
  } else {
   params = append(params, output.Parameters...)
  }
 }
 return params, err
}
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterParameters in der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void describeDbClusterParameters(RdsClient rdsClient, String
dbCLusterGroupName, int flag) {
       try {
           DescribeDbClusterParametersRequest dbParameterGroupsRequest;
           if (flag == 0) {
               dbParameterGroupsRequest =
DescribeDbClusterParametersRequest.builder()
                       .dbClusterParameterGroupName(dbCLusterGroupName)
                       .build();
           } else {
               dbParameterGroupsRequest =
DescribeDbClusterParametersRequest.builder()
                       .dbClusterParameterGroupName(dbCLusterGroupName)
                       .source("user")
                       .build();
           }

           DescribeDbClusterParametersResponse response = rdsClient
                   .describeDBClusterParameters(dbParameterGroupsRequest);
           List<Parameter> dbParameters = response.parameters();
           String paraName;
           for (Parameter para : dbParameters) {
               // Only print out information about either auto_increment_offset
or
               // auto_increment_increment.
               paraName = para.parameterName();
               if ((paraName.compareTo("auto_increment_offset") == 0)
                       || (paraName.compareTo("auto_increment_increment ") ==
0)) {
                   System.out.println("*** The parameter name is  " + paraName);
                   System.out.println("*** The parameter value is  " +
para.parameterValue());
                   System.out.println("*** The parameter data type is " +
para.dataType());
                   System.out.println("*** The parameter description is " +
para.description());
                   System.out.println("*** The parameter allowed values  is " +
para.allowedValues());
               }
           }

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
```

```
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterParameters in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun describeDbClusterParameters(
    dbCLusterGroupName: String?,
    flag: Int,
) {
    val dbParameterGroupsRequest: DescribeDbClusterParametersRequest
    dbParameterGroupsRequest =
        if (flag == 0) {
            DescribeDbClusterParametersRequest {
                dbClusterParameterGroupName = dbCLusterGroupName
            }
        } else {
            DescribeDbClusterParametersRequest {
                dbClusterParameterGroupName = dbCLusterGroupName
                source = "user"
            }
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response =
 rdsClient.describeDbClusterParameters(dbParameterGroupsRequest)
        response.parameters?.forEach { para ->
            // Only print out information about either auto_increment_offset or
 auto_increment_increment.
```

```
            val paraName = para.parameterName
            if (paraName != null) {
                if (paraName.compareTo("auto_increment_offset") == 0 ||
 paraName.compareTo("auto_increment_increment ") == 0) {
                    println("*** The parameter name is  $paraName")
                    println("*** The parameter value is  ${para.parameterValue}")
                    println("*** The parameter data type is ${para.dataType}")
                    println("*** The parameter description is
 ${para.description}")
                    println("*** The parameter allowed values  is
 ${para.allowedValues}")
                }
            }
        }
    }
}
```

- API-Details finden Sie unter DescribeDB ClusterParameters in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client
```

```
    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_parameters(self, parameter_group_name, name_prefix="", source=None):
        """
        Gets the parameters that are contained in a DB cluster parameter group.

        :param parameter_group_name: The name of the parameter group to query.
        :param name_prefix: When specified, the retrieved list of parameters is
filtered
                            to contain only parameters that start with this
prefix.
        :param source: When specified, only parameters from this source are
retrieved.
                       For example, a source of 'user' retrieves only parameters
that
                       were set by a user.
        :return: The list of requested parameters.
        """
        try:
            kwargs = {"DBClusterParameterGroupName": parameter_group_name}
            if source is not None:
                kwargs["Source"] = source
            parameters = []
            paginator =
self.rds_client.get_paginator("describe_db_cluster_parameters")
            for page in paginator.paginate(**kwargs):
                parameters += [
                    p
                    for p in page["Parameters"]
                    if p["ParameterName"].startswith(name_prefix)
                ]
        except ClientError as err:
            logger.error(
                "Couldn't get parameters for %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
```

```
            )
            raise
        else:
            return parameters
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterParameters in AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   // Get the parameter group. rds.DescribeDbClusterParameterGroups
   // Get parameters in the group. This is a long list so you will have to
paginate. Find the auto_increment_offset and auto_increment_increment parameters
(by ParameterName). rds.DescribeDbClusterParameters
   // Parse the ParameterName, Description, and AllowedValues values and display
them.
   pub async fn cluster_parameters(&self) ->
Result<Vec<AuroraScenarioParameter>, ScenarioError> {
       let parameters_output = self
           .rds
           .describe_db_cluster_parameters(DB_CLUSTER_PARAMETER_GROUP_NAME)
           .await;

       if let Err(err) = parameters_output {
           return Err(ScenarioError::new(
               format!("Failed to retrieve parameters for
{DB_CLUSTER_PARAMETER_GROUP_NAME}"),
               &err,
           ));
       }
```

```
        let parameters = parameters_output
            .unwrap()
            .into_iter()
            .flat_map(|p| p.parameters.unwrap_or_default().into_iter())
            .filter(|p|
 FILTER_PARAMETER_NAMES.contains(p.parameter_name().unwrap_or_default()))
            .map(AuroraScenarioParameter::from)
            .collect::<Vec<_>>();

        Ok(parameters)
    }

    pub async fn describe_db_cluster_parameters(
        &self,
        name: &str,
    ) -> Result<Vec<DescribeDbClusterParametersOutput>,
 SdkError<DescribeDBClusterParametersError>>
    {
        self.inner
            .describe_db_cluster_parameters()
            .db_cluster_parameter_group_name(name)
            .into_paginator()
            .send()
            .try_collect()
            .await
    }

#[tokio::test]
async fn test_scenario_cluster_parameters() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_db_cluster_parameters()
        .with(eq("RustSDKCodeExamplesDBParameterGroup"))
        .return_once(|_| {
            Ok(vec![DescribeDbClusterParametersOutput::builder()
                .parameters(Parameter::builder().parameter_name("a").build())
                .parameters(Parameter::builder().parameter_name("b").build())
                .parameters(
                    Parameter::builder()
                        .parameter_name("auto_increment_offset")
                        .build(),
                )
                .parameters(Parameter::builder().parameter_name("c").build())
```

```
                .parameters(
                    Parameter::builder()
                        .parameter_name("auto_increment_increment")
                        .build(),
                )
                .parameters(Parameter::builder().parameter_name("d").build())
                .build()])
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("RustSDKCodeExamplesDBCluster".into());

    let params = scenario.cluster_parameters().await.expect("cluster params");
    let names: Vec<String> = params.into_iter().map(|p| p.name).collect();
    assert_eq!(
        names,
        vec!["auto_increment_offset", "auto_increment_increment"]
    );
}

#[tokio::test]
async fn test_scenario_cluster_parameters_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_db_cluster_parameters()
        .with(eq("RustSDKCodeExamplesDBParameterGroup"))
        .return_once(|_| {
            Err(SdkError::service_error(
                DescribeDBClusterParametersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe_db_cluster_parameters_error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("RustSDKCodeExamplesDBCluster".into());
    let params = scenario.cluster_parameters().await;
    assert_matches!(params, Err(ScenarioError { message, context: _ }) if message
 == "Failed to retrieve parameters for RustSDKCodeExamplesDBParameterGroup");
}
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterParameters in der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeDBClusterSnapshots`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeDBClusterSnapshots`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Return a list of DB snapshots for a particular DB cluster.
    /// </summary>
    /// <param name="dbClusterIdentifier">DB cluster identifier.</param>
    /// <returns>List of DB snapshots.</returns>
    public async Task<List<DBClusterSnapshot>>
DescribeDBClusterSnapshotsByIdentifierAsync(string dbClusterIdentifier)
    {
        var results = new List<DBClusterSnapshot>();
```

```
        DescribeDBClusterSnapshotsResponse response;
        DescribeDBClusterSnapshotsRequest request = new
DescribeDBClusterSnapshotsRequest
        {
            DBClusterIdentifier = dbClusterIdentifier
        };
        // Get the full list if there are multiple pages.
        do
        {
            response = await _amazonRDS.DescribeDBClusterSnapshotsAsync(request);
            results.AddRange(response.DBClusterSnapshots);
            request.Marker = response.Marker;
        }
        while (response.Marker is not null);
        return results;
    }
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterSnapshots in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

            Aws::RDS::Model::DescribeDBClusterSnapshotsRequest request;
            request.SetDBClusterSnapshotIdentifier(snapshotID);

            Aws::RDS::Model::DescribeDBClusterSnapshotsOutcome outcome =
```

```
                    client.DescribeDBClusterSnapshots(request);

            if (outcome.IsSuccess()) {
                snapshot = outcome.GetResult().GetDBClusterSnapshots()[0];
            }
            else {
                std::cerr << "Error with Aurora::DescribeDBClusterSnapshots. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
                                 DB_CLUSTER_IDENTIFIER, DB_INSTANCE_IDENTIFIER,
 client);
                return false;
            }
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterSnapshots in der AWS SDK for C++ API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// GetClusterSnapshot gets a DB cluster snapshot.
func (clusters *DbClusters) GetClusterSnapshot(snapshotName string)
 (*types.DBClusterSnapshot, error) {
 output, err := clusters.AuroraClient.DescribeDBClusterSnapshots(context.TODO(),
  &rds.DescribeDBClusterSnapshotsInput{
```

```
   DBClusterSnapshotIdentifier: aws.String(snapshotName),
  })
 if err != nil {
  log.Printf("Couldn't get snapshot %v: %v\n", snapshotName, err)
  return nil, err
 } else {
  return &output.DBClusterSnapshots[0], nil
 }
}
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterSnapshots in der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void waitForSnapshotReady(RdsClient rdsClient, String
dbSnapshotIdentifier,
           String dbInstanceClusterIdentifier) {
       try {
           boolean snapshotReady = false;
           String snapshotReadyStr;
           System.out.println("Waiting for the snapshot to become available.");

           DescribeDbClusterSnapshotsRequest snapshotsRequest =
DescribeDbClusterSnapshotsRequest.builder()
                   .dbClusterSnapshotIdentifier(dbSnapshotIdentifier)
                   .dbClusterIdentifier(dbInstanceClusterIdentifier)
                   .build();

           while (!snapshotReady) {
```

```
                DescribeDbClusterSnapshotsResponse response =
 rdsClient.describeDBClusterSnapshots(snapshotsRequest);
                List<DBClusterSnapshot> snapshotList =
 response.dbClusterSnapshots();
                for (DBClusterSnapshot snapshot : snapshotList) {
                    snapshotReadyStr = snapshot.status();
                    if (snapshotReadyStr.contains("available")) {
                        snapshotReady = true;
                    } else {
                        System.out.println(".");
                        Thread.sleep(sleepTime * 5000);
                    }
                }
            }

            System.out.println("The Snapshot is available!");

        } catch (RdsException | InterruptedException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterSnapshots in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun waitSnapshotReady(
    dbSnapshotIdentifier: String?,
    dbInstanceClusterIdentifier: String?,
) {
```

```
    var snapshotReady = false
    var snapshotReadyStr: String
    println("Waiting for the snapshot to become available.")

    val snapshotsRequest =
        DescribeDbClusterSnapshotsRequest {
            dbClusterSnapshotIdentifier = dbSnapshotIdentifier
            dbClusterIdentifier = dbInstanceClusterIdentifier
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        while (!snapshotReady) {
            val response = rdsClient.describeDbClusterSnapshots(snapshotsRequest)
            val snapshotList = response.dbClusterSnapshots
            if (snapshotList != null) {
                for (snapshot in snapshotList) {
                    snapshotReadyStr = snapshot.status.toString()
                    if (snapshotReadyStr.contains("available")) {
                        snapshotReady = true
                    } else {
                        println(".")
                        delay(slTime * 5000)
                    }
                }
            }
        }
    }
    println("The Snapshot is available!")
}
```

- API-Details finden Sie unter DescribeDB ClusterSnapshots in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_cluster_snapshot(self, snapshot_id):
        """
        Gets a DB cluster snapshot.

        :param snapshot_id: The ID of the snapshot to retrieve.
        :return: The retrieved snapshot.
        """
        try:
            response = self.rds_client.describe_db_cluster_snapshots(
                DBClusterSnapshotIdentifier=snapshot_id
            )
            snapshot = response["DBClusterSnapshots"][0]
        except ClientError as err:
```

```
            logger.error(
                "Couldn't get DB cluster snapshot %s. Here's why: %s: %s",
                snapshot_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return snapshot
```

- Einzelheiten zur API finden Sie unter DescribeDB ClusterSnapshots in AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeDBClusters`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeDBClusters`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Returns a list of DB clusters.
```

```
    /// </summary>
    /// <param name="dbInstanceIdentifier">Optional name of a specific DB
cluster.</param>
    /// <returns>List of DB clusters.</returns>
    public async Task<List<DBCluster>> DescribeDBClustersPagedAsync(string?
dbClusterIdentifier = null)
    {
        var results = new List<DBCluster>();

        DescribeDBClustersResponse response;
        DescribeDBClustersRequest request = new DescribeDBClustersRequest
        {
            DBClusterIdentifier = dbClusterIdentifier
        };
        // Get the full list if there are multiple pages.
        do
        {
            response = await _amazonRDS.DescribeDBClustersAsync(request);
            results.AddRange(response.DBClusters);
            request.Marker = response.Marker;
        }
        while (response.Marker is not null);
        return results;
    }
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zu AWS SDK for .NET .

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
```

```
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

//! Routine which gets a DB cluster description.
/*!
 \sa describeDBCluster()
 \param dbClusterIdentifier: A DB cluster identifier.
 \param clusterResult: The 'DBCluster' object containing the description.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::describeDBCluster(const Aws::String &dbClusterIdentifier,
                                       Aws::RDS::Model::DBCluster &clusterResult,
                                       const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBClustersRequest request;
    request.SetDBClusterIdentifier(dbClusterIdentifier);

    Aws::RDS::Model::DescribeDBClustersOutcome outcome =
            client.DescribeDBClusters(request);

    bool result = true;
    if (outcome.IsSuccess()) {
        clusterResult = outcome.GetResult().GetDBClusters()[0];
    }
    else if (outcome.GetError().GetErrorType() !=
             Aws::RDS::RDSErrors::D_B_CLUSTER_NOT_FOUND_FAULT) {
        result = false;
        std::cerr << "Error with Aurora::GDescribeDBClusters. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
        // This example does not log an error if the DB cluster does not exist.
        // Instead, clusterResult is set to empty.
    else {
        clusterResult = Aws::RDS::Model::DBCluster();
    }

    return result;

}
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zu AWS SDK for C++ .

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// GetDbCluster gets data about an Aurora DB cluster.
func (clusters *DbClusters) GetDbCluster(clusterName string) (*types.DBCluster,
 error) {
 output, err := clusters.AuroraClient.DescribeDBClusters(context.TODO(),
  &rds.DescribeDBClustersInput{
   DBClusterIdentifier: aws.String(clusterName),
  })
 if err != nil {
  var notFoundError *types.DBClusterNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("DB cluster %v does not exist.\n", clusterName)
   err = nil
  } else {
   log.Printf("Couldn't get DB cluster %v: %v\n", clusterName, err)
  }
  return nil, err
 } else {
  return &output.DBClusters[0], err
 }
}
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zu AWS SDK for Go .

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void describeDbClusterParameters(RdsClient rdsClient, String
dbCLusterGroupName, int flag) {
       try {
           DescribeDbClusterParametersRequest dbParameterGroupsRequest;
           if (flag == 0) {
               dbParameterGroupsRequest =
DescribeDbClusterParametersRequest.builder()
                       .dbClusterParameterGroupName(dbCLusterGroupName)
                       .build();
           } else {
               dbParameterGroupsRequest =
DescribeDbClusterParametersRequest.builder()
                       .dbClusterParameterGroupName(dbCLusterGroupName)
                       .source("user")
                       .build();
           }

           DescribeDbClusterParametersResponse response = rdsClient
                   .describeDBClusterParameters(dbParameterGroupsRequest);
           List<Parameter> dbParameters = response.parameters();
           String paraName;
           for (Parameter para : dbParameters) {
               // Only print out information about either auto_increment_offset
or
               // auto_increment_increment.
               paraName = para.parameterName();
```

```
                if ((paraName.compareTo("auto_increment_offset") == 0)
                        || (paraName.compareTo("auto_increment_increment ") ==
 0)) {
                    System.out.println("*** The parameter name is  " + paraName);
                    System.out.println("*** The parameter value is  " +
 para.parameterValue());
                    System.out.println("*** The parameter data type is " +
 para.dataType());
                    System.out.println("*** The parameter description is " +
 para.description());
                    System.out.println("*** The parameter allowed values  is " +
 para.allowedValues());
                }
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zu AWS SDK for Java 2.x .

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun describeDbClusterParameters(
    dbCLusterGroupName: String?,
    flag: Int,
) {
    val dbParameterGroupsRequest: DescribeDbClusterParametersRequest
    dbParameterGroupsRequest =
```

```
        if (flag == 0) {
            DescribeDbClusterParametersRequest {
                dbClusterParameterGroupName = dbCLusterGroupName
            }
        } else {
            DescribeDbClusterParametersRequest {
                dbClusterParameterGroupName = dbCLusterGroupName
                source = "user"
            }
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response =
 rdsClient.describeDbClusterParameters(dbParameterGroupsRequest)
        response.parameters?.forEach { para ->
            // Only print out information about either auto_increment_offset or
 auto_increment_increment.
            val paraName = para.parameterName
            if (paraName != null) {
                if (paraName.compareTo("auto_increment_offset") == 0 ||
 paraName.compareTo("auto_increment_increment ") == 0) {
                    println("*** The parameter name is  $paraName")
                    println("*** The parameter value is  ${para.parameterValue}")
                    println("*** The parameter data type is ${para.dataType}")
                    println("*** The parameter description is
 ${para.description}")
                    println("*** The parameter allowed values  is
 ${para.allowedValues}")
                }
            }
        }
    }
}
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_db_cluster(self, cluster_name):
        """
        Gets data about an Aurora DB cluster.

        :param cluster_name: The name of the DB cluster to retrieve.
        :return: The retrieved DB cluster.
        """
        try:
            response = self.rds_client.describe_db_clusters(
                DBClusterIdentifier=cluster_name
            )
            cluster = response["DBClusters"][0]
        except ClientError as err:
```

```
            if err.response["Error"]["Code"] == "DBClusterNotFoundFault":
                logger.info("Cluster %s does not exist.", cluster_name)
            else:
                logger.error(
                    "Couldn't verify the existence of DB cluster %s. Here's why:
%s: %s",
                    cluster_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return cluster
```

- Weitere API-Informationen finden Sie unter DescribeDBClusters in der API-Referenz zum AWS SDK für Python (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   // Get a list of allowed engine versions.
rds.DescribeDbEngineVersions(Engine='aurora-mysql', DBParameterGroupFamily=<the
family used to create your parameter group in step 2>)
   // Create an Aurora DB cluster database cluster that contains a MySql
database and uses the parameter group you created.
   // Wait for DB cluster to be ready. Call rds.DescribeDBClusters and check for
Status == 'available'.
   // Get a list of instance classes available for the selected engine
and engine version. rds.DescribeOrderableDbInstanceOptions(Engine='mysql',
EngineVersion=).

   // Create a database instance in the cluster.
```

```
   // Wait for DB instance to be ready. Call rds.DescribeDbInstances and check
for DBInstanceStatus == 'available'.
   pub async fn start_cluster_and_instance(&mut self) -> Result<(),
ScenarioError> {
       if self.password.is_none() {
           return Err(ScenarioError::with(
               "Must set Secret Password before starting a cluster",
           ));
       }
       let create_db_cluster = self
           .rds
           .create_db_cluster(
               DB_CLUSTER_IDENTIFIER,
               DB_CLUSTER_PARAMETER_GROUP_NAME,
               DB_ENGINE,
               self.engine_version.as_deref().expect("engine version"),
               self.username.as_deref().expect("username"),
               self.password
                   .replace(SecretString::new("".to_string()))
                   .expect("password"),
           )
           .await;
       if let Err(err) = create_db_cluster {
           return Err(ScenarioError::new(
               "Failed to create DB Cluster with cluster group",
               &err,
           ));
       }

       self.db_cluster_identifier = create_db_cluster
           .unwrap()
           .db_cluster
           .and_then(|c| c.db_cluster_identifier);

       if self.db_cluster_identifier.is_none() {
           return Err(ScenarioError::with("Created DB Cluster missing
Identifier"));
       }

       info!(
           "Started a db cluster: {}",
           self.db_cluster_identifier
               .as_deref()
               .unwrap_or("Missing ARN")
```

```
        );

        let create_db_instance = self
            .rds
            .create_db_instance(
                self.db_cluster_identifier.as_deref().expect("cluster name"),
                DB_INSTANCE_IDENTIFIER,
                self.instance_class.as_deref().expect("instance class"),
                DB_ENGINE,
            )
            .await;
        if let Err(err) = create_db_instance {
            return Err(ScenarioError::new(
                "Failed to create Instance in DB Cluster",
                &err,
            ));
        }

        self.db_instance_identifier = create_db_instance
            .unwrap()
            .db_instance
            .and_then(|i| i.db_instance_identifier);

        // Cluster creation can take up to 20 minutes to become available
        let cluster_max_wait = Duration::from_secs(20 * 60);
        let waiter = Waiter::builder().max(cluster_max_wait).build();
        while waiter.sleep().await.is_ok() {
            let cluster = self
                .rds
                .describe_db_clusters(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = cluster {
                warn!(?err, "Failed to describe cluster while waiting for
ready");
                continue;
            }

            let instance = self
                .rds
```

```
                .describe_db_instance(
                    self.db_instance_identifier
                        .as_deref()
                        .expect("instance identifier"),
                )
                .await;
            if let Err(err) = instance {
                return Err(ScenarioError::new(
                    "Failed to find instance for cluster",
                    &err,
                ));
            }

            let instances_available = instance
                .unwrap()
                .db_instances()
                .iter()
                .all(|instance| instance.db_instance_status() ==
Some("Available"));

            let endpoints = self
                .rds
                .describe_db_cluster_endpoints(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = endpoints {
                return Err(ScenarioError::new(
                    "Failed to find endpoint for cluster",
                    &err,
                ));
            }

            let endpoints_available = endpoints
                .unwrap()
                .db_cluster_endpoints()
                .iter()
                .all(|endpoint| endpoint.status() == Some("available"));

            if instances_available && endpoints_available {
                return Ok(());
```

```
            }
        }

        Err(ScenarioError::with("timed out waiting for cluster"))
    }

    pub async fn describe_db_clusters(
        &self,
        id: &str,
    ) -> Result<DescribeDbClustersOutput, SdkError<DescribeDBClustersError>> {
        self.inner
            .describe_db_clusters()
            .db_cluster_identifier(id)
            .send()
            .await
    }

#[tokio::test]
async fn test_start_cluster_and_instance() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
```

```
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_describe_db_instance()
        .with(eq("RustSDKCodeExamplesDBInstance"))
        .return_once(|name| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_instance_identifier(name)
                        .db_instance_status("Available")
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| {
```

```
            Ok(DescribeDbClusterEndpointsOutput::builder()

 .db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
        assert!(scenario
            .password
            .replace(SecretString::new("BAD SECRET".into()))
            .unwrap()
            .expose_secret()
            .is_empty());
        assert_eq!(
            scenario.db_cluster_identifier,
            Some("RustSDKCodeExamplesDBCluster".into())
        );
    });
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Err(SdkError::service_error(
                CreateDBClusterError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db cluster error",
                ))),
```

```
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _}) if message
 == "Failed to create DB Cluster with cluster group")
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_missing_id() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()
                .db_cluster(DbCluster::builder().build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context:_ }) if message
 == "Created DB Cluster missing Identifier");
}

#[tokio::test]
async fn test_start_cluster_and_instance_instance_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
```

```
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .return_once(|_, _, _, _| {
            Err(SdkError::service_error(
                CreateDBInstanceError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db instance error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _ }) if message
 == "Failed to create Instance in DB Cluster")
}

#[tokio::test]
async fn test_start_cluster_and_instance_wait_hiccup() {
    let mut mock_rds = MockRdsImpl::default();
```

```
    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

.db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
```

```
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe cluster error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        })
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds.expect_describe_db_instance().return_once(|name| {
        Ok(DescribeDbInstancesOutput::builder()
            .db_instances(
                DbInstance::builder()
                    .db_instance_identifier(name)
                    .db_instance_status("Available")
                    .build(),
            )
            .build())
    });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()

.db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));
```

```
    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
    let _ = assertions.await;
}
```

- Informationen zu APIs finden Sie unter DescribeDBClusters in der API-Referenz zum AWS -SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeDBEngineVersions`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeDBEngineVersions`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Get a list of DB engine versions for a particular DB engine.
    /// </summary>
    /// <param name="engine">The name of the engine.</param>
    /// <param name="parameterGroupFamily">Optional parameter group family
name.</param>
    /// <returns>A list of DBEngineVersions.</returns>
    public async Task<List<DBEngineVersion>>
DescribeDBEngineVersionsForEngineAsync(string engine,
        string? parameterGroupFamily = null)
    {
        var response = await _amazonRDS.DescribeDBEngineVersionsAsync(
            new DescribeDBEngineVersionsRequest()
            {
                Engine = engine,
                DBParameterGroupFamily = parameterGroupFamily
            });
        return response.DBEngineVersions;
    }
```

- Einzelheiten zur API finden Sie unter DescribeDB EngineVersions in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);
```

```
//! Routine which gets available DB engine versions for an engine name and
//! an optional parameter group family.
/*!
 \sa getDBEngineVersions()
 \param engineName: A DB engine name.
 \param parameterGroupFamily: A parameter group family name, ignored if empty.
 \param engineVersionsResult: Vector of 'DBEngineVersion' objects returned by the
 routine.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::getDBEngineVersions(const Aws::String &engineName,
                                         const Aws::String &parameterGroupFamily,

 Aws::Vector<Aws::RDS::Model::DBEngineVersion> &engineVersionsResult,
                                         const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBEngineVersionsRequest request;
    request.SetEngine(engineName);
    if (!parameterGroupFamily.empty()) {
        request.SetDBParameterGroupFamily(parameterGroupFamily);
    }

    engineVersionsResult.clear();
    Aws::String marker; // The marker is used for pagination.
    do {
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::RDS::Model::DescribeDBEngineVersionsOutcome outcome =
                client.DescribeDBEngineVersions(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::DBEngineVersion> &engineVersions =
                    outcome.GetResult().GetDBEngineVersions();

            engineVersionsResult.insert(engineVersionsResult.end(),
                                        engineVersions.begin(),
 engineVersions.end());
            marker  = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with Aurora::DescribeDBEngineVersionsRequest. "
                      << outcome.GetError().GetMessage()
```

```
                        << std::endl;
        }
    } while (!marker.empty());

    return true;
}
```

- Einzelheiten zur API finden Sie unter DescribeDB EngineVersions in der AWS SDK for C++ API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// GetEngineVersions gets database engine versions that are available for the
 specified engine
// and parameter group family.
func (clusters *DbClusters) GetEngineVersions(engine string, parameterGroupFamily
 string) (
 []types.DBEngineVersion, error) {
 output, err := clusters.AuroraClient.DescribeDBEngineVersions(context.TODO(),
  &rds.DescribeDBEngineVersionsInput{
   Engine:                 aws.String(engine),
   DBParameterGroupFamily: aws.String(parameterGroupFamily),
  })
 if err != nil {
  log.Printf("Couldn't get engine versions for %v: %v\n", engine, err)
```

```
  return nil, err
 } else {
  return output.DBEngineVersions, nil
 }
}
```

- Einzelheiten zur API finden Sie unter DescribeDB EngineVersions in der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public static void describeDBEngines(RdsClient rdsClient) {
        try {
            DescribeDbEngineVersionsRequest engineVersionsRequest =
DescribeDbEngineVersionsRequest.builder()
                    .engine("aurora-mysql")
                    .defaultOnly(true)
                    .maxRecords(20)
                    .build();

            DescribeDbEngineVersionsResponse response =
rdsClient.describeDBEngineVersions(engineVersionsRequest);
            List<DBEngineVersion> engines = response.dbEngineVersions();

            // Get all DBEngineVersion objects.
            for (DBEngineVersion engineOb : engines) {
                System.out.println("The name of the DB parameter group family for
the database engine is "
                        + engineOb.dbParameterGroupFamily());
                System.out.println("The name of the database engine " +
engineOb.engine());
```

```
                System.out.println("The version number of the database engine " +
 engineOb.engineVersion());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie unter DescribeDB EngineVersions in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// Get a list of allowed engine versions.
suspend fun getAllowedClusterEngines(dbParameterGroupFamilyVal: String?) {
    val versionsRequest =
        DescribeDbEngineVersionsRequest {
            dbParameterGroupFamily = dbParameterGroupFamilyVal
            engine = "aurora-mysql"
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbEngineVersions(versionsRequest)
        response.dbEngineVersions?.forEach { dbEngine ->
            println("The engine version is ${dbEngine.engineVersion}")
            println("The engine description is ${dbEngine.dbEngineDescription}")
        }
    }
}
```

- API-Details finden Sie unter DescribeDB EngineVersions in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_engine_versions(self, engine, parameter_group_family=None):
        """
        Gets database engine versions that are available for the specified engine
        and parameter group family.

        :param engine: The database engine to look up.
        :param parameter_group_family: When specified, restricts the returned
 list of
```

```
                                        engine versions to those that are
compatible with
                                        this parameter group family.
        :return: The list of database engine versions.
        """
        try:
            kwargs = {"Engine": engine}
            if parameter_group_family is not None:
                kwargs["DBParameterGroupFamily"] = parameter_group_family
            response = self.rds_client.describe_db_engine_versions(**kwargs)
            versions = response["DBEngineVersions"]
        except ClientError as err:
            logger.error(
                "Couldn't get engine versions for %s. Here's why: %s: %s",
                engine,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return versions
```

- Einzelheiten zur API finden Sie unter DescribeDB EngineVersions in AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    // Get available engine families for Aurora MySql.
rds.DescribeDbEngineVersions(Engine='aurora-mysql') and build a set of the
'DBParameterGroupFamily' field values. I get {aurora-mysql8.0, aurora-mysql5.7}.
```

```
   pub async fn get_engines(&self) -> Result<HashMap<String, Vec<String>>,
ScenarioError> {
       let describe_db_engine_versions =
self.rds.describe_db_engine_versions(DB_ENGINE).await;
       trace!(versions=?describe_db_engine_versions, "full list of versions");

       if let Err(err) = describe_db_engine_versions {
           return Err(ScenarioError::new(
               "Failed to retrieve DB Engine Versions",
               &err,
           ));
       };

       let version_count = describe_db_engine_versions
           .as_ref()
           .map(|o| o.db_engine_versions().len())
           .unwrap_or_default();
       info!(version_count, "got list of versions");

       // Create a map of engine families to their available versions.
       let mut versions = HashMap::<String, Vec<String>>::new();
       describe_db_engine_versions
           .unwrap()
           .db_engine_versions()
           .iter()
           .filter_map(
               |v| match (&v.db_parameter_group_family, &v.engine_version) {
                   (Some(family), Some(version)) => Some((family.clone(),
version.clone())),
                   _ => None,
               },
           )
           .for_each(|(family, version)|
versions.entry(family).or_default().push(version));

       Ok(versions)
   }

   pub async fn describe_db_engine_versions(
       &self,
       engine: &str,
   ) -> Result<DescribeDbEngineVersionsOutput,
SdkError<DescribeDBEngineVersionsError>> {
       self.inner
```

```
            .describe_db_engine_versions()
            .engine(engine)
            .send()
            .await
    }

#[tokio::test]
async fn test_scenario_get_engines() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_db_engine_versions()
        .with(eq("aurora-mysql"))
        .return_once(|_| {
            Ok(DescribeDbEngineVersionsOutput::builder()
                .db_engine_versions(
                    DbEngineVersion::builder()
                        .db_parameter_group_family("f1")
                        .engine_version("f1a")
                        .build(),
                )
                .db_engine_versions(
                    DbEngineVersion::builder()
                        .db_parameter_group_family("f1")
                        .engine_version("f1b")
                        .build(),
                )
                .db_engine_versions(
                    DbEngineVersion::builder()
                        .db_parameter_group_family("f2")
                        .engine_version("f2a")
                        .build(),
                )
                .db_engine_versions(DbEngineVersion::builder().build())
                .build())
        });

    let scenario = AuroraScenario::new(mock_rds);

    let versions_map = scenario.get_engines().await;

    assert_eq!(
        versions_map,
        Ok(HashMap::from([
```

```
            ("f1".into(), vec!["f1a".into(), "f1b".into()]),
            ("f2".into(), vec!["f2a".into()])
        ]))
    );
}

#[tokio::test]
async fn test_scenario_get_engines_failed() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_db_engine_versions()
        .with(eq("aurora-mysql"))
        .return_once(|_| {
            Err(SdkError::service_error(
                DescribeDBEngineVersionsError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe_db_engine_versions error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let scenario = AuroraScenario::new(mock_rds);

    let versions_map = scenario.get_engines().await;
    assert_matches!(
        versions_map,
        Err(ScenarioError { message, context: _ }) if message == "Failed to
 retrieve DB Engine Versions"
    );
}
```

- Einzelheiten zur API finden Sie unter DescribeDB EngineVersions in der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeDBInstances`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeDBInstances`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   /// <summary>
   /// Returns a list of DB instances.
   /// </summary>
   /// <param name="dbInstanceIdentifier">Optional name of a specific DB
instance.</param>
   /// <returns>List of DB instances.</returns>
   public async Task<List<DBInstance>> DescribeDBInstancesPagedAsync(string?
dbInstanceIdentifier = null)
   {
       var results = new List<DBInstance>();
       var instancesPaginator = _amazonRDS.Paginators.DescribeDBInstances(
           new DescribeDBInstancesRequest
           {
               DBInstanceIdentifier = dbInstanceIdentifier
           });
       // Get the entire list using the paginator.
       await foreach (var instances in instancesPaginator.DBInstances)
       {
           results.Add(instances);
       }
       return results;
   }
```

- Weitere API-Informationen finden Sie unter DescribeDBInstances in der API-Referenz zu AWS SDK for .NET .

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);


//! Routine which gets a DB instance description.
/*!
 \sa describeDBCluster()
 \param dbInstanceIdentifier: A DB instance identifier.
 \param instanceResult: The 'DBInstance' object containing the description.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::describeDBInstance(const Aws::String &dbInstanceIdentifier,
                                        Aws::RDS::Model::DBInstance
 &instanceResult,
                                        const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBInstancesRequest request;
    request.SetDBInstanceIdentifier(dbInstanceIdentifier);

    Aws::RDS::Model::DescribeDBInstancesOutcome outcome =
            client.DescribeDBInstances(request);

    bool result = true;
```

```
    if (outcome.IsSuccess()) {
        instanceResult = outcome.GetResult().GetDBInstances()[0];
    }
    else if (outcome.GetError().GetErrorType() !=
             Aws::RDS::RDSErrors::D_B_INSTANCE_NOT_FOUND_FAULT) {
        result = false;
        std::cerr << "Error with Aurora::DescribeDBInstances. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
        // This example does not log an error if the DB instance does not exist.
        // Instead, instanceResult is set to empty.
    else {
        instanceResult = Aws::RDS::Model::DBInstance();
    }

    return result;
}
```

- Weitere API-Informationen finden Sie unter DescribeDBInstances in der API-Referenz zu AWS SDK for C++ .

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// GetInstance gets data about a DB instance.
```

```
func (clusters *DbClusters) GetInstance(instanceName string) (
 *types.DBInstance, error) {
 output, err := clusters.AuroraClient.DescribeDBInstances(context.TODO(),
  &rds.DescribeDBInstancesInput{
   DBInstanceIdentifier: aws.String(instanceName),
  })
 if err != nil {
  var notFoundError *types.DBInstanceNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("DB instance %v does not exist.\n", instanceName)
   err = nil
  } else {
   log.Printf("Couldn't get instance %v: %v\n", instanceName, err)
  }
  return nil, err
 } else {
  return &output.DBInstances[0], nil
 }
}
```

- Weitere API-Informationen finden Sie unter DescribeDBInstances in der API-Referenz zu AWS SDK for Go .

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    // Waits until the database instance is available.
    public static void waitForInstanceReady(RdsClient rdsClient, String
dbClusterIdentifier) {
        boolean instanceReady = false;
        String instanceReadyStr;
        System.out.println("Waiting for instance to become available.");
```

```
        try {
            DescribeDbClustersRequest instanceRequest =
DescribeDbClustersRequest.builder()
                    .dbClusterIdentifier(dbClusterIdentifier)
                    .build();

            while (!instanceReady) {
                DescribeDbClustersResponse response =
rdsClient.describeDBClusters(instanceRequest);
                List<DBCluster> clusterList = response.dbClusters();
                for (DBCluster cluster : clusterList) {
                    instanceReadyStr = cluster.status();
                    if (instanceReadyStr.contains("available")) {
                        instanceReady = true;
                    } else {
                        System.out.print(".");
                        Thread.sleep(sleepTime * 1000);
                    }
                }
            }
            System.out.println("Database cluster is available!");

        } catch (RdsException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Weitere API-Informationen finden Sie unter DescribeDBInstances in der API-Referenz zu AWS SDK for Java 2.x .

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun waitDBAuroraInstanceReady(dbInstanceIdentifierVal: String?) {
    var instanceReady = false
    var instanceReadyStr: String
    println("Waiting for instance to become available.")
    val instanceRequest =
        DescribeDbInstancesRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
        }

    var endpoint = ""
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        while (!instanceReady) {
            val response = rdsClient.describeDbInstances(instanceRequest)
            response.dbInstances?.forEach { instance ->
                instanceReadyStr = instance.dbInstanceStatus.toString()
                if (instanceReadyStr.contains("available")) {
                    endpoint = instance.endpoint?.address.toString()
                    instanceReady = true
                } else {
                    print(".")
                    delay(sleepTime * 1000)
                }
            }
        }
    }
    println("Database instance is available! The connection endpoint is
 $endpoint")
}
```

- Weitere API-Informationen finden Sie unter DescribeDBInstances in der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_db_instance(self, instance_id):
        """
        Gets data about a DB instance.

        :param instance_id: The ID of the DB instance to retrieve.
        :return: The retrieved DB instance.
        """
        try:
            response = self.rds_client.describe_db_instances(
                DBInstanceIdentifier=instance_id
            )
            db_inst = response["DBInstances"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBInstanceNotFound":
                logger.info("Instance %s does not exist.", instance_id)
            else:
                logger.error(
                    "Couldn't get DB instance %s. Here's why: %s: %s",
                    instance_id,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
```

```
            return db_inst
```

- Weitere API-Informationen finden Sie unter DescribeDBInstances in der API-Referenz zum AWS SDK für Phyton (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    pub async fn clean_up(self) -> Result<(), Vec<ScenarioError>> {
        let mut clean_up_errors: Vec<ScenarioError> = vec![];

        // Delete the instance. rds.DeleteDbInstance.
        let delete_db_instance = self
            .rds
            .delete_db_instance(
                self.db_instance_identifier
                    .as_deref()
                    .expect("instance identifier"),
            )
            .await;
        if let Err(err) = delete_db_instance {
            let identifier = self
                .db_instance_identifier
                .as_deref()
                .unwrap_or("Missing Instance Identifier");
            let message = format!("failed to delete db instance {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance to delete
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
```

```
                let describe_db_instances =
self.rds.describe_db_instances().await;
                if let Err(err) = describe_db_instances {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check instance state during deletion",
                        &err,
                    ));
                    break;
                }
                let db_instances = describe_db_instances
                    .unwrap()
                    .db_instances()
                    .iter()
                    .filter(|instance| instance.db_cluster_identifier ==
self.db_cluster_identifier)
                    .cloned()
                    .collect::<Vec<DbInstance>>();

                if db_instances.is_empty() {
                    trace!("Delete Instance waited and no instances were found");
                    break;
                }
                match db_instances.first().unwrap().db_instance_status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but instances is in
{status}");
                        continue;
                    }
                    None => {
                        warn!("No status for DB instance");
                        break;
                    }
                }
            }
        }

        // Delete the DB cluster. rds.DeleteDbCluster.
        let delete_db_cluster = self
            .rds
            .delete_db_cluster(
                self.db_cluster_identifier
                    .as_deref()
                    .expect("cluster identifier"),
```

```
            )
            .await;

        if let Err(err) = delete_db_cluster {
            let identifier = self
                .db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing DB Cluster Identifier");
            let message = format!("failed to delete db cluster {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance and cluster to fully delete.
rds.DescribeDbInstances and rds.DescribeDbClusters until both are not found.
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
                let describe_db_clusters = self
                    .rds
                    .describe_db_clusters(
                        self.db_cluster_identifier
                            .as_deref()
                            .expect("cluster identifier"),
                    )
                    .await;
                if let Err(err) = describe_db_clusters {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check cluster state during deletion",
                        &err,
                    ));
                    break;
                }
                let describe_db_clusters = describe_db_clusters.unwrap();
                let db_clusters = describe_db_clusters.db_clusters();
                if db_clusters.is_empty() {
                    trace!("Delete cluster waited and no clusters were found");
                    break;
                }
                match db_clusters.first().unwrap().status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but clusters is in
{status}");
                        continue;
                    }
                    None => {
```

```
                        warn!("No status for DB cluster");
                        break;
                    }
                }
            }
        }

        // Delete the DB cluster parameter group.
 rds.DeleteDbClusterParameterGroup.
        let delete_db_cluster_parameter_group = self
            .rds
            .delete_db_cluster_parameter_group(
                self.db_cluster_parameter_group
                    .map(|g| {
                        g.db_cluster_parameter_group_name
                            .unwrap_or_else(||
 DB_CLUSTER_PARAMETER_GROUP_NAME.to_string())
                    })
                    .as_deref()
                    .expect("cluster parameter group name"),
            )
            .await;
        if let Err(error) = delete_db_cluster_parameter_group {
            clean_up_errors.push(ScenarioError::new(
                "Failed to delete the db cluster parameter group",
                &error,
            ))
        }

        if clean_up_errors.is_empty() {
            Ok(())
        } else {
            Err(clean_up_errors)
        }
    }

    pub async fn describe_db_instances(
        &self,
    ) -> Result<DescribeDbInstancesOutput, SdkError<DescribeDBInstancesError>> {
        self.inner.describe_db_instances().send().await
    }

#[tokio::test]
async fn test_scenario_clean_up() {
```

```
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| Ok(DescribeDbInstancesOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
```

```
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| Ok(DescribeDbClustersOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
 Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_scenario_clean_up_errors() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
```

```
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| {
            Err(SdkError::service_error(
                DescribeDBInstancesError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db instances error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
```

```
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db clusters error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_err());
        let errs = clean_up.unwrap_err();
        assert_eq!(errs.len(), 2);
        assert_matches!(errs.get(0), Some(ScenarioError {message, context: _}) if
message == "Failed to check instance state during deletion");
        assert_matches!(errs.get(1), Some(ScenarioError {message, context: _}) if
message == "Failed to check cluster state during deletion");
    });
```

```
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}
```

- Informationen zu APIs finden Sie unter DescribeDBInstances in der API-Referenz zum AWS -SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeOrderableDBInstanceOptions`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeOrderableDBInstanceOptions`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Get a list of orderable DB instance options for a specific
    /// engine and engine version.
    /// </summary>
    /// <param name="engine">Name of the engine.</param>
    /// <param name="engineVersion">Version of the engine.</param>
    /// <returns>List of OrderableDBInstanceOptions.</returns>
    public async Task<List<OrderableDBInstanceOption>>
DescribeOrderableDBInstanceOptionsPagedAsync(string engine, string
engineVersion)
    {
        // Use a paginator to get a list of DB instance options.
        var results = new List<OrderableDBInstanceOption>();
        var paginateInstanceOptions =
_amazonRDS.Paginators.DescribeOrderableDBInstanceOptions(
            new DescribeOrderableDBInstanceOptionsRequest()
            {
                Engine = engine,
                EngineVersion = engineVersion,
            });
        // Get the entire list using the paginator.
        await foreach (var instanceOptions in
paginateInstanceOptions.OrderableDBInstanceOptions)
        {
            results.Add(instanceOptions);
        }
        return results;
    }
```

- Einzelheiten zur API finden Sie unter DescribeOrderableDB InstanceOptions in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);


//! Routine which gets available DB instance classes, displays the list
//! to the user, and returns the user selection.
/*!
 \sa chooseDBInstanceClass()
 \param engineName: The DB engine name.
 \param engineVersion: The DB engine version.
 \param dbInstanceClass: String for DB instance class chosen by the user.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::chooseDBInstanceClass(const Aws::String &engine,
                                           const Aws::String &engineVersion,
                                           Aws::String &dbInstanceClass,
                                           const Aws::RDS::RDSClient &client) {
    std::vector<Aws::String> instanceClasses;
    Aws::String marker; // The marker is used for pagination.
    do {
        Aws::RDS::Model::DescribeOrderableDBInstanceOptionsRequest request;
        request.SetEngine(engine);
        request.SetEngineVersion(engineVersion);
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::RDS::Model::DescribeOrderableDBInstanceOptionsOutcome outcome =
                client.DescribeOrderableDBInstanceOptions(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::OrderableDBInstanceOption>
 &options =
                    outcome.GetResult().GetOrderableDBInstanceOptions();
            for (const Aws::RDS::Model::OrderableDBInstanceOption &option:
 options) {
                const Aws::String &instanceClass = option.GetDBInstanceClass();
                if (std::find(instanceClasses.begin(), instanceClasses.end(),
                              instanceClass) == instanceClasses.end()) {
```

```
                    instanceClasses.push_back(instanceClass);
                }
            }
            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with Aurora::DescribeOrderableDBInstanceOptions.
 "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!marker.empty());

    std::cout << "The available DB instance classes for your database engine
 are:"
              << std::endl;
    for (int i = 0; i < instanceClasses.size(); ++i) {
        std::cout << "   " << i + 1 << ": " << instanceClasses[i] << std::endl;
    }

    int choice = askQuestionForIntRange(
            "Which DB instance class do you want to use? ",
            1, static_cast<int>(instanceClasses.size()));
    dbInstanceClass = instanceClasses[choice - 1];
    return true;
}
```

- Einzelheiten zur API finden Sie unter DescribeOrderableDB InstanceOptions in der AWS SDK for C++ API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// GetOrderableInstances uses a paginator to get DB instance options that can be
 used to create DB instances that are
// compatible with a set of specifications.
func (clusters *DbClusters) GetOrderableInstances(engine string, engineVersion
 string) (
 []types.OrderableDBInstanceOption, error) {

 var output *rds.DescribeOrderableDBInstanceOptionsOutput
 var instances []types.OrderableDBInstanceOption
 var err error
 orderablePaginator :=
 rds.NewDescribeOrderableDBInstanceOptionsPaginator(clusters.AuroraClient,
  &rds.DescribeOrderableDBInstanceOptionsInput{
   Engine:        aws.String(engine),
   EngineVersion: aws.String(engineVersion),
  })
 for orderablePaginator.HasMorePages() {
  output, err = orderablePaginator.NextPage(context.TODO())
  if err != nil {
   log.Printf("Couldn't get orderable DB instances: %v\n", err)
   break
  } else {
   instances = append(instances, output.OrderableDBInstanceOptions...)
  }
 }
 return instances, err
}
```

- Einzelheiten zur API finden Sie unter DescribeOrderableDB InstanceOptions in der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void describeDBEngines(RdsClient rdsClient) {
       try {
           DescribeDbEngineVersionsRequest engineVersionsRequest =
DescribeDbEngineVersionsRequest.builder()
                   .engine("aurora-mysql")
                   .defaultOnly(true)
                   .maxRecords(20)
                   .build();

           DescribeDbEngineVersionsResponse response =
rdsClient.describeDBEngineVersions(engineVersionsRequest);
           List<DBEngineVersion> engines = response.dbEngineVersions();

           // Get all DBEngineVersion objects.
           for (DBEngineVersion engineOb : engines) {
               System.out.println("The name of the DB parameter group family for
the database engine is "
                       + engineOb.dbParameterGroupFamily());
               System.out.println("The name of the database engine " +
engineOb.engine());
               System.out.println("The version number of the database engine " +
engineOb.engineVersion());
           }

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Einzelheiten zur API finden Sie unter DescribeOrderableDB InstanceOptions in der AWS SDK for Java 2.x API-Referenz.

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel werden die DB-Engine-Versionen aufgeführt, die eine bestimmte DB-Instance-Klasse in einem unterstützen AWS-Region.

```
$params = @{
  Engine = 'aurora-postgresql'
  DBInstanceClass = 'db.r5.large'
  Region = 'us-east-1'
}
Get-RDSOrderableDBInstanceOption @params
```

Beispiel 2: In diesem Beispiel werden die DB-Instance-Klassen aufgeführt, die für eine bestimmte DB-Engine-Version in einem unterstützt werden AWS-Region.

```
$params = @{
  Engine = 'aurora-postgresql'
  EngineVersion = '13.6'
  Region = 'us-east-1'
}
Get-RDSOrderableDBInstanceOption @params
```

- Einzelheiten zur API finden Sie unter DescribeOrderableDB InstanceOptions in AWS Tools for PowerShell Cmdlet Reference.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_orderable_instances(self, db_engine, db_engine_version):
        """
        Gets DB instance options that can be used to create DB instances that are
        compatible with a set of specifications.

        :param db_engine: The database engine that must be supported by the DB
 instance.
        :param db_engine_version: The engine version that must be supported by
 the DB instance.
        :return: The list of DB instance options that can be used to create a
 compatible DB instance.
        """
        try:
            inst_opts = []
            paginator = self.rds_client.get_paginator(
                "describe_orderable_db_instance_options"
            )
            for page in paginator.paginate(
                Engine=db_engine, EngineVersion=db_engine_version
            ):
                inst_opts += page["OrderableDBInstanceOptions"]
        except ClientError as err:
            logger.error(
                "Couldn't get orderable DB instances. Here's why: %s: %s",
```

```
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return inst_opts
```

- API-Einzelheiten finden Sie unter DescribeOrderableDB InstanceOptions in AWS SDK for Python (Boto3) API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   pub async fn get_instance_classes(&self) -> Result<Vec<String>,
ScenarioError> {
        let describe_orderable_db_instance_options_items = self
            .rds
            .describe_orderable_db_instance_options(
                DB_ENGINE,
                self.engine_version
                    .as_ref()
                    .expect("engine version for db instance options")
                    .as_str(),
            )
            .await;

        describe_orderable_db_instance_options_items
            .map(|options| {
                options
                    .iter()
                    .map(|o|
o.db_instance_class().unwrap_or_default().to_string())
```

```
                    .collect::<Vec<String>>()
            })
            .map_err(|err| ScenarioError::new("Could not get available instance
 classes", &err))
    }

    pub async fn describe_orderable_db_instance_options(
        &self,
        engine: &str,
        engine_version: &str,
    ) -> Result<Vec<OrderableDbInstanceOption>,
 SdkError<DescribeOrderableDBInstanceOptionsError>>
    {
        self.inner
            .describe_orderable_db_instance_options()
            .engine(engine)
            .engine_version(engine_version)
            .into_paginator()
            .items()
            .send()
            .try_collect()
            .await
    }

#[tokio::test]
async fn test_scenario_get_instance_classes() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .return_once(|_, _, _| {
            Ok(CreateDbClusterParameterGroupOutput::builder()

 .db_cluster_parameter_group(DbClusterParameterGroup::builder().build())
                .build())
        });

    mock_rds
        .expect_describe_orderable_db_instance_options()
        .with(eq("aurora-mysql"), eq("aurora-mysql8.0"))
        .return_once(|_, _| {
            Ok(vec![
                OrderableDbInstanceOption::builder()
                    .db_instance_class("t1")
```

```
                    .build(),
                OrderableDbInstanceOption::builder()
                    .db_instance_class("t2")
                    .build(),
                OrderableDbInstanceOption::builder()
                    .db_instance_class("t3")
                    .build(),
            ])
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario
        .set_engine("aurora-mysql", "aurora-mysql8.0")
        .await
        .expect("set engine");

    let instance_classes = scenario.get_instance_classes().await;

    assert_eq!(
        instance_classes,
        Ok(vec!["t1".into(), "t2".into(), "t3".into()])
    );
}

#[tokio::test]
async fn test_scenario_get_instance_classes_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_orderable_db_instance_options()
        .with(eq("aurora-mysql"), eq("aurora-mysql8.0"))
        .return_once(|_, _| {
            Err(SdkError::service_error(

 DescribeOrderableDBInstanceOptionsError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe_orderable_db_instance_options_error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
```

```
    scenario.engine_family = Some("aurora-mysql".into());
    scenario.engine_version = Some("aurora-mysql8.0".into());

    let instance_classes = scenario.get_instance_classes().await;

    assert_matches!(
        instance_classes,
        Err(ScenarioError {message, context: _}) if message == "Could not get
 available instance classes"
    );
}
```

- Einzelheiten zur API finden Sie unter DescribeOrderableDatenbank InstanceOptions im AWS SDK für die Rust-API-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ModifyDBClusterParameterGroup`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ModifyDBClusterParameterGroup`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit DB-Clustern

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Modify the specified integer parameters with new values from user input.
    /// </summary>
    /// <param name="groupName">The group name for the parameters.</param>
    /// <param name="parameters">The list of integer parameters to modify.</
param>
    /// <param name="newValue">Optional int value to set for parameters.</param>
    /// <returns>The name of the group that was modified.</returns>
    public async Task<string> ModifyIntegerParametersInGroupAsync(string
 groupName, List<Parameter> parameters, int newValue = 0)
    {
        foreach (var p in parameters)
        {
            if (p.IsModifiable && p.DataType == "integer")
            {
                while (newValue == 0)
                {
                    Console.WriteLine(
                        $"Enter a new value for {p.ParameterName} from the
 allowed values {p.AllowedValues} ");

                    var choice = Console.ReadLine();
                    int.TryParse(choice, out newValue);
                }

                p.ParameterValue = newValue.ToString();
            }
        }

        var request = new ModifyDBClusterParameterGroupRequest
        {
            Parameters = parameters,
            DBClusterParameterGroupName = groupName,
        };

        var result = await
 _amazonRDS.ModifyDBClusterParameterGroupAsync(request);
        return result.DBClusterParameterGroupName;
    }
```

- Einzelheiten zur API finden Sie unter ModifyDB ClusterParameter Group in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::ModifyDBClusterParameterGroupRequest request;
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);
        request.SetParameters(updateParameters);

        Aws::RDS::Model::ModifyDBClusterParameterGroupOutcome outcome =
                client.ModifyDBClusterParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB cluster parameter group was successfully
modified."
                      << std::endl;
        }
        else {
            std::cerr << "Error with Aurora::ModifyDBClusterParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
```

- Einzelheiten zur API finden Sie unter ModifyDB ClusterParameter Group in der AWS SDK for C++ API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
type DbClusters struct {
 AuroraClient *rds.Client
}



// UpdateParameters updates parameters in a named DB cluster parameter group.
func (clusters *DbClusters) UpdateParameters(parameterGroupName string, params
 []types.Parameter) error {
 _, err := clusters.AuroraClient.ModifyDBClusterParameterGroup(context.TODO(),
  &rds.ModifyDBClusterParameterGroupInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
   Parameters:                  params,
  })
 if err != nil {
  log.Printf("Couldn't update parameters in %v: %v\n", parameterGroupName, err)
  return err
 } else {
  return nil
 }
}
```

- Einzelheiten zur API finden Sie unter ModifyDB ClusterParameter Group in der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   public static void describeDbClusterParameterGroups(RdsClient rdsClient,
String dbClusterGroupName) {
       try {
           DescribeDbClusterParameterGroupsRequest groupsRequest =
DescribeDbClusterParameterGroupsRequest.builder()
                   .dbClusterParameterGroupName(dbClusterGroupName)
                   .maxRecords(20)
                   .build();

           List<DBClusterParameterGroup> groups =
rdsClient.describeDBClusterParameterGroups(groupsRequest)
                   .dbClusterParameterGroups();
           for (DBClusterParameterGroup group : groups) {
               System.out.println("The group name is " +
group.dbClusterParameterGroupName());
               System.out.println("The group ARN is " +
group.dbClusterParameterGroupArn());
           }

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Einzelheiten zur API finden Sie unter ModifyDB ClusterParameter Group in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// Modify the auto_increment_offset parameter.
suspend fun modifyDBClusterParas(dClusterGroupName: String?) {
    val parameter1 =
        Parameter {
            parameterName = "auto_increment_offset"
            applyMethod = ApplyMethod.fromValue("immediate")
            parameterValue = "5"
        }

    val paraList = ArrayList<Parameter>()
    paraList.add(parameter1)
    val groupRequest =
        ModifyDbClusterParameterGroupRequest {
            dbClusterParameterGroupName = dClusterGroupName
            parameters = paraList
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.modifyDbClusterParameterGroup(groupRequest)
        println("The parameter group ${response.dbClusterParameterGroupName} was
 successfully modified")
    }
}
```

- API-Details finden Sie unter ModifyDB ClusterParameter Group in der AWS SDK for Kotlin API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def update_parameters(self, parameter_group_name, update_parameters):
        """
        Updates parameters in a custom DB cluster parameter group.

        :param parameter_group_name: The name of the parameter group to update.
        :param update_parameters: The parameters to update in the group.
        :return: Data about the modified parameter group.
        """
        try:
            response = self.rds_client.modify_db_cluster_parameter_group(
                DBClusterParameterGroupName=parameter_group_name,
                Parameters=update_parameters,
            )
```

```
        except ClientError as err:
            logger.error(
                "Couldn't update parameters in %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- Einzelheiten zur API finden Sie unter ModifyDB ClusterParameter Group in der API-Referenz für AWS SDK for Python (Boto3).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   // Modify both the auto_increment_offset and auto_increment_increment
parameters in one call in the custom parameter group. Set their ParameterValue
fields to a new allowable value. rds.ModifyDbClusterParameterGroup.
   pub async fn update_auto_increment(
       &self,
       offset: u8,
       increment: u8,
   ) -> Result<(), ScenarioError> {
       let modify_db_cluster_parameter_group = self
           .rds
           .modify_db_cluster_parameter_group(
               DB_CLUSTER_PARAMETER_GROUP_NAME,
               vec![
                   Parameter::builder()
                       .parameter_name("auto_increment_offset")
```

```
                        .parameter_value(format!("{offset}"))
                        .apply_method(aws_sdk_rds::types::ApplyMethod::Immediate)
                        .build(),
                    Parameter::builder()
                        .parameter_name("auto_increment_increment")
                        .parameter_value(format!("{increment}"))
                        .apply_method(aws_sdk_rds::types::ApplyMethod::Immediate)
                        .build(),
                ],
            )
            .await;

        if let Err(error) = modify_db_cluster_parameter_group {
            return Err(ScenarioError::new(
                "Failed to modify cluster parameter group",
                &error,
            ));
        }

        Ok(())
    }

    pub async fn modify_db_cluster_parameter_group(
        &self,
        name: &str,
        parameters: Vec<Parameter>,
    ) -> Result<ModifyDbClusterParameterGroupOutput,
 SdkError<ModifyDBClusterParameterGroupError>>
    {
        self.inner
            .modify_db_cluster_parameter_group()
            .db_cluster_parameter_group_name(name)
            .set_parameters(Some(parameters))
            .send()
            .await
    }

#[tokio::test]
async fn test_scenario_update_auto_increment() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_modify_db_cluster_parameter_group()
        .withf(|name, params| {
```

```
            assert_eq!(name, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(
                params,
                &vec![
                    Parameter::builder()
                        .parameter_name("auto_increment_offset")
                        .parameter_value("10")
                        .apply_method(aws_sdk_rds::types::ApplyMethod::Immediate)
                        .build(),
                    Parameter::builder()
                        .parameter_name("auto_increment_increment")
                        .parameter_value("20")
                        .apply_method(aws_sdk_rds::types::ApplyMethod::Immediate)
                        .build(),
                ]
            );
            true
        })
        .return_once(|_, _|
 Ok(ModifyDbClusterParameterGroupOutput::builder().build()));

    let scenario = AuroraScenario::new(mock_rds);

    scenario
        .update_auto_increment(10, 20)
        .await
        .expect("update auto increment");
}

#[tokio::test]
async fn test_scenario_update_auto_increment_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_modify_db_cluster_parameter_group()
        .return_once(|_, _| {
            Err(SdkError::service_error(

 ModifyDBClusterParameterGroupError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "modify_db_cluster_parameter_group_error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
```

```
            ))
        });

    let scenario = AuroraScenario::new(mock_rds);

    let update = scenario.update_auto_increment(10, 20).await;
    assert_matches!(update, Err(ScenarioError { message, context: _}) if message
 == "Failed to modify cluster parameter group");
}
```

- Einzelheiten zur API finden Sie unter ModifyDB ClusterParameter Group in der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Szenarien für Aurora mit AWS SDKs

Die folgenden Codebeispiele zeigen Ihnen, wie Sie gängige Szenarien in Aurora mit AWS SDKs implementieren. Diese Szenarien zeigen Ihnen, wie Sie bestimmte Aufgaben durch den Aufruf mehrerer Funktionen innerhalb von Aurora erledigen können. Jedes Szenario enthält einen Link zu GitHub, wo Sie Anweisungen zur Einrichtung und Ausführung des Codes finden.

Beispiele

- Erste Schritte mit Aurora-DB-Clustern mithilfe eines AWS SDK

Erste Schritte mit Aurora-DB-Clustern mithilfe eines AWS SDK

Die folgenden Code-Beispiele veranschaulichen Folgendes:

- Erstellen Sie eine benutzerdefinierte Aurora-DB-Cluster-Parametergruppe und legen Sie Parameterwerte fest.
- Erstellen Sie einen DB-Cluster, der die Parametergruppe verwendet.
- Erstellen Sie eine DB-Instance, die eine Datenbank enthält.
- Erstellen Sie einen Snapshot des DB-Clusters und bereinigen Sie dann die Ressourcen.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung aus.

```
using Amazon.RDS;
using Amazon.RDS.Model;
using AuroraActions;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;
using Microsoft.Extensions.Logging;
using Microsoft.Extensions.Logging.Console;
using Microsoft.Extensions.Logging.Debug;

namespace AuroraScenario;

/// <summary>
/// Scenario for Amazon Aurora examples.
/// </summary>
public class AuroraScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.

    This .NET example performs the following tasks:
    1.  Return a list of the available DB engine families for Aurora MySql using
 the DescribeDBEngineVersionsAsync method.
    2.  Select an engine family and create a custom DB cluster parameter group
 using the CreateDBClusterParameterGroupAsync method.
    3.  Get the parameter group using the DescribeDBClusterParameterGroupsAsync
 method.
    4.  Get some parameters in the group using the
 DescribeDBClusterParametersAsync method.
    5.  Parse and display some parameters in the group.
```

```
   6.  Modify the auto_increment_offset and auto_increment_increment parameters
       using the ModifyDBClusterParameterGroupAsync method.
   7.  Get and display the updated parameters using the
DescribeDBClusterParametersAsync method with a source of "user".
   8.  Get a list of allowed engine versions using the
DescribeDBEngineVersionsAsync method.
   9.  Create an Aurora DB cluster that contains a MySql database and uses the
parameter group.
       using the CreateDBClusterAsync method.
   10. Wait for the DB cluster to be ready using the DescribeDBClustersAsync
method.
   11. Display and select from a list of instance classes available for the
selected engine and version
       using the paginated DescribeOrderableDBInstanceOptions method.
   12. Create a database instance in the cluster using the CreateDBInstanceAsync
method.
   13. Wait for the DB instance to be ready using the DescribeDBInstances
method.
   14. Display the connection endpoint string for the new DB cluster.
   15. Create a snapshot of the DB cluster using the
CreateDBClusterSnapshotAsync method.
   16. Wait for DB snapshot to be ready using the
DescribeDBClusterSnapshotsAsync method.
   17. Delete the DB instance using the DeleteDBInstanceAsync method.
   18. Delete the DB cluster using the DeleteDBClusterAsync method.
   19. Wait for DB cluster to be deleted using the DescribeDBClustersAsync
methods.
   20. Delete the cluster parameter group using the
DeleteDBClusterParameterGroupAsync.
   */

   private static readonly string sepBar = new('-', 80);
   private static AuroraWrapper auroraWrapper = null!;
   private static ILogger logger = null!;
   private static readonly string engine = "aurora-mysql";
   static async Task Main(string[] args)
   {
       // Set up dependency injection for the Amazon Relational Database Service
(Amazon RDS).
       using var host = Host.CreateDefaultBuilder(args)
           .ConfigureLogging(logging =>
               logging.AddFilter("System", LogLevel.Debug)
                   .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
```

```
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRDS>()
                    .AddTransient<AuroraWrapper>()
            )
            .Build();

        logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger<AuroraScenario>();

        auroraWrapper = host.Services.GetRequiredService<AuroraWrapper>();

        Console.WriteLine(sepBar);
        Console.WriteLine(
            "Welcome to the Amazon Aurora: get started with DB clusters
example.");
        Console.WriteLine(sepBar);

        DBClusterParameterGroup parameterGroup = null!;
        DBCluster? newCluster = null;
        DBInstance? newInstance = null;

        try
        {
            var parameterGroupFamily = await ChooseParameterGroupFamilyAsync();

            parameterGroup = await
CreateDBParameterGroupAsync(parameterGroupFamily);

            var parameters = await
DescribeParametersInGroupAsync(parameterGroup.DBClusterParameterGroupName,
                new List<string> { "auto_increment_offset",
"auto_increment_increment" });

            await
ModifyParametersAsync(parameterGroup.DBClusterParameterGroupName, parameters);

            await
DescribeUserSourceParameters(parameterGroup.DBClusterParameterGroupName);
```

```
            var engineVersionChoice = await
ChooseDBEngineVersionAsync(parameterGroupFamily);

            var newClusterIdentifier = "Example-Cluster-" + DateTime.Now.Ticks;

            newCluster = await CreateNewCluster
            (
                parameterGroup,
                engine,
                engineVersionChoice.EngineVersion,
                newClusterIdentifier
            );

            var instanceClassChoice = await ChooseDBInstanceClass(engine,
engineVersionChoice.EngineVersion);

            var newInstanceIdentifier = "Example-Instance-" + DateTime.Now.Ticks;

            newInstance = await CreateNewInstance(
                newClusterIdentifier,
                engine,
                engineVersionChoice.EngineVersion,
                instanceClassChoice.DBInstanceClass,
                newInstanceIdentifier
            );

            DisplayConnectionString(newCluster!);
            await CreateSnapshot(newCluster!);
            await CleanupResources(newInstance, newCluster, parameterGroup);

            Console.WriteLine("Scenario complete.");
            Console.WriteLine(sepBar);
        }
        catch (Exception ex)

        {
            await CleanupResources(newInstance, newCluster, parameterGroup);
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// Choose the Aurora DB parameter group family from a list of available
options.
```

```
    /// </summary>
    /// <returns>The selected parameter group family.</returns>
    public static async Task<string> ChooseParameterGroupFamilyAsync()
    {
        Console.WriteLine(sepBar);
        // 1. Get a list of available engines.
        var engines = await
auroraWrapper.DescribeDBEngineVersionsForEngineAsync(engine);

        Console.WriteLine($"1. The following is a list of available DB parameter
group families for engine {engine}:");

        var parameterGroupFamilies =
            engines.GroupBy(e => e.DBParameterGroupFamily).ToList();
        for (var i = 1; i <= parameterGroupFamilies.Count; i++)
        {
            var parameterGroupFamily = parameterGroupFamilies[i - 1];
            // List the available parameter group families.
            Console.WriteLine(
                $"\t{i}. Family: {parameterGroupFamily.Key}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > parameterGroupFamilies.Count)
        {
            Console.WriteLine("2. Select an available DB parameter group family
by entering a number from the preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        var parameterGroupFamilyChoice = parameterGroupFamilies[choiceNumber -
1];
        Console.WriteLine(sepBar);
        return parameterGroupFamilyChoice.Key;
    }

    /// <summary>
    /// Create and get information on a DB parameter group.
    /// </summary>
    /// <param name="dbParameterGroupFamily">The DBParameterGroupFamily for the
new DB parameter group.</param>
    /// <returns>The new DBParameterGroup.</returns>
    public static async Task<DBClusterParameterGroup>
CreateDBParameterGroupAsync(string dbParameterGroupFamily)
```

```
    {
        Console.WriteLine(sepBar);
        Console.WriteLine($"2. Create new DB parameter group with family
 {dbParameterGroupFamily}:");

        var parameterGroup = await
 auroraWrapper.CreateCustomClusterParameterGroupAsync(
            dbParameterGroupFamily,
            "ExampleParameterGroup-" + DateTime.Now.Ticks,
            "New example parameter group");

        var groupInfo =
            await
 auroraWrapper.DescribeCustomDBClusterParameterGroupAsync(parameterGroup.DBClusterParamet

        Console.WriteLine(
            $"3. New DB parameter group created: \n\t{groupInfo?.Description}, \n
\tARN {groupInfo?.DBClusterParameterGroupName}");
        Console.WriteLine(sepBar);
        return parameterGroup;
    }

    /// <summary>
    /// Get and describe parameters from a DBParameterGroup.
    /// </summary>
    /// <param name="parameterGroupName">The name of the DBParameterGroup.</
param>
    /// <param name="parameterNames">Optional specific names of parameters to
 describe.</param>
    /// <returns>The list of requested parameters.</returns>
    public static async Task<List<Parameter>>
 DescribeParametersInGroupAsync(string parameterGroupName, List<string>?
 parameterNames = null)
    {
        Console.WriteLine(sepBar);
        Console.WriteLine("4. Get some parameters from the group.");
        Console.WriteLine(sepBar);

        var parameters =
            await
 auroraWrapper.DescribeDBClusterParametersInGroupAsync(parameterGroupName);

        var matchingParameters =
```

```
            parameters.Where(p => parameterNames == null ||
 parameterNames.Contains(p.ParameterName)).ToList();

        Console.WriteLine("5. Parameter information:");
        matchingParameters.ForEach(p =>
            Console.WriteLine(
                $"\n\tParameter: {p.ParameterName}." +
                $"\n\tDescription: {p.Description}." +
                $"\n\tAllowed Values: {p.AllowedValues}." +
                $"\n\tValue: {p.ParameterValue}."));

        Console.WriteLine(sepBar);

        return matchingParameters;
    }

    /// <summary>
    /// Modify a parameter from a DBParameterGroup.
    /// </summary>
    /// <param name="parameterGroupName">Name of the DBParameterGroup.</param>
    /// <param name="parameters">The parameters to modify.</param>
    /// <returns>Async task.</returns>
    public static async Task ModifyParametersAsync(string parameterGroupName,
 List<Parameter> parameters)
    {
        Console.WriteLine(sepBar);
        Console.WriteLine("6. Modify some parameters in the group.");

        await
 auroraWrapper.ModifyIntegerParametersInGroupAsync(parameterGroupName,
 parameters);

        Console.WriteLine(sepBar);
    }

    /// <summary>
    /// Describe the user source parameters in the group.
    /// </summary>
    /// <param name="parameterGroupName">The name of the DBParameterGroup.</
param>
    /// <returns>Async task.</returns>
    public static async Task DescribeUserSourceParameters(string
 parameterGroupName)
    {
```

```
        Console.WriteLine(sepBar);
        Console.WriteLine("7. Describe updated user source parameters in the
group.");

        var parameters =
            await
auroraWrapper.DescribeDBClusterParametersInGroupAsync(parameterGroupName,
"user");

        parameters.ForEach(p =>
            Console.WriteLine(
                $"\n\tParameter: {p.ParameterName}." +
                $"\n\tDescription: {p.Description}." +
                $"\n\tAllowed Values: {p.AllowedValues}." +
                $"\n\tValue: {p.ParameterValue}."));

        Console.WriteLine(sepBar);
    }

    /// <summary>
    /// Choose a DB engine version.
    /// </summary>
    /// <param name="dbParameterGroupFamily">DB parameter group family for engine
choice.</param>
    /// <returns>The selected engine version.</returns>
    public static async Task<DBEngineVersion> ChooseDBEngineVersionAsync(string
dbParameterGroupFamily)
    {
        Console.WriteLine(sepBar);
        // Get a list of allowed engines.
        var allowedEngines =
            await auroraWrapper.DescribeDBEngineVersionsForEngineAsync(engine,
dbParameterGroupFamily);

        Console.WriteLine($"Available DB engine versions for parameter group
family {dbParameterGroupFamily}:");
        int i = 1;
        foreach (var version in allowedEngines)
        {
            Console.WriteLine(
                $"\t{i}. {version.DBEngineVersionDescription}.");
            i++;
        }
```

```
        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > allowedEngines.Count)
        {
            Console.WriteLine("8. Select an available DB engine version by
 entering a number from the list above:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        var engineChoice = allowedEngines[choiceNumber - 1];
        Console.WriteLine(sepBar);
        return engineChoice;
    }

    /// <summary>
    /// Create a new RDS DB cluster.
    /// </summary>
    /// <param name="parameterGroup">Parameter group to use for the DB cluster.</
param>
    /// <param name="engineName">Engine to use for the DB cluster.</param>
    /// <param name="engineVersion">Engine version to use for the DB cluster.</
param>
    /// <param name="clusterIdentifier">Cluster identifier to use for the DB
 cluster.</param>
    /// <returns>The new DB cluster.</returns>
    public static async Task<DBCluster?> CreateNewCluster(DBClusterParameterGroup
 parameterGroup,
        string engineName, string engineVersion, string clusterIdentifier)
    {
        Console.WriteLine(sepBar);
        Console.WriteLine($"9. Create a new DB cluster with identifier
 {clusterIdentifier}.");

        DBCluster newCluster;
        var clusters = await auroraWrapper.DescribeDBClustersPagedAsync();
        var isClusterCreated = clusters.Any(i => i.DBClusterIdentifier ==
 clusterIdentifier);

        if (isClusterCreated)
        {
            Console.WriteLine("Cluster already created.");
            newCluster = clusters.First(i => i.DBClusterIdentifier ==
 clusterIdentifier);
        }
```

```
        else
        {
            Console.WriteLine("Enter an admin username:");
            var username = Console.ReadLine();

            Console.WriteLine("Enter an admin password:");
            var password = Console.ReadLine();

            newCluster = await auroraWrapper.CreateDBClusterWithAdminAsync(
                "ExampleDatabase",
                clusterIdentifier,
                parameterGroup.DBClusterParameterGroupName,
                engineName,
                engineVersion,
                username!,
                password!
            );

            Console.WriteLine("10. Waiting for DB cluster to be ready...");
            while (newCluster.Status != "available")
            {
                Console.Write(".");
                Thread.Sleep(5000);
                clusters = await
 auroraWrapper.DescribeDBClustersPagedAsync(clusterIdentifier);
                newCluster = clusters.First();
            }
        }

        Console.WriteLine(sepBar);
        return newCluster;
    }

    /// <summary>
    /// Choose a DB instance class for a particular engine and engine version.
    /// </summary>
    /// <param name="engine">DB engine for DB instance choice.</param>
    /// <param name="engineVersion">DB engine version for DB instance choice.</
param>
    /// <returns>The selected orderable DB instance option.</returns>
    public static async Task<OrderableDBInstanceOption>
 ChooseDBInstanceClass(string engine, string engineVersion)
    {
        Console.WriteLine(sepBar);
```

```
        // Get a list of allowed DB instance classes.
        var allowedInstances =
            await
 auroraWrapper.DescribeOrderableDBInstanceOptionsPagedAsync(engine,
 engineVersion);

        Console.WriteLine($"Available DB instance classes for engine {engine} and
 version {engineVersion}:");
        int i = 1;


        foreach (var instance in allowedInstances)
        {
            Console.WriteLine(
                $"\t{i}. Instance class: {instance.DBInstanceClass} (storage type
 {instance.StorageType})");
            i++;
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > allowedInstances.Count)
        {
            Console.WriteLine("11. Select an available DB instance class by
 entering a number from the preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        var instanceChoice = allowedInstances[choiceNumber - 1];
        Console.WriteLine(sepBar);
        return instanceChoice;
    }

    /// <summary>
    /// Create a new DB instance.
    /// </summary>
    /// <param name="engineName">Engine to use for the DB instance.</param>
    /// <param name="engineVersion">Engine version to use for the DB instance.</
param>
    /// <param name="instanceClass">Instance class to use for the DB instance.</
param>
    /// <param name="instanceIdentifier">Instance identifier to use for the DB
 instance.</param>
    /// <returns>The new DB instance.</returns>
```

```
   public static async Task<DBInstance?> CreateNewInstance(
       string clusterIdentifier,
       string engineName,
       string engineVersion,
       string instanceClass,
       string instanceIdentifier)
   {
       Console.WriteLine(sepBar);
       Console.WriteLine($"12. Create a new DB instance with identifier
{instanceIdentifier}.");
       bool isInstanceReady = false;
       DBInstance newInstance;
       var instances = await auroraWrapper.DescribeDBInstancesPagedAsync();
       isInstanceReady = instances.FirstOrDefault(i =>
           i.DBInstanceIdentifier == instanceIdentifier)?.DBInstanceStatus ==
"available";

       if (isInstanceReady)
       {
           Console.WriteLine("Instance already created.");
           newInstance = instances.First(i => i.DBInstanceIdentifier ==
instanceIdentifier);
       }
       else
       {

           newInstance = await auroraWrapper.CreateDBInstanceInClusterAsync(
               clusterIdentifier,
               instanceIdentifier,
               engineName,
               engineVersion,
               instanceClass
           );

           Console.WriteLine("13. Waiting for DB instance to be ready...");
           while (!isInstanceReady)
           {
               Console.Write(".");
               Thread.Sleep(5000);
               instances = await
auroraWrapper.DescribeDBInstancesPagedAsync(instanceIdentifier);
               isInstanceReady = instances.FirstOrDefault()?.DBInstanceStatus ==
"available";
               newInstance = instances.First();
```

```
            }
        }

        Console.WriteLine(sepBar);
        return newInstance;
    }

    /// <summary>
    /// Display a connection string for an Amazon RDS DB cluster.
    /// </summary>
    /// <param name="cluster">The DB cluster to use to get a connection string.</
param>
    public static void DisplayConnectionString(DBCluster cluster)
    {
        Console.WriteLine(sepBar);
        // Display the connection string.
        Console.WriteLine("14. New DB cluster connection string: ");
        Console.WriteLine(
            $"\n{engine} -h {cluster.Endpoint} -P {cluster.Port} "
            + $"-u {cluster.MasterUsername} -p [YOUR PASSWORD]\n");

        Console.WriteLine(sepBar);
    }

    /// <summary>
    /// Create a snapshot from an Amazon RDS DB cluster.
    /// </summary>
    /// <param name="cluster">DB cluster to use when creating a snapshot.</param>
    /// <returns>The snapshot object.</returns>
    public static async Task<DBClusterSnapshot> CreateSnapshot(DBCluster cluster)
    {
        Console.WriteLine(sepBar);
        // Create a snapshot.
        Console.WriteLine($"15. Creating snapshot from DB cluster
 {cluster.DBClusterIdentifier}.");
       var snapshot = await
 auroraWrapper.CreateClusterSnapshotByIdentifierAsync(
            cluster.DBClusterIdentifier,
            "ExampleSnapshot-" + DateTime.Now.Ticks);

        // Wait for the snapshot to be available.
        bool isSnapshotReady = false;

        Console.WriteLine($"16. Waiting for snapshot to be ready...");
```

```
        while (!isSnapshotReady)
        {
            Console.Write(".");
            Thread.Sleep(5000);
            var snapshots =
                await
auroraWrapper.DescribeDBClusterSnapshotsByIdentifierAsync(cluster.DBClusterIdentifier);
            isSnapshotReady = snapshots.FirstOrDefault()?.Status == "available";
            snapshot = snapshots.First();
        }

        Console.WriteLine(
            $"Snapshot {snapshot.DBClusterSnapshotIdentifier} status is
{snapshot.Status}.");
        Console.WriteLine(sepBar);
        return snapshot;
    }

    /// <summary>
    /// Clean up resources from the scenario.
    /// </summary>
    /// <param name="newInstance">The instance to clean up.</param>
    /// <param name="newCluster">The cluster to clean up.</param>
    /// <param name="parameterGroup">The parameter group to clean up.</param>
    /// <returns>Async Task.</returns>
    private static async Task CleanupResources(
        DBInstance? newInstance,
        DBCluster? newCluster,
        DBClusterParameterGroup? parameterGroup)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"Clean up resources.");

        if (newInstance is not null && GetYesNoResponse($"\tClean up instance
{newInstance.DBInstanceIdentifier}? (y/n)"))
        {
            // Delete the DB instance.
            Console.WriteLine($"17. Deleting the DB instance
{newInstance.DBInstanceIdentifier}.");
            await
auroraWrapper.DeleteDBInstanceByIdentifierAsync(newInstance.DBInstanceIdentifier);
        }
```

```
        if (newCluster is not null && GetYesNoResponse($"\tClean up cluster
 {newCluster.DBClusterIdentifier}? (y/n)"))
        {
            // Delete the DB cluster.
            Console.WriteLine($"18. Deleting the DB cluster
 {newCluster.DBClusterIdentifier}.");
            await
 auroraWrapper.DeleteDBClusterByIdentifierAsync(newCluster.DBClusterIdentifier);

            // Wait for the DB cluster to delete.
            Console.WriteLine($"19. Waiting for the DB cluster to delete...");
            bool isClusterDeleted = false;

            while (!isClusterDeleted)
            {
                Console.Write(".");
                Thread.Sleep(5000);
                var cluster = await auroraWrapper.DescribeDBClustersPagedAsync();
                isClusterDeleted = cluster.All(i => i.DBClusterIdentifier !=
 newCluster.DBClusterIdentifier);
            }

            Console.WriteLine("DB cluster deleted.");
        }

        if (parameterGroup is not null && GetYesNoResponse($"\tClean up parameter
 group? (y/n)"))
        {
            Console.WriteLine($"20. Deleting the DB parameter group
 {parameterGroup.DBClusterParameterGroupName}.");
            await
 auroraWrapper.DeleteClusterParameterGroupByNameAsync(parameterGroup.DBClusterParameterGr
            Console.WriteLine("Parameter group deleted.");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Get a yes or no response from the user.
    /// </summary>
    /// <param name="question">The question string to print on the console.</
param>
    /// <returns>True if the user responds with a yes.</returns>
```

```
    private static bool GetYesNoResponse(string question)
    {
        Console.WriteLine(question);
        var ynResponse = Console.ReadLine();
        var response = ynResponse != null &&
                       ynResponse.Equals("y",
                           StringComparison.InvariantCultureIgnoreCase);
        return response;
    }
```

Wrapper-Methoden, die vom Szenario aufgerufen werden, um Aurora-Aktionen zu verwalten.

```
using Amazon.RDS;
using Amazon.RDS.Model;

namespace AuroraActions;

/// <summary>
/// Wrapper for the Amazon Aurora cluster client operations.
/// </summary>
public class AuroraWrapper
{
    private readonly IAmazonRDS _amazonRDS;
    public AuroraWrapper(IAmazonRDS amazonRDS)
    {
        _amazonRDS = amazonRDS;
    }

    /// <summary>
    /// Get a list of DB engine versions for a particular DB engine.
    /// </summary>
    /// <param name="engine">The name of the engine.</param>
    /// <param name="parameterGroupFamily">Optional parameter group family
 name.</param>
    /// <returns>A list of DBEngineVersions.</returns>
    public async Task<List<DBEngineVersion>>
 DescribeDBEngineVersionsForEngineAsync(string engine,
        string? parameterGroupFamily = null)
    {
        var response = await _amazonRDS.DescribeDBEngineVersionsAsync(
            new DescribeDBEngineVersionsRequest()
```

```
            {
                Engine = engine,
                DBParameterGroupFamily = parameterGroupFamily
            });
        return response.DBEngineVersions;
    }

    /// <summary>
    /// Create a custom cluster parameter group.
    /// </summary>
    /// <param name="parameterGroupFamily">The family of the parameter group.</
param>
    /// <param name="groupName">The name for the new parameter group.</param>
    /// <param name="description">A description for the new parameter group.</
param>
    /// <returns>The new parameter group object.</returns>
    public async Task<DBClusterParameterGroup>
 CreateCustomClusterParameterGroupAsync(
        string parameterGroupFamily,
        string groupName,
        string description)
    {
        var request = new CreateDBClusterParameterGroupRequest
        {
            DBParameterGroupFamily = parameterGroupFamily,
            DBClusterParameterGroupName = groupName,
            Description = description,
        };

        var response = await
 _amazonRDS.CreateDBClusterParameterGroupAsync(request);
        return response.DBClusterParameterGroup;
    }

    /// <summary>
    /// Describe the cluster parameters in a parameter group.
    /// </summary>
    /// <param name="groupName">The name of the parameter group.</param>
    /// <param name="source">The optional name of the source filter.</param>
    /// <returns>The collection of parameters.</returns>
    public async Task<List<Parameter>>
 DescribeDBClusterParametersInGroupAsync(string groupName, string? source = null)
    {
        var paramList = new List<Parameter>();
```

```
        DescribeDBClusterParametersResponse response;
        var request = new DescribeDBClusterParametersRequest
        {
            DBClusterParameterGroupName = groupName,
            Source = source,
        };

        // Get the full list if there are multiple pages.
        do
        {
            response = await
 _amazonRDS.DescribeDBClusterParametersAsync(request);
            paramList.AddRange(response.Parameters);

            request.Marker = response.Marker;
        }
        while (response.Marker is not null);

        return paramList;
    }

    /// <summary>
    /// Get the description of a DB cluster parameter group by name.
    /// </summary>
    /// <param name="name">The name of the DB parameter group to describe.</
param>
    /// <returns>The parameter group description.</returns>
    public async Task<DBClusterParameterGroup?>
 DescribeCustomDBClusterParameterGroupAsync(string name)
    {
        var response = await _amazonRDS.DescribeDBClusterParameterGroupsAsync(
            new DescribeDBClusterParameterGroupsRequest()
            {
                DBClusterParameterGroupName = name
            });
        return response.DBClusterParameterGroups.FirstOrDefault();
    }

    /// <summary>
    /// Modify the specified integer parameters with new values from user input.
    /// </summary>
    /// <param name="groupName">The group name for the parameters.</param>
```

```
    /// <param name="parameters">The list of integer parameters to modify.</
param>
    /// <param name="newValue">Optional int value to set for parameters.</param>
    /// <returns>The name of the group that was modified.</returns>
    public async Task<string> ModifyIntegerParametersInGroupAsync(string
 groupName, List<Parameter> parameters, int newValue = 0)
    {
        foreach (var p in parameters)
        {
            if (p.IsModifiable && p.DataType == "integer")
            {
                while (newValue == 0)
                {
                    Console.WriteLine(
                        $"Enter a new value for {p.ParameterName} from the
 allowed values {p.AllowedValues} ");

                    var choice = Console.ReadLine();
                    int.TryParse(choice, out newValue);
                }

                p.ParameterValue = newValue.ToString();
            }
        }

        var request = new ModifyDBClusterParameterGroupRequest
        {
            Parameters = parameters,
            DBClusterParameterGroupName = groupName,
        };

        var result = await
 _amazonRDS.ModifyDBClusterParameterGroupAsync(request);
        return result.DBClusterParameterGroupName;
    }


    /// <summary>
    /// Get a list of orderable DB instance options for a specific
    /// engine and engine version.
    /// </summary>
    /// <param name="engine">Name of the engine.</param>
    /// <param name="engineVersion">Version of the engine.</param>
    /// <returns>List of OrderableDBInstanceOptions.</returns>
```

```
   public async Task<List<OrderableDBInstanceOption>>
DescribeOrderableDBInstanceOptionsPagedAsync(string engine, string
engineVersion)
   {
       // Use a paginator to get a list of DB instance options.
       var results = new List<OrderableDBInstanceOption>();
       var paginateInstanceOptions =
_amazonRDS.Paginators.DescribeOrderableDBInstanceOptions(
           new DescribeOrderableDBInstanceOptionsRequest()
           {
               Engine = engine,
               EngineVersion = engineVersion,
           });
       // Get the entire list using the paginator.
       await foreach (var instanceOptions in
paginateInstanceOptions.OrderableDBInstanceOptions)
       {
           results.Add(instanceOptions);
       }
       return results;
   }

   /// <summary>
   /// Delete a particular parameter group by name.
   /// </summary>
   /// <param name="groupName">The name of the parameter group.</param>
   /// <returns>True if successful.</returns>
   public async Task<bool> DeleteClusterParameterGroupByNameAsync(string
groupName)
   {
       var request = new DeleteDBClusterParameterGroupRequest
       {
           DBClusterParameterGroupName = groupName,
       };

       var response = await
_amazonRDS.DeleteDBClusterParameterGroupAsync(request);
       return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
   }

   /// <summary>
   /// Create a new cluster and database.
   /// </summary>
   /// <param name="dbName">The name of the new database.</param>
```

```
    /// <param name="clusterIdentifier">The identifier of the cluster.</param>
    /// <param name="parameterGroupName">The name of the parameter group.</param>
    /// <param name="dbEngine">The engine to use for the new cluster.</param>
    /// <param name="dbEngineVersion">The version of the engine to use.</param>
    /// <param name="adminName">The admin username.</param>
    /// <param name="adminPassword">The primary admin password.</param>
    /// <returns>The cluster object.</returns>
    public async Task<DBCluster> CreateDBClusterWithAdminAsync(
        string dbName,
        string clusterIdentifier,
        string parameterGroupName,
        string dbEngine,
        string dbEngineVersion,
        string adminName,
        string adminPassword)
    {
        var request = new CreateDBClusterRequest
        {
            DatabaseName = dbName,
            DBClusterIdentifier = clusterIdentifier,
            DBClusterParameterGroupName = parameterGroupName,
            Engine = dbEngine,
            EngineVersion = dbEngineVersion,
            MasterUsername = adminName,
            MasterUserPassword = adminPassword,
        };

        var response = await _amazonRDS.CreateDBClusterAsync(request);
        return response.DBCluster;
    }

    /// <summary>
    /// Returns a list of DB instances.
    /// </summary>
    /// <param name="dbInstanceIdentifier">Optional name of a specific DB
instance.</param>
    /// <returns>List of DB instances.</returns>
    public async Task<List<DBInstance>> DescribeDBInstancesPagedAsync(string?
dbInstanceIdentifier = null)
    {
        var results = new List<DBInstance>();
        var instancesPaginator = _amazonRDS.Paginators.DescribeDBInstances(
            new DescribeDBInstancesRequest
            {
```

```
                DBInstanceIdentifier = dbInstanceIdentifier
            });
        // Get the entire list using the paginator.
        await foreach (var instances in instancesPaginator.DBInstances)
        {
            results.Add(instances);
        }
        return results;
    }

    /// <summary>
    /// Returns a list of DB clusters.
    /// </summary>
    /// <param name="dbInstanceIdentifier">Optional name of a specific DB
cluster.</param>
    /// <returns>List of DB clusters.</returns>
    public async Task<List<DBCluster>> DescribeDBClustersPagedAsync(string?
dbClusterIdentifier = null)
    {
        var results = new List<DBCluster>();

        DescribeDBClustersResponse response;
        DescribeDBClustersRequest request = new DescribeDBClustersRequest
        {
            DBClusterIdentifier = dbClusterIdentifier
        };
        // Get the full list if there are multiple pages.
        do
        {
            response = await _amazonRDS.DescribeDBClustersAsync(request);
            results.AddRange(response.DBClusters);
            request.Marker = response.Marker;
        }
        while (response.Marker is not null);
        return results;
    }

    /// <summary>
    /// Create an Amazon Relational Database Service (Amazon RDS) DB instance
    /// with a particular set of properties. Use the action
DescribeDBInstancesAsync
    /// to determine when the DB instance is ready to use.
    /// </summary>
    /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
```

```
    /// <param name="dbClusterIdentifier">DB cluster identifier.</param>
    /// <param name="dbEngine">The engine for the DB instance.</param>
    /// <param name="dbEngineVersion">Version for the DB instance.</param>
    /// <param name="instanceClass">Class for the DB instance.</param>
    /// <returns>DB instance object.</returns>
    public async Task<DBInstance> CreateDBInstanceInClusterAsync(
        string dbClusterIdentifier,
        string dbInstanceIdentifier,
        string dbEngine,
        string dbEngineVersion,
        string instanceClass)
    {
        // When creating the instance within a cluster, do not specify the name
or size.
        var response = await _amazonRDS.CreateDBInstanceAsync(
            new CreateDBInstanceRequest()
            {
                DBClusterIdentifier = dbClusterIdentifier,
                DBInstanceIdentifier = dbInstanceIdentifier,
                Engine = dbEngine,
                EngineVersion = dbEngineVersion,
                DBInstanceClass = instanceClass
            });

        return response.DBInstance;
    }

    /// <summary>
    /// Create a snapshot of a cluster.
    /// </summary>
    /// <param name="dbClusterIdentifier">DB cluster identifier.</param>
    /// <param name="snapshotIdentifier">Identifier for the snapshot.</param>
    /// <returns>DB snapshot object.</returns>
    public async Task<DBClusterSnapshot>
CreateClusterSnapshotByIdentifierAsync(string dbClusterIdentifier, string
snapshotIdentifier)
    {
        var response = await _amazonRDS.CreateDBClusterSnapshotAsync(
            new CreateDBClusterSnapshotRequest()
            {
                DBClusterIdentifier = dbClusterIdentifier,
                DBClusterSnapshotIdentifier = snapshotIdentifier,
            });
```

```
        return response.DBClusterSnapshot;
    }

    /// <summary>
    /// Return a list of DB snapshots for a particular DB cluster.
    /// </summary>
    /// <param name="dbClusterIdentifier">DB cluster identifier.</param>
    /// <returns>List of DB snapshots.</returns>
    public async Task<List<DBClusterSnapshot>>
DescribeDBClusterSnapshotsByIdentifierAsync(string dbClusterIdentifier)
    {
        var results = new List<DBClusterSnapshot>();

        DescribeDBClusterSnapshotsResponse response;
        DescribeDBClusterSnapshotsRequest request = new
DescribeDBClusterSnapshotsRequest
        {
            DBClusterIdentifier = dbClusterIdentifier
        };
        // Get the full list if there are multiple pages.
        do
        {
            response = await _amazonRDS.DescribeDBClusterSnapshotsAsync(request);
            results.AddRange(response.DBClusterSnapshots);
            request.Marker = response.Marker;
        }
        while (response.Marker is not null);
        return results;
    }

    /// <summary>
    /// Delete a particular DB cluster.
    /// </summary>
    /// <param name="dbClusterIdentifier">DB cluster identifier.</param>
    /// <returns>DB cluster object.</returns>
    public async Task<DBCluster> DeleteDBClusterByIdentifierAsync(string
dbClusterIdentifier)
    {
        var response = await _amazonRDS.DeleteDBClusterAsync(
            new DeleteDBClusterRequest()
            {
                DBClusterIdentifier = dbClusterIdentifier,
                SkipFinalSnapshot = true
            });
```

```
        return response.DBCluster;
    }

    /// <summary>
    /// Delete a particular DB instance.
    /// </summary>
    /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
    /// <returns>DB instance object.</returns>
    public async Task<DBInstance> DeleteDBInstanceByIdentifierAsync(string
 dbInstanceIdentifier)
    {
        var response = await _amazonRDS.DeleteDBInstanceAsync(
            new DeleteDBInstanceRequest()
            {
                DBInstanceIdentifier = dbInstanceIdentifier,
                SkipFinalSnapshot = true,
                DeleteAutomatedBackups = true
            });

        return response.DBInstance;
    }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for .NET -API-Referenz.
  - CreateDBCluster
  - DB-Gruppe erstellt ClusterParameter
  - DB wurde erstellt ClusterSnapshot
  - CreateDBInstance
  - DeleteDBCluster
  - DB-Gruppe gelöscht ClusterParameter
  - DeleteDBInstance
  - Beschriebene ClusterParameter DB-Gruppen
  - BeschriebenDB ClusterParameters
  - BeschriebenB ClusterSnapshots
  - DescribeDBClusters
  - BeschriebenB EngineVersions

- DescribeDBInstances
- DescribeOrderableDB InstanceOptions
- DB-Gruppe ändern ClusterParameter

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

//! Routine which creates an Amazon Aurora DB cluster and demonstrates several
 operations
//! on that cluster.
/*!
 \sa gettingStartedWithDBClusters()
 \param clientConfiguration: AWS client configuration.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::gettingStartedWithDBClusters(
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::RDS::RDSClient client(clientConfig);

    printAsterisksLine();
    std::cout << "Welcome to the Amazon Relational Database Service (Amazon
 Aurora)"
              << std::endl;
    std::cout << "get started with DB clusters demo." << std::endl;
    printAsterisksLine();

    std::cout << "Checking for an existing DB cluster parameter group named '" <<
              CLUSTER_PARAMETER_GROUP_NAME << "'." << std::endl;
    Aws::String dbParameterGroupFamily("Undefined");
    bool parameterGroupFound = true;
```

```
    {
        // 1. Check if the DB cluster parameter group already exists.
        Aws::RDS::Model::DescribeDBClusterParameterGroupsRequest request;
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);

        Aws::RDS::Model::DescribeDBClusterParameterGroupsOutcome outcome =
                client.DescribeDBClusterParameterGroups(request);

        if (outcome.IsSuccess()) {
            std::cout << "DB cluster parameter group named '" <<
                      CLUSTER_PARAMETER_GROUP_NAME << "' already exists." <<
 std::endl;
            dbParameterGroupFamily =
 outcome.GetResult().GetDBClusterParameterGroups()
[0].GetDBParameterGroupFamily();
        }
        else if (outcome.GetError().GetErrorType() ==
                 Aws::RDS::RDSErrors::D_B_PARAMETER_GROUP_NOT_FOUND_FAULT) {
            std::cout << "DB cluster parameter group named '" <<
                      CLUSTER_PARAMETER_GROUP_NAME << "' does not exist." <<
 std::endl;
            parameterGroupFound = false;
        }
        else {
            std::cerr << "Error with Aurora::DescribeDBClusterParameterGroups. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    }

    if (!parameterGroupFound) {
        Aws::Vector<Aws::RDS::Model::DBEngineVersion> engineVersions;

        // 2. Get available parameter group families for the specified engine.
        if (!getDBEngineVersions(DB_ENGINE, NO_PARAMETER_GROUP_FAMILY,
                                 engineVersions, client)) {
            return false;
        }

        std::cout << "Getting available parameter group families for " <<
 DB_ENGINE
                  << "."
                  << std::endl;
```

```
        std::vector<Aws::String> families;
        for (const Aws::RDS::Model::DBEngineVersion &version: engineVersions) {
            Aws::String family = version.GetDBParameterGroupFamily();
            if (std::find(families.begin(), families.end(), family) ==
                families.end()) {
                families.push_back(family);
                std::cout << "  " << families.size() << ": " << family <<
std::endl;
            }
        }

        int choice = askQuestionForIntRange("Which family do you want to use? ",
1,
                                            static_cast<int>(families.size()));
        dbParameterGroupFamily = families[choice - 1];
    }
    if (!parameterGroupFound) {
        // 3.  Create a DB cluster parameter group.
        Aws::RDS::Model::CreateDBClusterParameterGroupRequest request;
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);
        request.SetDBParameterGroupFamily(dbParameterGroupFamily);
        request.SetDescription("Example cluster parameter group.");

        Aws::RDS::Model::CreateDBClusterParameterGroupOutcome outcome =
                client.CreateDBClusterParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB cluster parameter group was successfully
created."
                      << std::endl;
        }
        else {
            std::cerr << "Error with Aurora::CreateDBClusterParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    }

    printAsterisksLine();
    std::cout << "Let's set some parameter values in your cluster parameter
group."
              << std::endl;
```

```
    Aws::Vector<Aws::RDS::Model::Parameter> autoIncrementParameters;
    // 4.  Get the parameters in the DB cluster parameter group.
    if (!getDBClusterParameters(CLUSTER_PARAMETER_GROUP_NAME,
AUTO_INCREMENT_PREFIX,
                                NO_SOURCE,
                                autoIncrementParameters,
                                client)) {
        cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, "", "", client);
        return false;
    }

    Aws::Vector<Aws::RDS::Model::Parameter> updateParameters;

    for (Aws::RDS::Model::Parameter &autoIncParameter: autoIncrementParameters) {
        if (autoIncParameter.GetIsModifiable() &&
            (autoIncParameter.GetDataType() == "integer")) {
            std::cout << "The " << autoIncParameter.GetParameterName()
                      << " is described as: " <<
                      autoIncParameter.GetDescription() << "." << std::endl;
            if (autoIncParameter.ParameterValueHasBeenSet()) {
                std::cout << "The current value is "
                          << autoIncParameter.GetParameterValue()
                          << "." << std::endl;
            }
            std::vector<int> splitValues = splitToInts(
                    autoIncParameter.GetAllowedValues(), '-');
            if (splitValues.size() == 2) {
                int newValue = askQuestionForIntRange(
                        Aws::String("Enter a new value between ") +
                        autoIncParameter.GetAllowedValues() + ": ",
                        splitValues[0], splitValues[1]);
                autoIncParameter.SetParameterValue(std::to_string(newValue));
                updateParameters.push_back(autoIncParameter);

            }
            else {
                std::cerr << "Error parsing " <<
autoIncParameter.GetAllowedValues()
                          << std::endl;
            }
        }
    }

    {
```

```
        // 5.  Modify the auto increment parameters in the DB cluster parameter
group.
        Aws::RDS::Model::ModifyDBClusterParameterGroupRequest request;
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);
        request.SetParameters(updateParameters);

        Aws::RDS::Model::ModifyDBClusterParameterGroupOutcome outcome =
                client.ModifyDBClusterParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB cluster parameter group was successfully
modified."
                      << std::endl;
        }
        else {
            std::cerr << "Error with Aurora::ModifyDBClusterParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
    }

    std::cout
            << "You can get a list of parameters you've set by specifying a
source of 'user'."
            << std::endl;

    Aws::Vector<Aws::RDS::Model::Parameter> userParameters;
    // 6.  Display the modified parameters in the DB cluster parameter group.
    if (!getDBClusterParameters(CLUSTER_PARAMETER_GROUP_NAME, NO_NAME_PREFIX,
"user",
                                userParameters,
                                client)) {
        cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, "", "", client);
        return false;
    }

    for (const auto &userParameter: userParameters) {
        std::cout << "  " << userParameter.GetParameterName() << ", " <<
                  userParameter.GetDescription() << ", parameter value - "
                  << userParameter.GetParameterValue() << std::endl;
    }

    printAsterisksLine();
    std::cout << "Checking for an existing DB Cluster." << std::endl;
```

```
   Aws::RDS::Model::DBCluster dbCluster;
   // 7.  Check if the DB cluster already exists.
   if (!describeDBCluster(DB_CLUSTER_IDENTIFIER, dbCluster, client)) {
       cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, "", "", client);
       return false;
   }

   Aws::String engineVersionName;
   Aws::String engineName;
   if (dbCluster.DBClusterIdentifierHasBeenSet()) {
       std::cout << "The DB cluster already exists." << std::endl;
       engineVersionName = dbCluster.GetEngineVersion();
       engineName = dbCluster.GetEngine();

   }
   else {
       std::cout << "Let's create a DB cluster." << std::endl;
       const Aws::String administratorName = askQuestion(
               "Enter an administrator username for the database: ");
       const Aws::String administratorPassword = askQuestion(
               "Enter a password for the administrator (at least 8 characters):
");
       Aws::Vector<Aws::RDS::Model::DBEngineVersion> engineVersions;

       // 8.  Get a list of engine versions for the parameter group family.
       if (!getDBEngineVersions(DB_ENGINE, dbParameterGroupFamily,
engineVersions,
                                client)) {
           cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, "", "", client);
           return false;
       }

       std::cout << "The available engines for your parameter group family are:"
                 << std::endl;

       int index = 1;
       for (const Aws::RDS::Model::DBEngineVersion &engineVersion:
engineVersions) {
           std::cout << "   " << index << ": " <<
engineVersion.GetEngineVersion()
                     << std::endl;
           ++index;
       }
```

```
        int choice = askQuestionForIntRange("Which engine do you want to use? ",
1,

static_cast<int>(engineVersions.size()));
        const Aws::RDS::Model::DBEngineVersion engineVersion =
engineVersions[choice -
                                                                              1];

        engineName = engineVersion.GetEngine();
        engineVersionName = engineVersion.GetEngineVersion();
        std::cout << "Creating a DB cluster named '" << DB_CLUSTER_IDENTIFIER
                  << "' and database '" << DB_NAME << "'.\n"
                  << "The DB cluster is configured to use your custom cluster
parameter group '"
                  << CLUSTER_PARAMETER_GROUP_NAME << "', and \n"
                  << "selected engine version " <<
engineVersion.GetEngineVersion()
                  << ".\nThis typically takes several minutes." << std::endl;

        Aws::RDS::Model::CreateDBClusterRequest request;
        request.SetDBClusterIdentifier(DB_CLUSTER_IDENTIFIER);
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);
        request.SetEngine(engineName);
        request.SetEngineVersion(engineVersionName);
        request.SetMasterUsername(administratorName);
        request.SetMasterUserPassword(administratorPassword);

        Aws::RDS::Model::CreateDBClusterOutcome outcome =
                client.CreateDBCluster(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB cluster creation has started."
                      << std::endl;
        }
        else {
            std::cerr << "Error with Aurora::CreateDBCluster. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, "", "", client);
            return false;
        }
    }

    std::cout << "Waiting for the DB cluster to become available." << std::endl;
```

```
    int counter = 0;
    // 11. Wait for the DB cluster to become available.
    do {
        std::this_thread::sleep_for(std::chrono::seconds(1));
        ++counter;
        if (counter > 900) {
            std::cerr << "Wait for cluster to become available timed out ofter "
                      << counter
                      << " seconds." << std::endl;
            cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
                             DB_CLUSTER_IDENTIFIER, "", client);
            return false;
        }

        dbCluster = Aws::RDS::Model::DBCluster();
        if (!describeDBCluster(DB_CLUSTER_IDENTIFIER, dbCluster, client)) {
            cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
                             DB_CLUSTER_IDENTIFIER, "", client);
            return false;
        }

        if ((counter % 20) == 0) {
            std::cout << "Current DB cluster status is '"
                      << dbCluster.GetStatus()
                      << "' after " << counter << " seconds." << std::endl;
        }
    } while (dbCluster.GetStatus() != "available");

    if (dbCluster.GetStatus() == "available") {
        std::cout << "The DB cluster has been created." << std::endl;
    }

    printAsterisksLine();
    Aws::RDS::Model::DBInstance dbInstance;
    // 11.  Check if the DB instance already exists.
    if (!describeDBInstance(DB_INSTANCE_IDENTIFIER, dbInstance, client)) {
        cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, DB_CLUSTER_IDENTIFIER, "",
                         client);
        return false;
    }

    if (dbInstance.DbInstancePortHasBeenSet()) {
        std::cout << "The DB instance already exists." << std::endl;
```

```
    }
    else {
        std::cout << "Let's create a DB instance." << std::endl;

        Aws::String dbInstanceClass;
        // 12.  Get a list of instance classes.
        if (!chooseDBInstanceClass(engineName,
                                   engineVersionName,
                                   dbInstanceClass,
                                   client)) {
            cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, DB_CLUSTER_IDENTIFIER,
 "",
                             client);
            return false;
        }

        std::cout << "Creating a DB instance named '" << DB_INSTANCE_IDENTIFIER
                  << "' with selected DB instance class '" << dbInstanceClass
                  << "'.\nThis typically takes several minutes." << std::endl;

        // 13. Create a DB instance.
        Aws::RDS::Model::CreateDBInstanceRequest request;
        request.SetDBInstanceIdentifier(DB_INSTANCE_IDENTIFIER);
        request.SetDBClusterIdentifier(DB_CLUSTER_IDENTIFIER);
        request.SetEngine(engineName);
        request.SetDBInstanceClass(dbInstanceClass);

        Aws::RDS::Model::CreateDBInstanceOutcome outcome =
                client.CreateDBInstance(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB instance creation has started."
                      << std::endl;
        }
        else {
            std::cerr << "Error with RDS::CreateDBInstance. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME, DB_CLUSTER_IDENTIFIER,
 "",
                             client);
            return false;
        }
    }
```

```
   std::cout << "Waiting for the DB instance to become available." << std::endl;

   counter = 0;
   // 14. Wait for the DB instance to become available.
   do {
       std::this_thread::sleep_for(std::chrono::seconds(1));
       ++counter;
       if (counter > 900) {
           std::cerr << "Wait for instance to become available timed out ofter "
                     << counter
                     << " seconds." << std::endl;
           cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
                            DB_CLUSTER_IDENTIFIER, DB_INSTANCE_IDENTIFIER,
client);
           return false;
       }

       dbInstance = Aws::RDS::Model::DBInstance();
       if (!describeDBInstance(DB_INSTANCE_IDENTIFIER, dbInstance, client)) {
           cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
                            DB_CLUSTER_IDENTIFIER, DB_INSTANCE_IDENTIFIER,
client);
           return false;
       }

       if ((counter % 20) == 0) {
           std::cout << "Current DB instance status is '"
                     << dbInstance.GetDBInstanceStatus()
                     << "' after " << counter << " seconds." << std::endl;
       }
   } while (dbInstance.GetDBInstanceStatus() != "available");

   if (dbInstance.GetDBInstanceStatus() == "available") {
       std::cout << "The DB instance has been created." << std::endl;
   }

   // 15. Display the connection string that can be used to connect a 'mysql'
shell to the database.
   displayConnection(dbCluster);

   printAsterisksLine();

   if (askYesNoQuestion(
```

```
            "Do you want to create a snapshot of your DB cluster (y/n)? ")) {
        Aws::String snapshotID(DB_CLUSTER_IDENTIFIER + "-" +
                               Aws::String(Aws::Utils::UUID::RandomUUID()));
        {
            std::cout << "Creating a snapshot named " << snapshotID << "." <<
std::endl;
            std::cout << "This typically takes a few minutes." << std::endl;

            // 16. Create a snapshot of the DB cluster. (CreateDBClusterSnapshot)
            Aws::RDS::Model::CreateDBClusterSnapshotRequest request;
            request.SetDBClusterIdentifier(DB_CLUSTER_IDENTIFIER);
            request.SetDBClusterSnapshotIdentifier(snapshotID);

            Aws::RDS::Model::CreateDBClusterSnapshotOutcome outcome =
                    client.CreateDBClusterSnapshot(request);

            if (outcome.IsSuccess()) {
                std::cout << "Snapshot creation has started."
                          << std::endl;
            }
            else {
                std::cerr << "Error with Aurora::CreateDBClusterSnapshot. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
                                 DB_CLUSTER_IDENTIFIER, DB_INSTANCE_IDENTIFIER,
client);
                return false;
            }
        }

        std::cout << "Waiting for the snapshot to become available." <<
std::endl;

        Aws::RDS::Model::DBClusterSnapshot snapshot;
        counter = 0;
        do {
            std::this_thread::sleep_for(std::chrono::seconds(1));
            ++counter;
            if (counter > 600) {
                std::cerr << "Wait for snapshot to be available timed out ofter "
                          << counter
                          << " seconds." << std::endl;
                cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
```

```
                                DB_CLUSTER_IDENTIFIER, DB_INSTANCE_IDENTIFIER,
client);
                return false;
            }

            // 17. Wait for the snapshot to become available.
            Aws::RDS::Model::DescribeDBClusterSnapshotsRequest request;
            request.SetDBClusterSnapshotIdentifier(snapshotID);

            Aws::RDS::Model::DescribeDBClusterSnapshotsOutcome outcome =
                    client.DescribeDBClusterSnapshots(request);

            if (outcome.IsSuccess()) {
                snapshot = outcome.GetResult().GetDBClusterSnapshots()[0];
            }
            else {
                std::cerr << "Error with Aurora::DescribeDBClusterSnapshots. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
                                DB_CLUSTER_IDENTIFIER, DB_INSTANCE_IDENTIFIER,
client);
                return false;
            }

            if ((counter % 20) == 0) {
                std::cout << "Current snapshot status is '"
                          << snapshot.GetStatus()
                          << "' after " << counter << " seconds." << std::endl;
            }
        } while (snapshot.GetStatus() != "available");

        if (snapshot.GetStatus() != "available") {
            std::cout << "A snapshot has been created." << std::endl;
        }
    }

    printAsterisksLine();

    bool result = true;
    if (askYesNoQuestion(
            "Do you want to delete the DB cluster, DB instance, and parameter
group (y/n)? ")) {
        result = cleanUpResources(CLUSTER_PARAMETER_GROUP_NAME,
```

```
                                    DB_CLUSTER_IDENTIFIER, DB_INSTANCE_IDENTIFIER,
                                    client);
    }

    return result;
}

//! Routine which gets a DB cluster description.
/*!
 \sa describeDBCluster()
 \param dbClusterIdentifier: A DB cluster identifier.
 \param clusterResult: The 'DBCluster' object containing the description.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::describeDBCluster(const Aws::String &dbClusterIdentifier,
                                       Aws::RDS::Model::DBCluster &clusterResult,
                                       const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBClustersRequest request;
    request.SetDBClusterIdentifier(dbClusterIdentifier);

    Aws::RDS::Model::DescribeDBClustersOutcome outcome =
            client.DescribeDBClusters(request);

    bool result = true;
    if (outcome.IsSuccess()) {
        clusterResult = outcome.GetResult().GetDBClusters()[0];
    }
    else if (outcome.GetError().GetErrorType() !=
             Aws::RDS::RDSErrors::D_B_CLUSTER_NOT_FOUND_FAULT) {
        result = false;
        std::cerr << "Error with Aurora::GDescribeDBClusters. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
        // This example does not log an error if the DB cluster does not exist.
        // Instead, clusterResult is set to empty.
    else {
        clusterResult = Aws::RDS::Model::DBCluster();
    }

    return result;

}
```

```
//! Routine which gets DB parameters using the 'DescribeDBClusterParameters' api.
/*!
 \sa getDBCLusterParameters()
 \param parameterGroupName: The name of the cluster parameter group.
 \param namePrefix: Prefix string to filter results by parameter name.
 \param source: A source such as 'user', ignored if empty.
 \param parametersResult: Vector of 'Parameter' objects returned by the routine.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::getDBCLusterParameters(const Aws::String
 &parameterGroupName,
                                             const Aws::String &namePrefix,
                                             const Aws::String &source,

 Aws::Vector<Aws::RDS::Model::Parameter> &parametersResult,
                                             const Aws::RDS::RDSClient &client) {
    Aws::String marker; // The marker is used for pagination.
    do {
        Aws::RDS::Model::DescribeDBClusterParametersRequest request;
        request.SetDBClusterParameterGroupName(CLUSTER_PARAMETER_GROUP_NAME);
        if (!marker.empty()) {
            request.SetMarker(marker);
        }
        if (!source.empty()) {
            request.SetSource(source);
        }

        Aws::RDS::Model::DescribeDBClusterParametersOutcome outcome =
                client.DescribeDBClusterParameters(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::Parameter> &parameters =
                    outcome.GetResult().GetParameters();
            for (const Aws::RDS::Model::Parameter &parameter: parameters) {
                if (!namePrefix.empty()) {
                    if (parameter.GetParameterName().find(namePrefix) == 0) {
                        parametersResult.push_back(parameter);
                    }
                }
                else {
                    parametersResult.push_back(parameter);
```

```
                }
            }

            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with Aurora::DescribeDBClusterParameters. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!marker.empty());

    return true;
}


//! Routine which gets available DB engine versions for an engine name and
//! an optional parameter group family.
/*!
 \sa getDBEngineVersions()
 \param engineName: A DB engine name.
 \param parameterGroupFamily: A parameter group family name, ignored if empty.
 \param engineVersionsResult: Vector of 'DBEngineVersion' objects returned by the
 routine.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::getDBEngineVersions(const Aws::String &engineName,
                                         const Aws::String &parameterGroupFamily,

 Aws::Vector<Aws::RDS::Model::DBEngineVersion> &engineVersionsResult,
                                         const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBEngineVersionsRequest request;
    request.SetEngine(engineName);
    if (!parameterGroupFamily.empty()) {
        request.SetDBParameterGroupFamily(parameterGroupFamily);
    }

    engineVersionsResult.clear();
    Aws::String marker; // The marker is used for pagination.
    do {
        if (!marker.empty()) {
            request.SetMarker(marker);
```

```
        }

        Aws::RDS::Model::DescribeDBEngineVersionsOutcome outcome =
                client.DescribeDBEngineVersions(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::DBEngineVersion> &engineVersions =
                    outcome.GetResult().GetDBEngineVersions();

            engineVersionsResult.insert(engineVersionsResult.end(),
                                        engineVersions.begin(),
 engineVersions.end());
            marker  = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with Aurora::DescribeDBEngineVersionsRequest. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
    } while (!marker.empty());

    return true;
}


//! Routine which gets a DB instance description.
/*!
 \sa describeDBCluster()
 \param dbInstanceIdentifier: A DB instance identifier.
 \param instanceResult: The 'DBInstance' object containing the description.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::describeDBInstance(const Aws::String &dbInstanceIdentifier,
                                        Aws::RDS::Model::DBInstance
 &instanceResult,
                                        const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBInstancesRequest request;
    request.SetDBInstanceIdentifier(dbInstanceIdentifier);

    Aws::RDS::Model::DescribeDBInstancesOutcome outcome =
            client.DescribeDBInstances(request);

    bool result = true;
```

```
    if (outcome.IsSuccess()) {
        instanceResult = outcome.GetResult().GetDBInstances()[0];
    }
    else if (outcome.GetError().GetErrorType() !=
             Aws::RDS::RDSErrors::D_B_INSTANCE_NOT_FOUND_FAULT) {
        result = false;
        std::cerr << "Error with Aurora::DescribeDBInstances. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
        // This example does not log an error if the DB instance does not exist.
        // Instead, instanceResult is set to empty.
    else {
        instanceResult = Aws::RDS::Model::DBInstance();
    }

    return result;
}


//! Routine which gets available DB instance classes, displays the list
//! to the user, and returns the user selection.
/*!
 \sa chooseDBInstanceClass()
 \param engineName: The DB engine name.
 \param engineVersion: The DB engine version.
 \param dbInstanceClass: String for DB instance class chosen by the user.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::Aurora::chooseDBInstanceClass(const Aws::String &engine,
                                           const Aws::String &engineVersion,
                                           Aws::String &dbInstanceClass,
                                           const Aws::RDS::RDSClient &client) {
    std::vector<Aws::String> instanceClasses;
    Aws::String marker; // The marker is used for pagination.
    do {
        Aws::RDS::Model::DescribeOrderableDBInstanceOptionsRequest request;
        request.SetEngine(engine);
        request.SetEngineVersion(engineVersion);
        if (!marker.empty()) {
            request.SetMarker(marker);
        }
```

```
        Aws::RDS::Model::DescribeOrderableDBInstanceOptionsOutcome outcome =
                client.DescribeOrderableDBInstanceOptions(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::OrderableDBInstanceOption>
 &options =
                    outcome.GetResult().GetOrderableDBInstanceOptions();
            for (const Aws::RDS::Model::OrderableDBInstanceOption &option:
 options) {
                const Aws::String &instanceClass = option.GetDBInstanceClass();
                if (std::find(instanceClasses.begin(), instanceClasses.end(),
                              instanceClass) == instanceClasses.end()) {
                    instanceClasses.push_back(instanceClass);
                }
            }
            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with Aurora::DescribeOrderableDBInstanceOptions.
 "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!marker.empty());

    std::cout << "The available DB instance classes for your database engine
 are:"
              << std::endl;
    for (int i = 0; i < instanceClasses.size(); ++i) {
        std::cout << "   " << i + 1 << ": " << instanceClasses[i] << std::endl;
    }

    int choice = askQuestionForIntRange(
            "Which DB instance class do you want to use? ",
            1, static_cast<int>(instanceClasses.size()));
    dbInstanceClass = instanceClasses[choice - 1];
    return true;
}

//! Routine which deletes resources created by the scenario.
/*!
\sa cleanUpResources()
\param parameterGroupName: A parameter group name, this may be empty.
```

```
\param dbInstanceIdentifier: A DB instance identifier, this may be empty.
\param client: 'RDSClient' instance.
\return bool: Successful completion.
*/
bool AwsDoc::Aurora::cleanUpResources(const Aws::String &parameterGroupName,
                                      const Aws::String &dbClusterIdentifier,
                                      const Aws::String &dbInstanceIdentifier,
                                      const Aws::RDS::RDSClient &client) {
    bool result = true;
    bool instanceDeleting = false;
    bool clusterDeleting = false;
    if (!dbInstanceIdentifier.empty()) {
        {
            // 18. Delete the DB instance.
            Aws::RDS::Model::DeleteDBInstanceRequest request;
            request.SetDBInstanceIdentifier(dbInstanceIdentifier);
            request.SetSkipFinalSnapshot(true);
            request.SetDeleteAutomatedBackups(true);

            Aws::RDS::Model::DeleteDBInstanceOutcome outcome =
                    client.DeleteDBInstance(request);

            if (outcome.IsSuccess()) {
                std::cout << "DB instance deletion has started."
                          << std::endl;
                instanceDeleting = true;
                std::cout
                        << "Waiting for DB instance to delete before deleting the
 parameter group."
                        << std::endl;
            }
            else {
                std::cerr << "Error with Aurora::DeleteDBInstance. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                result = false;
            }
        }
    }

    if (!dbClusterIdentifier.empty()) {
        {
            // 19. Delete the DB cluster.
            Aws::RDS::Model::DeleteDBClusterRequest request;
```

```
            request.SetDBClusterIdentifier(dbClusterIdentifier);
            request.SetSkipFinalSnapshot(true);

            Aws::RDS::Model::DeleteDBClusterOutcome outcome =
                    client.DeleteDBCluster(request);

            if (outcome.IsSuccess()) {
                std::cout << "DB cluster deletion has started."
                          << std::endl;
                clusterDeleting = true;
                std::cout
                        << "Waiting for DB cluster to delete before deleting the
parameter group."
                        << std::endl;
                std::cout << "This may take a while." << std::endl;
            }
            else {
                std::cerr << "Error with Aurora::DeleteDBCluster. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                result = false;
            }
        }
    }
    int counter = 0;

    while (clusterDeleting || instanceDeleting) {
        // 20. Wait for the DB cluster and instance to be deleted.
        std::this_thread::sleep_for(std::chrono::seconds(1));
        ++counter;
        if (counter > 800) {
            std::cerr << "Wait for instance to delete timed out ofter " <<
counter
                      << " seconds." << std::endl;
            return false;
        }

        Aws::RDS::Model::DBInstance dbInstance = Aws::RDS::Model::DBInstance();
        if (instanceDeleting) {
            if (!describeDBInstance(dbInstanceIdentifier, dbInstance, client)) {
                return false;
            }
            instanceDeleting = dbInstance.DBInstanceIdentifierHasBeenSet();
        }
```

```
        Aws::RDS::Model::DBCluster dbCluster = Aws::RDS::Model::DBCluster();
        if (clusterDeleting) {
            if (!describeDBCluster(dbClusterIdentifier, dbCluster, client)) {
                return false;
            }

            clusterDeleting = dbCluster.DBClusterIdentifierHasBeenSet();
        }

        if ((counter % 20) == 0) {
            if (instanceDeleting) {
                std::cout << "Current DB instance status is '"
                          << dbInstance.GetDBInstanceStatus() << "." <<
std::endl;
            }

            if (clusterDeleting) {
                std::cout << "Current DB cluster status is '"
                          << dbCluster.GetStatus() << "." << std::endl;
            }
        }
    }

    if (!parameterGroupName.empty()) {
        // 21. Delete the DB cluster parameter group.
        Aws::RDS::Model::DeleteDBClusterParameterGroupRequest request;
        request.SetDBClusterParameterGroupName(parameterGroupName);

        Aws::RDS::Model::DeleteDBClusterParameterGroupOutcome outcome =
                client.DeleteDBClusterParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB parameter group was successfully deleted."
                      << std::endl;
        }
        else {
            std::cerr << "Error with Aurora::DeleteDBClusterParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            result = false;
        }
    }
```

```
    return result;
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for C++ -API-Referenz.
  - CreateDBCluster
  - DB-Gruppe erstellt ClusterParameter
  - DB wurde erstellt ClusterSnapshot
  - CreateDBInstance
  - DeleteDBCluster
  - DB-Gruppe gelöscht ClusterParameter
  - DeleteDBInstance
  - Beschriebene ClusterParameter DB-Gruppen
  - BeschriebenDB ClusterParameters
  - BeschriebenB ClusterSnapshots
  - DescribeDBClusters
  - BeschriebenB EngineVersions
  - DescribeDBInstances
  - DescribeOrderableDB InstanceOptions
  - DB-Gruppe ändern ClusterParameter

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung aus.

```
// GetStartedClusters is an interactive example that shows you how to use the AWS
 SDK for Go
// with Amazon Aurora to do the following:
//
// 1. Create a custom DB cluster parameter group and set parameter values.
// 2. Create an Aurora DB cluster that is configured to use the parameter group.
// 3. Create a DB instance in the DB cluster that contains a database.
// 4. Take a snapshot of the DB cluster.
// 5. Delete the DB instance, DB cluster, and parameter group.
type GetStartedClusters struct {
 sdkConfig  aws.Config
 dbClusters actions.DbClusters
 questioner demotools.IQuestioner
 helper     IScenarioHelper
 isTestRun  bool
}

// NewGetStartedClusters constructs a GetStartedClusters instance from a
 configuration.
// It uses the specified config to get an Amazon Relational Database Service
 (Amazon RDS)
// client and create wrappers for the actions used in the scenario.
func NewGetStartedClusters(sdkConfig aws.Config, questioner
 demotools.IQuestioner,
 helper IScenarioHelper) GetStartedClusters {
 auroraClient := rds.NewFromConfig(sdkConfig)
 return GetStartedClusters{
  sdkConfig:  sdkConfig,
  dbClusters: actions.DbClusters{AuroraClient: auroraClient},
  questioner: questioner,
  helper:     helper,
 }
}

// Run runs the interactive scenario.
func (scenario GetStartedClusters) Run(dbEngine string, parameterGroupName
 string,
 clusterName string, dbName string) {
 defer func() {
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
  }
 }()
```

```
 log.Println(strings.Repeat("-", 88))
 log.Println("Welcome to the Amazon Aurora DB Cluster demo.")
 log.Println(strings.Repeat("-", 88))

 parameterGroup := scenario.CreateParameterGroup(dbEngine, parameterGroupName)
 scenario.SetUserParameters(parameterGroupName)
 cluster := scenario.CreateCluster(clusterName, dbEngine, dbName, parameterGroup)
 scenario.helper.Pause(5)
 dbInstance := scenario.CreateInstance(cluster)
 scenario.DisplayConnection(cluster)
 scenario.CreateSnapshot(clusterName)
 scenario.Cleanup(dbInstance, cluster, parameterGroup)

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}

// CreateParameterGroup shows how to get available engine versions for a
 specified
// database engine and create a DB cluster parameter group that is compatible
 with a
// selected engine family.
func (scenario GetStartedClusters) CreateParameterGroup(dbEngine string,
 parameterGroupName string) *types.DBClusterParameterGroup {

 log.Printf("Checking for an existing DB cluster parameter group named %v.\n",
  parameterGroupName)
 parameterGroup, err := scenario.dbClusters.GetParameterGroup(parameterGroupName)
 if err != nil {
  panic(err)
 }
 if parameterGroup == nil {
  log.Printf("Getting available database engine versions for %v.\n", dbEngine)
  engineVersions, err := scenario.dbClusters.GetEngineVersions(dbEngine, "")
  if err != nil {
   panic(err)
  }

  familySet := map[string]struct{}{}
  for _, family := range engineVersions {
   familySet[*family.DBParameterGroupFamily] = struct{}{}
  }
  var families []string
```

```
  for family := range familySet {
   families = append(families, family)
  }
  sort.Strings(families)
  familyIndex := scenario.questioner.AskChoice("Which family do you want to use?
\n", families)
  log.Println("Creating a DB cluster parameter group.")
  _, err = scenario.dbClusters.CreateParameterGroup(
   parameterGroupName, families[familyIndex], "Example parameter group.")
  if err != nil {
   panic(err)
  }
  parameterGroup, err = scenario.dbClusters.GetParameterGroup(parameterGroupName)
  if err != nil {
   panic(err)
  }
 }
 log.Printf("Parameter group %v:\n", *parameterGroup.DBParameterGroupFamily)
 log.Printf("\tName: %v\n", *parameterGroup.DBClusterParameterGroupName)
 log.Printf("\tARN: %v\n", *parameterGroup.DBClusterParameterGroupArn)
 log.Printf("\tFamily: %v\n", *parameterGroup.DBParameterGroupFamily)
 log.Printf("\tDescription: %v\n", *parameterGroup.Description)
 log.Println(strings.Repeat("-", 88))
 return parameterGroup

}

// SetUserParameters shows how to get the parameters contained in a custom
 parameter
// group and update some of the parameter values in the group.
func (scenario GetStartedClusters) SetUserParameters(parameterGroupName string) {
 log.Println("Let's set some parameter values in your parameter group.")
 dbParameters, err := scenario.dbClusters.GetParameters(parameterGroupName, "")
 if err != nil {
  panic(err)
 }
 var updateParams []types.Parameter
 for _, dbParam := range dbParameters {
  if strings.HasPrefix(*dbParam.ParameterName, "auto_increment") &&
   dbParam.IsModifiable && *dbParam.DataType == "integer" {
   log.Printf("The %v parameter is described as:\n\t%v",
    *dbParam.ParameterName, *dbParam.Description)
   rangeSplit := strings.Split(*dbParam.AllowedValues, "-")
   lower, _ := strconv.Atoi(rangeSplit[0])
```

```
   upper, _ := strconv.Atoi(rangeSplit[1])
   newValue := scenario.questioner.AskInt(
    fmt.Sprintf("Enter a value between %v and %v:", lower, upper),
    demotools.InIntRange{Lower: lower, Upper: upper})
   dbParam.ParameterValue = aws.String(strconv.Itoa(newValue))
   updateParams = append(updateParams, dbParam)
  }
 }
 err = scenario.dbClusters.UpdateParameters(parameterGroupName, updateParams)
 if err != nil {
  panic(err)
 }
 log.Println("You can get a list of parameters you've set by specifying a source
 of 'user'.")
 userParameters, err := scenario.dbClusters.GetParameters(parameterGroupName,
 "user")
 if err != nil {
  panic(err)
 }
 log.Println("Here are the parameters you've set:")
 for _, param := range userParameters {
  log.Printf("\t%v: %v\n", *param.ParameterName, *param.ParameterValue)
 }
 log.Println(strings.Repeat("-", 88))
}

// CreateCluster shows how to create an Aurora DB cluster that contains a
 database
// of a specified type. The database is also configured to use a custom DB
 cluster
// parameter group.
func (scenario GetStartedClusters) CreateCluster(clusterName string, dbEngine
 string,
 dbName string, parameterGroup *types.DBClusterParameterGroup) *types.DBCluster {

 log.Println("Checking for an existing DB cluster.")
 cluster, err := scenario.dbClusters.GetDbCluster(clusterName)
 if err != nil {
  panic(err)
 }
 if cluster == nil {
  adminUsername := scenario.questioner.Ask(
   "Enter an administrator user name for the database: ", demotools.NotEmpty{})
  adminPassword := scenario.questioner.Ask(
```

```
    "Enter a password for the administrator (at least 8 characters): ",
  demotools.NotEmpty{})
   engineVersions, err := scenario.dbClusters.GetEngineVersions(dbEngine,
  *parameterGroup.DBParameterGroupFamily)
   if err != nil {
    panic(err)
   }
   var engineChoices []string
   for _, engine := range engineVersions {
    engineChoices = append(engineChoices, *engine.EngineVersion)
   }
   log.Println("The available engines for your parameter group are:")
   engineIndex := scenario.questioner.AskChoice("Which engine do you want to use?
\n", engineChoices)
   log.Printf("Creating DB cluster %v and database %v.\n", clusterName, dbName)
   log.Printf("The DB cluster is configured to use\nyour custom parameter group %v
\n",
    *parameterGroup.DBClusterParameterGroupName)
   log.Printf("and selected engine %v.\n", engineChoices[engineIndex])
   log.Println("This typically takes several minutes.")
   cluster, err = scenario.dbClusters.CreateDbCluster(
    clusterName, *parameterGroup.DBClusterParameterGroupName, dbName, dbEngine,
    engineChoices[engineIndex], adminUsername, adminPassword)
   if err != nil {
    panic(err)
   }
   for *cluster.Status != "available" {
    scenario.helper.Pause(30)
    cluster, err = scenario.dbClusters.GetDbCluster(clusterName)
    if err != nil {
     panic(err)
    }
    log.Println("Cluster created and available.")
   }
  }
  log.Println("Cluster data:")
  log.Printf("\tDBClusterIdentifier: %v\n", *cluster.DBClusterIdentifier)
  log.Printf("\tARN: %v\n", *cluster.DBClusterArn)
  log.Printf("\tStatus: %v\n", *cluster.Status)
  log.Printf("\tEngine: %v\n", *cluster.Engine)
  log.Printf("\tEngine version: %v\n", *cluster.EngineVersion)
  log.Printf("\tDBClusterParameterGroup: %v\n", *cluster.DBClusterParameterGroup)
  log.Printf("\tEngineMode: %v\n", *cluster.EngineMode)
  log.Println(strings.Repeat("-", 88))
```

```
 return cluster
}

// CreateInstance shows how to create a DB instance in an existing Aurora DB
 cluster.
// A new DB cluster contains no DB instances, so you must add one. The first DB
 instance
// that is added to a DB cluster defaults to a read-write DB instance.
func (scenario GetStartedClusters) CreateInstance(cluster *types.DBCluster)
 *types.DBInstance {
 log.Println("Checking for an existing database instance.")
 dbInstance, err := scenario.dbClusters.GetInstance(*cluster.DBClusterIdentifier)
 if err != nil {
  panic(err)
 }
 if dbInstance == nil {
  log.Println("Let's create a database instance in your DB cluster.")
  log.Println("First, choose a DB instance type:")
  instOpts, err := scenario.dbClusters.GetOrderableInstances(
   *cluster.Engine, *cluster.EngineVersion)
  if err != nil {
   panic(err)
  }
  var instChoices []string
  for _, opt := range instOpts {
   instChoices = append(instChoices, *opt.DBInstanceClass)
  }
  instIndex := scenario.questioner.AskChoice(
   "Which DB instance class do you want to use?\n", instChoices)
  log.Println("Creating a database instance. This typically takes several
 minutes.")
  dbInstance, err = scenario.dbClusters.CreateInstanceInCluster(
   *cluster.DBClusterIdentifier, *cluster.DBClusterIdentifier, *cluster.Engine,
   instChoices[instIndex])
  if err != nil {
   panic(err)
  }
  for *dbInstance.DBInstanceStatus != "available" {
   scenario.helper.Pause(30)
   dbInstance, err =
 scenario.dbClusters.GetInstance(*cluster.DBClusterIdentifier)
   if err != nil {
    panic(err)
   }
```

```
  }
 }
 log.Println("Instance data:")
 log.Printf("\tDBInstanceIdentifier: %v\n", *dbInstance.DBInstanceIdentifier)
 log.Printf("\tARN: %v\n", *dbInstance.DBInstanceArn)
 log.Printf("\tStatus: %v\n", *dbInstance.DBInstanceStatus)
 log.Printf("\tEngine: %v\n", *dbInstance.Engine)
 log.Printf("\tEngine version: %v\n", *dbInstance.EngineVersion)
 log.Println(strings.Repeat("-", 88))
 return dbInstance
}

// DisplayConnection displays connection information about an Aurora DB cluster
 and tips
// on how to connect to it.
func (scenario GetStartedClusters) DisplayConnection(cluster *types.DBCluster) {
 log.Println(
  "You can now connect to your database using your favorite MySql client.\n" +
   "One way to connect is by using the 'mysql' shell on an Amazon EC2 instance\n"
 +
   "that is running in the same VPC as your database cluster. Pass the endpoint,
\n" +
   "port, and administrator user name to 'mysql' and enter your password\n" +
   "when prompted:")
 log.Printf("\n\tmysql -h %v -P %v -u %v -p\n",
  *cluster.Endpoint, *cluster.Port, *cluster.MasterUsername)
 log.Println("For more information, see the User Guide for Aurora:\n" +
  "\thttps://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/
CHAP_GettingStartedAurora.CreatingConnecting.Aurora.html#CHAP_GettingStartedAurora.Aurora
 log.Println(strings.Repeat("-", 88))
}

// CreateSnapshot shows how to create a DB cluster snapshot and wait until it's
 available.
func (scenario GetStartedClusters) CreateSnapshot(clusterName string) {
 if scenario.questioner.AskBool(
  "Do you want to create a snapshot of your DB cluster (y/n)? ", "y") {
  snapshotId := fmt.Sprintf("%v-%v", clusterName, scenario.helper.UniqueId())
  log.Printf("Creating a snapshot named %v. This typically takes a few minutes.
\n", snapshotId)
  snapshot, err := scenario.dbClusters.CreateClusterSnapshot(clusterName,
 snapshotId)
  if err != nil {
   panic(err)
```

```
  }
  for *snapshot.Status != "available" {
   scenario.helper.Pause(30)
   snapshot, err = scenario.dbClusters.GetClusterSnapshot(snapshotId)
   if err != nil {
    panic(err)
   }
  }
  log.Println("Snapshot data:")
  log.Printf("\tDBClusterSnapshotIdentifier: %v\n",
 *snapshot.DBClusterSnapshotIdentifier)
  log.Printf("\tARN: %v\n", *snapshot.DBClusterSnapshotArn)
  log.Printf("\tStatus: %v\n", *snapshot.Status)
  log.Printf("\tEngine: %v\n", *snapshot.Engine)
  log.Printf("\tEngine version: %v\n", *snapshot.EngineVersion)
  log.Printf("\tDBClusterIdentifier: %v\n", *snapshot.DBClusterIdentifier)
  log.Printf("\tSnapshotCreateTime: %v\n", *snapshot.SnapshotCreateTime)
  log.Println(strings.Repeat("-", 88))
 }
}

// Cleanup shows how to clean up a DB instance, DB cluster, and DB cluster
 parameter group.
// Before the DB cluster parameter group can be deleted, all associated DB
 instances and
// DB clusters must first be deleted.
func (scenario GetStartedClusters) Cleanup(dbInstance *types.DBInstance, cluster
 *types.DBCluster,
 parameterGroup *types.DBClusterParameterGroup) {

 if scenario.questioner.AskBool(
  "\nDo you want to delete the database instance, DB cluster, and parameter group
 (y/n)? ", "y") {
  log.Printf("Deleting database instance %v.\n",
 *dbInstance.DBInstanceIdentifier)
  err := scenario.dbClusters.DeleteInstance(*dbInstance.DBInstanceIdentifier)
  if err != nil {
   panic(err)
  }
  log.Printf("Deleting database cluster %v.\n", *cluster.DBClusterIdentifier)
  err = scenario.dbClusters.DeleteDbCluster(*cluster.DBClusterIdentifier)
  if err != nil {
   panic(err)
  }
```

```
  log.Println(
   "Waiting for the DB instance and DB cluster to delete. This typically takes
 several minutes.")
  for dbInstance != nil || cluster != nil {
   scenario.helper.Pause(30)
   if dbInstance != nil {
    dbInstance, err =
 scenario.dbClusters.GetInstance(*dbInstance.DBInstanceIdentifier)
    if err != nil {
     panic(err)
    }
   }
   if cluster != nil {
    cluster, err = scenario.dbClusters.GetDbCluster(*cluster.DBClusterIdentifier)
    if err != nil {
     panic(err)
    }
   }
  }
  log.Printf("Deleting parameter group %v.",
 *parameterGroup.DBClusterParameterGroupName)
  err =
 scenario.dbClusters.DeleteParameterGroup(*parameterGroup.DBClusterParameterGroupName)
  if err != nil {
   panic(err)
  }
 }
}
```

Definieren Sie Funktionen, die vom Szenario aufgerufen werden, um Aurora-Aktionen zu verwalten.

```
type DbClusters struct {
 AuroraClient *rds.Client
}


// GetParameterGroup gets a DB cluster parameter group by name.
func (clusters *DbClusters) GetParameterGroup(parameterGroupName string) (
 *types.DBClusterParameterGroup, error) {
```

```
 output, err := clusters.AuroraClient.DescribeDBClusterParameterGroups(
  context.TODO(), &rds.DescribeDBClusterParameterGroupsInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
  })
 if err != nil {
  var notFoundError *types.DBParameterGroupNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("Parameter group %v does not exist.\n", parameterGroupName)
   err = nil
  } else {
   log.Printf("Error getting parameter group %v: %v\n", parameterGroupName, err)
  }
  return nil, err
 } else {
  return &output.DBClusterParameterGroups[0], err
 }
}


// CreateParameterGroup creates a DB cluster parameter group that is based on the
 specified
// parameter group family.
func (clusters *DbClusters) CreateParameterGroup(
 parameterGroupName string, parameterGroupFamily string, description string) (
 *types.DBClusterParameterGroup, error) {

 output, err :=
 clusters.AuroraClient.CreateDBClusterParameterGroup(context.TODO(),
  &rds.CreateDBClusterParameterGroupInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
   DBParameterGroupFamily:      aws.String(parameterGroupFamily),
   Description:                 aws.String(description),
  })
 if err != nil {
  log.Printf("Couldn't create parameter group %v: %v\n", parameterGroupName, err)
  return nil, err
 } else {
  return output.DBClusterParameterGroup, err
 }
}



// DeleteParameterGroup deletes the named DB cluster parameter group.
```

```
func (clusters *DbClusters) DeleteParameterGroup(parameterGroupName string) error
 {
 _, err := clusters.AuroraClient.DeleteDBClusterParameterGroup(context.TODO(),
  &rds.DeleteDBClusterParameterGroupInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
  })
 if err != nil {
  log.Printf("Couldn't delete parameter group %v: %v\n", parameterGroupName, err)
  return err
 } else {
  return nil
 }
}



// GetParameters gets the parameters that are contained in a DB cluster parameter
 group.
func (clusters *DbClusters) GetParameters(parameterGroupName string, source
 string) (
 []types.Parameter, error) {

 var output *rds.DescribeDBClusterParametersOutput
 var params []types.Parameter
 var err error
 parameterPaginator :=
 rds.NewDescribeDBClusterParametersPaginator(clusters.AuroraClient,
  &rds.DescribeDBClusterParametersInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
   Source:                      aws.String(source),
  })
 for parameterPaginator.HasMorePages() {
  output, err = parameterPaginator.NextPage(context.TODO())
  if err != nil {
   log.Printf("Couldn't get paramaeters for %v: %v\n", parameterGroupName, err)
   break
  } else {
   params = append(params, output.Parameters...)
  }
 }
 return params, err
}
```

```
// UpdateParameters updates parameters in a named DB cluster parameter group.
func (clusters *DbClusters) UpdateParameters(parameterGroupName string, params
 []types.Parameter) error {
 _, err := clusters.AuroraClient.ModifyDBClusterParameterGroup(context.TODO(),
  &rds.ModifyDBClusterParameterGroupInput{
   DBClusterParameterGroupName: aws.String(parameterGroupName),
   Parameters:                  params,
  })
 if err != nil {
  log.Printf("Couldn't update parameters in %v: %v\n", parameterGroupName, err)
  return err
 } else {
  return nil
 }
}



// GetDbCluster gets data about an Aurora DB cluster.
func (clusters *DbClusters) GetDbCluster(clusterName string) (*types.DBCluster,
 error) {
 output, err := clusters.AuroraClient.DescribeDBClusters(context.TODO(),
  &rds.DescribeDBClustersInput{
   DBClusterIdentifier: aws.String(clusterName),
  })
 if err != nil {
  var notFoundError *types.DBClusterNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("DB cluster %v does not exist.\n", clusterName)
   err = nil
  } else {
   log.Printf("Couldn't get DB cluster %v: %v\n", clusterName, err)
  }
  return nil, err
 } else {
  return &output.DBClusters[0], err
 }
}



// CreateDbCluster creates a DB cluster that is configured to use the specified
 parameter group.
```

```
// The newly created DB cluster contains a database that uses the specified
 engine and
// engine version.
func (clusters *DbClusters) CreateDbCluster(clusterName string,
 parameterGroupName string,
 dbName string, dbEngine string, dbEngineVersion string, adminName string,
 adminPassword string) (
 *types.DBCluster, error) {

 output, err := clusters.AuroraClient.CreateDBCluster(context.TODO(),
 &rds.CreateDBClusterInput{
  DBClusterIdentifier:         aws.String(clusterName),
  Engine:                      aws.String(dbEngine),
  DBClusterParameterGroupName: aws.String(parameterGroupName),
  DatabaseName:                aws.String(dbName),
  EngineVersion:               aws.String(dbEngineVersion),
  MasterUserPassword:          aws.String(adminPassword),
  MasterUsername:              aws.String(adminName),
 })
 if err != nil {
  log.Printf("Couldn't create DB cluster %v: %v\n", clusterName, err)
  return nil, err
 } else {
  return output.DBCluster, err
 }
}



// DeleteDbCluster deletes a DB cluster without keeping a final snapshot.
func (clusters *DbClusters) DeleteDbCluster(clusterName string) error {
 _, err := clusters.AuroraClient.DeleteDBCluster(context.TODO(),
 &rds.DeleteDBClusterInput{
  DBClusterIdentifier: aws.String(clusterName),
  SkipFinalSnapshot:   true,
 })
 if err != nil {
  log.Printf("Couldn't delete DB cluster %v: %v\n", clusterName, err)
  return err
 } else {
  return nil
 }
}
```

```
// CreateClusterSnapshot creates a snapshot of a DB cluster.
func (clusters *DbClusters) CreateClusterSnapshot(clusterName string,
 snapshotName string) (
 *types.DBClusterSnapshot, error) {
 output, err := clusters.AuroraClient.CreateDBClusterSnapshot(context.TODO(),
 &rds.CreateDBClusterSnapshotInput{
  DBClusterIdentifier:         aws.String(clusterName),
  DBClusterSnapshotIdentifier: aws.String(snapshotName),
 })
 if err != nil {
  log.Printf("Couldn't create snapshot %v: %v\n", snapshotName, err)
  return nil, err
 } else {
  return output.DBClusterSnapshot, nil
 }
}



// GetClusterSnapshot gets a DB cluster snapshot.
func (clusters *DbClusters) GetClusterSnapshot(snapshotName string)
 (*types.DBClusterSnapshot, error) {
 output, err := clusters.AuroraClient.DescribeDBClusterSnapshots(context.TODO(),
  &rds.DescribeDBClusterSnapshotsInput{
   DBClusterSnapshotIdentifier: aws.String(snapshotName),
  })
 if err != nil {
  log.Printf("Couldn't get snapshot %v: %v\n", snapshotName, err)
  return nil, err
 } else {
  return &output.DBClusterSnapshots[0], nil
 }
}



// CreateInstanceInCluster creates a database instance in an existing DB cluster.
 The first database that is
// created defaults to a read-write DB instance.
func (clusters *DbClusters) CreateInstanceInCluster(clusterName string,
 instanceName string,
 dbEngine string, dbInstanceClass string) (*types.DBInstance, error) {
```

```
 output, err := clusters.AuroraClient.CreateDBInstance(context.TODO(),
 &rds.CreateDBInstanceInput{
  DBInstanceIdentifier: aws.String(instanceName),
  DBClusterIdentifier:  aws.String(clusterName),
  Engine:               aws.String(dbEngine),
  DBInstanceClass:      aws.String(dbInstanceClass),
 })
 if err != nil {
  log.Printf("Couldn't create instance %v: %v\n", instanceName, err)
  return nil, err
 } else {
  return output.DBInstance, nil
 }
}



// GetInstance gets data about a DB instance.
func (clusters *DbClusters) GetInstance(instanceName string) (
 *types.DBInstance, error) {
 output, err := clusters.AuroraClient.DescribeDBInstances(context.TODO(),
  &rds.DescribeDBInstancesInput{
   DBInstanceIdentifier: aws.String(instanceName),
  })
 if err != nil {
  var notFoundError *types.DBInstanceNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("DB instance %v does not exist.\n", instanceName)
   err = nil
  } else {
   log.Printf("Couldn't get instance %v: %v\n", instanceName, err)
  }
  return nil, err
 } else {
  return &output.DBInstances[0], nil
 }
}



// DeleteInstance deletes a DB instance.
func (clusters *DbClusters) DeleteInstance(instanceName string) error {
 _, err := clusters.AuroraClient.DeleteDBInstance(context.TODO(),
 &rds.DeleteDBInstanceInput{
```

```
  DBInstanceIdentifier:   aws.String(instanceName),
  SkipFinalSnapshot:      true,
  DeleteAutomatedBackups: aws.Bool(true),
 })
 if err != nil {
  log.Printf("Couldn't delete instance %v: %v\n", instanceName, err)
  return err
 } else {
  return nil
 }
}



// GetEngineVersions gets database engine versions that are available for the
 specified engine
// and parameter group family.
func (clusters *DbClusters) GetEngineVersions(engine string, parameterGroupFamily
 string) (
 []types.DBEngineVersion, error) {
 output, err := clusters.AuroraClient.DescribeDBEngineVersions(context.TODO(),
  &rds.DescribeDBEngineVersionsInput{
   Engine:                 aws.String(engine),
   DBParameterGroupFamily: aws.String(parameterGroupFamily),
  })
 if err != nil {
  log.Printf("Couldn't get engine versions for %v: %v\n", engine, err)
  return nil, err
 } else {
  return output.DBEngineVersions, nil
 }
}



// GetOrderableInstances uses a paginator to get DB instance options that can be
 used to create DB instances that are
// compatible with a set of specifications.
func (clusters *DbClusters) GetOrderableInstances(engine string, engineVersion
 string) (
 []types.OrderableDBInstanceOption, error) {

 var output *rds.DescribeOrderableDBInstanceOptionsOutput
 var instances []types.OrderableDBInstanceOption
```

```
 var err error
 orderablePaginator :=
 rds.NewDescribeOrderableDBInstanceOptionsPaginator(clusters.AuroraClient,
  &rds.DescribeOrderableDBInstanceOptionsInput{
   Engine:        aws.String(engine),
   EngineVersion: aws.String(engineVersion),
  })
 for orderablePaginator.HasMorePages() {
  output, err = orderablePaginator.NextPage(context.TODO())
  if err != nil {
   log.Printf("Couldn't get orderable DB instances: %v\n", err)
   break
  } else {
   instances = append(instances, output.OrderableDBInstanceOptions...)
  }
 }
 return instances, err
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Go -API-Referenz.
  - CreateDBCluster
  - DB-Gruppe erstellt ClusterParameter
  - DB wurde erstellt ClusterSnapshot
  - CreateDBInstance
  - DeleteDBCluster
  - DB-Gruppe gelöscht ClusterParameter
  - DeleteDBInstance
  - Beschriebene ClusterParameter DB-Gruppen
  - BeschriebenDB ClusterParameters
  - BeschriebenB ClusterSnapshots
  - DescribeDBClusters
  - BeschriebenB EngineVersions
  - DescribeDBInstances
  - DescribeOrderableDB InstanceOptions
  - DB-Gruppe ändern ClusterParameter

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example requires an AWS Secrets Manager secret that contains the
 * database credentials. If you do not create a
 * secret, this example will not work. For details, see:
 *
 * https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_how-
services-use-secrets_RS.html
 *
 * This Java example performs the following tasks:
 *
 * 1. Gets available engine families for Amazon Aurora MySQL-Compatible Edition
 * by calling the DescribeDbEngineVersions(Engine='aurora-mysql') method.
 * 2. Selects an engine family and creates a custom DB cluster parameter group
 * by invoking the describeDBClusterParameters method.
 * 3. Gets the parameter groups by invoking the describeDBClusterParameterGroups
 * method.
 * 4. Gets parameters in the group by invoking the describeDBClusterParameters
 * method.
 * 5. Modifies the auto_increment_offset parameter by invoking the
 * modifyDbClusterParameterGroupRequest method.
 * 6. Gets and displays the updated parameters.
 * 7. Gets a list of allowed engine versions by invoking the
 * describeDbEngineVersions method.
 * 8. Creates an Aurora DB cluster database cluster that contains a MySQL
```

```
 * database.
 * 9. Waits for DB instance to be ready.
 * 10. Gets a list of instance classes available for the selected engine.
 * 11. Creates a database instance in the cluster.
 * 12. Waits for DB instance to be ready.
 * 13. Creates a snapshot.
 * 14. Waits for DB snapshot to be ready.
 * 15. Deletes the DB cluster.
 * 16. Deletes the DB cluster group.
 */
public class AuroraScenario {
    public static long sleepTime = 20;
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) throws InterruptedException {
        final String usage = "\n" +
                "Usage:\n" +
                "    <dbClusterGroupName> <dbParameterGroupFamily>
 <dbInstanceClusterIdentifier> <dbInstanceIdentifier> <dbName>
 <dbSnapshotIdentifier><secretName>"
                +
                "Where:\n" +
                "    dbClusterGroupName - The name of the DB cluster parameter
 group. \n" +
                "    dbParameterGroupFamily - The DB cluster parameter group
 family name (for example, aurora-mysql5.7). \n"
                +
                "    dbInstanceClusterIdentifier - The instance cluster
 identifier value.\n" +
                "    dbInstanceIdentifier - The database instance identifier.\n"
 +
                "    dbName - The database name.\n" +
                "    dbSnapshotIdentifier - The snapshot identifier.\n" +
                "    secretName - The name of the AWS Secrets Manager secret that
 contains the database credentials\"\n";
        ;

        if (args.length != 7) {
            System.out.println(usage);
            System.exit(1);
        }

        String dbClusterGroupName = args[0];
```

```
        String dbParameterGroupFamily = args[1];
        String dbInstanceClusterIdentifier = args[2];
        String dbInstanceIdentifier = args[3];
        String dbName = args[4];
        String dbSnapshotIdentifier = args[5];
        String secretName = args[6];

        // Retrieve the database credentials using AWS Secrets Manager.
        Gson gson = new Gson();
        User user = gson.fromJson(String.valueOf(getSecretValues(secretName)),
User.class);
        String username = user.getUsername();
        String userPassword = user.getPassword();

        Region region = Region.US_WEST_2;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Welcome to the Amazon Aurora example scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. Return a list of the available DB engines");
        describeDBEngines(rdsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Create a custom parameter group");
        createDBClusterParameterGroup(rdsClient, dbClusterGroupName,
dbParameterGroupFamily);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Get the parameter group");
        describeDbClusterParameterGroups(rdsClient, dbClusterGroupName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get the parameters in the group");
        describeDbClusterParameters(rdsClient, dbClusterGroupName, 0);
        System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("5. Modify the auto_increment_offset parameter");
        modifyDBClusterParas(rdsClient, dbClusterGroupName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Display the updated parameter value");
        describeDbClusterParameters(rdsClient, dbClusterGroupName, -1);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Get a list of allowed engine versions");
        getAllowedEngines(rdsClient, dbParameterGroupFamily);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Create an Aurora DB cluster database");
        String arnClusterVal = createDBCluster(rdsClient, dbClusterGroupName,
dbName, dbInstanceClusterIdentifier,
                username, userPassword);
        System.out.println("The ARN of the cluster is " + arnClusterVal);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Wait for DB instance to be ready");
        waitForInstanceReady(rdsClient, dbInstanceClusterIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of instance classes available for the
selected engine");
        String instanceClass = getListInstanceClasses(rdsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("11. Create a database instance in the cluster.");
        String clusterDBARN = createDBInstanceCluster(rdsClient,
dbInstanceIdentifier, dbInstanceClusterIdentifier,
                instanceClass);
        System.out.println("The ARN of the database is " + clusterDBARN);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("12. Wait for DB instance to be ready");
```

```
        waitDBInstanceReady(rdsClient, dbInstanceIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("13. Create a snapshot");
        createDBClusterSnapshot(rdsClient, dbInstanceClusterIdentifier,
dbSnapshotIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("14. Wait for DB snapshot to be ready");
        waitForSnapshotReady(rdsClient, dbSnapshotIdentifier,
dbInstanceClusterIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("14. Delete the DB instance");
        deleteDatabaseInstance(rdsClient, dbInstanceIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("15. Delete the DB cluster");
        deleteCluster(rdsClient, dbInstanceClusterIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("16. Delete the DB cluster group");
        deleteDBClusterGroup(rdsClient, dbClusterGroupName, clusterDBARN);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("The Scenario has successfully completed.");
        System.out.println(DASHES);
        rdsClient.close();
    }

    private static SecretsManagerClient getSecretClient() {
        Region region = Region.US_WEST_2;
        return SecretsManagerClient.builder()
                .region(region)

.credentialsProvider(EnvironmentVariableCredentialsProvider.create())
                .build();
    }
```

```
   private static String getSecretValues(String secretName) {
       SecretsManagerClient secretClient = getSecretClient();
       GetSecretValueRequest valueRequest = GetSecretValueRequest.builder()
               .secretId(secretName)
               .build();

       GetSecretValueResponse valueResponse =
secretClient.getSecretValue(valueRequest);
       return valueResponse.secretString();
   }

   public static void deleteDBClusterGroup(RdsClient rdsClient, String
dbClusterGroupName, String clusterDBARN)
           throws InterruptedException {
       try {
           boolean isDataDel = false;
           boolean didFind;
           String instanceARN;

           // Make sure that the database has been deleted.
           while (!isDataDel) {
               DescribeDbInstancesResponse response =
rdsClient.describeDBInstances();
               List<DBInstance> instanceList = response.dbInstances();
               int listSize = instanceList.size();
               didFind = false;
               int index = 1;
               for (DBInstance instance : instanceList) {
                   instanceARN = instance.dbInstanceArn();
                   if (instanceARN.compareTo(clusterDBARN) == 0) {
                       System.out.println(clusterDBARN + " still exists");
                       didFind = true;
                   }
                   if ((index == listSize) && (!didFind)) {
                       // Went through the entire list and did not find the
database ARN.
                       isDataDel = true;
                   }
                   Thread.sleep(sleepTime * 1000);
                   index++;
               }
           }
```

```
            DeleteDbClusterParameterGroupRequest clusterParameterGroupRequest =
DeleteDbClusterParameterGroupRequest
                    .builder()
                    .dbClusterParameterGroupName(dbClusterGroupName)
                    .build();


rdsClient.deleteDBClusterParameterGroup(clusterParameterGroupRequest);
            System.out.println(dbClusterGroupName + " was deleted.");

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void deleteCluster(RdsClient rdsClient, String
dbInstanceClusterIdentifier) {
        try {
            DeleteDbClusterRequest deleteDbClusterRequest =
DeleteDbClusterRequest.builder()
                    .dbClusterIdentifier(dbInstanceClusterIdentifier)
                    .skipFinalSnapshot(true)
                    .build();

            rdsClient.deleteDBCluster(deleteDbClusterRequest);
            System.out.println(dbInstanceClusterIdentifier + " was deleted!");

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void deleteDatabaseInstance(RdsClient rdsClient, String
dbInstanceIdentifier) {
        try {
            DeleteDbInstanceRequest deleteDbInstanceRequest =
DeleteDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .deleteAutomatedBackups(true)
                    .skipFinalSnapshot(true)
                    .build();
```

```
            DeleteDbInstanceResponse response =
rdsClient.deleteDBInstance(deleteDbInstanceRequest);
            System.out.println("The status of the database is " +
response.dbInstance().dbInstanceStatus());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void waitForSnapshotReady(RdsClient rdsClient, String
dbSnapshotIdentifier,
            String dbInstanceClusterIdentifier) {
        try {
            boolean snapshotReady = false;
            String snapshotReadyStr;
            System.out.println("Waiting for the snapshot to become available.");

            DescribeDbClusterSnapshotsRequest snapshotsRequest =
DescribeDbClusterSnapshotsRequest.builder()
                    .dbClusterSnapshotIdentifier(dbSnapshotIdentifier)
                    .dbClusterIdentifier(dbInstanceClusterIdentifier)
                    .build();

            while (!snapshotReady) {
                DescribeDbClusterSnapshotsResponse response =
rdsClient.describeDBClusterSnapshots(snapshotsRequest);
                List<DBClusterSnapshot> snapshotList =
response.dbClusterSnapshots();
                for (DBClusterSnapshot snapshot : snapshotList) {
                    snapshotReadyStr = snapshot.status();
                    if (snapshotReadyStr.contains("available")) {
                        snapshotReady = true;
                    } else {
                        System.out.println(".");
                        Thread.sleep(sleepTime * 5000);
                    }
                }
            }

            System.out.println("The Snapshot is available!");

        } catch (RdsException | InterruptedException e) {
```

```
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void createDBClusterSnapshot(RdsClient rdsClient, String
dbInstanceClusterIdentifier,
            String dbSnapshotIdentifier) {
        try {
            CreateDbClusterSnapshotRequest snapshotRequest =
CreateDbClusterSnapshotRequest.builder()
                    .dbClusterIdentifier(dbInstanceClusterIdentifier)
                    .dbClusterSnapshotIdentifier(dbSnapshotIdentifier)
                    .build();

            CreateDbClusterSnapshotResponse response =
rdsClient.createDBClusterSnapshot(snapshotRequest);
            System.out.println("The Snapshot ARN is " +
response.dbClusterSnapshot().dbClusterSnapshotArn());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void waitDBInstanceReady(RdsClient rdsClient, String
dbInstanceIdentifier) {
        boolean instanceReady = false;
        String instanceReadyStr;
        System.out.println("Waiting for instance to become available.");
        try {
            DescribeDbInstancesRequest instanceRequest =
DescribeDbInstancesRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .build();

            String endpoint = "";
            while (!instanceReady) {
                DescribeDbInstancesResponse response =
rdsClient.describeDBInstances(instanceRequest);
                List<DBInstance> instanceList = response.dbInstances();
                for (DBInstance instance : instanceList) {
                    instanceReadyStr = instance.dbInstanceStatus();
```

```
                    if (instanceReadyStr.contains("available")) {
                        endpoint = instance.endpoint().address();
                        instanceReady = true;
                    } else {
                        System.out.print(".");
                        Thread.sleep(sleepTime * 1000);
                    }
                }
            }
            System.out.println("Database instance is available! The connection
endpoint is " + endpoint);

        } catch (RdsException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static String createDBInstanceCluster(RdsClient rdsClient,
            String dbInstanceIdentifier,
            String dbInstanceClusterIdentifier,
            String instanceClass) {
        try {
            CreateDbInstanceRequest instanceRequest =
CreateDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .dbClusterIdentifier(dbInstanceClusterIdentifier)
                    .engine("aurora-mysql")
                    .dbInstanceClass(instanceClass)
                    .build();

            CreateDbInstanceResponse response =
rdsClient.createDBInstance(instanceRequest);
            System.out.print("The status is " +
response.dbInstance().dbInstanceStatus());
            return response.dbInstance().dbInstanceArn();

        } catch (RdsException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }
```

```
   public static String getListInstanceClasses(RdsClient rdsClient) {
       try {
           DescribeOrderableDbInstanceOptionsRequest optionsRequest =
DescribeOrderableDbInstanceOptionsRequest
                   .builder()
                   .engine("aurora-mysql")
                   .maxRecords(20)
                   .build();

           DescribeOrderableDbInstanceOptionsResponse response = rdsClient
                   .describeOrderableDBInstanceOptions(optionsRequest);
           List<OrderableDBInstanceOption> instanceOptions =
response.orderableDBInstanceOptions();
           String instanceClass = "";
           for (OrderableDBInstanceOption instanceOption : instanceOptions) {
               instanceClass = instanceOption.dbInstanceClass();
               System.out.println("The instance class is " +
instanceOption.dbInstanceClass());
               System.out.println("The engine version is " +
instanceOption.engineVersion());
           }
           return instanceClass;

       } catch (RdsException e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
       return "";
   }

   // Waits until the database instance is available.
   public static void waitForInstanceReady(RdsClient rdsClient, String
dbClusterIdentifier) {
       boolean instanceReady = false;
       String instanceReadyStr;
       System.out.println("Waiting for instance to become available.");
       try {
           DescribeDbClustersRequest instanceRequest =
DescribeDbClustersRequest.builder()
                   .dbClusterIdentifier(dbClusterIdentifier)
                   .build();

           while (!instanceReady) {
```

```
                DescribeDbClustersResponse response =
rdsClient.describeDBClusters(instanceRequest);
                List<DBCluster> clusterList = response.dbClusters();
                for (DBCluster cluster : clusterList) {
                    instanceReadyStr = cluster.status();
                    if (instanceReadyStr.contains("available")) {
                        instanceReady = true;
                    } else {
                        System.out.print(".");
                        Thread.sleep(sleepTime * 1000);
                    }
                }
            }
            System.out.println("Database cluster is available!");

        } catch (RdsException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static String createDBCluster(RdsClient rdsClient, String
dbParameterGroupFamily, String dbName,
            String dbClusterIdentifier, String userName, String password) {
        try {
            CreateDbClusterRequest clusterRequest =
CreateDbClusterRequest.builder()
                    .databaseName(dbName)
                    .dbClusterIdentifier(dbClusterIdentifier)
                    .dbClusterParameterGroupName(dbParameterGroupFamily)
                    .engine("aurora-mysql")
                    .masterUsername(userName)
                    .masterUserPassword(password)
                    .build();

            CreateDbClusterResponse response =
rdsClient.createDBCluster(clusterRequest);
            return response.dbCluster().dbClusterArn();

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
```

```
   }

   // Get a list of allowed engine versions.
   public static void getAllowedEngines(RdsClient rdsClient, String
dbParameterGroupFamily) {
       try {
           DescribeDbEngineVersionsRequest versionsRequest =
DescribeDbEngineVersionsRequest.builder()
                   .dbParameterGroupFamily(dbParameterGroupFamily)
                   .engine("aurora-mysql")
                   .build();

           DescribeDbEngineVersionsResponse response =
rdsClient.describeDBEngineVersions(versionsRequest);
           List<DBEngineVersion> dbEngines = response.dbEngineVersions();
           for (DBEngineVersion dbEngine : dbEngines) {
               System.out.println("The engine version is " +
dbEngine.engineVersion());
               System.out.println("The engine description is " +
dbEngine.dbEngineDescription());
           }

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }

   // Modify the auto_increment_offset parameter.
   public static void modifyDBClusterParas(RdsClient rdsClient, String
dClusterGroupName) {
       try {
           Parameter parameter1 = Parameter.builder()
                   .parameterName("auto_increment_offset")
                   .applyMethod("immediate")
                   .parameterValue("5")
                   .build();

           List<Parameter> paraList = new ArrayList<>();
           paraList.add(parameter1);
           ModifyDbClusterParameterGroupRequest groupRequest =
ModifyDbClusterParameterGroupRequest.builder()
                   .dbClusterParameterGroupName(dClusterGroupName)
                   .parameters(paraList)
```

```
                    .build();

            ModifyDbClusterParameterGroupResponse response =
rdsClient.modifyDBClusterParameterGroup(groupRequest);
            System.out.println(
                    "The parameter group " +
response.dbClusterParameterGroupName() + " was successfully modified");

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeDbClusterParameters(RdsClient rdsClient, String
dbCLusterGroupName, int flag) {
        try {
            DescribeDbClusterParametersRequest dbParameterGroupsRequest;
            if (flag == 0) {
                dbParameterGroupsRequest =
DescribeDbClusterParametersRequest.builder()
                        .dbClusterParameterGroupName(dbCLusterGroupName)
                        .build();
            } else {
                dbParameterGroupsRequest =
DescribeDbClusterParametersRequest.builder()
                        .dbClusterParameterGroupName(dbCLusterGroupName)
                        .source("user")
                        .build();
            }

            DescribeDbClusterParametersResponse response = rdsClient
                    .describeDBClusterParameters(dbParameterGroupsRequest);
            List<Parameter> dbParameters = response.parameters();
            String paraName;
            for (Parameter para : dbParameters) {
                // Only print out information about either auto_increment_offset
or
                // auto_increment_increment.
                paraName = para.parameterName();
                if ((paraName.compareTo("auto_increment_offset") == 0)
                        || (paraName.compareTo("auto_increment_increment ") ==
0)) {
                    System.out.println("*** The parameter name is  " + paraName);
```

```
                    System.out.println("*** The parameter value is  " +
para.parameterValue());
                    System.out.println("*** The parameter data type is " +
para.dataType());
                    System.out.println("*** The parameter description is " +
para.description());
                    System.out.println("*** The parameter allowed values  is " +
para.allowedValues());
                }
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeDbClusterParameterGroups(RdsClient rdsClient,
String dbClusterGroupName) {
        try {
            DescribeDbClusterParameterGroupsRequest groupsRequest =
DescribeDbClusterParameterGroupsRequest.builder()
                    .dbClusterParameterGroupName(dbClusterGroupName)
                    .maxRecords(20)
                    .build();

            List<DBClusterParameterGroup> groups =
rdsClient.describeDBClusterParameterGroups(groupsRequest)
                    .dbClusterParameterGroups();
            for (DBClusterParameterGroup group : groups) {
                System.out.println("The group name is " +
group.dbClusterParameterGroupName());
                System.out.println("The group ARN is " +
group.dbClusterParameterGroupArn());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void createDBClusterParameterGroup(RdsClient rdsClient, String
dbClusterGroupName,
```

```
            String dbParameterGroupFamily) {
        try {
            CreateDbClusterParameterGroupRequest groupRequest =
CreateDbClusterParameterGroupRequest.builder()
                    .dbClusterParameterGroupName(dbClusterGroupName)
                    .dbParameterGroupFamily(dbParameterGroupFamily)
                    .description("Created by using the AWS SDK for Java")
                    .build();

            CreateDbClusterParameterGroupResponse response =
rdsClient.createDBClusterParameterGroup(groupRequest);
            System.out.println("The group name is " +
response.dbClusterParameterGroup().dbClusterParameterGroupName());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeDBEngines(RdsClient rdsClient) {
        try {
            DescribeDbEngineVersionsRequest engineVersionsRequest =
DescribeDbEngineVersionsRequest.builder()
                    .engine("aurora-mysql")
                    .defaultOnly(true)
                    .maxRecords(20)
                    .build();

            DescribeDbEngineVersionsResponse response =
rdsClient.describeDBEngineVersions(engineVersionsRequest);
            List<DBEngineVersion> engines = response.dbEngineVersions();

            // Get all DBEngineVersion objects.
            for (DBEngineVersion engineOb : engines) {
                System.out.println("The name of the DB parameter group family for
the database engine is "
                        + engineOb.dbParameterGroupFamily());
                System.out.println("The name of the database engine " +
engineOb.engine());
                System.out.println("The version number of the database engine " +
engineOb.engineVersion());
            }
```

```
        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Java 2.x -API-Referenz.
  - CreateDBCluster
  - DB-Gruppe erstellt ClusterParameter
  - DB wurde erstellt ClusterSnapshot
  - CreateDBInstance
  - DeleteDBCluster
  - DB-Gruppe gelöscht ClusterParameter
  - DeleteDBInstance
  - Beschriebene ClusterParameter DB-Gruppen
  - BeschriebenDB ClusterParameters
  - BeschriebenB ClusterSnapshots
  - DescribeDBClusters
  - BeschriebenB EngineVersions
  - DescribeDBInstances
  - DescribeOrderableDB InstanceOptions
  - DB-Gruppe ändern ClusterParameter

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/**
Before running this Kotlin code example, set up your development environment,
 including your credentials.

For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

This example requires an AWS Secrets Manager secret that contains the database
 credentials. If you do not create a
secret, this example will not work. For more details, see:

https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_how-
services-use-secrets_RS.html

This Kotlin example performs the following tasks:

1. Returns a list of the available DB engines.
2. Creates a custom DB parameter group.
3. Gets the parameter groups.
4. Gets the parameters in the group.
5. Modifies the auto_increment_increment parameter.
6. Displays the updated parameter value.
7. Gets a list of allowed engine versions.
8. Creates an Aurora DB cluster database.
9. Waits for DB instance to be ready.
10. Gets a list of instance classes available for the selected engine.
11. Creates a database instance in the cluster.
12. Waits for the database instance in the cluster to be ready.
13. Creates a snapshot.
14. Waits for DB snapshot to be ready.
15. Deletes the DB instance.
16. Deletes the DB cluster.
17. Deletes the DB cluster group.
 */

var slTime: Long = 20

suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
```

```
            <dbClusterGroupName> <dbParameterGroupFamily>
<dbInstanceClusterIdentifier> <dbName> <dbSnapshotIdentifier> <secretName>
       Where:
            dbClusterGroupName - The database group name.
            dbParameterGroupFamily - The database parameter group name.
            dbInstanceClusterIdentifier - The database instance identifier.
            dbName -  The database name.
            dbSnapshotIdentifier - The snapshot identifier.
            secretName - The name of the AWS Secrets Manager secret that contains
the database credentials.
   """

   if (args.size != 7) {
       println(usage)
       exitProcess(1)
   }

   val dbClusterGroupName = args[0]
   val dbParameterGroupFamily = args[1]
   val dbInstanceClusterIdentifier = args[2]
   val dbInstanceIdentifier = args[3]
   val dbName = args[4]
   val dbSnapshotIdentifier = args[5]
   val secretName = args[6]

   val gson = Gson()
   val user = gson.fromJson(getSecretValues(secretName).toString(),
User::class.java)
   val username = user.username
   val userPassword = user.password

   println("1. Return a list of the available DB engines")
   describeAuroraDBEngines()

   println("2. Create a custom parameter group")
   createDBClusterParameterGroup(dbClusterGroupName, dbParameterGroupFamily)

   println("3. Get the parameter group")
   describeDbClusterParameterGroups(dbClusterGroupName)

   println("4. Get the parameters in the group")
   describeDbClusterParameters(dbClusterGroupName, 0)

   println("5. Modify the auto_increment_offset parameter")
```

```
    modifyDBClusterParas(dbClusterGroupName)

    println("6. Display the updated parameter value")
    describeDbClusterParameters(dbClusterGroupName, -1)

    println("7. Get a list of allowed engine versions")
    getAllowedClusterEngines(dbParameterGroupFamily)

    println("8. Create an Aurora DB cluster database")
    val arnClusterVal = createDBCluster(dbClusterGroupName, dbName,
dbInstanceClusterIdentifier, username, userPassword)
    println("The ARN of the cluster is $arnClusterVal")

    println("9. Wait for DB instance to be ready")
    waitForClusterInstanceReady(dbInstanceClusterIdentifier)

    println("10. Get a list of instance classes available for the selected
engine")
    val instanceClass = getListInstanceClasses()

    println("11. Create a database instance in the cluster.")
    val clusterDBARN = createDBInstanceCluster(dbInstanceIdentifier,
dbInstanceClusterIdentifier, instanceClass)
    println("The ARN of the database is $clusterDBARN")

    println("12. Wait for DB instance to be ready")
    waitDBAuroraInstanceReady(dbInstanceIdentifier)

    println("13. Create a snapshot")
    createDBClusterSnapshot(dbInstanceClusterIdentifier, dbSnapshotIdentifier)

    println("14. Wait for DB snapshot to be ready")
    waitSnapshotReady(dbSnapshotIdentifier, dbInstanceClusterIdentifier)

    println("15. Delete the DB instance")
    deleteDBInstance(dbInstanceIdentifier)

    println("16. Delete the DB cluster")
    deleteCluster(dbInstanceClusterIdentifier)

    println("17. Delete the DB cluster group")
    if (clusterDBARN != null) {
        deleteDBClusterGroup(dbClusterGroupName, clusterDBARN)
    }
```

```
    println("The Scenario has successfully completed.")
}

@Throws(InterruptedException::class)
suspend fun deleteDBClusterGroup(
    dbClusterGroupName: String,
    clusterDBARN: String,
) {
    var isDataDel = false
    var didFind: Boolean
    var instanceARN: String

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        // Make sure that the database has been deleted.
        while (!isDataDel) {
            val response = rdsClient.describeDbInstances()
            val instanceList = response.dbInstances
            val listSize = instanceList?.size
            isDataDel = false
            didFind = false
            var index = 1
            if (instanceList != null) {
                for (instance in instanceList) {
                    instanceARN = instance.dbInstanceArn.toString()
                    if (instanceARN.compareTo(clusterDBARN) == 0) {
                        println("$clusterDBARN still exists")
                        didFind = true
                    }
                    if (index == listSize && !didFind) {
                        // Went through the entire list and did not find the
 database ARN.
                        isDataDel = true
                    }
                    delay(slTime * 1000)
                    index++
                }
            }
        }
        val clusterParameterGroupRequest =
            DeleteDbClusterParameterGroupRequest {
                dbClusterParameterGroupName = dbClusterGroupName
            }

        rdsClient.deleteDbClusterParameterGroup(clusterParameterGroupRequest)
```

```
        println("$dbClusterGroupName was deleted.")
    }
}

suspend fun deleteCluster(dbInstanceClusterIdentifier: String) {
    val deleteDbClusterRequest =
        DeleteDbClusterRequest {
            dbClusterIdentifier = dbInstanceClusterIdentifier
            skipFinalSnapshot = true
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        rdsClient.deleteDbCluster(deleteDbClusterRequest)
        println("$dbInstanceClusterIdentifier was deleted!")
    }
}

suspend fun deleteDBInstance(dbInstanceIdentifierVal: String) {
    val deleteDbInstanceRequest =
        DeleteDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            deleteAutomatedBackups = true
            skipFinalSnapshot = true
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.deleteDbInstance(deleteDbInstanceRequest)
        print("The status of the database is
 ${response.dbInstance?.dbInstanceStatus}")
    }
}

suspend fun waitSnapshotReady(
    dbSnapshotIdentifier: String?,
    dbInstanceClusterIdentifier: String?,
) {
    var snapshotReady = false
    var snapshotReadyStr: String
    println("Waiting for the snapshot to become available.")

    val snapshotsRequest =
        DescribeDbClusterSnapshotsRequest {
            dbClusterSnapshotIdentifier = dbSnapshotIdentifier
            dbClusterIdentifier = dbInstanceClusterIdentifier
```

```
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        while (!snapshotReady) {
            val response = rdsClient.describeDbClusterSnapshots(snapshotsRequest)
            val snapshotList = response.dbClusterSnapshots
            if (snapshotList != null) {
                for (snapshot in snapshotList) {
                    snapshotReadyStr = snapshot.status.toString()
                    if (snapshotReadyStr.contains("available")) {
                        snapshotReady = true
                    } else {
                        println(".")
                        delay(slTime * 5000)
                    }
                }
            }
        }
    }
    println("The Snapshot is available!")
}

suspend fun createDBClusterSnapshot(
    dbInstanceClusterIdentifier: String?,
    dbSnapshotIdentifier: String?,
) {
    val snapshotRequest =
        CreateDbClusterSnapshotRequest {
            dbClusterIdentifier = dbInstanceClusterIdentifier
            dbClusterSnapshotIdentifier = dbSnapshotIdentifier
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbClusterSnapshot(snapshotRequest)
        println("The Snapshot ARN is
 ${response.dbClusterSnapshot?.dbClusterSnapshotArn}")
    }
}

suspend fun waitDBAuroraInstanceReady(dbInstanceIdentifierVal: String?) {
    var instanceReady = false
    var instanceReadyStr: String
    println("Waiting for instance to become available.")
    val instanceRequest =
```

```
        DescribeDbInstancesRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
        }

    var endpoint = ""
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        while (!instanceReady) {
            val response = rdsClient.describeDbInstances(instanceRequest)
            response.dbInstances?.forEach { instance ->
                instanceReadyStr = instance.dbInstanceStatus.toString()
                if (instanceReadyStr.contains("available")) {
                    endpoint = instance.endpoint?.address.toString()
                    instanceReady = true
                } else {
                    print(".")
                    delay(sleepTime * 1000)
                }
            }
        }
    }
    println("Database instance is available! The connection endpoint is
 $endpoint")
}

suspend fun createDBInstanceCluster(
    dbInstanceIdentifierVal: String?,
    dbInstanceClusterIdentifierVal: String?,
    instanceClassVal: String?,
): String? {
    val instanceRequest =
        CreateDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            dbClusterIdentifier = dbInstanceClusterIdentifierVal
            engine = "aurora-mysql"
            dbInstanceClass = instanceClassVal
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbInstance(instanceRequest)
        print("The status is ${response.dbInstance?.dbInstanceStatus}")
        return response.dbInstance?.dbInstanceArn
    }
}
```

```
suspend fun getListInstanceClasses(): String {
    val optionsRequest =
        DescribeOrderableDbInstanceOptionsRequest {
            engine = "aurora-mysql"
            maxRecords = 20
        }
    var instanceClass = ""
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response =
 rdsClient.describeOrderableDbInstanceOptions(optionsRequest)
        response.orderableDbInstanceOptions?.forEach { instanceOption ->
            instanceClass = instanceOption.dbInstanceClass.toString()
            println("The instance class is ${instanceOption.dbInstanceClass}")
            println("The engine version is ${instanceOption.engineVersion}")
        }
    }
    return instanceClass
}

// Waits until the database instance is available.
suspend fun waitForClusterInstanceReady(dbClusterIdentifierVal: String?) {
    var instanceReady = false
    var instanceReadyStr: String
    println("Waiting for instance to become available.")

    val instanceRequest =
        DescribeDbClustersRequest {
            dbClusterIdentifier = dbClusterIdentifierVal
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        while (!instanceReady) {
            val response = rdsClient.describeDbClusters(instanceRequest)
            response.dbClusters?.forEach { cluster ->
                instanceReadyStr = cluster.status.toString()
                if (instanceReadyStr.contains("available")) {
                    instanceReady = true
                } else {
                    print(".")
                    delay(sleepTime * 1000)
                }
            }
        }
    }
```

```
    println("Database cluster is available!")
}

suspend fun createDBCluster(
    dbParameterGroupFamilyVal: String?,
    dbName: String?,
    dbClusterIdentifierVal: String?,
    userName: String?,
    password: String?,
): String? {
    val clusterRequest =
        CreateDbClusterRequest {
            databaseName = dbName
            dbClusterIdentifier = dbClusterIdentifierVal
            dbClusterParameterGroupName = dbParameterGroupFamilyVal
            engine = "aurora-mysql"
            masterUsername = userName
            masterUserPassword = password
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbCluster(clusterRequest)
        return response.dbCluster?.dbClusterArn
    }
}

// Get a list of allowed engine versions.
suspend fun getAllowedClusterEngines(dbParameterGroupFamilyVal: String?) {
    val versionsRequest =
        DescribeDbEngineVersionsRequest {
            dbParameterGroupFamily = dbParameterGroupFamilyVal
            engine = "aurora-mysql"
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbEngineVersions(versionsRequest)
        response.dbEngineVersions?.forEach { dbEngine ->
            println("The engine version is ${dbEngine.engineVersion}")
            println("The engine description is ${dbEngine.dbEngineDescription}")
        }
    }
}

// Modify the auto_increment_offset parameter.
```

```
suspend fun modifyDBClusterParas(dClusterGroupName: String?) {
    val parameter1 =
        Parameter {
            parameterName = "auto_increment_offset"
            applyMethod = ApplyMethod.fromValue("immediate")
            parameterValue = "5"
        }

    val paraList = ArrayList<Parameter>()
    paraList.add(parameter1)
    val groupRequest =
        ModifyDbClusterParameterGroupRequest {
            dbClusterParameterGroupName = dClusterGroupName
            parameters = paraList
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.modifyDbClusterParameterGroup(groupRequest)
        println("The parameter group ${response.dbClusterParameterGroupName} was
 successfully modified")
    }
}

suspend fun describeDbClusterParameters(
    dbCLusterGroupName: String?,
    flag: Int,
) {
    val dbParameterGroupsRequest: DescribeDbClusterParametersRequest
    dbParameterGroupsRequest =
        if (flag == 0) {
            DescribeDbClusterParametersRequest {
                dbClusterParameterGroupName = dbCLusterGroupName
            }
        } else {
            DescribeDbClusterParametersRequest {
                dbClusterParameterGroupName = dbCLusterGroupName
                source = "user"
            }
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response =
 rdsClient.describeDbClusterParameters(dbParameterGroupsRequest)
        response.parameters?.forEach { para ->
```

```
            // Only print out information about either auto_increment_offset or
 auto_increment_increment.
            val paraName = para.parameterName
            if (paraName != null) {
                if (paraName.compareTo("auto_increment_offset") == 0 ||
 paraName.compareTo("auto_increment_increment ") == 0) {
                    println("*** The parameter name is  $paraName")
                    println("*** The parameter value is  ${para.parameterValue}")
                    println("*** The parameter data type is ${para.dataType}")
                    println("*** The parameter description is
 ${para.description}")
                    println("*** The parameter allowed values  is
 ${para.allowedValues}")
                }
            }
        }
    }
}

suspend fun describeDbClusterParameterGroups(dbClusterGroupName: String?) {
    val groupsRequest =
        DescribeDbClusterParameterGroupsRequest {
            dbClusterParameterGroupName = dbClusterGroupName
            maxRecords = 20
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbClusterParameterGroups(groupsRequest)
        response.dbClusterParameterGroups?.forEach { group ->
            println("The group name is ${group.dbClusterParameterGroupName}")
            println("The group ARN is ${group.dbClusterParameterGroupArn}")
        }
    }
}

suspend fun createDBClusterParameterGroup(
    dbClusterGroupNameVal: String?,
    dbParameterGroupFamilyVal: String?,
) {
    val groupRequest =
        CreateDbClusterParameterGroupRequest {
            dbClusterParameterGroupName = dbClusterGroupNameVal
            dbParameterGroupFamily = dbParameterGroupFamilyVal
            description = "Created by using the AWS SDK for Kotlin"
```

```
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbClusterParameterGroup(groupRequest)
        println("The group name is
 ${response.dbClusterParameterGroup?.dbClusterParameterGroupName}")
    }
}

suspend fun describeAuroraDBEngines() {
    val engineVersionsRequest =
        DescribeDbEngineVersionsRequest {
            engine = "aurora-mysql"
            defaultOnly = true
            maxRecords = 20
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbEngineVersions(engineVersionsRequest)
        response.dbEngineVersions?.forEach { engineOb ->
            println("The name of the DB parameter group family for the database
 engine is ${engineOb.dbParameterGroupFamily}")
            println("The name of the database engine ${engineOb.engine}")
            println("The version number of the database engine
 ${engineOb.engineVersion}")
        }
    }
}
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Kotlin.
  - CreateDBCluster
  - DB-Gruppe erstellt ClusterParameter
  - DB wurde erstellt ClusterSnapshot
  - CreateDBInstance
  - DeleteDBCluster
  - DB-Gruppe gelöscht ClusterParameter
  - DeleteDBInstance

- Beschriebene ClusterParameter DB-Gruppen
- BeschriebenDB ClusterParameters
- BeschriebenB ClusterSnapshots
- DescribeDBClusters
- BeschriebenB EngineVersions
- DescribeDBInstances
- DescribeOrderableDB InstanceOptions
- DB-Gruppe ändern ClusterParameter

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung aus.

```
class AuroraClusterScenario:
    """Runs a scenario that shows how to get started using Aurora DB clusters."""

    def __init__(self, aurora_wrapper):
        """
        :param aurora_wrapper: An object that wraps Aurora DB cluster actions.
        """
        self.aurora_wrapper = aurora_wrapper

    def create_parameter_group(self, db_engine, parameter_group_name):
        """
        Shows how to get available engine versions for a specified database
 engine and
        create a DB cluster parameter group that is compatible with a selected
 engine family.

        :param db_engine: The database engine to use as a basis.
```

```
        :param parameter_group_name: The name given to the newly created
parameter group.
        :return: The newly created parameter group.
        """
        print(
            f"Checking for an existing DB cluster parameter group named
{parameter_group_name}."
        )
        parameter_group =
self.aurora_wrapper.get_parameter_group(parameter_group_name)
        if parameter_group is None:
            print(f"Getting available database engine versions for {db_engine}.")
            engine_versions = self.aurora_wrapper.get_engine_versions(db_engine)
            families = list({ver["DBParameterGroupFamily"] for ver in
engine_versions})
            family_index = q.choose("Which family do you want to use? ",
families)
            print(f"Creating a DB cluster parameter group.")
            self.aurora_wrapper.create_parameter_group(
                parameter_group_name, families[family_index], "Example parameter
group."
            )
            parameter_group = self.aurora_wrapper.get_parameter_group(
                parameter_group_name
            )
        print(f"Parameter group
{parameter_group['DBClusterParameterGroupName']}:")
        pp(parameter_group)
        print("-" * 88)
        return parameter_group

    def set_user_parameters(self, parameter_group_name):
        """
        Shows how to get the parameters contained in a custom parameter group and
        update some of the parameter values in the group.

        :param parameter_group_name: The name of the parameter group to query and
modify.
        """
        print("Let's set some parameter values in your parameter group.")
        auto_inc_parameters = self.aurora_wrapper.get_parameters(
            parameter_group_name, name_prefix="auto_increment"
        )
        update_params = []
```

```
        for auto_inc in auto_inc_parameters:
            if auto_inc["IsModifiable"] and auto_inc["DataType"] == "integer":
                print(f"The {auto_inc['ParameterName']} parameter is described
as:")
                print(f"\t{auto_inc['Description']}")
                param_range = auto_inc["AllowedValues"].split("-")
                auto_inc["ParameterValue"] = str(
                    q.ask(
                        f"Enter a value between {param_range[0]} and
{param_range[1]}: ",
                        q.is_int,
                        q.in_range(int(param_range[0]), int(param_range[1])),
                    )
                )
                update_params.append(auto_inc)
        self.aurora_wrapper.update_parameters(parameter_group_name,
update_params)
        print(
            "You can get a list of parameters you've set by specifying a source
of 'user'."
        )
        user_parameters = self.aurora_wrapper.get_parameters(
            parameter_group_name, source="user"
        )
        pp(user_parameters)
        print("-" * 88)

    def create_cluster(self, cluster_name, db_engine, db_name, parameter_group):
        """
        Shows how to create an Aurora DB cluster that contains a database of a
specified
        type. The database is also configured to use a custom DB cluster
parameter group.

        :param cluster_name: The name given to the newly created DB cluster.
        :param db_engine: The engine of the created database.
        :param db_name: The name given to the created database.
        :param parameter_group: The parameter group that is associated with the
DB cluster.
        :return: The newly created DB cluster.
        """
        print("Checking for an existing DB cluster.")
        cluster = self.aurora_wrapper.get_db_cluster(cluster_name)
        if cluster is None:
```

```
            admin_username = q.ask(
                "Enter an administrator user name for the database: ",
q.non_empty
            )
            admin_password = q.ask(
                "Enter a password for the administrator (at least 8 characters):
",
                q.non_empty,
            )
            engine_versions = self.aurora_wrapper.get_engine_versions(
                db_engine, parameter_group["DBParameterGroupFamily"]
            )
            engine_choices = [ver["EngineVersionDescription"] for ver in
engine_versions]
            print("The available engines for your parameter group are:")
            engine_index = q.choose("Which engine do you want to use? ",
engine_choices)
            print(
                f"Creating DB cluster {cluster_name} and database {db_name}.\n"
                f"The DB cluster is configured to use\n"
                f"your custom parameter group
{parameter_group['DBClusterParameterGroupName']}\n"
                f"and selected engine {engine_choices[engine_index]}.\n"
                f"This typically takes several minutes."
            )
            cluster = self.aurora_wrapper.create_db_cluster(
                cluster_name,
                parameter_group["DBClusterParameterGroupName"],
                db_name,
                db_engine,
                engine_versions[engine_index]["EngineVersion"],
                admin_username,
                admin_password,
            )
            while cluster.get("Status") != "available":
                wait(30)
                cluster = self.aurora_wrapper.get_db_cluster(cluster_name)
            print("Cluster created and available.\n")
        print("Cluster data:")
        pp(cluster)
        print("-" * 88)
        return cluster

    def create_instance(self, cluster):
```

```
        """
        Shows how to create a DB instance in an existing Aurora DB cluster. A new
DB cluster
        contains no DB instances, so you must add one. The first DB instance that
is added
        to a DB cluster defaults to a read-write DB instance.

        :param cluster: The DB cluster where the DB instance is added.
        :return: The newly created DB instance.
        """
        print("Checking for an existing database instance.")
        cluster_name = cluster["DBClusterIdentifier"]
        db_inst = self.aurora_wrapper.get_db_instance(cluster_name)
        if db_inst is None:
            print("Let's create a database instance in your DB cluster.")
            print("First, choose a DB instance type:")
            inst_opts = self.aurora_wrapper.get_orderable_instances(
                cluster["Engine"], cluster["EngineVersion"]
            )
            inst_choices = list({opt["DBInstanceClass"] + ", storage type: " +
opt["StorageType"] for opt in inst_opts})
            inst_index = q.choose(
                "Which DB instance class do you want to use? ", inst_choices
            )
            print(
                f"Creating a database instance. This typically takes several
minutes."
            )
            db_inst = self.aurora_wrapper.create_instance_in_cluster(
                cluster_name, cluster_name, cluster["Engine"],
inst_opts[inst_index]["DBInstanceClass"]
            )
            while db_inst.get("DBInstanceStatus") != "available":
                wait(30)
                db_inst = self.aurora_wrapper.get_db_instance(cluster_name)
        print("Instance data:")
        pp(db_inst)
        print("-" * 88)
        return db_inst

    @staticmethod
    def display_connection(cluster):
        """
```

```
        Displays connection information about an Aurora DB cluster and tips on
 how to
        connect to it.

        :param cluster: The DB cluster to display.
        """
        print(
            "You can now connect to your database using your favorite MySql
 client.\n"
            "One way to connect is by using the 'mysql' shell on an Amazon EC2
 instance\n"
            "that is running in the same VPC as your database cluster. Pass the
 endpoint,\n"
            "port, and administrator user name to 'mysql' and enter your password
\n"
            "when prompted:\n"
        )
        print(
            f"\n\tmysql -h {cluster['Endpoint']} -P {cluster['Port']} -u
 {cluster['MasterUsername']} -p\n"
        )
        print(
            "For more information, see the User Guide for Aurora:\n"
            "\thttps://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/
CHAP_GettingStartedAurora.CreatingConnecting.Aurora.html#CHAP_GettingStartedAurora.Aurora
        )
        print("-" * 88)

    def create_snapshot(self, cluster_name):
        """
        Shows how to create a DB cluster snapshot and wait until it's available.

        :param cluster_name: The name of a DB cluster to snapshot.
        """
        if q.ask(
            "Do you want to create a snapshot of your DB cluster (y/n)? ",
 q.is_yesno
        ):
            snapshot_id = f"{cluster_name}-{uuid.uuid4()}"
            print(
                f"Creating a snapshot named {snapshot_id}. This typically takes a
 few minutes."
            )
            snapshot = self.aurora_wrapper.create_cluster_snapshot(
```

```
                snapshot_id, cluster_name
            )
            while snapshot.get("Status") != "available":
                wait(30)
                snapshot = self.aurora_wrapper.get_cluster_snapshot(snapshot_id)
            pp(snapshot)
            print("-" * 88)

    def cleanup(self, db_inst, cluster, parameter_group):
        """
        Shows how to clean up a DB instance, DB cluster, and DB cluster parameter
group.
        Before the DB cluster parameter group can be deleted, all associated DB
instances and
        DB clusters must first be deleted.

        :param db_inst: The DB instance to delete.
        :param cluster: The DB cluster to delete.
        :param parameter_group: The DB cluster parameter group to delete.
        """
        cluster_name = cluster["DBClusterIdentifier"]
        parameter_group_name = parameter_group["DBClusterParameterGroupName"]
        if q.ask(
            "\nDo you want to delete the database instance, DB cluster, and
parameter "
            "group (y/n)? ",
            q.is_yesno,
        ):
            print(f"Deleting database instance
{db_inst['DBInstanceIdentifier']}.")

self.aurora_wrapper.delete_db_instance(db_inst["DBInstanceIdentifier"])
            print(f"Deleting database cluster {cluster_name}.")
            self.aurora_wrapper.delete_db_cluster(cluster_name)
            print(
                "Waiting for the DB instance and DB cluster to delete.\n"
                "This typically takes several minutes."
            )
            while db_inst is not None or cluster is not None:
                wait(30)
                if db_inst is not None:
                    db_inst = self.aurora_wrapper.get_db_instance(
                        db_inst["DBInstanceIdentifier"]
                    )
```

```
                if cluster is not None:
                    cluster = self.aurora_wrapper.get_db_cluster(
                        cluster["DBClusterIdentifier"]
                    )
            print(f"Deleting parameter group {parameter_group_name}.")
            self.aurora_wrapper.delete_parameter_group(parameter_group_name)

    def run_scenario(self, db_engine, parameter_group_name, cluster_name,
 db_name):
        print("-" * 88)
        print(
            "Welcome to the Amazon Relational Database Service (Amazon RDS) get
 started\n"
            "with Aurora DB clusters demo."
        )
        print("-" * 88)

        parameter_group = self.create_parameter_group(db_engine,
 parameter_group_name)
        self.set_user_parameters(parameter_group_name)
        cluster = self.create_cluster(cluster_name, db_engine, db_name,
 parameter_group)
        wait(5)
        db_inst = self.create_instance(cluster)
        self.display_connection(cluster)
        self.create_snapshot(cluster_name)
        self.cleanup(db_inst, cluster, parameter_group)

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    logging.basicConfig(level=logging.INFO, format="%(levelname)s: %(message)s")
    try:
        scenario = AuroraClusterScenario(AuroraWrapper.from_client())
        scenario.run_scenario(
            "aurora-mysql",
            "doc-example-cluster-parameter-group",
            "doc-example-aurora",
            "docexampledb",
        )
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

Definieren Sie Funktionen, die vom Szenario aufgerufen werden, um Aurora-Aktionen zu verwalten.

```
class AuroraWrapper:
    """Encapsulates Aurora DB cluster actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon Relational Database Service (Amazon
 RDS) client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_parameter_group(self, parameter_group_name):
        """
        Gets a DB cluster parameter group.

        :param parameter_group_name: The name of the parameter group to retrieve.
        :return: The requested parameter group.
        """
        try:
            response = self.rds_client.describe_db_cluster_parameter_groups(
                DBClusterParameterGroupName=parameter_group_name
            )
            parameter_group = response["DBClusterParameterGroups"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBParameterGroupNotFound":
                logger.info("Parameter group %s does not exist.",
 parameter_group_name)
            else:
                logger.error(
                    "Couldn't get parameter group %s. Here's why: %s: %s",
```

```
                    parameter_group_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return parameter_group


    def create_parameter_group(
        self, parameter_group_name, parameter_group_family, description
    ):
        """
        Creates a DB cluster parameter group that is based on the specified
parameter group
        family.

        :param parameter_group_name: The name of the newly created parameter
group.
        :param parameter_group_family: The family that is used as the basis of
the new
                                       parameter group.
        :param description: A description given to the parameter group.
        :return: Data about the newly created parameter group.
        """
        try:
            response = self.rds_client.create_db_cluster_parameter_group(
                DBClusterParameterGroupName=parameter_group_name,
                DBParameterGroupFamily=parameter_group_family,
                Description=description,
            )
        except ClientError as err:
            logger.error(
                "Couldn't create parameter group %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response


    def delete_parameter_group(self, parameter_group_name):
```

```
        """
        Deletes a DB cluster parameter group.

        :param parameter_group_name: The name of the parameter group to delete.
        :return: Data about the parameter group.
        """
        try:
            response = self.rds_client.delete_db_cluster_parameter_group(
                DBClusterParameterGroupName=parameter_group_name
            )
        except ClientError as err:
            logger.error(
                "Couldn't delete parameter group %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response


    def get_parameters(self, parameter_group_name, name_prefix="", source=None):
        """
        Gets the parameters that are contained in a DB cluster parameter group.

        :param parameter_group_name: The name of the parameter group to query.
        :param name_prefix: When specified, the retrieved list of parameters is
filtered
                            to contain only parameters that start with this
prefix.
        :param source: When specified, only parameters from this source are
retrieved.
                       For example, a source of 'user' retrieves only parameters
that
                       were set by a user.
        :return: The list of requested parameters.
        """
        try:
            kwargs = {"DBClusterParameterGroupName": parameter_group_name}
            if source is not None:
                kwargs["Source"] = source
            parameters = []
```

```
            paginator =
 self.rds_client.get_paginator("describe_db_cluster_parameters")
            for page in paginator.paginate(**kwargs):
                parameters += [
                    p
                    for p in page["Parameters"]
                    if p["ParameterName"].startswith(name_prefix)
                ]
        except ClientError as err:
            logger.error(
                "Couldn't get parameters for %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return parameters


    def update_parameters(self, parameter_group_name, update_parameters):
        """
        Updates parameters in a custom DB cluster parameter group.

        :param parameter_group_name: The name of the parameter group to update.
        :param update_parameters: The parameters to update in the group.
        :return: Data about the modified parameter group.
        """
        try:
            response = self.rds_client.modify_db_cluster_parameter_group(
                DBClusterParameterGroupName=parameter_group_name,
                Parameters=update_parameters,
            )
        except ClientError as err:
            logger.error(
                "Couldn't update parameters in %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

```
    def get_db_cluster(self, cluster_name):
        """
        Gets data about an Aurora DB cluster.

        :param cluster_name: The name of the DB cluster to retrieve.
        :return: The retrieved DB cluster.
        """
        try:
            response = self.rds_client.describe_db_clusters(
                DBClusterIdentifier=cluster_name
            )
            cluster = response["DBClusters"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBClusterNotFoundFault":
                logger.info("Cluster %s does not exist.", cluster_name)
            else:
                logger.error(
                    "Couldn't verify the existence of DB cluster %s. Here's why:
%s: %s",
                    cluster_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return cluster


    def create_db_cluster(
        self,
        cluster_name,
        parameter_group_name,
        db_name,
        db_engine,
        db_engine_version,
        admin_name,
        admin_password,
    ):
        """
        Creates a DB cluster that is configured to use the specified parameter
group.
        The newly created DB cluster contains a database that uses the specified
engine and
```

```
        engine version.

        :param cluster_name: The name of the DB cluster to create.
        :param parameter_group_name: The name of the parameter group to associate
with
                                     the DB cluster.
        :param db_name: The name of the database to create.
        :param db_engine: The database engine of the database that is created,
such as MySql.
        :param db_engine_version: The version of the database engine.
        :param admin_name: The user name of the database administrator.
        :param admin_password: The password of the database administrator.
        :return: The newly created DB cluster.
        """
        try:
            response = self.rds_client.create_db_cluster(
                DatabaseName=db_name,
                DBClusterIdentifier=cluster_name,
                DBClusterParameterGroupName=parameter_group_name,
                Engine=db_engine,
                EngineVersion=db_engine_version,
                MasterUsername=admin_name,
                MasterUserPassword=admin_password,
            )
            cluster = response["DBCluster"]
        except ClientError as err:
            logger.error(
                "Couldn't create database %s. Here's why: %s: %s",
                db_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return cluster


    def delete_db_cluster(self, cluster_name):
        """
        Deletes a DB cluster.

        :param cluster_name: The name of the DB cluster to delete.
        """
        try:
```

```
            self.rds_client.delete_db_cluster(
                DBClusterIdentifier=cluster_name, SkipFinalSnapshot=True
            )
            logger.info("Deleted DB cluster %s.", cluster_name)
        except ClientError:
            logger.exception("Couldn't delete DB cluster %s.", cluster_name)
            raise


    def create_cluster_snapshot(self, snapshot_id, cluster_id):
        """
        Creates a snapshot of a DB cluster.

        :param snapshot_id: The ID to give the created snapshot.
        :param cluster_id: The DB cluster to snapshot.
        :return: Data about the newly created snapshot.
        """
        try:
            response = self.rds_client.create_db_cluster_snapshot(
                DBClusterSnapshotIdentifier=snapshot_id,
DBClusterIdentifier=cluster_id
            )
            snapshot = response["DBClusterSnapshot"]
        except ClientError as err:
            logger.error(
                "Couldn't create snapshot of %s. Here's why: %s: %s",
                cluster_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return snapshot


    def get_cluster_snapshot(self, snapshot_id):
        """
        Gets a DB cluster snapshot.

        :param snapshot_id: The ID of the snapshot to retrieve.
        :return: The retrieved snapshot.
        """
        try:
            response = self.rds_client.describe_db_cluster_snapshots(
```

```
                DBClusterSnapshotIdentifier=snapshot_id
            )
            snapshot = response["DBClusterSnapshots"][0]
        except ClientError as err:
            logger.error(
                "Couldn't get DB cluster snapshot %s. Here's why: %s: %s",
                snapshot_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return snapshot


    def create_instance_in_cluster(
        self, instance_id, cluster_id, db_engine, instance_class
    ):
        """
        Creates a database instance in an existing DB cluster. The first database
that is
        created defaults to a read-write DB instance.

        :param instance_id: The ID to give the newly created DB instance.
        :param cluster_id: The ID of the DB cluster where the DB instance is
created.
        :param db_engine: The database engine of a database to create in the DB
instance.
                          This must be compatible with the configured parameter
group
                          of the DB cluster.
        :param instance_class: The DB instance class for the newly created DB
instance.
        :return: Data about the newly created DB instance.
        """
        try:
            response = self.rds_client.create_db_instance(
                DBInstanceIdentifier=instance_id,
                DBClusterIdentifier=cluster_id,
                Engine=db_engine,
                DBInstanceClass=instance_class,
            )
            db_inst = response["DBInstance"]
        except ClientError as err:
```

```
            logger.error(
                "Couldn't create DB instance %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return db_inst


    def get_engine_versions(self, engine, parameter_group_family=None):
        """
        Gets database engine versions that are available for the specified engine
        and parameter group family.

        :param engine: The database engine to look up.
        :param parameter_group_family: When specified, restricts the returned
list of
                                       engine versions to those that are
compatible with
                                       this parameter group family.
        :return: The list of database engine versions.
        """
        try:
            kwargs = {"Engine": engine}
            if parameter_group_family is not None:
                kwargs["DBParameterGroupFamily"] = parameter_group_family
            response = self.rds_client.describe_db_engine_versions(**kwargs)
            versions = response["DBEngineVersions"]
        except ClientError as err:
            logger.error(
                "Couldn't get engine versions for %s. Here's why: %s: %s",
                engine,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return versions


    def get_orderable_instances(self, db_engine, db_engine_version):
        """
```

```
        Gets DB instance options that can be used to create DB instances that are
        compatible with a set of specifications.

        :param db_engine: The database engine that must be supported by the DB
instance.
        :param db_engine_version: The engine version that must be supported by
the DB instance.
        :return: The list of DB instance options that can be used to create a
compatible DB instance.
        """
        try:
            inst_opts = []
            paginator = self.rds_client.get_paginator(
                "describe_orderable_db_instance_options"
            )
            for page in paginator.paginate(
                Engine=db_engine, EngineVersion=db_engine_version
            ):
                inst_opts += page["OrderableDBInstanceOptions"]
        except ClientError as err:
            logger.error(
                "Couldn't get orderable DB instances. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return inst_opts


    def get_db_instance(self, instance_id):
        """
        Gets data about a DB instance.

        :param instance_id: The ID of the DB instance to retrieve.
        :return: The retrieved DB instance.
        """
        try:
            response = self.rds_client.describe_db_instances(
                DBInstanceIdentifier=instance_id
            )
            db_inst = response["DBInstances"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBInstanceNotFound":
```

```
                logger.info("Instance %s does not exist.", instance_id)
            else:
                logger.error(
                    "Couldn't get DB instance %s. Here's why: %s: %s",
                    instance_id,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return db_inst


    def delete_db_instance(self, instance_id):
        """
        Deletes a DB instance.

        :param instance_id: The ID of the DB instance to delete.
        :return: Data about the deleted DB instance.
        """
        try:
            response = self.rds_client.delete_db_instance(
                DBInstanceIdentifier=instance_id,
                SkipFinalSnapshot=True,
                DeleteAutomatedBackups=True,
            )
            db_inst = response["DBInstance"]
        except ClientError as err:
            logger.error(
                "Couldn't delete DB instance %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return db_inst
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Python (Boto3).
  - CreateDBCluster
  - DB-Gruppe erstellt ClusterParameter
  - DB wurde erstellt ClusterSnapshot
  - CreateDBInstance
  - DeleteDBCluster
  - DB-Gruppe gelöscht ClusterParameter
  - DeleteDBInstance
  - Beschriebene ClusterParameter DB-Gruppen
  - BeschriebenDB ClusterParameters
  - BeschriebenB ClusterSnapshots
  - DescribeDBClusters
  - BeschriebenB EngineVersions
  - DescribeDBInstances
  - DescribeOrderableDB InstanceOptions
  - DB-Gruppe ändern ClusterParameter

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Eine Bibliothek, die die szenariospezifischen Funktionen für das Aurora-Szenario enthält.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

use phf::{phf_set, Set};
use secrecy::SecretString;
```

```
use std::{collections::HashMap, fmt::Display, time::Duration};

use aws_sdk_rds::{
    error::ProvideErrorMetadata,

 operation::create_db_cluster_parameter_group::CreateDbClusterParameterGroupOutput,
    types::{DbCluster, DbClusterParameterGroup, DbClusterSnapshot, DbInstance,
 Parameter},
};
use sdk_examples_test_utils::waiter::Waiter;
use tracing::{info, trace, warn};

const DB_ENGINE: &str = "aurora-mysql";
const DB_CLUSTER_PARAMETER_GROUP_NAME: &str =
 "RustSDKCodeExamplesDBParameterGroup";
const DB_CLUSTER_PARAMETER_GROUP_DESCRIPTION: &str =
    "Parameter Group created by Rust SDK Code Example";
const DB_CLUSTER_IDENTIFIER: &str = "RustSDKCodeExamplesDBCluster";
const DB_INSTANCE_IDENTIFIER: &str = "RustSDKCodeExamplesDBInstance";

static FILTER_PARAMETER_NAMES: Set<&'static str> = phf_set! {
    "auto_increment_offset",
    "auto_increment_increment",
};

#[derive(Debug, PartialEq, Eq)]
struct MetadataError {
    message: Option<String>,
    code: Option<String>,
}

impl MetadataError {
    fn from(err: &dyn ProvideErrorMetadata) -> Self {
        MetadataError {
            message: err.message().map(String::from),
            code: err.code().map(String::from),
        }
    }
}

impl Display for MetadataError {
    fn fmt(&self, f: &mut std::fmt::Formatter<'_>) -> std::fmt::Result {
        let display = match (&self.message, &self.code) {
            (None, None) => "Unknown".to_string(),
```

```
            (None, Some(code)) => format!("({code})"),
            (Some(message), None) => message.to_string(),
            (Some(message), Some(code)) => format!("{message} ({code})"),
        };
        write!(f, "{display}")
    }
}

#[derive(Debug, PartialEq, Eq)]
pub struct ScenarioError {
    message: String,
    context: Option<MetadataError>,
}

impl ScenarioError {
    pub fn with(message: impl Into<String>) -> Self {
        ScenarioError {
            message: message.into(),
            context: None,
        }
    }

    pub fn new(message: impl Into<String>, err: &dyn ProvideErrorMetadata) ->
 Self {
        ScenarioError {
            message: message.into(),
            context: Some(MetadataError::from(err)),
        }
    }
}

impl std::error::Error for ScenarioError {}
impl Display for ScenarioError {
    fn fmt(&self, f: &mut std::fmt::Formatter<'_>) -> std::fmt::Result {
        match &self.context {
            Some(c) => write!(f, "{}: {}", self.message, c),
            None => write!(f, "{}", self.message),
        }
    }
}

// Parse the ParameterName, Description, and AllowedValues values and display
 them.
#[derive(Debug)]
```

```
pub struct AuroraScenarioParameter {
    name: String,
    allowed_values: String,
    current_value: String,
}

impl Display for AuroraScenarioParameter {
    fn fmt(&self, f: &mut std::fmt::Formatter<'_>) -> std::fmt::Result {
        write!(
            f,
            "{}: {} (allowed: {})",
            self.name, self.current_value, self.allowed_values
        )
    }
}

impl From<aws_sdk_rds::types::Parameter> for AuroraScenarioParameter {
    fn from(value: aws_sdk_rds::types::Parameter) -> Self {
        AuroraScenarioParameter {
            name: value.parameter_name.unwrap_or_default(),
            allowed_values: value.allowed_values.unwrap_or_default(),
            current_value: value.parameter_value.unwrap_or_default(),
        }
    }
}

pub struct AuroraScenario {
    rds: crate::rds::Rds,
    engine_family: Option<String>,
    engine_version: Option<String>,
    instance_class: Option<String>,
    db_cluster_parameter_group: Option<DbClusterParameterGroup>,
    db_cluster_identifier: Option<String>,
    db_instance_identifier: Option<String>,
    username: Option<String>,
    password: Option<SecretString>,
}

impl AuroraScenario {
    pub fn new(client: crate::rds::Rds) -> Self {
        AuroraScenario {
            rds: client,
            engine_family: None,
            engine_version: None,
```

```
            instance_class: None,
            db_cluster_parameter_group: None,
            db_cluster_identifier: None,
            db_instance_identifier: None,
            username: None,
            password: None,
        }
    }

    // snippet-start:[rust.aurora.get_engines.usage]
    // Get available engine families for Aurora MySql.
rds.DescribeDbEngineVersions(Engine='aurora-mysql') and build a set of the
'DBParameterGroupFamily' field values. I get {aurora-mysql8.0, aurora-mysql5.7}.
    pub async fn get_engines(&self) -> Result<HashMap<String, Vec<String>>,
ScenarioError> {
        let describe_db_engine_versions =
self.rds.describe_db_engine_versions(DB_ENGINE).await;
        trace!(versions=?describe_db_engine_versions, "full list of versions");

        if let Err(err) = describe_db_engine_versions {
            return Err(ScenarioError::new(
                "Failed to retrieve DB Engine Versions",
                &err,
            ));
        };

        let version_count = describe_db_engine_versions
            .as_ref()
            .map(|o| o.db_engine_versions().len())
            .unwrap_or_default();
        info!(version_count, "got list of versions");

        // Create a map of engine families to their available versions.
        let mut versions = HashMap::<String, Vec<String>>::new();
        describe_db_engine_versions
            .unwrap()
            .db_engine_versions()
            .iter()
            .filter_map(
                |v| match (&v.db_parameter_group_family, &v.engine_version) {
                    (Some(family), Some(version)) => Some((family.clone(),
version.clone())),
                    _ => None,
                },
```

```
            )
            .for_each(|(family, version)|
versions.entry(family).or_default().push(version));

        Ok(versions)
    }
    // snippet-end:[rust.aurora.get_engines.usage]

    // snippet-start:[rust.aurora.get_instance_classes.usage]
    pub async fn get_instance_classes(&self) -> Result<Vec<String>,
ScenarioError> {
        let describe_orderable_db_instance_options_items = self
            .rds
            .describe_orderable_db_instance_options(
                DB_ENGINE,
                self.engine_version
                    .as_ref()
                    .expect("engine version for db instance options")
                    .as_str(),
            )
            .await;

        describe_orderable_db_instance_options_items
            .map(|options| {
                options
                    .iter()
                    .map(|o|
o.db_instance_class().unwrap_or_default().to_string())
                    .collect::<Vec<String>>()
            })
            .map_err(|err| ScenarioError::new("Could not get available instance
classes", &err))
    }
    // snippet-end:[rust.aurora.get_instance_classes.usage]

    // snippet-start:[rust.aurora.set_engine.usage]
    // Select an engine family and create a custom DB cluster parameter group.
rds.CreateDbClusterParameterGroup(DBParameterGroupFamily='aurora-mysql8.0')
    pub async fn set_engine(&mut self, engine: &str, version: &str) -> Result<(),
ScenarioError> {
        self.engine_family = Some(engine.to_string());
        self.engine_version = Some(version.to_string());
        let create_db_cluster_parameter_group = self
            .rds
```

```
            .create_db_cluster_parameter_group(
                DB_CLUSTER_PARAMETER_GROUP_NAME,
                DB_CLUSTER_PARAMETER_GROUP_DESCRIPTION,
                engine,
            )
            .await;

        match create_db_cluster_parameter_group {
            Ok(CreateDbClusterParameterGroupOutput {
                db_cluster_parameter_group: None,
                ..
            }) => {
                return Err(ScenarioError::with(
                    "CreateDBClusterParameterGroup had empty response",
                ));
            }
            Err(error) => {
                if error.code() == Some("DBParameterGroupAlreadyExists") {
                    info!("Cluster Parameter Group already exists, nothing to
do");
                } else {
                    return Err(ScenarioError::new(
                        "Could not create Cluster Parameter Group",
                        &error,
                    ));
                }
            }
            _ => {
                info!("Created Cluster Parameter Group");
            }
        }

        Ok(())
    }
    // snippet-end:[rust.aurora.set_engine.usage]

    pub fn set_instance_class(&mut self, instance_class: Option<String>) {
        self.instance_class = instance_class;
    }

    pub fn set_login(&mut self, username: Option<String>, password:
Option<SecretString>) {
        self.username = username;
        self.password = password;
```

```
    }

    pub async fn connection_string(&self) -> Result<String, ScenarioError> {
        let cluster = self.get_cluster().await?;
        let endpoint = cluster.endpoint().unwrap_or_default();
        let port = cluster.port().unwrap_or_default();
        let username = cluster.master_username().unwrap_or_default();
        Ok(format!("mysql -h {endpoint} -P {port} -u {username} -p"))
    }

    // snippet-start:[rust.aurora.get_cluster.usage]
    pub async fn get_cluster(&self) -> Result<DbCluster, ScenarioError> {
        let describe_db_clusters_output = self
            .rds
            .describe_db_clusters(
                self.db_cluster_identifier
                    .as_ref()
                    .expect("cluster identifier")
                    .as_str(),
            )
            .await;
        if let Err(err) = describe_db_clusters_output {
            return Err(ScenarioError::new("Failed to get cluster", &err));
        }

        let db_cluster = describe_db_clusters_output
            .unwrap()
            .db_clusters
            .and_then(|output| output.first().cloned());

        db_cluster.ok_or_else(|| ScenarioError::with("Did not find the cluster"))
    }
    // snippet-end:[rust.aurora.get_cluster.usage]

    // snippet-start:[rust.aurora.cluster_parameters.usage]
    // Get the parameter group. rds.DescribeDbClusterParameterGroups
    // Get parameters in the group. This is a long list so you will have to
paginate. Find the auto_increment_offset and auto_increment_increment parameters
(by ParameterName). rds.DescribeDbClusterParameters
    // Parse the ParameterName, Description, and AllowedValues values and display
them.
    pub async fn cluster_parameters(&self) ->
Result<Vec<AuroraScenarioParameter>, ScenarioError> {
        let parameters_output = self
```

```
            .rds
            .describe_db_cluster_parameters(DB_CLUSTER_PARAMETER_GROUP_NAME)
            .await;

        if let Err(err) = parameters_output {
            return Err(ScenarioError::new(
                format!("Failed to retrieve parameters for
{DB_CLUSTER_PARAMETER_GROUP_NAME}"),
                &err,
            ));
        }

        let parameters = parameters_output
            .unwrap()
            .into_iter()
            .flat_map(|p| p.parameters.unwrap_or_default().into_iter())
            .filter(|p|
FILTER_PARAMETER_NAMES.contains(p.parameter_name().unwrap_or_default()))
            .map(AuroraScenarioParameter::from)
            .collect::<Vec<_>>();

        Ok(parameters)
    }
    // snippet-end:[rust.aurora.cluster_parameters.usage]

    // snippet-start:[rust.aurora.update_auto_increment.usage]
    // Modify both the auto_increment_offset and auto_increment_increment
parameters in one call in the custom parameter group. Set their ParameterValue
fields to a new allowable value. rds.ModifyDbClusterParameterGroup.
    pub async fn update_auto_increment(
        &self,
        offset: u8,
        increment: u8,
    ) -> Result<(), ScenarioError> {
        let modify_db_cluster_parameter_group = self
            .rds
            .modify_db_cluster_parameter_group(
                DB_CLUSTER_PARAMETER_GROUP_NAME,
                vec![
                    Parameter::builder()
                        .parameter_name("auto_increment_offset")
                        .parameter_value(format!("{offset}"))
                        .apply_method(aws_sdk_rds::types::ApplyMethod::Immediate)
                        .build(),
```

```
                    Parameter::builder()
                        .parameter_name("auto_increment_increment")
                        .parameter_value(format!("{increment}"))
                        .apply_method(aws_sdk_rds::types::ApplyMethod::Immediate)
                        .build(),
                ],
            )
            .await;

        if let Err(error) = modify_db_cluster_parameter_group {
            return Err(ScenarioError::new(
                "Failed to modify cluster parameter group",
                &error,
            ));
        }

        Ok(())
    }
    // snippet-end:[rust.aurora.update_auto_increment.usage]

    // snippet-start:[rust.aurora.start_cluster_and_instance.usage]
    // Get a list of allowed engine versions.
rds.DescribeDbEngineVersions(Engine='aurora-mysql', DBParameterGroupFamily=<the
family used to create your parameter group in step 2>)
    // Create an Aurora DB cluster database cluster that contains a MySql
database and uses the parameter group you created.
    // Wait for DB cluster to be ready. Call rds.DescribeDBClusters and check for
Status == 'available'.
    // Get a list of instance classes available for the selected engine
and engine version. rds.DescribeOrderableDbInstanceOptions(Engine='mysql',
EngineVersion=).

    // Create a database instance in the cluster.
    // Wait for DB instance to be ready. Call rds.DescribeDbInstances and check
for DBInstanceStatus == 'available'.
    pub async fn start_cluster_and_instance(&mut self) -> Result<(),
ScenarioError> {
        if self.password.is_none() {
            return Err(ScenarioError::with(
                "Must set Secret Password before starting a cluster",
            ));
        }
        let create_db_cluster = self
            .rds
```

```
            .create_db_cluster(
                DB_CLUSTER_IDENTIFIER,
                DB_CLUSTER_PARAMETER_GROUP_NAME,
                DB_ENGINE,
                self.engine_version.as_deref().expect("engine version"),
                self.username.as_deref().expect("username"),
                self.password
                    .replace(SecretString::new("".to_string()))
                    .expect("password"),
            )
            .await;
        if let Err(err) = create_db_cluster {
            return Err(ScenarioError::new(
                "Failed to create DB Cluster with cluster group",
                &err,
            ));
        }

        self.db_cluster_identifier = create_db_cluster
            .unwrap()
            .db_cluster
            .and_then(|c| c.db_cluster_identifier);

        if self.db_cluster_identifier.is_none() {
            return Err(ScenarioError::with("Created DB Cluster missing
Identifier"));
        }

        info!(
            "Started a db cluster: {}",
            self.db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing ARN")
        );

        let create_db_instance = self
            .rds
            .create_db_instance(
                self.db_cluster_identifier.as_deref().expect("cluster name"),
                DB_INSTANCE_IDENTIFIER,
                self.instance_class.as_deref().expect("instance class"),
                DB_ENGINE,
            )
            .await;
```

```
        if let Err(err) = create_db_instance {
            return Err(ScenarioError::new(
                "Failed to create Instance in DB Cluster",
                &err,
            ));
        }

        self.db_instance_identifier = create_db_instance
            .unwrap()
            .db_instance
            .and_then(|i| i.db_instance_identifier);

        // Cluster creation can take up to 20 minutes to become available
        let cluster_max_wait = Duration::from_secs(20 * 60);
        let waiter = Waiter::builder().max(cluster_max_wait).build();
        while waiter.sleep().await.is_ok() {
            let cluster = self
                .rds
                .describe_db_clusters(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = cluster {
                warn!(?err, "Failed to describe cluster while waiting for
ready");
                continue;
            }

            let instance = self
                .rds
                .describe_db_instance(
                    self.db_instance_identifier
                        .as_deref()
                        .expect("instance identifier"),
                )
                .await;
            if let Err(err) = instance {
                return Err(ScenarioError::new(
                    "Failed to find instance for cluster",
                    &err,
                ));
```

```
            }

            let instances_available = instance
                .unwrap()
                .db_instances()
                .iter()
                .all(|instance| instance.db_instance_status() ==
Some("Available"));

            let endpoints = self
                .rds
                .describe_db_cluster_endpoints(
                    self.db_cluster_identifier
                        .as_deref()
                        .expect("cluster identifier"),
                )
                .await;

            if let Err(err) = endpoints {
                return Err(ScenarioError::new(
                    "Failed to find endpoint for cluster",
                    &err,
                ));
            }

            let endpoints_available = endpoints
                .unwrap()
                .db_cluster_endpoints()
                .iter()
                .all(|endpoint| endpoint.status() == Some("available"));

            if instances_available && endpoints_available {
                return Ok(());
            }
        }

        Err(ScenarioError::with("timed out waiting for cluster"))
    }
    // snippet-end:[rust.aurora.start_cluster_and_instance.usage]

    // snippet-start:[rust.aurora.snapshot.usage]
    // Create a snapshot of the DB cluster. rds.CreateDbClusterSnapshot.
    // Wait for the snapshot to create. rds.DescribeDbClusterSnapshots until
Status == 'available'.
```

```
   pub async fn snapshot(&self, name: &str) -> Result<DbClusterSnapshot,
ScenarioError> {
       let id = self.db_cluster_identifier.as_deref().unwrap_or_default();
       let snapshot = self
           .rds
           .snapshot_cluster(id, format!("{id}_{name}").as_str())
           .await;
       match snapshot {
           Ok(output) => match output.db_cluster_snapshot {
               Some(snapshot) => Ok(snapshot),
               None => Err(ScenarioError::with("Missing Snapshot")),
           },
           Err(err) => Err(ScenarioError::new("Failed to create snapshot",
&err)),
       }
   }
   // snippet-end:[rust.aurora.snapshot.usage]

   // snippet-start:[rust.aurora.clean_up.usage]
   pub async fn clean_up(self) -> Result<(), Vec<ScenarioError>> {
       let mut clean_up_errors: Vec<ScenarioError> = vec![];

       // Delete the instance. rds.DeleteDbInstance.
       let delete_db_instance = self
           .rds
           .delete_db_instance(
               self.db_instance_identifier
                   .as_deref()
                   .expect("instance identifier"),
           )
           .await;
       if let Err(err) = delete_db_instance {
           let identifier = self
               .db_instance_identifier
               .as_deref()
               .unwrap_or("Missing Instance Identifier");
           let message = format!("failed to delete db instance {identifier}");
           clean_up_errors.push(ScenarioError::new(message, &err));
       } else {
           // Wait for the instance to delete
           let waiter = Waiter::default();
           while waiter.sleep().await.is_ok() {
               let describe_db_instances =
self.rds.describe_db_instances().await;
```

```
                if let Err(err) = describe_db_instances {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check instance state during deletion",
                        &err,
                    ));
                    break;
                }
                let db_instances = describe_db_instances
                    .unwrap()
                    .db_instances()
                    .iter()
                    .filter(|instance| instance.db_cluster_identifier ==
self.db_cluster_identifier)
                    .cloned()
                    .collect::<Vec<DbInstance>>();

                if db_instances.is_empty() {
                    trace!("Delete Instance waited and no instances were found");
                    break;
                }
                match db_instances.first().unwrap().db_instance_status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but instances is in
{status}");
                        continue;
                    }
                    None => {
                        warn!("No status for DB instance");
                        break;
                    }
                }
            }
        }

        // Delete the DB cluster. rds.DeleteDbCluster.
        let delete_db_cluster = self
            .rds
            .delete_db_cluster(
                self.db_cluster_identifier
                    .as_deref()
                    .expect("cluster identifier"),
            )
            .await;
```

```
        if let Err(err) = delete_db_cluster {
            let identifier = self
                .db_cluster_identifier
                .as_deref()
                .unwrap_or("Missing DB Cluster Identifier");
            let message = format!("failed to delete db cluster {identifier}");
            clean_up_errors.push(ScenarioError::new(message, &err));
        } else {
            // Wait for the instance and cluster to fully delete.
rds.DescribeDbInstances and rds.DescribeDbClusters until both are not found.
            let waiter = Waiter::default();
            while waiter.sleep().await.is_ok() {
                let describe_db_clusters = self
                    .rds
                    .describe_db_clusters(
                        self.db_cluster_identifier
                            .as_deref()
                            .expect("cluster identifier"),
                    )
                    .await;
                if let Err(err) = describe_db_clusters {
                    clean_up_errors.push(ScenarioError::new(
                        "Failed to check cluster state during deletion",
                        &err,
                    ));
                    break;
                }
                let describe_db_clusters = describe_db_clusters.unwrap();
                let db_clusters = describe_db_clusters.db_clusters();
                if db_clusters.is_empty() {
                    trace!("Delete cluster waited and no clusters were found");
                    break;
                }
                match db_clusters.first().unwrap().status() {
                    Some("Deleting") => continue,
                    Some(status) => {
                        info!("Attempting to delete but clusters is in
{status}");
                        continue;
                    }
                    None => {
                        warn!("No status for DB cluster");
                        break;
```

```
                    }
                }
            }
        }

        // Delete the DB cluster parameter group.
 rds.DeleteDbClusterParameterGroup.
        let delete_db_cluster_parameter_group = self
            .rds
            .delete_db_cluster_parameter_group(
                self.db_cluster_parameter_group
                    .map(|g| {
                        g.db_cluster_parameter_group_name
                            .unwrap_or_else(||
 DB_CLUSTER_PARAMETER_GROUP_NAME.to_string())
                    })
                    .as_deref()
                    .expect("cluster parameter group name"),
            )
            .await;
        if let Err(error) = delete_db_cluster_parameter_group {
            clean_up_errors.push(ScenarioError::new(
                "Failed to delete the db cluster parameter group",
                &error,
            ))
        }

        if clean_up_errors.is_empty() {
            Ok(())
        } else {
            Err(clean_up_errors)
        }
    }
    // snippet-end:[rust.aurora.clean_up.usage]
}

#[cfg(test)]
pub mod tests;
```

Tests für die Bibliothek, die Automocks für den RDS-Client-Wrapper nutzen.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
// SPDX-License-Identifier: Apache-2.0

use crate::rds::MockRdsImpl;

use super::*;

use std::io::{Error, ErrorKind};

use assert_matches::assert_matches;
use aws_sdk_rds::{
    error::SdkError,
    operation::{
        create_db_cluster::{CreateDBClusterError, CreateDbClusterOutput},
        create_db_cluster_parameter_group::CreateDBClusterParameterGroupError,
        create_db_cluster_snapshot::{CreateDBClusterSnapshotError,
 CreateDbClusterSnapshotOutput},
        create_db_instance::{CreateDBInstanceError, CreateDbInstanceOutput},
        delete_db_cluster::DeleteDbClusterOutput,
        delete_db_cluster_parameter_group::DeleteDbClusterParameterGroupOutput,
        delete_db_instance::DeleteDbInstanceOutput,
        describe_db_cluster_endpoints::DescribeDbClusterEndpointsOutput,
        describe_db_cluster_parameters::{
            DescribeDBClusterParametersError, DescribeDbClusterParametersOutput,
        },
        describe_db_clusters::{DescribeDBClustersError,
 DescribeDbClustersOutput},
        describe_db_engine_versions::{
            DescribeDBEngineVersionsError, DescribeDbEngineVersionsOutput,
        },
        describe_db_instances::{DescribeDBInstancesError,
 DescribeDbInstancesOutput},

 describe_orderable_db_instance_options::DescribeOrderableDBInstanceOptionsError,
        modify_db_cluster_parameter_group::{
            ModifyDBClusterParameterGroupError,
 ModifyDbClusterParameterGroupOutput,
        },
    },
    types::{
        error::DbParameterGroupAlreadyExistsFault, DbClusterEndpoint,
 DbEngineVersion,
        OrderableDbInstanceOption,
    },
};
```

```
use aws_smithy_runtime_api::http::{Response, StatusCode};
use aws_smithy_types::body::SdkBody;
use mockall::predicate::eq;
use secrecy::ExposeSecret;

// snippet-start:[rust.aurora.set_engine.test]
#[tokio::test]
async fn test_scenario_set_engine() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .with(
            eq("RustSDKCodeExamplesDBParameterGroup"),
            eq("Parameter Group created by Rust SDK Code Example"),
            eq("aurora-mysql"),
        )
        .return_once(|_, _, _| {
            Ok(CreateDbClusterParameterGroupOutput::builder()

 .db_cluster_parameter_group(DbClusterParameterGroup::builder().build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);

    let set_engine = scenario.set_engine("aurora-mysql", "aurora-
mysql8.0").await;

    assert_eq!(set_engine, Ok(()));
    assert_eq!(Some("aurora-mysql"), scenario.engine_family.as_deref());
    assert_eq!(Some("aurora-mysql8.0"), scenario.engine_version.as_deref());
}

#[tokio::test]
async fn test_scenario_set_engine_not_create() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .with(
            eq("RustSDKCodeExamplesDBParameterGroup"),
            eq("Parameter Group created by Rust SDK Code Example"),
            eq("aurora-mysql"),
```

```
        )
        .return_once(|_, _, _|
 Ok(CreateDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);

    let set_engine = scenario.set_engine("aurora-mysql", "aurora-
mysql8.0").await;

    assert!(set_engine.is_err());
}

#[tokio::test]
async fn test_scenario_set_engine_param_group_exists() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .withf(|_, _, _| true)
        .return_once(|_, _, _| {
            Err(SdkError::service_error(

 CreateDBClusterParameterGroupError::DbParameterGroupAlreadyExistsFault(
                    DbParameterGroupAlreadyExistsFault::builder().build(),
                ),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);

    let set_engine = scenario.set_engine("aurora-mysql", "aurora-
mysql8.0").await;

    assert!(set_engine.is_err());
}
// snippet-end:[rust.aurora.set_engine.test]

// snippet-start:[rust.aurora.get_engines.test]
#[tokio::test]
async fn test_scenario_get_engines() {
    let mut mock_rds = MockRdsImpl::default();
```

```
    mock_rds
        .expect_describe_db_engine_versions()
        .with(eq("aurora-mysql"))
        .return_once(|_| {
            Ok(DescribeDbEngineVersionsOutput::builder()
                .db_engine_versions(
                    DbEngineVersion::builder()
                        .db_parameter_group_family("f1")
                        .engine_version("f1a")
                        .build(),
                )
                .db_engine_versions(
                    DbEngineVersion::builder()
                        .db_parameter_group_family("f1")
                        .engine_version("f1b")
                        .build(),
                )
                .db_engine_versions(
                    DbEngineVersion::builder()
                        .db_parameter_group_family("f2")
                        .engine_version("f2a")
                        .build(),
                )
                .db_engine_versions(DbEngineVersion::builder().build())
                .build())
        });

    let scenario = AuroraScenario::new(mock_rds);

    let versions_map = scenario.get_engines().await;

    assert_eq!(
        versions_map,
        Ok(HashMap::from([
            ("f1".into(), vec!["f1a".into(), "f1b".into()]),
            ("f2".into(), vec!["f2a".into()])
        ]))
    );
}

#[tokio::test]
async fn test_scenario_get_engines_failed() {
    let mut mock_rds = MockRdsImpl::default();
```

```
    mock_rds
        .expect_describe_db_engine_versions()
        .with(eq("aurora-mysql"))
        .return_once(|_| {
            Err(SdkError::service_error(
                DescribeDBEngineVersionsError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe_db_engine_versions error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let scenario = AuroraScenario::new(mock_rds);

    let versions_map = scenario.get_engines().await;
    assert_matches!(
        versions_map,
        Err(ScenarioError { message, context: _ }) if message == "Failed to
 retrieve DB Engine Versions"
    );
}
// snippet-end:[rust.aurora.get_engines.test]

// snippet-start:[rust.aurora.get_instance_classes.test]
#[tokio::test]
async fn test_scenario_get_instance_classes() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .return_once(|_, _, _| {
            Ok(CreateDbClusterParameterGroupOutput::builder()

 .db_cluster_parameter_group(DbClusterParameterGroup::builder().build())
                .build())
        });

    mock_rds
        .expect_describe_orderable_db_instance_options()
        .with(eq("aurora-mysql"), eq("aurora-mysql8.0"))
        .return_once(|_, _| {
            Ok(vec![
```

```
                OrderableDbInstanceOption::builder()
                    .db_instance_class("t1")
                    .build(),
                OrderableDbInstanceOption::builder()
                    .db_instance_class("t2")
                    .build(),
                OrderableDbInstanceOption::builder()
                    .db_instance_class("t3")
                    .build(),
            ])
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario
        .set_engine("aurora-mysql", "aurora-mysql8.0")
        .await
        .expect("set engine");

    let instance_classes = scenario.get_instance_classes().await;

    assert_eq!(
        instance_classes,
        Ok(vec!["t1".into(), "t2".into(), "t3".into()])
    );
}

#[tokio::test]
async fn test_scenario_get_instance_classes_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_orderable_db_instance_options()
        .with(eq("aurora-mysql"), eq("aurora-mysql8.0"))
        .return_once(|_, _| {
            Err(SdkError::service_error(

 DescribeOrderableDBInstanceOptionsError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe_orderable_db_instance_options_error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });
```

```
    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_family = Some("aurora-mysql".into());
    scenario.engine_version = Some("aurora-mysql8.0".into());

    let instance_classes = scenario.get_instance_classes().await;

    assert_matches!(
        instance_classes,
        Err(ScenarioError {message, context: _}) if message == "Could not get
 available instance classes"
    );
}
// snippet-end:[rust.aurora.get_instance_classes.test]

// snippet-start:[rust.aurora.get_cluster.test]
#[tokio::test]
async fn test_scenario_get_cluster() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(DbCluster::builder().build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("RustSDKCodeExamplesDBCluster".into());
    let cluster = scenario.get_cluster().await;

    assert!(cluster.is_ok());
}

#[tokio::test]
async fn test_scenario_get_cluster_missing_cluster() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .return_once(|_, _, _| {
            Ok(CreateDbClusterParameterGroupOutput::builder()
```

```
 .db_cluster_parameter_group(DbClusterParameterGroup::builder().build())
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| Ok(DescribeDbClustersOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("RustSDKCodeExamplesDBCluster".into());
    let cluster = scenario.get_cluster().await;

    assert_matches!(cluster, Err(ScenarioError { message, context: _ }) if
 message == "Did not find the cluster");
}

#[tokio::test]
async fn test_scenario_get_cluster_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster_parameter_group()
        .return_once(|_, _, _| {
            Ok(CreateDbClusterParameterGroupOutput::builder()

 .db_cluster_parameter_group(DbClusterParameterGroup::builder().build())
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe_db_clusters_error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });
```

```
    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("RustSDKCodeExamplesDBCluster".into());
    let cluster = scenario.get_cluster().await;

    assert_matches!(cluster, Err(ScenarioError { message, context: _ }) if
 message == "Failed to get cluster");
}
// snippet-end:[rust.aurora.get_cluster.test]

#[tokio::test]
async fn test_scenario_connection_string() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .endpoint("test_endpoint")
                        .port(3306)
                        .master_username("test_username")
                        .build(),
                )
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("RustSDKCodeExamplesDBCluster".into());
    let connection_string = scenario.connection_string().await;

    assert_eq!(
        connection_string,
        Ok("mysql -h test_endpoint -P 3306 -u test_username -p".into())
    );
}

// snippet-start:[rust.aurora.cluster_parameters.test]
#[tokio::test]
async fn test_scenario_cluster_parameters() {
    let mut mock_rds = MockRdsImpl::default();
```

```
    mock_rds
        .expect_describe_db_cluster_parameters()
        .with(eq("RustSDKCodeExamplesDBParameterGroup"))
        .return_once(|_| {
            Ok(vec![DescribeDbClusterParametersOutput::builder()
                .parameters(Parameter::builder().parameter_name("a").build())
                .parameters(Parameter::builder().parameter_name("b").build())
                .parameters(
                    Parameter::builder()
                        .parameter_name("auto_increment_offset")
                        .build(),
                )
                .parameters(Parameter::builder().parameter_name("c").build())
                .parameters(
                    Parameter::builder()
                        .parameter_name("auto_increment_increment")
                        .build(),
                )
                .parameters(Parameter::builder().parameter_name("d").build())
                .build()])
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("RustSDKCodeExamplesDBCluster".into());

    let params = scenario.cluster_parameters().await.expect("cluster params");
    let names: Vec<String> = params.into_iter().map(|p| p.name).collect();
    assert_eq!(
        names,
        vec!["auto_increment_offset", "auto_increment_increment"]
    );
}

#[tokio::test]
async fn test_scenario_cluster_parameters_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_describe_db_cluster_parameters()
        .with(eq("RustSDKCodeExamplesDBParameterGroup"))
        .return_once(|_| {
            Err(SdkError::service_error(
                DescribeDBClusterParametersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
```

```
                    "describe_db_cluster_parameters_error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("RustSDKCodeExamplesDBCluster".into());
    let params = scenario.cluster_parameters().await;
    assert_matches!(params, Err(ScenarioError { message, context: _ }) if message
 == "Failed to retrieve parameters for RustSDKCodeExamplesDBParameterGroup");
}
// snippet-end:[rust.aurora.cluster_parameters.test]

// snippet-start:[rust.aurora.update_auto_increment.test]
#[tokio::test]
async fn test_scenario_update_auto_increment() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_modify_db_cluster_parameter_group()
        .withf(|name, params| {
            assert_eq!(name, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(
                params,
                &vec![
                    Parameter::builder()
                        .parameter_name("auto_increment_offset")
                        .parameter_value("10")
                        .apply_method(aws_sdk_rds::types::ApplyMethod::Immediate)
                        .build(),
                    Parameter::builder()
                        .parameter_name("auto_increment_increment")
                        .parameter_value("20")
                        .apply_method(aws_sdk_rds::types::ApplyMethod::Immediate)
                        .build(),
                ]
            );
            true
        })
        .return_once(|_, _|
 Ok(ModifyDbClusterParameterGroupOutput::builder().build()));
```

```
    let scenario = AuroraScenario::new(mock_rds);

    scenario
        .update_auto_increment(10, 20)
        .await
        .expect("update auto increment");
}

#[tokio::test]
async fn test_scenario_update_auto_increment_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_modify_db_cluster_parameter_group()
        .return_once(|_, _| {
            Err(SdkError::service_error(

 ModifyDBClusterParameterGroupError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "modify_db_cluster_parameter_group_error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let scenario = AuroraScenario::new(mock_rds);

    let update = scenario.update_auto_increment(10, 20).await;
    assert_matches!(update, Err(ScenarioError { message, context: _}) if message
 == "Failed to modify cluster parameter group");
}
// snippet-end:[rust.aurora.update_auto_increment.test]

// snippet-start:[rust.aurora.start_cluster_and_instance.test]
#[tokio::test]
async fn test_start_cluster_and_instance() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
```

```
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

.db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });
```

```
    mock_rds
        .expect_describe_db_instance()
        .with(eq("RustSDKCodeExamplesDBInstance"))
        .return_once(|name| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_instance_identifier(name)
                        .db_instance_status("Available")
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()

.db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
        assert!(scenario
            .password
            .replace(SecretString::new("BAD SECRET".into()))
            .unwrap()
            .expose_secret()
            .is_empty());
        assert_eq!(
            scenario.db_cluster_identifier,
            Some("RustSDKCodeExamplesDBCluster".into())
        );
```

```
    });
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Err(SdkError::service_error(
                CreateDBClusterError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db cluster error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _}) if message
 == "Failed to create DB Cluster with cluster group")
}

#[tokio::test]
async fn test_start_cluster_and_instance_cluster_create_missing_id() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .return_once(|_, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()
                .db_cluster(DbCluster::builder().build())
                .build())
```

```
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context:_ }) if message
 == "Created DB Cluster missing Identifier");
}

#[tokio::test]
async fn test_start_cluster_and_instance_instance_create_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .return_once(|_, _, _, _| {
            Err(SdkError::service_error(
                CreateDBInstanceError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create db instance error",
                ))),
```

```
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    let create = scenario.start_cluster_and_instance().await;
    assert_matches!(create, Err(ScenarioError { message, context: _ }) if message
 == "Failed to create Instance in DB Cluster")
}

#[tokio::test]
async fn test_start_cluster_and_instance_wait_hiccup() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_create_db_cluster()
        .withf(|id, params, engine, version, username, password| {
            assert_eq!(id, "RustSDKCodeExamplesDBCluster");
            assert_eq!(params, "RustSDKCodeExamplesDBParameterGroup");
            assert_eq!(engine, "aurora-mysql");
            assert_eq!(version, "aurora-mysql8.0");
            assert_eq!(username, "test username");
            assert_eq!(password.expose_secret(), "test password");
            true
        })
        .return_once(|id, _, _, _, _, _| {
            Ok(CreateDbClusterOutput::builder()

 .db_cluster(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds
        .expect_create_db_instance()
        .withf(|cluster, name, class, engine| {
            assert_eq!(cluster, "RustSDKCodeExamplesDBCluster");
            assert_eq!(name, "RustSDKCodeExamplesDBInstance");
            assert_eq!(class, "m5.large");
```

```
            assert_eq!(engine, "aurora-mysql");
            true
        })
        .return_once(|cluster, name, class, _| {
            Ok(CreateDbInstanceOutput::builder()
                .db_instance(
                    DbInstance::builder()
                        .db_cluster_identifier(cluster)
                        .db_instance_identifier(name)
                        .db_instance_class(class)
                        .build(),
                )
                .build())
        });

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
        .returning(|_| {
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe cluster error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        })
        .with(eq("RustSDKCodeExamplesDBCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()

.db_clusters(DbCluster::builder().db_cluster_identifier(id).build())
                .build())
        });

    mock_rds.expect_describe_db_instance().return_once(|name| {
        Ok(DescribeDbInstancesOutput::builder()
            .db_instances(
                DbInstance::builder()
                    .db_instance_identifier(name)
                    .db_instance_status("Available")
```

```
                    .build(),
            )
            .build())
    });

    mock_rds
        .expect_describe_db_cluster_endpoints()
        .return_once(|_| {
            Ok(DescribeDbClusterEndpointsOutput::builder()

 .db_cluster_endpoints(DbClusterEndpoint::builder().status("available").build())
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.engine_version = Some("aurora-mysql8.0".into());
    scenario.instance_class = Some("m5.large".into());
    scenario.username = Some("test username".into());
    scenario.password = Some(SecretString::new("test password".into()));

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let create = scenario.start_cluster_and_instance().await;
        assert!(create.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::advance(Duration::from_secs(1)).await;
    tokio::time::resume();
    let _ = assertions.await;
}
// snippet-end:[rust.aurora.start_cluster_and_instance.test]

// snippet-start:[rust.aurora.clean_up.test]
#[tokio::test]
async fn test_scenario_clean_up() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
```

```
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| Ok(DescribeDbInstancesOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| Ok(DescribeDbClustersOutput::builder().build()));

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
```

```
        .return_once(|_|
 Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_ok());
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
 Describe Cluster
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}

#[tokio::test]
async fn test_scenario_clean_up_errors() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_delete_db_instance()
        .with(eq("MockInstance"))
        .return_once(|_| Ok(DeleteDbInstanceOutput::builder().build()));

    mock_rds
        .expect_describe_db_instances()
        .with()
        .times(1)
        .returning(|| {
```

```
            Ok(DescribeDbInstancesOutput::builder()
                .db_instances(
                    DbInstance::builder()
                        .db_cluster_identifier("MockCluster")
                        .db_instance_status("Deleting")
                        .build(),
                )
                .build())
        })
        .with()
        .times(1)
        .returning(|| {
            Err(SdkError::service_error(
                DescribeDBInstancesError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db instances error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster()
        .with(eq("MockCluster"))
        .return_once(|_| Ok(DeleteDbClusterOutput::builder().build()));

    mock_rds
        .expect_describe_db_clusters()
        .with(eq("MockCluster"))
        .times(1)
        .returning(|id| {
            Ok(DescribeDbClustersOutput::builder()
                .db_clusters(
                    DbCluster::builder()
                        .db_cluster_identifier(id)
                        .status("Deleting")
                        .build(),
                )
                .build())
        })
        .with(eq("MockCluster"))
        .times(1)
        .returning(|_| {
```

```
            Err(SdkError::service_error(
                DescribeDBClustersError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "describe db clusters error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
SdkBody::empty()),
            ))
        });

    mock_rds
        .expect_delete_db_cluster_parameter_group()
        .with(eq("MockParamGroup"))
        .return_once(|_|
Ok(DeleteDbClusterParameterGroupOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some(String::from("MockCluster"));
    scenario.db_instance_identifier = Some(String::from("MockInstance"));
    scenario.db_cluster_parameter_group = Some(
        DbClusterParameterGroup::builder()
            .db_cluster_parameter_group_name("MockParamGroup")
            .build(),
    );

    tokio::time::pause();
    let assertions = tokio::spawn(async move {
        let clean_up = scenario.clean_up().await;
        assert!(clean_up.is_err());
        let errs = clean_up.unwrap_err();
        assert_eq!(errs.len(), 2);
        assert_matches!(errs.get(0), Some(ScenarioError {message, context: _}) if
message == "Failed to check instance state during deletion");
        assert_matches!(errs.get(1), Some(ScenarioError {message, context: _}) if
message == "Failed to check cluster state during deletion");
    });

    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
Describe Instances
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for first
Describe Cluster
```

```
    tokio::time::advance(Duration::from_secs(1)).await; // Wait for second
 Describe Cluster
    tokio::time::resume();
    let _ = assertions.await;
}
// snippet-end:[rust.aurora.clean_up.test]

// snippet-start:[rust.aurora.snapshot.test]
#[tokio::test]
async fn test_scenario_snapshot() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_snapshot_cluster()
        .with(eq("MockCluster"), eq("MockCluster_MockSnapshot"))
        .times(1)
        .return_once(|_, _| {
            Ok(CreateDbClusterSnapshotOutput::builder()
                .db_cluster_snapshot(
                    DbClusterSnapshot::builder()
                        .db_cluster_identifier("MockCluster")

 .db_cluster_snapshot_identifier("MockCluster_MockSnapshot")
                        .build(),
                )
                .build())
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("MockCluster".into());
    let create_snapshot = scenario.snapshot("MockSnapshot").await;
    assert!(create_snapshot.is_ok());
}

#[tokio::test]
async fn test_scenario_snapshot_error() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_snapshot_cluster()
        .with(eq("MockCluster"), eq("MockCluster_MockSnapshot"))
        .times(1)
        .return_once(|_, _| {
            Err(SdkError::service_error(
```

```
                CreateDBClusterSnapshotError::unhandled(Box::new(Error::new(
                    ErrorKind::Other,
                    "create snapshot error",
                ))),
                Response::new(StatusCode::try_from(400).unwrap(),
 SdkBody::empty()),
            ))
        });

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("MockCluster".into());
    let create_snapshot = scenario.snapshot("MockSnapshot").await;
    assert_matches!(create_snapshot, Err(ScenarioError { message, context: _}) if
 message == "Failed to create snapshot");
}

#[tokio::test]
async fn test_scenario_snapshot_invalid() {
    let mut mock_rds = MockRdsImpl::default();

    mock_rds
        .expect_snapshot_cluster()
        .with(eq("MockCluster"), eq("MockCluster_MockSnapshot"))
        .times(1)
        .return_once(|_, _|
 Ok(CreateDbClusterSnapshotOutput::builder().build()));

    let mut scenario = AuroraScenario::new(mock_rds);
    scenario.db_cluster_identifier = Some("MockCluster".into());
    let create_snapshot = scenario.snapshot("MockSnapshot").await;
    assert_matches!(create_snapshot, Err(ScenarioError { message, context: _}) if
 message == "Missing Snapshot");
}
// snippet-end:[rust.aurora.snapshot.test]
```

Eine Binärdatei zum vollständigen Ausführen des Szenarios, wobei Inquirer verwendet wird, damit der Benutzer einige Entscheidungen treffen kann.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

use std::fmt::Display;
```

```
use anyhow::anyhow;
use aurora_code_examples::{
    aurora_scenario::{AuroraScenario, ScenarioError},
    rds::Rds as RdsClient,
};
use aws_sdk_rds::Client;
use inquire::{validator::StringValidator, CustomUserError};
use secrecy::SecretString;
use tracing::warn;

#[derive(Default, Debug)]
struct Warnings(Vec<String>);

impl Warnings {
    fn new() -> Self {
        Warnings(Vec::with_capacity(5))
    }

    fn push(&mut self, warning: &str, error: ScenarioError) {
        let formatted = format!("{warning}: {error}");
        warn!("{formatted}");
        self.0.push(formatted);
    }

    fn is_empty(&self) -> bool {
        self.0.is_empty()
    }
}

impl Display for Warnings {
    fn fmt(&self, f: &mut std::fmt::Formatter<'_>) -> std::fmt::Result {
        writeln!(f, "Warnings:")?;
        for warning in &self.0 {
            writeln!(f, "{: >4}- {warning}", "")?;
        }
        Ok(())
    }
}

fn select(
    prompt: &str,
    choices: Vec<String>,
    error_message: &str,
```

```
) -> Result<String, anyhow::Error> {
    inquire::Select::new(prompt, choices)
        .prompt()
        .map_err(|error| anyhow!("{error_message}: {error}"))
}

// Prepare the Aurora Scenario. Prompt for several settings that are optional to
 the Scenario, but that the user should choose for the demo.
// This includes the engine, engine version, and instance class.
async fn prepare_scenario(rds: RdsClient) -> Result<AuroraScenario,
 anyhow::Error> {
    let mut scenario = AuroraScenario::new(rds);

    // Get available engine families for Aurora MySql.
 rds.DescribeDbEngineVersions(Engine='aurora-mysql') and build a set of the
 'DBParameterGroupFamily' field values. I get {aurora-mysql8.0, aurora-mysql5.7}.
    let available_engines = scenario.get_engines().await;
    if let Err(error) = available_engines {
        return Err(anyhow!("Failed to get available engines: {}", error));
    }
    let available_engines = available_engines.unwrap();

    // Select an engine family and create a custom DB cluster parameter group.
 rds.CreateDbClusterParameterGroup(DBParameterGroupFamily='aurora-mysql8.0')
    let engine = select(
        "Select an Aurora engine family",
        available_engines.keys().cloned().collect::<Vec<String>>(),
        "Invalid engine selection",
    )?;

    let version = select(
        format!("Select an Aurora engine version for {engine}").as_str(),
        available_engines.get(&engine).cloned().unwrap_or_default(),
        "Invalid engine version selection",
    )?;

    let set_engine = scenario.set_engine(engine.as_str(),
 version.as_str()).await;
    if let Err(error) = set_engine {
        return Err(anyhow!("Could not set engine: {}", error));
    }

    let instance_classes = scenario.get_instance_classes().await;
    match instance_classes {
```

```
        Ok(classes) => {
            let instance_class = select(
                format!("Select an Aurora instance class for {engine}").as_str(),
                classes,
                "Invalid instance class selection",
            )?;
            scenario.set_instance_class(Some(instance_class))
        }
        Err(err) => return Err(anyhow!("Failed to get instance classes for
 engine: {err}")),
    }

    Ok(scenario)
}

// Prepare the cluster, creating a custom parameter group overriding some group
 parameters based on user input.
async fn prepare_cluster(scenario: &mut AuroraScenario, warnings: &mut Warnings)
 -> Result<(), ()> {
    show_parameters(scenario, warnings).await;

    let offset = prompt_number_or_default(warnings, "auto_increment_offset", 5);
    let increment = prompt_number_or_default(warnings,
 "auto_increment_increment", 3);

    // Modify both the auto_increment_offset and auto_increment_increment
 parameters in one call in the custom parameter group. Set their ParameterValue
 fields to a new allowable value. rds.ModifyDbClusterParameterGroup.
    let update_auto_increment = scenario.update_auto_increment(offset,
 increment).await;

    if let Err(error) = update_auto_increment {
        warnings.push("Failed to update auto increment", error);
        return Err(());
    }

    // Get and display the updated parameters. Specify Source of 'user' to get
 just the modified parameters. rds.DescribeDbClusterParameters(Source='user')
    show_parameters(scenario, warnings).await;

    let username = inquire::Text::new("Username for the database (default
 'testuser')")
        .with_default("testuser")
        .with_initial_value("testuser")
```

```
        .prompt();

    if let Err(error) = username {
        warnings.push(
            "Failed to get username, using default",
            ScenarioError::with(format!("Error from inquirer: {error}")),
        );
        return Err(());
    }
    let username = username.unwrap();

    let password = inquire::Text::new("Password for the database (minimum 8
 characters)")
        .with_validator(|i: &str| {
            if i.len() >= 8 {
                Ok(inquire::validator::Validation::Valid)
            } else {
                Ok(inquire::validator::Validation::Invalid(
                    "Password must be at least 8 characters".into(),
                ))
            }
        })
        .prompt();

    let password: Option<SecretString> = match password {
        Ok(password) => Some(SecretString::from(password)),
        Err(error) => {
            warnings.push(
                "Failed to get password, using none (and not starting a DB)",
                ScenarioError::with(format!("Error from inquirer: {error}")),
            );
            return Err(());
        }
    };

    scenario.set_login(Some(username), password);

    Ok(())
}

// Start a single instance in the cluster,
async fn run_instance(scenario: &mut AuroraScenario) -> Result<(), ScenarioError>
 {
```

```
    // Create an Aurora DB cluster database cluster that contains a MySql
 database and uses the parameter group you created.
    // Create a database instance in the cluster.
    // Wait for DB instance to be ready. Call rds.DescribeDbInstances and check
 for DBInstanceStatus == 'available'.
    scenario.start_cluster_and_instance().await?;

    let connection_string = scenario.connection_string().await?;

    println!("Database ready: {connection_string}",);

    let _ = inquire::Text::new("Use the database with the connection string. When
 you're finished, press enter key to continue.").prompt();

    // Create a snapshot of the DB cluster. rds.CreateDbClusterSnapshot.
    // Wait for the snapshot to create. rds.DescribeDbClusterSnapshots until
 Status == 'available'.
    let snapshot_name = inquire::Text::new("Provide a name for the snapshot")
        .prompt()
        .unwrap_or(String::from("ScenarioRun"));
    let snapshot = scenario.snapshot(snapshot_name.as_str()).await?;
    println!(
        "Snapshot is available: {}",
        snapshot.db_cluster_snapshot_arn().unwrap_or("Missing ARN")
    );

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), anyhow::Error> {
    tracing_subscriber::fmt::init();
    let sdk_config = aws_config::from_env().load().await;
    let client = Client::new(&sdk_config);
    let rds = RdsClient::new(client);
    let mut scenario = prepare_scenario(rds).await?;

    // At this point, the scenario has things in AWS and needs to get cleaned up.
    let mut warnings = Warnings::new();

    if prepare_cluster(&mut scenario, &mut warnings).await.is_ok() {
        println!("Configured database cluster, starting an instance.");
        if let Err(err) = run_instance(&mut scenario).await {
            warnings.push("Problem running instance", err);
```

```
        }
    }

    // Clean up the instance, cluster, and parameter group, waiting for the
 instance and cluster to delete before moving on.
    let clean_up = scenario.clean_up().await;
    if let Err(errors) = clean_up {
        for error in errors {
            warnings.push("Problem cleaning up scenario", error);
        }
    }

    if warnings.is_empty() {
        Ok(())
    } else {
        println!("There were problems running the scenario:");
        println!("{warnings}");
        Err(anyhow!("There were problems running the scenario"))
    }
}

#[derive(Clone)]
struct U8Validator {}
impl StringValidator for U8Validator {
    fn validate(&self, input: &str) -> Result<inquire::validator::Validation,
 CustomUserError> {
        if input.parse::<u8>().is_err() {
            Ok(inquire::validator::Validation::Invalid(
                "Can't parse input as number".into(),
            ))
        } else {
            Ok(inquire::validator::Validation::Valid)
        }
    }
}

async fn show_parameters(scenario: &AuroraScenario, warnings: &mut Warnings) {
    let parameters = scenario.cluster_parameters().await;

    match parameters {
        Ok(parameters) => {
            println!("Current parameters");
            for parameter in parameters {
                println!("\t{parameter}");
```

```
            }
        }
        Err(error) => warnings.push("Could not find cluster parameters", error),
    }
}

fn prompt_number_or_default(warnings: &mut Warnings, name: &str, default: u8) ->
 u8 {
    let input = inquire::Text::new(format!("Updated {name}:").as_str())
        .with_validator(U8Validator {})
        .prompt();

    match input {
        Ok(increment) => match increment.parse::<u8>() {
            Ok(increment) => increment,
            Err(error) => {
                warnings.push(
                    format!("Invalid updated {name} (using {default}
 instead)").as_str(),
                    ScenarioError::with(format!("{error}")),
                );
                default
            }
        },
        Err(error) => {
            warnings.push(
                format!("Invalid updated {name} (using {default}
 instead)").as_str(),
                ScenarioError::with(format!("{error}")),
            );
            default
        }
    }
}
```

Ein Wrapper für den Service Amazon RDS, der Automocking für Tests ermöglicht.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

use aws_sdk_rds::{
    error::SdkError,
```

```
    operation::{
        create_db_cluster::{CreateDBClusterError, CreateDbClusterOutput},
        create_db_cluster_parameter_group::CreateDBClusterParameterGroupError,
        create_db_cluster_parameter_group::CreateDbClusterParameterGroupOutput,
        create_db_cluster_snapshot::{CreateDBClusterSnapshotError,
 CreateDbClusterSnapshotOutput},
        create_db_instance::{CreateDBInstanceError, CreateDbInstanceOutput},
        delete_db_cluster::{DeleteDBClusterError, DeleteDbClusterOutput},
        delete_db_cluster_parameter_group::{
            DeleteDBClusterParameterGroupError,
 DeleteDbClusterParameterGroupOutput,
        },
        delete_db_instance::{DeleteDBInstanceError, DeleteDbInstanceOutput},
        describe_db_cluster_endpoints::{
            DescribeDBClusterEndpointsError, DescribeDbClusterEndpointsOutput,
        },
        describe_db_cluster_parameters::{
            DescribeDBClusterParametersError, DescribeDbClusterParametersOutput,
        },
        describe_db_clusters::{DescribeDBClustersError,
 DescribeDbClustersOutput},
        describe_db_engine_versions::{
            DescribeDBEngineVersionsError, DescribeDbEngineVersionsOutput,
        },
        describe_db_instances::{DescribeDBInstancesError,
 DescribeDbInstancesOutput},

 describe_orderable_db_instance_options::DescribeOrderableDBInstanceOptionsError,
        modify_db_cluster_parameter_group::{
            ModifyDBClusterParameterGroupError,
 ModifyDbClusterParameterGroupOutput,
        },
    },
    types::{OrderableDbInstanceOption, Parameter},
    Client as RdsClient,
};
use secrecy::{ExposeSecret, SecretString};

#[cfg(test)]
use mockall::automock;

#[cfg(test)]
pub use MockRdsImpl as Rds;
#[cfg(not(test))]
```

```
pub use RdsImpl as Rds;

pub struct RdsImpl {
    pub inner: RdsClient,
}

#[cfg_attr(test, automock)]
impl RdsImpl {
    pub fn new(inner: RdsClient) -> Self {
        RdsImpl { inner }
    }

    // snippet-start:[rust.aurora.describe_db_engine_versions.wrapper]
    pub async fn describe_db_engine_versions(
        &self,
        engine: &str,
    ) -> Result<DescribeDbEngineVersionsOutput,
 SdkError<DescribeDBEngineVersionsError>> {
        self.inner
            .describe_db_engine_versions()
            .engine(engine)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.describe_db_engine_versions.wrapper]

    // snippet-start:[rust.aurora.describe_orderable_db_instance_options.wrapper]
    pub async fn describe_orderable_db_instance_options(
        &self,
        engine: &str,
        engine_version: &str,
    ) -> Result<Vec<OrderableDbInstanceOption>,
 SdkError<DescribeOrderableDBInstanceOptionsError>>
    {
        self.inner
            .describe_orderable_db_instance_options()
            .engine(engine)
            .engine_version(engine_version)
            .into_paginator()
            .items()
            .send()
            .try_collect()
            .await
    }
```

```
    // snippet-end:[rust.aurora.describe_orderable_db_instance_options.wrapper]

    // snippet-start:[rust.aurora.create_db_cluster_parameter_group.wrapper]
    pub async fn create_db_cluster_parameter_group(
        &self,
        name: &str,
        description: &str,
        family: &str,
    ) -> Result<CreateDbClusterParameterGroupOutput,
SdkError<CreateDBClusterParameterGroupError>>
    {
        self.inner
            .create_db_cluster_parameter_group()
            .db_cluster_parameter_group_name(name)
            .description(description)
            .db_parameter_group_family(family)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.create_db_cluster_parameter_group.wrapper]

    // snippet-start:[rust.aurora.describe_db_clusters.wrapper]
    pub async fn describe_db_clusters(
        &self,
        id: &str,
    ) -> Result<DescribeDbClustersOutput, SdkError<DescribeDBClustersError>> {
        self.inner
            .describe_db_clusters()
            .db_cluster_identifier(id)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.describe_db_clusters.wrapper]

    // snippet-start:[rust.aurora.describe_db_cluster_parameters.wrapper]
    pub async fn describe_db_cluster_parameters(
        &self,
        name: &str,
    ) -> Result<Vec<DescribeDbClusterParametersOutput>,
SdkError<DescribeDBClusterParametersError>>
    {
        self.inner
            .describe_db_cluster_parameters()
            .db_cluster_parameter_group_name(name)
```

```
            .into_paginator()
            .send()
            .try_collect()
            .await
    }
    // snippet-end:[rust.aurora.describe_db_cluster_parameters.wrapper]

    // snippet-start:[rust.aurora.modify_db_cluster_parameter_group.wrapper]
    pub async fn modify_db_cluster_parameter_group(
        &self,
        name: &str,
        parameters: Vec<Parameter>,
    ) -> Result<ModifyDbClusterParameterGroupOutput,
SdkError<ModifyDBClusterParameterGroupError>>
    {
        self.inner
            .modify_db_cluster_parameter_group()
            .db_cluster_parameter_group_name(name)
            .set_parameters(Some(parameters))
            .send()
            .await
    }
    // snippet-end:[rust.aurora.modify_db_cluster_parameter_group.wrapper]

    // snippet-start:[rust.aurora.create_db_cluster.wrapper]
    pub async fn create_db_cluster(
        &self,
        name: &str,
        parameter_group: &str,
        engine: &str,
        version: &str,
        username: &str,
        password: SecretString,
    ) -> Result<CreateDbClusterOutput, SdkError<CreateDBClusterError>> {
        self.inner
            .create_db_cluster()
            .db_cluster_identifier(name)
            .db_cluster_parameter_group_name(parameter_group)
            .engine(engine)
            .engine_version(version)
            .master_username(username)
            .master_user_password(password.expose_secret())
            .send()
            .await
```

```
    }
    // snippet-end:[rust.aurora.create_db_cluster.wrapper]

    // snippet-start:[rust.aurora.create_db_instance.wrapper]
    pub async fn create_db_instance(
        &self,
        cluster_name: &str,
        instance_name: &str,
        instance_class: &str,
        engine: &str,
    ) -> Result<CreateDbInstanceOutput, SdkError<CreateDBInstanceError>> {
        self.inner
            .create_db_instance()
            .db_cluster_identifier(cluster_name)
            .db_instance_identifier(instance_name)
            .db_instance_class(instance_class)
            .engine(engine)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.create_db_instance.wrapper]

    // snippet-start:[rust.aurora.describe_db_instance.wrapper]
    pub async fn describe_db_instance(
        &self,
        instance_identifier: &str,
    ) -> Result<DescribeDbInstancesOutput, SdkError<DescribeDBInstancesError>> {
        self.inner
            .describe_db_instances()
            .db_instance_identifier(instance_identifier)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.describe_db_instance.wrapper]

    // snippet-start:[rust.aurora.create_db_cluster_snapshot.wrapper]
    pub async fn snapshot_cluster(
        &self,
        db_cluster_identifier: &str,
        snapshot_name: &str,
    ) -> Result<CreateDbClusterSnapshotOutput,
SdkError<CreateDBClusterSnapshotError>> {
        self.inner
            .create_db_cluster_snapshot()
```

```
            .db_cluster_identifier(db_cluster_identifier)
            .db_cluster_snapshot_identifier(snapshot_name)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.create_db_cluster_snapshot.wrapper]

    // snippet-start:[rust.aurora.describe_db_instances.wrapper]
    pub async fn describe_db_instances(
        &self,
    ) -> Result<DescribeDbInstancesOutput, SdkError<DescribeDBInstancesError>> {
        self.inner.describe_db_instances().send().await
    }
    // snippet-end:[rust.aurora.describe_db_instances.wrapper]

    // snippet-start:[rust.aurora.describe_db_cluster_endpoints.wrapper]
    pub async fn describe_db_cluster_endpoints(
        &self,
        cluster_identifier: &str,
    ) -> Result<DescribeDbClusterEndpointsOutput,
SdkError<DescribeDBClusterEndpointsError>> {
        self.inner
            .describe_db_cluster_endpoints()
            .db_cluster_identifier(cluster_identifier)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.describe_db_cluster_endpoints.wrapper]

    // snippet-start:[rust.aurora.delete_db_instance.wrapper]
    pub async fn delete_db_instance(
        &self,
        instance_identifier: &str,
    ) -> Result<DeleteDbInstanceOutput, SdkError<DeleteDBInstanceError>> {
        self.inner
            .delete_db_instance()
            .db_instance_identifier(instance_identifier)
            .skip_final_snapshot(true)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.delete_db_instance.wrapper]

    // snippet-start:[rust.aurora.delete_db_cluster.wrapper]
```

```
    pub async fn delete_db_cluster(
        &self,
        cluster_identifier: &str,
    ) -> Result<DeleteDbClusterOutput, SdkError<DeleteDBClusterError>> {
        self.inner
            .delete_db_cluster()
            .db_cluster_identifier(cluster_identifier)
            .skip_final_snapshot(true)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.delete_db_cluster.wrapper]

    // snippet-start:[rust.aurora.delete_db_cluster_parameter_group.wrapper]
    pub async fn delete_db_cluster_parameter_group(
        &self,
        name: &str,
    ) -> Result<DeleteDbClusterParameterGroupOutput,
 SdkError<DeleteDBClusterParameterGroupError>>
    {
        self.inner
            .delete_db_cluster_parameter_group()
            .db_cluster_parameter_group_name(name)
            .send()
            .await
    }
    // snippet-end:[rust.aurora.delete_db_cluster_parameter_group.wrapper]
}
```

Die Datei „Cargo.toml“ mit in diesem Szenario verwendeten Abhängigkeiten.

```
[package]
name = "aurora-code-examples"
authors = [
  "David Souther <dpsouth@amazon.com>",
]
edition = "2021"
version = "0.1.0"

# See more keys and their definitions at https://doc.rust-lang.org/cargo/
reference/manifest.html
```

```
[dependencies]
anyhow = "1.0.75"
assert_matches = "1.5.0"
aws-config = { version = "1.0.1", features = ["behavior-version-latest"] }
aws-smithy-types = { version = "1.0.1" }
aws-smithy-runtime-api = { version = "1.0.1" }
aws-sdk-rds = { version = "1.3.0" }
inquire = "0.6.2"
mockall = "0.11.4"
phf = { version = "0.11.2", features = ["std", "macros"] }
sdk-examples-test-utils = { path = "../../test-utils" }
secrecy = "0.8.0"
tokio = { version = "1.20.1", features = ["full", "test-util"] }
tracing = "0.1.37"
tracing-subscriber = { version = "0.3.15", features = ["env-filter"] }
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zu AWS - SDK für Rust.
  - CreateDBCluster
  - DB-Gruppe erstellt ClusterParameter
  - DB wurde erstellt ClusterSnapshot
  - CreateDBInstance
  - DeleteDBCluster
  - DB-Gruppe gelöscht ClusterParameter
  - DeleteDBInstance
  - Beschriebene ClusterParameter DB-Gruppen
  - BeschriebenDB ClusterParameters
  - BeschriebenB ClusterSnapshots
  - DescribeDBClusters
  - BeschriebenB EngineVersions
  - DescribeDBInstances
  - DescribeOrderableDB InstanceOptions
  - DB-Gruppe ändern ClusterParameter

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwenden dieses Dienstes mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Serviceübergreifende Beispiele für Aurora mit SDKs AWS

Die folgenden Beispielanwendungen verwenden AWS SDKs, um Aurora mit anderen AWS-Services zu kombinieren. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zur Einrichtung und Ausführung der Anwendung finden.

Beispiele

- Leihbibliothek-REST-API erstellen
- Erstellen eines Trackers für Aurora-Serverless-Arbeitsaufgaben

Leihbibliothek-REST-API erstellen

Im folgenden Codebeispiel wird veranschaulicht, wie man eine Leihbibliothek erstellt, in der Kunden Bücher mithilfe einer REST-API ausleihen und zurückgeben können, die von einer Amazon-Aurora-Datenbank unterstützt wird.

Python

SDK für Python (Boto3)

Zeigt, wie die AWS SDK for Python (Boto3) mit der Amazon Relational Database Service (Amazon RDS) API und AWS Chalice verwendet wird, um eine REST-API zu erstellen, die von einer Amazon Aurora Aurora-Datenbank unterstützt wird. Der Webservice ist vollständig Serverless und stellt eine einfache Leihbibliothek dar, in der die Kunden Bücher ausleihen und zurückgeben können. Lernen Sie Folgendes:

- Erstellen und verwalten Sie einen Serverless-Aurora-Datenbank-Cluster.
- Wird AWS Secrets Manager zur Verwaltung von Datenbankanmeldedaten verwendet.
- Implementieren Sie einen Datenspeicher-Layer, der Amazon RDS verwendet, um Daten in die und aus der Datenbank zu verschieben.
- Verwenden Sie AWS Chalice, um eine serverlose REST-API für Amazon API Gateway bereitzustellen und. AWS Lambda
- Verwenden Sie das Anforderungspaket, um Anfragen an den Webservice zu senden.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter. GitHub

In diesem Beispiel verwendete Dienste

- API Gateway
- Aurora
- Lambda
- Secrets Manager

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen eines Trackers für Aurora-Serverless-Arbeitsaufgaben

Die folgenden Code-Beispiele zeigen, wie eine Webanwendung erstellt wird, die Arbeitselemente in einer Amazon Aurora Serverless-Datenbank verfolgt und mithilfe von Amazon Simple Email Service (Amazon SES) Berichte sendet.

.NET

AWS SDK for .NET

Zeigt, wie Sie mithilfe von Amazon Simple Email Service (Amazon SES) eine Webanwendung erstellen, die Arbeitsaufgaben in einer Amazon Aurora Aurora-Datenbank nachverfolgt und Berichte per E-Mail versendet. AWS SDK for .NET In diesem Beispiel wird ein mit React.js erstelltes Frontend verwendet, um mit einem RESTful-.NET-Backend zu interagieren.

- Integrieren Sie eine React-Webanwendung in AWS Dienste.
- Auflisten, Hinzufügen, Aktualisieren und Löschen von Elementen in einer Aurora-Tabelle.
- Senden Sie einen E-Mail-Bericht über gefilterte Arbeitselemente mit Amazon SES.
- Stellen Sie Beispielressourcen mit dem mitgelieferten AWS CloudFormation Skript bereit und verwalten Sie sie.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

C++

SDK für C++

Zeigt, wie eine Webanwendung erstellt wird, die in einer Amazon-Aurora-Serverless-Datenbank gespeicherte Arbeitselemente verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer C++-REST-API, die Amazon Aurora Aurora-Serverless-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

Java

SDK für Java 2.x

Zeigt, wie eine Webanwendung erstellt wird, die Arbeitselemente, die in einer Amazon RDS-Datenbank gespeichert sind, verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer Spring REST-API, die Amazon Aurora Aurora-Serverless-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

Den vollständigen Quellcode und Anweisungen zum Einrichten und Ausführen eines Beispiels, das die JDBC-API verwendet, finden Sie im vollständigen Beispiel unter. GitHub

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

JavaScript

SDK für JavaScript (v3)

Zeigt, wie Sie mit AWS SDK for JavaScript (v3) eine Webanwendung erstellen, die Arbeitsaufgaben in einer Amazon Aurora Aurora-Datenbank verfolgt und Berichte mithilfe von Amazon Simple Email Service (Amazon SES) per E-Mail versendet. In diesem Beispiel wird ein mit React.js erstelltes Frontend verwendet, um mit einem Express-Node.js-Backend zu interagieren.

- Integrieren Sie eine React.js Webanwendung mit AWS-Services.
- Auflisten, hinzufügen und aktualisieren von Elementen in einer Aurora-Tabelle.
- Senden Sie einen E-Mail-Bericht über gefilterte Arbeitselemente mit Amazon SES.
- Stellen Sie Beispielressourcen mit dem mitgelieferten AWS CloudFormation Skript bereit und verwalten Sie sie.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

Kotlin

SDK für Kotlin

Zeigt, wie eine Webanwendung erstellt wird, die Arbeitselemente, die in einer Amazon RDS-Datenbank gespeichert sind, verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer Spring REST-API, die Amazon Aurora Aurora-Serverless-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

PHP

SDK für PHP

Zeigt, wie Sie mithilfe von Amazon Simple Email Service (Amazon SES) eine Webanwendung erstellen, die Arbeitselemente in einer Amazon RDS-Datenbank verfolgt und Berichte per E-Mail versendet. AWS SDK for PHP In diesem Beispiel wird ein mit React.js erstelltes Frontend verwendet, um mit einem RESTful-PHP-Backend zu interagieren.

- Integrieren Sie eine React.js -Webanwendung in AWS Dienste.
- In einer Amazon-RDS-Tabelle können Sie Elemente auflisten, aktualisieren und löschen.
- Senden Sie einen E-Mail-Bericht über gefilterte Arbeitselemente mit Amazon SES.
- Stellen Sie Beispielressourcen mit dem mitgelieferten AWS CloudFormation Skript bereit und verwalten Sie sie.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

Python

SDK für Python (Boto3)

Zeigt, wie Sie mithilfe von Amazon Simple Email Service (Amazon SES) einen REST-Service erstellen, der Arbeitselemente in einer Amazon Aurora Aurora-Serverless-Datenbank nachverfolgt und Berichte per E-Mail versendet. AWS SDK for Python (Boto3) In diesem Beispiel wird das Flask-Web-Framework für das HTTP-Routing verwendet und in eine React-Webseite integriert, um eine voll funktionsfähige Webanwendung zu präsentieren.

- Erstellen Sie einen Flask-REST-Service, der sich in integrieren lässt. AWS-Services
- Lesen, schreiben und aktualisieren Sie Arbeitsaufgaben, die in einer Aurora-Serverless-Datenbank gespeichert sind.
- Erstellen Sie ein AWS Secrets Manager Geheimnis, das Datenbankanmeldedaten enthält, und verwenden Sie es, um Aufrufe an die Datenbank zu authentifizieren.
- Verwenden Sie Amazon SES, um E-Mail-Berichte über Arbeitsaufgaben zu senden.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwenden dieses Dienstes mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Bewährte Methoden mit Amazon Aurora

Nachstehend finden Sie Informationen zu allgemeinen bewährten Methoden und zu Optionen für die Verwendung oder Migration von Daten zu einem Amazon Aurora-DB-Cluster.

Einige der bewährten Methoden für Amazon Aurora sind spezifisch für eine bestimmte Datenbank-Engine. Weitere Informationen zu den bewährten Methoden in Aurora für eine spezifische Datenbank-Engine finden Sie im Folgenden.

Datenbank-Engine	Bewährte Methoden
Amazon Aurora MySQL	Siehe Bewährte Methoden mit Amazon Aurora MySQL
Amazon Aurora PostgreSQL	Siehe Bewährte Methoden mit Amazon Aurora PostgreSQL

> **Note**
>
> Allgemeine Empfehlungen für Aurora finden Sie unter Anzeigen und Beantworten von Amazon-Aurora-Empfehlungen.

Themen

- Grundlegende Anleitungen für Amazon Aurora
- RAM-Empfehlungen für DB-Instances
- AWS Datenbanktreiber
- Überwachen von Amazon Aurora
- Arbeiten mit DB-Parametergruppen und DB-Cluster-Parametergruppen
- Video zu bewährten Amazon-Aurora-Methoden

Grundlegende Anleitungen für Amazon Aurora

Im Folgenden finden Sie einige grundlegende Anleitungen für die Ausführung, die bei der Arbeit mit Amazon Aurora befolgt werden sollten. Das Amazon RDS Service Level Agreement setzt voraussetzt, dass Sie diese Anleitungen befolgen:

- Sie müssen die Nutzung von Arbeitsspeicher, CPU und Speicher überwachen. Sie können Amazon so einrichten CloudWatch , dass Sie benachrichtigt werden, wenn sich die Nutzungsmuster ändern oder wenn Sie sich der Kapazität Ihrer Bereitstellung nähern. Auf diese Weise können Sie leichter die Leistung und Verfügbarkeit des Systems wahren.
- Wenn Ihre Client-Anwendung die Domain Name Service (DNS) -Daten Ihrer DB-Instances zwischenspeichert, legen Sie einen time-to-live (TTL) -Wert von weniger als 30 Sekunden fest. Die zugrunde liegende IP-Adresse einer DB-Instance kann sich nach einem Failover ändern. Daher kann das Zwischenspeichern der DNS-Daten über einen längeren Zeitraum zu Verbindungsfehlern führen, wenn Ihre Anwendung versucht, eine Verbindung mit einer IP-Adresse herzustellen, die nicht mehr verwendet wird. Bei Aurora-DB-Clustern mit mehreren Lesereplikaten kann es auch zu Verbindungsfehlern kommen, wenn Verbindungen den Leser-Endpunkt verwenden und eine der Lesereplikat-Instances gewartet wird oder gelöscht wurde.
- Testen Sie den Failover für Ihren DB-Cluster, um zu verstehen, wie lange der Vorgang für Ihren Anwendungsfall dauert. Durch Testen des Failovers können Sie sicherstellen, dass die Anwendung, die auf Ihren DB-Cluster zugreift, nach dem Failover automatisch eine Verbindung zum neuen DB-Cluster herstellen kann.

RAM-Empfehlungen für DB-Instances

Um die Leistung zu optimieren, sollten Sie ausreichend RAM zuteilen, damit sich Ihr Arbeitssatz beinahe vollständig im Arbeitsspeicher befindet. Um festzustellen, ob Ihr Arbeitssatz fast vollständig im Arbeitsspeicher ist, überprüfen Sie die folgenden Kennzahlen in Amazon CloudWatch:

- `VolumeReadIOPS`: Diese Metrik misst die durchschnittliche Anzahl von I/O-Lesevorgängen aus einem Cluster-Volume, die in 5-minütigen Intervallen gemeldet werden. Der Wert für `VolumeReadIOPS` sollte klein und stabil sein. In einigen Fällen stellen Sie möglicherweise fest, dass Ihre Lese-I/O steil ansteigt oder höher ist als üblich. Untersuchen Sie in diesem Fall die DB-Instances in Ihrem DB-Cluster, um festzustellen, welche DB-Instances die erhöhte I/O verursachen.

> **Tip**
>
> Wenn Ihr Aurora MySQL Cluster eine parallele Abfrage verwendet, wird möglicherweise eine Zunahme der `VolumeReadIOPS`-Werte. Parallel Query verwendet den Bufferpool nicht. Obwohl die Abfragen schnell sind, kann diese optimierte Verarbeitung zu einem Anstieg der Lesevorgänge und damit verbundenen Gebühren führen.

- `BufferCacheHitRatio`: Diese Metrik misst den Prozentsatz der Anfragen, die vom Puffer-Cache einer DB-Instance in Ihrem DB-Cluster verarbeitet werden. Diese Metrik stellt Ihnen Einsichten in die Menge der Daten bereit, die vom Arbeitsspeicher bereitgestellt werden.

  Eine hohe Trefferrate bedeutet, dass Ihre DB-Instance über genügend Speicher verfügt. Wenn die Trefferrate niedrig ist, zeigt dies an, dass Ihre Abfragen für diese DB-Instance häufig zum Datenträger geleitet werden. Untersuchen Sie den Workload darauf, welche Abfragen dieses Verhalten verursachen.

Wenn Sie aufgrund der Untersuchung des Workloads feststellen, dass Sie mehr Arbeitsspeicher benötigen, sollten Sie erwägen, die DB-Instance-Klasse auf eine Klasse mit mehr RAM zu skalieren. Anschließend können Sie die voranstehend beschriebene Metrik untersuchen und weiter skalieren wie erforderlich. Wenn Ihr Aurora-Cluster größer als 40 TB ist, verwenden Sie nicht die Instanzklassen db.t2, db.t3 oder db.t4g.

Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken für Amazon Aurora.

AWS Datenbanktreiber

Wir empfehlen die AWS Treibersuite für die Anwendungskonnektivität. Die Treiber wurden so konzipiert, dass sie schnellere Switchover- und Failover-Zeiten sowie Authentifizierung mit AWS Secrets Manager, AWS Identity and Access Management (IAM) und Federated Identity unterstützen. Die AWS Treiber sind darauf angewiesen, den Status des DB-Clusters zu überwachen und die Clustertopologie zu kennen, um den neuen Writer zu ermitteln. Dieser Ansatz reduziert die Switchover- und Failover-Zeiten auf einstellige Sekunden, im Vergleich zu mehreren zehn Sekunden bei Open-Source-Treibern.

Im Zuge der Einführung neuer Servicefunktionen besteht das Ziel der AWS Treibersuite darin, eine integrierte Unterstützung für diese Servicefunktionen zu bieten.

Weitere Informationen finden Sie unter Mit den AWS Treibern eine Verbindung zu Aurora-DB-Clustern herstellen.

Überwachen von Amazon Aurora

Amazon Aurora stellt verschiedene Metriken und Erkenntnisse bereit, die Sie überwachen können, um den Zustand und die Leistung Ihres Aurora-DB-Clusters zu ermitteln. Sie können verschiedene Tools wie die, und CloudWatch API verwenden AWS Management Console AWS CLI, um Aurora-

Metriken anzuzeigen. Sie können die kombinierten Performance Insights und CloudWatch Metriken im Performance Insights Insights-Dashboard einsehen und Ihre DB-Instance überwachen. Performance Insights muss für Ihre DB-Instance aktiviert sein, damit diese Ansicht verwendet werden kann. Weitere Informationen zu dieser Überwachungsansicht finden Sie unter Anzeigen von kombinierten Metriken in der Amazon-RDS-Konsole.

Sie können einen Leistungsanalysebericht für einen bestimmten Zeitraum erstellen und sich die ermittelten Erkenntnisse und Empfehlungen zur Lösung der Probleme ansehen. Weitere Informationen finden Sie unter Erstellen eines Leistungsanalyseberichts.

Arbeiten mit DB-Parametergruppen und DB-Cluster-Parametergruppen

Es wird empfohlen, Änderungen für DB-Parametergruppen und DB-Cluster-Parametergruppen in einem DB-Test-Cluster zu testen, bevor Sie Änderungen für Parametergruppen auf Ihr DB-Produktions-Cluster anwenden. Wenn die Parameter für eine DB-Engine falsch festgelegt werden, kann dies unbeabsichtigte nachteilige Auswirkungen haben, einschließlich einer reduzierten Leistung und Systeminstabilität.

Gehen Sie stets vorsichtig vor, wenn Sie DB-Engine-Parameter ändern, und sichern Sie Ihren DB-Cluster, bevor Sie eine DB-Parametergruppe ändern. Informationen zum Sichern eines DB-Clusters finden Sie unter Sichern und Wiederherstellen eines Amazon-Aurora-DB-Clusters.

Video zu bewährten Amazon-Aurora-Methoden

Der Kanal AWS Online Tech Talks auf YouTube umfasst eine Videopräsentation mit bewährten Methoden für die Erstellung und Konfiguration eines Amazon Aurora Aurora-DB-Clusters, um sicherer und hochverfügbar zu sein. Siehe Bewährte Methoden für die Hochverfügbarkeit von Amazon Aurora.

Durchführen eines Machbarkeitsnachweises mit Amazon Aurora

Im Folgenden wird beschrieben, wie ein Machbarkeitsnachweises für Aurora eingerichtet und ausgeführt wird. Ein Machbarkeitsnachweis ist eine Untersuchung, die Sie selbst durchführen, um herauszufinden, ob Aurora für Ihre Anwendung geeignet ist. Mithilfe des Machbarkeitsnachweises können Sie die Aurora-Funktionen leichter im Rahmen Ihrer eigenen Datenbankanwendungen verstehen und Aurora mit Ihrer aktuellen Datenbankumgebung vergleichen. Er kann auch aufzeigen, wie groß der erforderliche Aufwand für das Verschieben von Daten, Portieren von SQL-Code, Leistungsoptimierung und Anpassen Ihrer aktuellen Verwaltungsverfahren ist.

In diesem Thema finden Sie eine Übersicht und einen step-by-step Überblick über die wichtigsten Verfahren und Entscheidungen im Zusammenhang mit der Ausführung eines Machbarkeitsnachweises, die im Folgenden aufgeführt sind. Eine ausführliche Anleitung finden Sie unter den Links zur vollständigen Dokumentation für bestimmte Themen.

Übersicht über einen Aurora-Machbarkeitsnachweis

Wenn Sie einen Machbarkeitsnachweis für Amazon Aurora durchführen, lernen Sie, was mit dem Portieren Ihrer vorhanden Daten und SQL-Anwendungen zu Aurora verbunden ist. Sie üben die wichtigsten Aspekte von Aurora im großen Umfang unter Verwendung eines Datenvolumens und von Aktivitäten, die für Ihre Produktionsumgebung repräsentativ sind. Ziel ist es, sich davon zu überzeugen, dass die Vorteile von Aurora den Herausforderungen gewachsen sind, denen Ihre vorherige Datenbankinfrastruktur nicht mehr gerecht wurde. Am Ende des Machbarkeitsnachweises haben Sie einen gründlichen Plan für die Durchführung von Benchmark-Tests und Anwendungstests im größeren Maßstab. An dieser Stelle haben Sie eine Vorstellung von den wichtigsten Arbeitsschritten auf Ihrem Weg zu einer Produktionsbereitstellung.

Mit den folgenden Ratschlägen zu bewährten Methoden lassen sich geläufige Fehler vermeiden, die beim Durchführen von Benchmark-Tests Probleme bereiten können. Dieses Thema behandelt jedoch nicht den step-by-step Prozess der Durchführung von Benchmarks und der Leistungsoptimierung. Diese Verfahren hängen von Ihrer Workload ab und welche Aurora-Funktionen Sie benutzen. Detaillierte Informationen können Sie der leistungsbezogenen Dokumentation entnehmen, z. B. Verwalten von Performance und Skalierung für einen Aurora-DB-Cluster, Amazon Aurora MySQL-Leistungserweiterungen, Verwalten von Amazon Aurora PostgreSQL und Überwachung mit Performance Insights auf .

Die Informationen in diesem Thema gelten hauptsächlich für Anwendungen, bei denen Ihre Organisation den Code verfasst und das Schema entwirft und von denen die MySQL- und PostgreSQL-Open-Source-Datenbank-Engines unterstützt werden. Wenn Sie eine kommerzielle Anwendung testen oder eine Anwendung, die von einem Anwendungs-Framework generiert wurde, haben Sie möglicherweise nicht die Flexibilität, alle Richtlinien anzuwenden. Erkundigen Sie sich in solchen Fällen bei Ihrem AWS-Mitarbeiter, ob für Ihren Typ von Anwendung bewährte Methode für Aurora oder Fallbeispiele vorhanden sind.

1. Identifizieren Ihrer Ziele

Wenn Sie Aurora als Teil des Machbarkeitsnachweises auswerten, wählen Sie die vorzunehmenden Messungen aus und wie der Erfolg der Übung zu bewerten ist.

Sie müssen sicherstellen, dass die gesamte Funktionalität Ihre Anwendung mit Aurora kompatibel ist. Da die Aurora-Hauptversionen wire-kompatibel mit entsprechenden Hauptversionen von MySQL und PostgreSQL sind, sind die meisten für diese Engines entwickelten Anwendungen ebenfalls mit Aurora kompatibel. Sie müssen die Kompatibilität jedoch weiterhin je nach Anwendung validieren.

So wirken sich beispielsweise einige der Konfigurationsoptionen, die Sie beim Einrichten eines Aurora-Clusters ausgewählt haben, darauf aus, ob Sie bestimmte Datenbankfunktionen verwenden können oder sollten. Sie können mit einem Aurora-Allzweck-Cluster beginnen der als bereitgestellt bezeichnet wird. Danach können Sie entscheiden, ob eine spezialisierte Konfiguration wie z. B. Serverless oder Parallelabfrage Vorteile für Ihre Workload bietet.

Anhand der folgenden Fragen können Sie Ihre Ziele leichter identifizieren und quantifizieren:

- Unterstützt Aurora alle funktionalen Anwendungsfälle Ihrer Workload?
- An welcher Datensatzgröße und Laststufe sind Sie interessiert? Können Sie auf diese Stufe skalieren?
- Was sind Ihre spezifischen Anforderungen für Abfragedurchsatz und Latenz? Können Sie sie erreichen?
- Was ist die akzeptable Mindestmenge an geplanten oder nicht geplanten Ausfallzeiten für Ihre Workload? Können Sie sie erzielen?
- Was sind die erforderlichen Metriken für Betriebseffizienz? Können Sie sie genau überwachen?
- Unterstützt Aurora Ihre spezifischen geschäftlichen Ziele, z. B. Kostenreduzierung, Zunahme der Bereitstellung oder Bereitstellungsgeschwindigkeit? Haben Sie eine Methode zur Quantifizierung dieser Ziele?

- Können Sie alle Sicherheits- und Compliance-Anforderung für Ihre Workload erfüllen?

Nehmen Sie sich etwas Zeit, sich mit Aurora-Datenbank-Engines und -Plattformfunktionen weiter vertraut zu machen, und sehen Sie Servicedokumentation ein. Notieren Sie sich alle Funktionen, die Ihnen helfen können, die von Ihnen angestrebten Ergebnisse zu erzielen. Eine dieser Funktionen könnte die Workload-Konsolidierung sein, die im AWS Database Blog-Beitrag How to plan and optimize Amazon Aurora with MySQL compatibility for consolidated workloads beschrieben wird. Eine andere könnte bedarfsorientierte Skalierung sein, die unter Verwenden von Amazon Aurora Auto Scaling mit Aurora Replicas im Amazon Aurora Benutzerhandbuch beschrieben wird. Weitere mögliche Funktionen sind Steigerung der Performance und vereinfachte Datenbankoperationen.

2. Verständnis der Workload-Eigenschaften

Bewerten Sie Aurora im Kontext Ihres beabsichtigten Anwendungsfalls. Aurora ist eine gute Wahl für Online-Transaktionsverarbeitungs-Workloads (OLTP). Sie können auch Berichte für den Cluster mit den Echtzeit-OLTP-Daten ausführen, ohne einen separaten Data Warehouse-Cluster bereitzustellen. Sie können erkennen, ob Ihr Anwendungsfall in diese Kategorien fällt, indem Sie die folgenden Merkmale überprüfen:

- Hohe Parallelität mit Dutzenden, Hunderten oder Tausenden gleichzeitigen Clients.
- Großes Volumen von schneller Abfragen (Millisekunden bis Sekunden).
- Kurze Echtzeit-Transaktionen.
- Hoch selektive Abfragemuster mit indexbasierten Suchvorgängen.
- Für HTAP können analytische Abfragen die Vorteile der Parallelabfrage von Aurora nutzen.

Einer der Schlüsselfaktoren, der bei der Auswahl Ihrer Datenbankoptionen eine Rolle spielt, ist die Geschwindigkeit der Daten. Hohe Geschwindigkeit bedeutet, dass Daten sehr häufig eingefügt und aktualisiert werden. Ein solches System kann Tausende von Verbindungen und Hunderttausende gleichzeitiger Abfragen haben, die gleichzeitig aus einer Datenbank gelesen und in sie geschrieben werden. Abfragen bei Systemen hoher Geschwindigkeit betreffen gewöhnlich eine relativ kleine Anzahl von Zeilen und greifen in der Regel auf mehrere Spalten in derselben Zeile zu.

Aurora ist auf die Verarbeitung von Daten hoher Geschwindigkeit ausgelegt. Abhängig von der Workload kann ein Aurora-Cluster mit einer einzigen r4.16xlarge-DB-Instance mehr als 600.000 `SELECT`-Anweisungen pro Sekunden verarbeiten. Auch hier kann ein solcher Cluster je nach Workload 200.000 `INSERT`, `UPDATE` und `DELETE`-Anweisungen pro Sekunde verarbeiten. Aurora

ist eine Zeilenspeicher-Datenbank und eignet sich ideal für hochvolumige, hochdurchsatzstarke und hochgradig parallelisierte OLTP-Workloads.

Aurora kann außerdem Berichtsabfragen in demselben Cluster durchführen, der die OLTP-Workload verarbeitet. Aurora unterstützt bis zu 15 Replikate, die jeweils innerhalb von 10-20 Millisekunden der primären Instance liegen. Analysten können OLTP-Daten in Echtzeit abfragen, ohne die Daten in einen separaten Data Warehouse-Cluster kopieren zu müssen. Mit Aurora-Clustern, die die Parallelabfragefunktion nutzen, können Sie viele der Verarbeitungs-, Filterungs- und Aggregationsvorgänge in das stark verteilte Aurora-Speichersubsystem verlagern.

Verwenden Sie diese Planungsphase, um sich mit den Funktionen von Aurora, anderen AWS Management Console-Services, der AWS und der AWS CLI vertraut zu machen. Finden Sie auch heraus, wie diese mit anderen Tools funktionieren, die Sie bei dem Machbarkeitsnachweis verwenden möchten.

3. Durchführen einer Übung mit der AWS Management Console oder der AWS CLI

Führen Sie als nächster Schritt eine Übung mit der AWS Management Console oder der AWS CLI durch, um sich mit diesen Tools und mit Aurora vertraut zu machen.

Durchführen einer Übung mit der AWS Management Console

Die folgenden anfänglichen Aktivitäten mit Aurora-Datenbank-Clustern sollen Ihnen in erster Linie Gelegenheit geben, sich mit der AWS Management Console-Umgebung vertraut zu machen und sich im Einrichten und Ändern von Aurora-Clustern zu üben. Wenn Sie die MySQL-kompatiblen und PostgreSQL-kompatiblen Datenbank-Engines mit Amazon RDS verwenden, kommen Ihnen diese Kenntnisse bei der Verwendung von Aurora zugute.

Durch Nutzung des freigegebenen Speichermodells von Aurora und von Funktionen wie Replikation und Snapshots können Sie gesamte Datenbank-Cluster wie andere Arten von Objekten verwenden, die Sie ganz nach Wunsch bearbeiten. Sie können Aurora-Cluster während des Machbarkeitsnachweises einrichten, außer Betrieb nehmen und ihre Kapazität häufig ändern. Sie sind nicht an frühzeitige Entscheidungen bezüglich Kapazität, Datenbankeinstellungen und physisches Daten-Layout gebunden.

Richten Sie zum Einsteig einen leeren Aurora-Cluster ein. Wählen Sie als Kapazitätstyp provisioned (bereitgestellt) und unter regional den Standort für Ihre anfänglichen Experimente aus.

Stellen Sie mit einem Client-Programm, wie z. B. einer SQL-Befehlszeilen-Anwendung, eine Verbindung mit diesem Cluster her. Anfänglich stellen Sie eine Verbindung über den Cluster-Endpunkt her. Sie stellen eine Verbindung mit diesem Endpunkt her, um Schreibvorgänge wie Data Definition Language (DDL)-Anweisungen und Extract, Transform, Load (ETL)-Prozesse durchzuführen. An späterer Stelle im Machbarkeitsnachweis verbinden Sie abfrageintensive Sitzungen über den Reader-Endpunkt, der die Abfrage-Workload über mehrere DB-Instances im Cluster verteilt.

Skalieren Sie den Cluster horizontal, indem Sie weitere Aurora Replicas hinzufügen. Informationen zu diesen Verfahren finden Sie unter Replikation mit Amazon Aurora. Skalieren Sie die DB-Instances horizontal nach oben oder unten, indem Sie die AWS-Instance-Klasse ändern. Verstehen Sie, wie Aurora diese Art von Vorgängen vereinfacht, sodass Sie später nicht wieder von vorne beginnen müssen, sollte Ihre anfängliche Schätzung der Systemkapazität falsch sein.

Erstellen Sie einen Snapshot und stellen Sie ihn in einem anderen Cluster wieder her.

Stellen Sie durch Untersuchen der Cluster-Metriken fest, welche Aktivitäten im Zeitverlauf auftreten und wie sich die Metriken auf die DB-Instances im Cluster beziehen.

Es ist hilfreich, sich damit vertraut zu machen, wie diese Aufgaben anfänglich über die AWS Management Console ausgeführt werden. Wenn Sie die Verwendungsmöglichkeiten von Aurora verstehen, können Sie dazu übergehen, diese Operationen mithilfe der AWS CLI zu automatisieren. In den folgenden Abschnitten finden Sie weitere Informationen zu den Verfahren und bewährten Methoden für diese Aktivitäten während des proof-of-concept Zeitraums.

Durchführen einer Übung mit der AWS CLI

Wir empfehlen, Bereitstellungs- und Verwaltungsverfahren auch in einer - proof-of-concept Einstellung zu automatisieren. Machen Sie sich hierzu mit der AWS CLI vertraut, sofern noch nicht geschehen. Wenn Sie die MySQL-kompatiblen und PostgreSQL-kompatiblen Datenbank-Engines mit Amazon RDS verwenden, kommen Ihnen diese Kenntnisse bei der Verwendung von Aurora zugute.

Aurora wirkt sich in der Regel auf Gruppen von DB-Instances aus, die als Cluster angeordnet sind. Viele Operationen bestehen daher daraus, zu bestimmen, welche DB-Instances zu einem Cluster gehören, und dann administrative Operationen als Schleife für alle Instances auszuführen.

Sie können beispielsweise Schritte automatisieren, um Aurora-Cluster zu erstellen und sie dann mit größeren Instance-Klassen nach oben oder mit zusätzlichen DB-Instances horizontal zu skalieren. Auf diese Weise können Sie beliebige Phasen des Machbarkeitsnachweises wiederholen und Was-wäre-wenn-Szenarien mit unterschiedlichen Konfigurationen von Aurora-Clustern zu erkunden.

Machen Sie sich mit den Fähigkeiten und Einschränkungen von Infrastruktur-Bereitstellungstools wie vertrau AWS CloudFormation. Möglicherweise stellen Sie fest, dass Aktivitäten, die Sie in einem proof-of-concept Kontext ausführen, nicht für den Produktionseinsatz geeignet sind. Das AWS CloudFormation-Verhalten bei Änderungen ist beispielsweise, eine neue Instance zu erstellen und die aktuelle Instance einschließlich ihrer Daten zu löschen. Weitere Einzelheiten zu diesem Verhalten finden Sie unter Aktualisierungsverhalten von Stack-Ressourcen im AWS CloudFormation-Benutzerhandbuch.

4. Erstellen Ihres Aurora-Clusters

Mit Aurora können Sie Was-wäre-wenn-Szenarien erkunden, indem Sie DB-Instances zum Cluster hinzufügen und die DB-Instances auf leistungsfähigere Instance-Klassen hochskalieren. Sie können auch Cluster mit anderen Konfigurationseinstellungen erstellen, um die gleiche Workload parallel auszuführen. Mit Aurora haben Sie sehr viel Flexibilität zum Einrichten, Außerbetriebnehmen und Neukonfigurieren von DB-Clustern. Vor diesem Hintergrund ist es hilfreich, diese Techniken in den Anfangsphasen des proof-of-concept Prozesses zu üben. Allgemeine Verfahren zum Erstellen von Aurora-Clustern finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Starten Sie nach Möglichkeit mit einem Cluster mit den folgenden Einstellungen. Überspringen Sie diesen Schritt nur, wenn Ihnen bestimmte Anwendungsfälle vorschweben. So können Sie diesen Schritt beispielsweise überspringen, wenn für Ihren Anwendungsfall eine besondere Art von Aurora-Cluster erforderlich ist. Oder Sie können ihn überspringen, wenn Sie an einer bestimmten Kombination von Datenbank-Engine und -Version interessiert sind.

- Deaktivieren Sie Easy create (Einfache Erstellung). Wir empfehlen, dass Sie sich für den Machbarkeitsnachweis über alle von Ihnen gewählten Einstellungen bewusst sind, sodass Sie anschließend identische oder geringfügig andere Cluster erstellen können.
- Verwenden Sie eine aktuelle DB-Engine-Version. Diese Kombinationen aus Datenbank-Engine und -Version bieten eine breite Kompatibilität mit anderen Aurora-Funktionen und eine erhebliche Kundennutzung für Produktionsanwendungen.
  - Aurora MySQL Version 3.x (MySQL 8.0-Kompatibilität)
  - Aurora PostgreSQL Version 15.x oder 16.x
- Wählen Sie die Vorlage Dev/Test. Diese Wahl ist für Ihre proof-of-concept Aktivitäten nicht von Bedeutung.

- Wählen Sie für DB instance class (DB-Instance-Klasse) die Option Memory optimized classes (Speicheroptimierte Klassen) und eine der xlarge-Instance-Klassen aus. Sie können die Instance-Klasse zu einem späteren Zeitpunkt nach oben oder unten skalieren.
- Wählen Sie unter Multi-AZ Deployment (Multi-AZ-Bereitstellung) die Option Create an Aurora Replica or Reader node in a different AZ (Aurora-Replikat- oder Reader-Knoten in anderer AZ erstellen) aus. Viele der nützlichsten Aspekte von Aurora betreffen Cluster aus mehreren DB-Instances. Es ist sinnvoll, immer mit mindestens zwei DB-Instances in einem neuen Cluster zu beginnen. Beim Testen unterschiedlicher Szenarien mit hoher Verfügbarkeit ist es hilfreich, für die zweite DB-Instance eine andere Availability Zone zu verwenden.
- Halten Sie sich bei der Wahl von Namen für die DB-Instances an eine generische Namenskonvention. Bezeichnen Sie keine Cluster-DB-Instance als „Writer“, da verschiedene DB-Instances diese Rollen nach Bedarf übernehmen. Wir empfehlen, so etwas wie `clustername-az-serialnumber` zu verwenden, z. B. `myprodappdb-a-01`. Durch diese Angaben werden die DB-Instance und ihre Platzierung eindeutig identifiziert.
- Legen Sie eine lange Aufbewahrungsfrist für Backups des Aurora-Clusters fest. Bei einem langen Aufbewahrungszeitraum können Sie die point-in-time Wiederherstellung (PITR) für einen Zeitraum von bis zu 35 Tagen durchführen. Sie können Ihre Datenbank nach dem Durchführen von Tests mit DDL- und Data Manipulation Language (DML)-Anweisungen auf einen bekannten Zustand zurücksetzen. Eine Wiederherstellung ist auch möglich, wenn Sie versehentlich Daten löschen oder ändern.
- Aktivieren Sie beim Erstellen des Clusters zusätzliche Wiederherstellungs-, Protokollierungs- und Überwachungsfunktionen. Aktivieren Sie alle Optionen, die unter Rückverfolgung, Performance Insights ,Überwachung und Protokollexporte verfügbar sind. Wenn diese Funktionen aktiviert sind, können Sie die Eignung von Funktionen wie Rückverfolgung, erweiterte Überwachung oder Performance Insights for Ihre Workload testen. Auf diese Weise lässt sich während des Machbarkeitsnachweises leicht die Leistung überprüfen und eine Fehlerbehebung durchführen.

5. Einrichten Ihres Schemas

Richten Sie im Aurora-Cluster Datenbanken, Tabellen, Indizes, Fremdschlüssel und andere Schemaobjekte für Ihre Anwendung ein. Wenn Sie bereits mit einem anderen MySQL-kompatiblen oder PostgreSQL-kompatiblen Datenbanksystem gearbeitet haben, ist zu erwarten, dass sich diese Phase einfach und schnell gestaltet. Sie verwenden für Ihre Datenbank-Engine die gleiche SQL-Syntax und Befehlszeile oder andere Client-Anwendungen, mit denen Sie vertraut sind.

Um SQL-Anweisungen in Ihrem Cluster auszugeben, identifizieren Sie den Cluster-Endpunkt und stellen Sie diesen Wert als Verbindungsparameter für Ihre Client-Anwendung bereit. Sie finden den Cluster-Endpunkt auf der Registerkarte Connectivity (Konnektivität) der Detailseite Ihres Clusters. Der Cluster-Endpunkt ist mit Writer beschriftet. Der andere mit Reader beschriftete Endpunkt stellt eine schreibgeschützte Verbindung dar, die Sie für Endbenutzer bereitstellen können, die Berichte oder andere schreibgeschützte Abfragen ausführen. Unterstützung bei Problemen mit dem Verbinden Ihres Clusters finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

Wenn Sie Ihr Schema und Ihre Daten von einem anderen Datenbanksystem portieren, müssen Sie an dieser Stelle wahrscheinlich einige Änderungen am Schema vornehmen. Diese Schemaänderungen sind entsprechend der SQL-Syntax und den Funktionen vorzunehmen, die in Aurora verfügbar sind. An dieser Stelle können Sie bestimmte Spalten, Einschränkungen, Auslöser oder andere Schemaobjekte weglassen. Dies kann insbesondere dann hilfreich sein, wenn für die Aurora-Kompatibilität Änderungen an Objekten erforderlich sind, die für Ihren beabsichtigten Machbarkeitsnachweis jedoch nicht signifikant sind.

Wenn Sie von einem Datenbanksystem mit einer anderen zugrunde liegenden Engine als der von Aurora migrieren, sollten Sie AWS Schema Conversion Tool (AWS SCT) verwenden, um den Prozess zu vereinfachen. Einzelheiten finden Sie im AWS-Schema-Conversion-Tool-Benutzerhandbuch. Allgemeine Informationen zu Migrations- und Portierungsaktivitäten finden Sie im AWS-Whitepaper Migration Ihrer Datenbanken auf Amazon Aurora.

Während dieser Phase können Sie Ihr Schema-Setup auf Ineffizienzen untersuchen, z. B. bei Ihrer Indizierungsstrategie oder bei anderen Tabellenstrukturen, wie z. B. partitionierten Tabellen. Solche Ineffizienzen können verstärkt werden, wenn Sie Ihre Anwendung auf einem Cluster mit mehreren DB-Instances und einer hohen Workload bereitstellen. Erwägen Sie, ob Sie solche Aspekte der Leistung zu diesem Zeitpunkt oder bei späteren Aktivitäten wie z. B. einem vollständigen Benchmark-Test, optimieren können.

6. Importieren Ihrer Daten

Während des Machbarkeitsnachweises verlagern Sie die Daten, oder eine repräsentative Stichprobe, von Ihrem ehemaligem Datenbanksystem. Richten Sie nach Möglichkeit mindestens einige Daten in Ihren Tabellen ein. Dadurch wird das Testen der Kompatibilität aller Datentypen und Schema-Funktionen ermöglicht. Wenn Sie eine Übung der grundlegenden Aurora-Funktionen durchgeführt haben, skalieren Sie die Datenmenge nach oben. Zu dem Zeitpunkt, wenn Sie Ihren Machbarkeitsnachweis fertigstellen, sollten Sie Ihre ETL-Tools, Abfragen und Gesamt-Workload mit einem Dataset testen, das groß genug für genaue Schlussfolgerungen ist.

Sie können mehrere Methoden zum Importieren von physischen oder logischen Sicherungsdaten in Aurora verwenden. Einzelheiten finden Sie unter Migrieren von Daten zu einem Amazon Aurora MySQL-DB-Cluster oder Migrieren von Daten nach Amazon Aurora mit PostgreSQL-Kompatibilität, abhängig von der Datenbank-Engine, die Sie bei dem Machbarkeitsnachweis verwenden.

Experimentieren Sie mit den ETL-Tools und Technologien, die Sie in Betracht ziehen. Sehen Sie, welche am besten Ihren Anforderungen genügen. Berücksichtigen Sie sowohl Durchsatz als auch Flexibilität. Einige ETL-Tools führen z. B. einmalige Übertragungen durch, während andere fortlaufende Replikationen von dem alten System zu Aurora umfassen.

Wenn Sie von einem MySQL-kompatiblen System zu Aurora MySQL migrieren, könne Sie die nativen Datenübertragungstools verwenden. Das Gleiche gilt, wenn Sie von einem PostgreSQL-kompatiblen System zu Aurora PostgreSQL migrieren. Wenn Sie von einem Datenbanksystem mit einer anderen zugrunde liegenden Engine als der von Aurora migrieren, können Sie mit AWS Database Migration Service (AWS DMS) experimentieren. Weitere Informationen zu AWS DMS finden Sie im AWS Database Migration Service-Benutzerhandbuch.

Einzelheiten zu Migrations- und Portierungsaktivitäten finden Sie im AWS-Whitepaper Aurora-Migrationshandbuch.

7. Portieren Ihres SQL-Codes

Der zum Ausprobieren von SQL und zugehörigen Anwendungen erforderliche Aufwand variiert je nach den unterschiedlichen Fällen. Der Aufwand ist insbesondere davon abhängig, ob Sie von einem MySQL-kompatiblen oder einem PostgreSQL-kompatiblen System oder von einer anderen Art von System portieren.

- Wenn Sie von RDS for MySQL oder RDS for PostgreSQL portieren, sind die SQL-Änderungen klein genug, sodass Sie den SQL-Originalcode mit Aurora ausprobieren und erforderliche Änderungen manuell einfügen können.
- Wenn Sie von einer lokalen Datenbank portieren, die mit MySQL oder PostgreSQL kompatibel ist, können Sie den SQL-Originalcode ebenfalls ausprobieren und erforderliche Änderungen manuell einfügen.
- Wenn Sie von einer anderen kommerziellen Datenbank portieren, sind die erforderlichen SQL-Änderungen etwas umfangreicher. Ziehen Sie in diesem Fall die Verwendung des in Betrach AWS SCT.

Während dieser Phase können Sie Ihr Schema-Setup auf Ineffizienzen untersuchen, z. B. bei Ihrer Indizierungsstrategie oder bei anderen Tabellenstrukturen, wie z. B. partitionierten Tabellen. Erwägen Sie, ob Sie solche Aspekte der Leistung zu diesem Zeitpunkt oder bei späteren Aktivitäten wie z. B. einem vollständigen Benchmark-Test, optimieren können.

Sie können die Logik der Datenbankverbindung in Ihrer Anwendung überprüfen. Um die Vorteile der verteilten Verarbeitung von Aurora nutzen zu können, müssen Sie möglicherweise separate Verbindungen für Lese- und Schreibvorgänge und relativ kurze Sitzungen für Abfrageoperationen verwenden. Weitere Informationen zu Verbindungen finden Sie unter 9. Verbinden mit Aurora.

Überlegen Sie, ob Sie Kompromisse eingehen und Abstriche machen müssen, um in Ihrer Produktionsdatenbank Probleme zu vermeiden. Integrieren Sie Zeit in den proof-of-concept Zeitplan, um Ihr Schemadesign und Ihre Abfragen zu verbessern. Um zu beurteilen, ob sich Leistung, Betriebskosten und Skalierbarkeit leicht verbessern lassen, probieren Sie die ursprünglichen und die abgewandelten Anwendungen nebeneinander in verschiedenen Aurora-Clustern aus.

Einzelheiten zu Migrations- und Portierungsaktivitäten finden Sie im AWS-Whitepaper Aurora-Migrationshandbuch.

8. Angeben der Konfigurationseinstellungen

Sie können im Rahmen der Aurora- proof-of-concept Übung auch Ihre Datenbankkonfigurationsparameter überprüfen. Sie haben Ihre MySQL- oder PostgreSQL-Konfigurationseinstellungen möglicherweise bereits für Leistung und Skalierbarkeit in Ihrer aktuellen Umgebung optimiert. Das Aurora-Speichersubsystem wird für eine verteilte Cloud-basierte Umgebung mit einem Speichersubsystem hoher Geschwindigkeit angepasst und optimiert. Dies hat zur Folge, dass viele ehemaligen Einstellungen der Datenbank-Engine nicht anwendbar sind. Wir empfehlen, Ihre anfänglichen Experimente mit Aurora-Standard-Konfigurationseinstellungen durchzuführen. Wenden Sie Einstellungen von Ihrer aktuellen Umgebung nur dann erneut an, falls Engpässe bezüglich der Leistung und Skalierbarkeit auftreten. Wenn Sie interessiert sind, können Sie sich unter Introducing the Aurora Storage Engine im AWS Database Blog näher mit diesem Thema beschäftigen.

Aurora erleichtert die Wiederverwendung der optimalen Konfigurationseinstellungen für eine bestimmte Anwendung oder einen bestimmten Anwendungsfall. Anstatt für jede DB-Instance eine separate Konfigurationsdatei zu bearbeiten, verwalten Sie Parametersätze, die Sie ganzen Clustern oder bestimmten DB-Instances zuweisen. So gilt die Zeitzoneneinstellung beispielsweise für alle DB-Instances im Cluster und Sie könne die Größeneinstellung des Seiten-Caches für jede DB-Instance anpassen.

Sie beginnen mit einem der Standard-Parametersätze und wenden nur auf die Parameter Änderungen an, die optimiert werden müssen. Details zur Arbeit mit Parametergruppen finden Sie unter Amazon Aurora-DB-Cluster und DB-Instance-Parameter. Konfigurationseinstellungen, die für Aurora-Cluster anwendbar oder nicht anwendbar sind, finden Sie unter Aurora MySQL Konfigurationsparameter oder Amazon-Aurora-PostgreSQL-Parameter, abhängig von Ihrer Datenbank-Engine.

9. Verbinden mit Aurora

Wie Sie beim Erstellen des anfänglichen Schemas und Daten-Setups und beim Ausführen von Beispielabfragen festgestellt haben, können Sie eine Verbindung mit verschiedenen Endpunkten in einem Aurora-Cluster herstellen. Welcher Endpunkt zu verwenden ist, hängt davon ab, ob die Operation ein Lesevorgang, wie z. B. eine `SELECT`-Anweisung, oder ein Schreibvorgang, wie z. B. eine `CREATE`- oder `INSERT`-Anweisung ist. Während Sie die Workload auf einem Aurora-Cluster erhöhen und mit Aurora-Funktionen experimentieren, ist es wichtig, dass Ihre Anwendung je Operation dem entsprechenden Endpunkt zuweist.

Indem Sie den Cluster-Endpunkt für Schreiboperationen verwenden, stellen Sie stets eine Verbindung mit einer DB-Instance in dem Cluster her, das eine Lese-Schreib-Funktionalität besitzt. Standardmäßig verfügt nur eine einzige DB-Instance in einem Aurora-Cluster über eine Lese-Schreib-Funktionalität. Diese DB-Instance wird als die primäre Instance bezeichnet. Wenn die ursprüngliche primäre Instance ausfällt, aktiviert Aurora einen Failover-Mechanismus und eine andere DB-Instance wird zur primären Instance.

Durch Weiterleiten von `SELECT`-Anweisungen an den Reader-Endpunkt verteilen Sie gleichermaßen die Arbeit von Verarbeitungsabfragen auf die DB-Instances im Cluster. Mithilfe der Round-Robin-DNS-Auflösung wird jede Reader-Verbindung einer anderen DB-Instance zugewiesen. Wenn die meisten Abfragevorgänge auf den schreibgeschützten DB-Aurora Replicas durchgeführt werden, verringert sich die Last auf der primären Instance, sodass sie mehr DDL- und DML-Anweisungen verarbeiten kann.

Durch Nutzung dieser Endpunkte wird die Abhängigkeit von hartcodierten Hostnamen reduziert und Ihre Anwendung kann bei DB-Instance-Ausfällen schneller wiederhergestellt werden.

> **Note**
>
> Aurora verfügt auch über benutzerdefinierte Endpunkte, die Sie erstellen. Diese Endpunkte müssen bei einem Machbarkeitsnachweis gewöhnlich nicht berücksichtigt werden.

Die Aurora Replicas unterliegen einer Replica-Verzögerung. Diese Verzögerung dauert gewöhnlich aber nur 10 bis 20 Milliseconds an. Sie können die Replikationsverzögerung überwachen und entscheiden, ob sie innerhalb des Bereichs Ihrer Datenkonsistenzanforderungen liegt. In einigen Fällen erfordern Ihre Leseabfragen möglicherweise eine starke Lesekonsistenz (read-after-write-Konsistenz). In diesen Fällen können Sie für sie weiterhin den Cluster-Endpunkt anstatt des Reader-Endpunkts verwenden.

Um die Aurora-Funktionen bei der verteilten Parallelausführung voll nutzen zu können, müssen Sie möglicherweise Änderungen an der Verbindungslogik vornehmen. Sie möchten vermeiden, dass alle Leseanforderungen an die primäre Instance gesendet werden. Die schreibgeschützten Aurora Replicas stehen mit genau denselben Daten für die Verarbeitung von `SELECT`-Anweisungen bereit. Kodieren Sie Ihre Anwendungslogik so, dass für jede Art von Vorgang der entsprechende Endpunkt verwendet wird. Befolgen Sie diese allgemeinen Richtlinien:

- Vermeiden Sie es, eine einzelne hartcodierte Verbindungszeichenfolge für alle Datenbanksitzungen zu verwenden.
- Sofern praktikabel, schließen Sie Schreiboperationen wie DDL- und DML-Anweisungen in Funktionen in Ihrem Client-Anwendungscode ein. Auf diese Weise können Sie bewirken, dass verschiedene Arten von Vorgängen bestimmte Verbindungen nutzen.
- Machen Sie separate Funktionen für Abfrageoperationen. Aurora weist jede neue Verbindung mit dem Reader-Endpunkt einem anderen Aurora-Replikat zu, um die Last leseintensiver Anwendungen auszugleichen.
- Schließen Sie bei Operationen mit Abfragesätzen die Verbindung mit dem Reader-Endpunkt und öffnen Sie sie erneut, wenn jeder Satz zugehöriger Abfragen abgeschlossen wurde. Nutzen Sie Verbindungspooling, sofern diese Funktion in Ihrem Software-Stack verfügbar ist. Durch die Weiterleitung von Abfragen zu verschiedenen Verbindungen kann Aurora die Lese-Workload leichter unter den DB-Instances im Cluster verteilen.

Allgemeine Informationen zur Verbindungsverwaltung und zu Endpunkten für Aurora finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster. Detaillierte Einblicke zu diesem Thema finden Sie in Aurora MySQL Database Administrator's Handbook – Connection Management.

10. Ausführen Ihrer Workload

Wenn Schema, Daten und Konfigurationseinstellungen vorhanden sind, können Sie mit der Arbeit mit dem Cluster beginnen, indem Sie Ihre Workload ausführen. Verwenden Sie im

Machbarkeitsnachweis eine Workload, die die Hauptaspekte Ihrer Produktions-Workload widerspiegelt. Wir empfehlen, Entscheidungen über die Leistung immer anhand von realen Tests und Workloads und nicht anhand von synthetischen Benchmark-Tests wie sysbench oder TPC-C zu treffen. Sammeln Sie, wo immer möglich, Messungen basierend auf Ihrem eigenen Schema, Abfragemustern und Nutzungsvolumen.

Sofern praktikabel, replizieren Sie die tatsächlichen Bedingungen, unter denen die Anwendung ausgeführt wird. Sie führen Ihren Anwendungscode beispielsweise gewöhnlich auf Amazon EC2-Instances in derselben AWS-Region und derselben Virtual Private Cloud (VPC) wie der Aurora-Cluster durch. Wenn Ihre Produktionsanwendung auf mehreren EC2-Instances ausgeführt wird, die sich über mehrere Availability Zones erstrecken, richten Sie Ihre proof-of-concept Umgebung auf die gleiche Weise ein. Weitere Informationen zu AWS-Regionen finden Sie unter Regionen und Availability Zones im Amazon-RDS-Benutzerhandbuch. Weitere Informationen zum Amazon VPC-Service finden Sie unter Was ist Amazon VPC? im Amazon VPC Benutzerhandbuch.

Nachdem Sie überprüft haben, dass die Grundfunktionen Ihrer Anwendung funktionieren und dass Sie über Aurora auf die Daten zugreifen können, können Sie mit Aspekten des Aurora-Clusters versuchsweise arbeiten. Einige Funktionen, die Sie ausführen sollten, sind gleichzeitige Verbindung mit Load Balancing, gleichzeitige Transaktionen und automatische Replikation.

An dieser Stelle sollten Sie mit den Mechanismen zur Datenübertragung vertraut sein und können mit einem größeren Teil von Beispieldaten Tests ausführen.

In dieser Phase sehen Sie die Auswirkungen von Änderungen an den Konfigurationseinstellungen, wie z. B. Speicherlimits und Verbindungslimits. Betrachten Sie sich erneut die Verfahren, die Sie unter erkundet habe 8. Angeben der Konfigurationseinstellungen.

Sie können auch mit Mechanismen wie Erstellen und Wiederherstellen von Snapshots experimentieren. So können Sie beispielsweise Cluster mit verschiedenen AWS-Instance-Klassen, einer unterschiedlichen Anzahl von AWS Replicas usw. erstellen. Sie können dann auf jedem Cluster den gleichen Snapshot mit Ihrem Schema und allen Ihren Daten wiederherstellen. Einzelheiten zu diesem Zyklus finden Sie unter Erstellen eines DB-Cluster-Snapshots and Wiederherstellen aus einem DB-Cluster-Snapshot.

11. Messen der Leistung

Die bewährten Methoden in diesem Bereich sollen sicherstellen, dass die richtigen Tools und Prozesse eingerichtet werden, um anormales Verhalten während Workload-Vorgängen schnell

aufzudecken. Sie sollen außerdem gut sichtbar sein, sodass Sie alle zutreffenden Ursachen zuverlässig identifizieren können.

Durch Ansicht der Registerkarte Monitoring (Überwachung) können Sie immer den aktuellen Zustand des Clusters sehen oder Trends im Zeitverlauf analysieren. Diese Registerkarte ist über die Detailseite der Konsole für jeden Aurora-Cluster oder jede DB-Instance verfügbar. Es zeigt Metriken aus dem Amazon- CloudWatch Überwachungsservice in Form von Diagrammen an. Sie können die Metriken nach Name, DB-Instance und Zeitraum filtern.

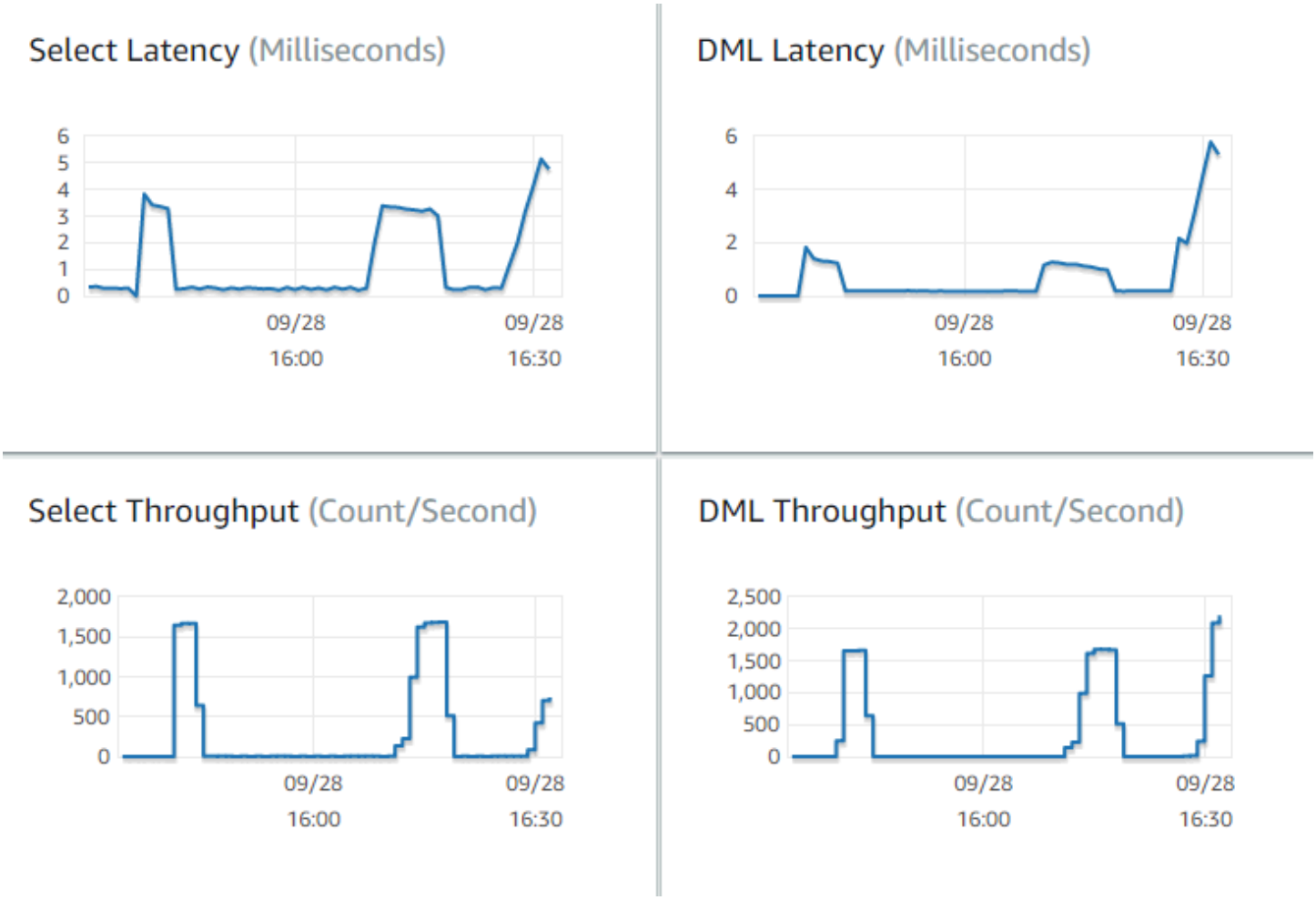
Wenn sich weitere Optionen auf der Registerkarte Monitoring (Überwachung) befinden, aktivieren Sie "Enhanced Monitoring (Erweiterte Überwachung)" und "Performance Insights" in den Cluster-Einstellungen. Sie können diese Optionen auch zu einem späteren Zeitpunkt aktvieren, sofern Sie sie beim Einrichten des Clusters nicht ausgewählt haben.

Zum Messen der Leistung stützen Sie sich größtenteils auf die Diagramme der Aktivitäten für den gesamten Aurora-Cluster. Sie können überprüfen, ob die Aurora Replicas ähnliche Lade- und Antwortzeiten aufweisen. Sie können auch erkennen, wie die Arbeit zwischen der primären Lese-Schreib-Instance und den schreibgeschützten Aurora-Replicas aufgeteilt wird. Bei einem Ungleichgewicht zwischen den DB-Instances oder bei einem Problem mit nur einer DB-Instance können Sie die Registerkarte Monitoring (Überwachung) bezüglich dieser spezifischen Instance untersuchen.

Nachdem die Umgebung und die tatsächliche Workload zum Emulieren Ihrer Produktionsumgebung eingerichtet wurden, können Sie die Leistung von Aurora messen. Die wichtigsten zu beantwortenden Fragen sind:

- Wie viele Abfragen pro Sekunden werden von Aurora verarbeitet? Sie können den Throughput (Durchsatz)-Metriken die Werte für verschiedene Arten von Vorgängen entnehmen.
- Wie lange braucht Aurora durchschnittlich zum Verarbeiten einer gegebenen Abfrage? Sie können den Latency (Latenz)-Metriken die Werte für verschiedene Arten von Vorgängen entnehmen.

Zeigen Sie hierzu wie nachfolgend dargestellt die Registerkarte Monitoring (Überwachung) für einen gegebenen Aurora-Cluster in der Amazon-RDS-Konsole an.



Wenn möglich, stellen Sie Baseline-Werte für diese Metriken in Ihrer aktuellen Umgebung auf. Wenn dies nicht praktikabel ist, erstellen Sie eine Baseline für den Aurora-Cluster, indem Sie eine Workload entsprechend Ihrer Produktionsanwendung ausführen. Führen Sie beispielsweise Ihre Aurora-Workload mit einer ähnlichen Anzahl gleichzeitiger Benutzer und Abfragen aus. Beobachten Sie dann, wie sich die Werte ändern, während Sie mit verschiedenen Instance-Klassen, Cluster-Größen, Konfigurationseinstellungen usw. experimentieren.

Wenn die Durchsatzwerte niedriger als erwartet sind, untersuchen Sie näher, welche Faktoren sich auf die Datenbank-Leistung Ihrer Workload auswirken. Untersuchen Sie höher als erwartete Latenzwerte gleichermaßen näher. Überwachen Sie hierzu die sekundären Metriken für den DB-Server (CPU, Arbeitsspeicher usw.). Sie können erkennen, ob sich die DB-Instances an ihre Grenzwerte annähern. Auch ist ersichtlich, über wie viel extra Kapazität Ihre DB-Instances für die Verarbeitung weiterer gleichzeitiger Abfragen, Abfragen großer Tabellen usw. verfügt.

> **Tip**
>
> Um Metrikwerte zu erkennen, die außerhalb des erwarteten Bereichs liegen, richten Sie CloudWatch Alarme ein.

Wenn Sie die ideale Aurora-Cluster-Größe und -Kapazität bewerten, können Sie herausfinden, mit welcher Konfiguration die Spitzenleistung der Anwendung erzielt wird, ohne unnötige Ressourcen bereitzustellen. Ein wichtiger Faktor ist, die angemessene Größe für die DB-Instances im Aurora-Cluster zu finden. Beginnen Sie mit der Wahl einer Instance-Größe mit einer ähnlichen CPU- und Arbeitsspeicher-Kapazität wie Ihre aktuelle Produktionsumgebung. Erfassen Sie Durchsatz- und Latenzwerte für die Workload bei dieser Instance-Größe. Skalieren Sie die Instance dann nach oben auf die nächste Größe. Überprüfen Sie, ob sich die Durchsatz- und Latenzwerte bessern. Skalieren Sie die Instance auch nach unten. Überprüfen Sie, ob die Latenz- und Durchsatzwerte gleich bleiben. Unser Ziel ist, den höchsten Durchsatz bei der geringsten Latenz für die kleinst mögliche Instance zu erreichen.

> **Tip**
>
> Bemessen Sie Ihre Aurora-Cluster und zugehörigen DB-Instances mit genug vorhandener Kapazität, um plötzlichen, nicht vorhersehbaren Datenverkehrsspitzen gewachsen zu sein. Belassen Sie für geschäftskritische Datenbanken mindestens 20 Prozent an Extrakapazität für CPU und Arbeitsspeicher.

Führen Sie Leistungstests lange genug aus, sodass die Datenbankleistung in einem warmen, stabilen Zustand gemessen wird. Sie müssen die Workload viele Minuten oder sogar einige Stunden lang ausführen, bis dieser stabile Zustand erreicht wird. Gewisse Abweichungen am Anfang der Ausführung sind normal. Diese Abweichungen sind dadurch bedingt, dass jedes Aurora Replica seinen Zwischenspeicher basierend auf den verarbeiteten `SELECT`-Abfragen aufwärmt.

Aurora weist die beste Leistung bei transaktionalen Workloads mit mehreren gleichzeitigen Benutzern und Abfragen auf. Um sicherzustellen, dass die verarbeitete Last für eine optimale Leistung ausreicht, führen Sie Benchmark-Tests mit Multithreading oder mehrere Instances von Leistungstests gleichzeitig aus. Messen Sie die Leistung mit Hunderten oder sogar Tausenden gleichzeitiger Client-Threads. Simulieren Sie die Anzahl gleichzeitiger Threads, die Sie in Ihrer Produktionsumgebung erwarten. Sie können auch zusätzliche Stresstests mit weiteren Threads durchführen, um die Aurora-Skalierbarkeit zu messen.

12. Ausführen der Aurora-Hochverfügbarkeit

Viele der Hauptfunktionen von Aurora umfassen hohe Verfügbarkeit. Zu diesen Funktionen gehören die automatische Replikation, das automatische Failover, automatische Backups mit point-in-time Wiederherstellung und die Möglichkeit, dem Cluster DB-Instances hinzuzufügen. Die Sicherheit und Zuverlässigkeit von Funktionen wie diesen ist für geschäftskritische Anwendungen wichtig.

Die Auswertung dieser Funktionen erfordert eine bestimmte Denkweise. Bei früheren Aktivitäten, wie Leistungsmessungen, beobachten Sie die Systemleistung, wenn alles richtig funktioniert. Beim Testen der hohen Verfügbarkeit müssen Sie Verhalten im Schlimmstfall durchdenken. Sie müssen sich verschiedene Arten von Fehlern vorstellen, selbst wenn solche Bedingungen nur selten auftreten. Sie führen möglicherweise absichtlich Probleme herbei, um sicherzustellen, dass der Systembetrieb richtig und schnell wiederhergestellt wird.

> **Tip**
>
> Richten Sie für einen Machbarkeitsnachweis alle DB-Instances in einem Aurora-Cluster mit derselben AWS-Instance-Klasse ein. Dadurch ist es möglich, Aurora-Verfügbarkeitsfunktionen ohne große Änderungen an der Leistung und Skalierbarkeit auszuprobieren, während Sie DB-Instances offline nehmen, um Fehler zu simulieren.

Wir empfehlen, in jedem Aurora-Cluster mindestens zwei Instances zu verwenden. Die DB-Instances in einem Aurora-Cluster können sich über bis zu drei Availability Zones (AZs) erstrecken. Suchen Sie jede der ersten zwei oder drei DB-Instances in einer anderen AZ. Wenn Sie mit der Verwendung größerer Cluster beginnen, verteilen Sie Ihre DB-Instances über alle AZs in Ihrer AWS-Region. Dadurch wird die Fähigkeit zur Fehlertoleranz erhöht. Wenn sich ein Problem auf die gesamte AZ auswirkt, kann Aurora ein Failover auf eine DB-Instance in einer anderen AZ durchführen. Wenn Sie einen Cluster mit mehr als drei Instances ausführen, verteilen Sie die DB-Instances so gleichmäßig wie möglich über alle drei AZs.

> **Tip**
>
> Der Speicher eines Aurora-Clusters ist unabhängig von den DB-Instances. Der Speicher eines jeden Aurora-Clusters erstreckt sich immer über drei AZs.
> Wenn Sie die Funktionen für hohe Verfügbarkeit testen, verwenden Sie immer DB-Instances mit identischer Kapazität in Ihrem Test-Cluster. Dadurch lassen sich unvorhersehbare

Änderungen in Leistung, Latenz usw. vermeiden, wenn eine DB-Instance die Rolle einer anderen übernimmt.

Informationen zum Simulieren von Fehlerbedingungen zum Testen von Funktionen für hohe Verfügbarkeit finden Sie unter Testen von Amazon Aurora MySQL unter Verwendung von Fehlersimulationsabfragen.

Im Rahmen Ihrer proof-of-concept Übung besteht ein Ziel darin, die ideale Anzahl von DB-Instances und die optimale Instance-Klasse für diese DB-Instances zu finden. Dazu müssen die Anforderungen für hohe Verfügbarkeit und für Leistung gegeneinander abgewogen werden.

Für Aurora gilt, dass je mehr DB-Instances sich in einem Cluster befinden, desto höher die Vorteile für hohe Verfügbarkeit sind. Mehr DB-Instances verbessern auch die Skalierbarkeit von leseintensiven Anwendungen. Aurora kann mehrere Verbindungen für `SELECT`-Abfragen unter den schreibgeschützten Aurora-Replikaten verteilen.

Andererseits wird durch Einschränken der Anzahl von DB-Instances der Replikationsdatenverkehr vom primären Knoten verringert. Der Replikationsdatenverkehr belegt Netzwerkbandbreite, wobei es sich um einen weiteren Aspekt der Gesamtleistung und Skalierbarkeit handelt. Daher ist bei schreibintensiven OLTP-Anwendungen eine kleiner Anzahl großer DB-Instances gegenüber vielen kleinen DB-Instances vorzuziehen.

In einem typischen Aurora-Cluster verarbeitet eine DB-Instance (die primäre Instance) alle DDL- und DML-Anweisungen. Die anderen DB-Instances (die Aurora Replicas) verarbeiten nur `SELECT`-Anweisungen. Obwohl die DB-Instances nicht genau die gleichen Aufgaben ausführen, raten wir zur Verwendung der gleichen Instance-Klasse für alle DB-Instances im Cluster. Wenn Aurora im Falle eines Ausfalls eine der schreibgeschützten DB-Instances auf die neue primäre Instance hochstuft, hat die primäre Instance auf diese Weise die gleiche Kapazität wie zuvor.

Wenn Sie in demselben Cluster DB-Instances unterschiedlicher Kapazitäten verwenden möchten, richten Sie Failover-Stufen für die DB-Instances ein. Diese Stufen bestimmen die Reihenfolge, in der Aurora Replicas durch den Failover-Mechanismus hochgestuft werden. Platzieren Sie DB-Instances, die sehr viel größer oder kleiner als die anderen sind, in eine niedrigere Failover-Stufe. Dadurch wird sichergestellt, dass sie zuletzt zum Hochstufen ausgewählt werden.

Führen Sie die Datenwiederherstellungsfunktionen von Aurora aus, z. B. automatische point-in-time Wiederherstellung, manuelle Snapshots und Wiederherstellung sowie Cluster-Rückverfolgung. Sofern

angemessen, kopieren Sie Snapshots aus anderen AWS-Regions und stellen Sie sie in anderen AWS-Regionen wieder her, um Szenarien zur Notfallwiederherstellung nachzuahmen.

Untersuchen Sie die Anforderungen Ihrer Organisation bezüglich Wiederherstellungsdauer (Restore Time Objective, RTO), Wiederherstellungspunkt (Restore Point Objective, RPO) und geografischer Redundanz. Die meisten Organisationen gruppieren diese Elemente unter der großen Kategorie der Notfallwiederherstellung. Bewerten Sie die Aurora-Funktionen für hohe Verfügbarkeit, die in diesem Abschnitt beschrieben werden, im Kontext Ihres Prozesses zur Notfallwiederherstellung, um sicherzustellen,dass Ihre RTO- und RPO-Anforderungen erfüllt werden.

13. Weitere Vorgehensweisen

Am Ende eines erfolgreichen proof-of-concept Prozesses bestätigen Sie, dass Aurora basierend auf der voraussichtlichen Workload eine geeignete Lösung für Sie ist. Durchweg durch den voranstehenden Prozess haben Sie überprüft, wie Aurora in einer realistischen Betriebsumgebung funktioniert und anhand Ihrer Erfolgskriterien gemessen.

Sobald Ihre Datenbankumgebung mit Aurora betriebsbereit ist, können Sie mit detaillierten Evaluierungsschritten fortfahren, die zu Ihrer endgültigen Migration und Produktionsbereitstellung führen. Abhängig von Ihrer Situation können diese anderen Schritte in den proof-of-concept Prozess aufgenommen werden oder nicht. Einzelheiten zu Migrations- und Portierungsaktivitäten finden Sie im AWS-Whitepaper Aurora-Migrationshandbuch.

Erwägen Sie in einem anderen Schritt die Sicherheitskonfigurationen, die für Ihre Workload relevant sind und darauf ausgelegt sind, Ihre Sicherheitsanforderungen in einer Produktionsumgebung zu erfüllen. Planen Sie, welche Kontrollen zum Schutz des Zugriffs auf die Masterbenutzeranmeldedaten des Aurora-Clusters implementiert werden sollen. Definieren Sie die Rollen und Zuständigkeiten von Datenbankbenutzern, um den Zugriff auf die im Aurora-Cluster gespeicherten Daten zu kontrollieren. Berücksichtigen Sie Datenbank-Zugriffsanforderungen für Anwendungen, Skripts und Drittanbieter-Tools und -Services. Erkunden Sie AWS-Services und -Funktionen wie z. B. AWS Secrets Manager und AWS Identity and Access Management-(IAM)-Authentifizierung.

An dieser Stelle sollten Sie die Verfahren und bewährten Methoden für die Ausführung von Benchmark-Tests mit Aurora verstehen. Sie stellen möglicherweise fest, dass eine zusätzliche Leistungsoptimierung erforderlich ist. Einzelheiten finden Sie unter Verwalten von Performance und Skalierung für einen Aurora-DB-Cluster, Amazon Aurora MySQL-Leistungserweiterungen, Verwalten von Amazon Aurora PostgreSQL und Überwachung mit Performance Insights auf . Wenn Sie eine zusätzliche Optimierung vornehmen, stellen Sie sicher, dass Sie mit den Metriken vertraut

sind, die Sie während des Machbarkeitsnachweises erfasst haben. Als nächster Schritt können Sie neue Cluster mit verschiedenen Optionen für Konfigurationseinstellungen, Datenbank-Engine und Datenbankversion erstellen. Oder Sie können spezialisierte Arten von Aurora-Clustern erstellen, um die Anforderungen bestimmter Anwendungsfälle zu erfüllen.

Beispielsweise können Sie Aurora-Parallelabfrage-Cluster für hybride Transaktions-/analytische Verarbeitungsanwendungen (HTAP) erkunden. Wenn eine breite geografische Verteilung für die Notfallwiederherstellung oder zum Minimieren der Latenz von zentraler Bedeutung ist, können Sie globale Aurora-Datenbanken erkunden. Wenn Ihre Workload unregelmäßig ist oder wenn Sie Aurora in einem Entwicklungs-/Test-Szenario einsetzen, können Sie Aurora Serverless-Cluster erwägen.

Ihre Produktions-Cluster müssen möglicherweise auch eingehende Verbindungen hohen Umfangs verarbeiten. Informationen zu diesen Techniken finden Sie im AWS-Whitepaper Aurora-MySQL-Datenbankadministratorhandbuch – Verbindungsverwaltung.

Wenn Sie nach dem Machbarkeitsnachweis beschließen, dass Ihr Anwendungsfall nicht für Aurora geeignet ist, erwägen Sie die folgenden anderen AWS-Services:

- Bei rein analytischen Anwendungsfällen profitieren Workloads von einem spaltenbasierten Speicherformat und anderen Funktionen, die besser geeignet für OLAP-Workloads sind. AWS-Services, die sich mit solchen Anwendungsfällen befassen, gehören:
  - Amazon Redshift
  - Amazon EMR
  - Amazon Athena
- Viele Workloads profitieren von einer Kombination aus Aurora mit einem oder mehreren dieser Services. Sie können Daten mit den folgenden Methoden zwischen diesen Services verschieben:
  - AWS Glue
  - AWS DMS
  - Importieren aus Amazon S3, wie im Amazon Aurora Benutzerhandbuch beschrieben
  - Exportieren zu Amazon S3, wie im Amazon Aurora Benutzerhandbuch beschrieben
  - Viele andere gängige ETL-Tools

Sicherheit in Amazon Aurora

Cloud-Sicherheit hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die eingerichtet wurde, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud: AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für Amazon Aurora (Aurora) gelten, finden Sie unter Vom Compliance-Programm abgedeckte AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Diese Dokumentation erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von Amazon Aurora zum Tragen kommt. Die folgenden Themen veranschaulichen, wie Sie Amazon Aurora zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre Amazon-Aurora-Ressourcen zu überwachen und zu schützen.

Sie können den Zugriff auf Ihre Amazon Aurora-Ressourcen und Ihre Datenbanken in einem DB-Cluster verwalten. Die Methode, die Sie verwenden, um den Zugriff zu verwalten, hängt vom Aufgabentyp ab, den der Benutzer mit Amazon Aurora ausführen möchte:

- Führen Sie Ihren DB-Cluster in einer Virtual Private Cloud (VPC) basierend auf dem Amazon VPC-Service für die größtmögliche Netzwerkzugriffskontrolle aus. Weitere Informationen zum Erstellen eines DB-Clusters in einer VPC finden Sie unter Amazon VPCs und Amazon Aurora.
- Verwenden Sie AWS Identity and Access Management-(IAM)-Zugriffsrichtlinien, um Berechtigungen zu erteilen, die festlegen, wer Amazon Aurora-Ressourcen verwalten darf. Beispielsweise können Sie IAM verwenden, um zu bestimmen, wer DB-Cluster erstellen, beschreiben, ändern und löschen, Ressourcen taggen oder Sicherheitsgruppen ändern darf.

IAM-Beispielrichtlinien finden Sie unter Beispiele für identitätsbasierte Amazon-Aurora-Richtlinien.

- Verwenden Sie Sicherheitsgruppen, um zu steuern, welche IP-Adressen oder Amazon EC2-Instances sich mit Ihren Datenbanken in einem DB-Cluster verbinden können. Wenn Sie zum ersten Mal einen DB-Cluster erstellen, verhindert deren/dessen Firewall jeglichen Datenbankzugriff, außer den Zugriff über Regeln, die in einer zugehörigen Sicherheitsgruppe festgelegt sind.
- Verwenden Sie Secure Socket Layer (SSL)- oder Transport Layer Security (TLS)-Verbindungen mit DB-Clustern, auf denen Aurora MySQL oder Aurora PostgreSQL ausgeführt wird. Weitere Informationen über die Verwendung von SSL/TLS mit DB-Clustern finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .
- Verwenden Sie die Amazon-Aurora-Verschlüsselung, um Ihre DB-Clusterund Schnappschüsse im Ruhezustand zu sichern. Die Amazon-Aurora-Verschlüsselung verwendet den branchenüblichen AES-256-Verschlüsselungsalgorithmus, um Ihre Daten auf dem Server zu verschlüsseln, der Ihren DB-Cluster hostet. Weitere Informationen finden Sie unter Verschlüsseln von Amazon Aurora-Ressourcen.
- Verwenden Sie die Sicherheitsfunktionen Ihrer DB-Engine, um zu steuern, wer sich bei Ihren Datenbanken in einem DB-Cluster anmelden kann. Diese Funktionen arbeiten genauso, als würden sich die Datenbanken in Ihrem lokalen Netzwerk befinden.

  Weitere Informationen zur Sicherheit im Zusammenhang mit Aurora MySQL finden Sie unter Sicherheit in Amazon Aurora MySQL. Weitere Informationen zur Sicherheit im Zusammenhang mit Aurora PostgreSQL finden Sie unter Sicherheit in Amazon Aurora PostgreSQL.

Aurora ist Teil des verwalteten Datenbankservices Amazon Relational Database Service (Amazon RDS). Amazon RDS ist ein Webservice, der das Einrichten, Betreiben und Skalieren einer relationalen Datenbank in der Cloud vereinfacht. Wenn Sie noch keine Erfahrung mit Amazon RDS haben, beachten Sie die Informationen im Amazon RDS-Benutzerhandbuch.

Aurora umfasst ein hochleistungsfähiges Speichersubsystem. Die mit MySQL und PostgreSQL kompatiblen Datenbank-Engines werden angepasst, um diesen schnellen verteilten Speicher zu nutzen. Aurora automatisiert und standardisiert auch das Clustering und die Replikation von Datenbanken, die normalerweise zu den schwierigsten Aspekten der Datenbankkonfiguration und -verwaltung gehören.

Bei Amazon RDS und Aurora können Sie programmgesteuert auf die RDS-API zugreifen und Sie können die AWS CLI für den interaktiven Zugriff auf die RDS-API verwenden. Einige RDS-API-Operationen und AWS CLI-Befehle gelten für Amazon RDS und Aurora, während andere entweder

für Amazon RDS oder für Aurora gelten. Weitere Informationen zu RDS-API-Operationen finden Sie in der Amazon RDS-API-Referenz. Weitere Informationen zur AWS CLI finden Sie in der AWS Command Line Interface-Amazon-RDS-Referenz.

> **Note**
>
> Sie müssen die Sicherheit nur für Ihre Anwendungsfälle konfigurieren. Sie müssen den Sicherheitszugriff für Prozesse, die Amazon Aurora verwaltet, nicht konfigurieren. Dazu gehört das Erstellen von Backups, automatischem Failover und anderen Prozessen.

Weitere Informationen zum Verwalten des Zugriffs auf Amazon-Aurora-Ressourcen und Ihre Datenbanken in einem DB-Cluster finden Sie unter den folgenden Themen.

Themen

- Datenbankauthentifizierung mit Amazon Aurora
- Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager
- Datenschutz in Amazon RDS
- Identity and Access Management für Amazon Aurora
- Protokollieren und Überwachen in Amazon Aurora
- Compliance-Validierung für Amazon Aurora
- Ausfallsicherheit in Amazon Aurora
- Sicherheit der Infrastruktur in Amazon Aurora
- Amazon-RDS-API und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)
- Bewährte Methoden für die Sicherheit in Amazon Aurora
- Zugriffskontrolle mit Sicherheitsgruppen
- Berechtigungen von Hauptbenutzerkonten
- Verwenden von serviceverknüpften Rollen für Amazon Aurora
- Amazon VPCs und Amazon Aurora

Datenbankauthentifizierung mit Amazon Aurora

Amazon Aurora unterstützt verschiedene Möglichkeiten, Datenbankbenutzer zu authentifizieren.

Die Passwort-Authentifizierung ist standardmäßig für alle DB-Cluster verfügbar. Für Aurora MySQL und Aurora PostgreSQL können Sie auch entweder IAM-Datenbank-Authentifizierung oder Kerberos-Authentifizierung oder beides für denselben DB-Cluster hinzufügen.

Passwort-, Kerberos- und IAM-Datenbank-Authentifizierung verwenden verschiedene Methoden zur Authentifizierung bei der Datenbank. Daher kann sich ein bestimmter Benutzer mit nur einer einzigen Authentifizierungsmethode bei einer Datenbank anmelden.

Verwenden Sie für PostgreSQL nur eine der folgenden Rolleneinstellungen für einen Benutzer einer bestimmten Datenbank:

- Um die IAM-Datenbank-Authentifizierung zu verwenden, weisen Sie die `rds_iam`-Rolle dem Benutzer zu.
- Um Kerberos-Authentifizierung zu verwenden, weisen Sie die `rds_ad`-Rolle dem Benutzer zu.
- Um die Passwort-Authentifizierung zu verwenden, weisen Sie keine der beiden `rds_iam`- oder `rds_ad`- Rollen dem Benutzer zu.

Weisen Sie nicht beide Rollen `rds_iam` und `rds_ad` einem Benutzer einer PostgreSQL-Datenbank zu, weder direkt noch indirekt durch verschachtelten gewährtem Zugriff. Wenn die `rds_iam`-Rolle dem Hauptbenutzer hinzugefügt wird, hat die IAM-Authentifizierung Vorrang vor der Passwort-Authentifizierung, so dass sich der Hauptbenutzer als IAM-Benutzer anmelden muss.

> **Important**
>
> Wir empfehlen Ihnen, den Hauptbenutzer nicht direkt in Ihren Anwendungen zu verwenden. Bleiben Sie stattdessen bei der bewährten Methode, einen Datenbankbenutzer zu verwenden, der mit den Mindestberechtigungen erstellt wurde, die für Ihre Anwendung erforderlich sind.

Themen

Passwortauthentifizierung

Mit der Passwortauthentifizierung führt Ihre Datenbank die gesamte Verwaltung von Benutzerkonten durch. Sie erstellen Benutzer mit SQL-Anweisungen wie `CREATE USER`, mit der entsprechenden Klausel, die von der DB-Engine zum Angeben von Kennwörtern benötigt wird. In MySQL lautet die Anweisung beispielsweise `CREATE USER-`*`Name`* `IDENTIFIED BY-`*`Passwort`*, während die Anweisung in PostgreSQL `CREATE USER-`*`Name`* `WITH PASSWORD-`*`Passwort`* ist.

Mit der Passwortauthentifizierung steuert und authentifiziert Ihre Datenbank Benutzerkonten. Wenn eine DB-Engine über starke Passwortverwaltungsfunktionen verfügt, können diese die Sicherheit erhöhen. Die Datenbankauthentifizierung ist möglicherweise einfacher mit der Passwortauthentifizierung zu verwalten, wenn Sie kleine Benutzergemeinschaften haben. Da in diesem Fall Klartext-Passwörter generiert werden, AWS Secrets Manager kann die Integration mit die Sicherheit erhöhen.

Weitere Informationen zur Verwendung von Secrets Manager mit Amazon Aurora finden Sie unter Erstellen eines Basis-Secrets und Rotations-Secrets für unterstützte Amazon-RDS-Datenbanken im AWS Secrets Manager -Benutzerhandbuch. Informationen zum programmgesteuerten Abrufen Ihrer Secrets in Ihren benutzerdefinierten Anwendungen finden Sie unter Abrufen des Secret-Werts im AWS Secrets Manager -Benutzerhandbuch.

IAM-Datenbankauthentifizierung

Sie können sich bei Ihrem mithilfe der AWS Identity and Access Management (IAM-) Datenbankauthentifizierung authentifizieren. Mit dieser Authentifizierungsmethode benötigen Sie kein Passwort, um eine Verbindung mit einer DB-Cluster herzustellen. Stattdessen verwenden Sie ein Authentifizierungstoken.

Weitere Informationen zur IAM-Datenbankauthentifizierung, einschließlich Informationen zur Verfügbarkeit bestimmter DB-Engines, finden Sie unter IAM-Datenbankauthentifizierung.

Kerberos-Authentifizierung

Amazon Aurora unterstützt die externe Authentifizierung von Datenbankbenutzern über Kerberos und Microsoft Active Directory. Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das Tickets und symmetrische Schlüsselkryptographie verwendet, um die Notwendigkeit der Übertragung von Passwörtern über das Netzwerk zu vermeiden. Kerberos wurde in Active Directory integriert und wurde entwickelt, um Benutzer gegenüber Netzwerkressourcen wie Datenbanken zu authentifizieren.

Die Amazon Aurora-Unterstützung für Kerberos und Active Directory bietet die Vorteile des Single Sign-Ons und der zentralisierten Authentifizierung von Datenbankbenutzern. Sie können Ihre Benutzeranmeldeinformationen in Active Directory speichern. Active Directory bietet einen zentralen Ort für die Speicherung und Verwaltung von Anmeldeinformationen für mehrere DB-Cluster.

Sie können Ihren Datenbankbenutzern die Authentifizierung bei DB-Clustern auf zwei Arten ermöglichen. Sie können Anmeldeinformationen verwenden, die entweder in AWS Directory Service for Microsoft Active Directory oder in Ihrem lokalen Active Directory gespeichert sind.

Aurora PostgreSQL unterstützt keinen selektiven Authentifizierungstyp in Forest Trust, sondern nur die gesamtstrukturweite Authentifizierung.

Derzeit unterstützt Aurora die Kerberos-Authentifizierung für DB-Cluster von Aurora MySQL und Aurora PostgreSQL. Weitere Informationen zur Kerberos-Authentifizierung für Aurora MySQL finden Sie unter Verwenden der Kerberos-Authentifizierung für Aurora MySQL.

Mit der Kerberos-Authentifizierung unterstützen Aurora PostgreSQL- DB-Cluster ein- und bidirektionale gesamtstrukturbasierte Vertrauensstellungen. Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung mit Aurora PostgreSQL.

Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager

Amazon Aurora lässt sich in Secrets Manager integrieren, um Hauptbenutzerpasswörter für Ihre DB--Cluster zu verwalten.

Themen

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen zur Verfügbarkeit von Versionen und Regionen für die Integration von Secrets Manager in Amazon Aurora finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für die Secrets Manager Manager-Integration.

Einschränkungen für die Integration von Secrets Manager in Amazon Aurora

Die Verwaltung von Hauptpasswörtern mit Secrets Manager wird für die folgenden Funktionen nicht unterstützt:

- Blau/Grün-Bereitstellungen von Amazon RDS
- DB-Cluster, die Teil einer globalen Aurora-Datenbank sind
- Aurora Serverless v1-DB-Cluster

- Regionsübergreifende Lesereplikate von Aurora MySQL
- Verwaltung des Hauptbenutzerpassworts mit Secrets Manager für ein Lesereplikat

Überblick über die Verwaltung von Masterbenutzerkennwörtern mit AWS Secrets Manager

Mit AWS Secrets Manager können Sie hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Datenbankkennwörtern, durch einen API-Aufruf an Secrets Manager ersetzen, um das Geheimnis programmgesteuert abzurufen. Weitere Informationen zu Secrets Manager finden Sie im Benutzerhandbuch für AWS Secrets Manager.

Wenn Sie Datenbankgeheimnisse in Secrets Manager speichern, AWS-Konto fallen Gebühren an. Informationen zu Preisen erhalten Sie unter AWS Secrets Manager -Preise.

Sie können angeben, dass Aurora das Hauptbenutzerpasswort in Secrets Manager für einen DB-Cluster von Amazon Aurora verwaltet, wenn Sie eine der folgenden Operationen ausführen:

- Den -DB-Cluster erstellen
- Den -DB-Cluster ändern
- Den DB-Cluster aus Amazon S3 wiederherstellen (nur Aurora MySQL)

Wenn Sie angeben, dass Aurora das Hauptbenutzerpasswort in Secrets Manager verwaltet, generiert Aurora das Passwort und speichert es in Secrets Manager. Sie können direkt mit dem Secret interagieren, um die Anmeldeinformationen für den Hauptbenutzer abzurufen. Sie können auch einen vom Kunden verwalteten Schlüssel angeben, um das Secret zu verschlüsseln, oder den KMS-Schlüssel verwenden, der von Secrets Manager bereitgestellt wird.

Aurora verwaltet die Einstellungen für das Secret und rotiert das Secret standardmäßig alle sieben Tage. Sie können einige Einstellungen ändern, wie zum Beispiel den Rotationsplan. Wenn Sie einen DB-Cluster löschen, der ein Secret in Secrets Manager verwaltet, werden das Secret und die zugehörigen Metadaten ebenfalls gelöscht.

Um eine Verbindung mit mit den Anmeldeinformationen in einem Secret herzustellen, können Sie das Secret von Secrets Manager abrufen. Weitere Informationen finden Sie im Benutzerhandbuch unter Abrufen von Geheimnissen aus AWS Secrets Manager und Herstellen einer Verbindung zu einer SQL-Datenbank mit Anmeldeinformationen in einem AWS Secrets Manager Geheimnis herstellen.AWS Secrets Manager

Vorteile der Verwaltung von Hauptbenutzerpasswörtern mit Secrets Manager

Die Verwaltung von Aurora-Hauptbenutzerpasswörtern mit Secrets Manager bietet die folgenden Vorteile:

- Aurora generiert automatisch Datenbankanmeldeinformationen.
- Aurora speichert und verwaltet automatisch Datenbankanmeldedaten in AWS Secrets Manager.
- Aurora rotiert die Datenbankanmeldeinformationen regelmäßig, ohne dass Anwendungsänderungen erforderlich sind.
- Secrets Manager schützt Datenbankanmeldeinformationen vor menschlichem Zugriff und der Klartextansicht.
- Secrets Manager ermöglicht das Abrufen von Datenbankanmeldeinformationen in Secrets für Datenbankverbindungen.
- Secrets Manager ermöglicht eine detaillierte Steuerung des Zugriffs auf Datenbankanmeldeinformationen in Secrets mithilfe von IAM.
- Optional können Sie die Datenbankverschlüsselung von der Anmeldeinformationsverschlüsselung mit unterschiedlichen KMS-Schlüsseln trennen.
- Sie können die manuelle Verwaltung und Rotation der Datenbankanmeldeinformationen vermeiden.
- Sie können Datenbankanmeldedaten einfach mit AWS CloudTrail Amazon überwachen CloudWatch.

Weitere Informationen zu den Vorteilen von Secrets Manager finden Sie im Benutzerhandbuch für AWS Secrets Manager.

Erforderliche Berechtigungen für die Integration von Secrets Manager

Benutzer müssen über die erforderlichen Berechtigungen verfügen, um Operationen im Zusammenhang mit der Integration von Secrets Manager auszuführen. Sie können IAM-Richtlinien erstellen, die die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die benötigt werden. Sie können diese Richtlinien dann den IAM-Berechtigungssätzen oder -Rollen zuordnen, die diese Berechtigungen benötigen. Weitere Informationen finden Sie unter Identity and Access Management für Amazon Aurora.

Für Erstellungs-, Änderungs- oder Wiederherstellungsoperationen muss der Benutzer, der angibt, dass Aurora das Hauptbenutzerpasswort in Secrets Manager verwaltet, über entsprechende Berechtigungen für folgende Operationen verfügen:

- `kms:DescribeKey`
- `secretsmanager:CreateSecret`
- `secretsmanager:TagResource`

Für Erstellungs-, Änderungs- oder Wiederherstellungsoperationen muss der Benutzer, der den benutzerdefinierten Schlüssel zum Entschlüsseln des Secrets in Secrets Manager angibt, über entsprechende Berechtigungen für folgende Operationen verfügen:

- `kms:Decrypt`
- `kms:GenerateDataKey`
- `kms:CreateGrant`

Für Änderungsoperationen muss der Benutzer, der das Hauptbenutzerpasswort in Secrets Manager rotiert, über entsprechende Berechtigungen für die folgende Operation verfügen:

- `secretsmanager:RotateSecret`

Durchsetzung der Verwaltung des Masterbenutzerkennworts durch Aurora in AWS Secrets Manager

Sie können IAM-Bedingungsschlüssel verwenden, um die Aurora-Verwaltung des Hauptbenutzerpassworts in AWS Secrets Manager zu erzwingen. Die folgende Richtlinie erlaubt Benutzern nicht, DB-Instances oder DB-Cluster zu erstellen oder wiederherzustellen, es sei denn, das Hauptbenutzerpasswort wird von Aurora in Secrets Manager verwaltet.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["rds:CreateDBInstance", "rds:CreateDBCluster",
 "rds:RestoreDBInstanceFromS3", "rds:RestoreDBClusterFromS3"],
            "Resource": "*",
```

```
            "Condition": {
                "Bool": {
                    "rds:ManageMasterUserPassword": false
                }
            }
        }
    ]
}
```

> **Note**
>
> Diese Richtlinie erzwingt die Passwortverwaltung bereits AWS Secrets Manager bei der Erstellung. Sie können die Secrets-Manager-Integration jedoch nach wie vor deaktivieren und ein Hauptpasswort manuell festlegen, indem Sie den Cluster ändern.
> Um dies zu verhindern, nehmen Sie `rds:ModifyDBInstance`, `rds:ModifyDBCluster` in den Aktionsblock der Richtlinie auf. Beachten Sie, dass der Benutzer dadurch keine weiteren Änderungen an vorhandenen Clustern vornehmen kann, für die die Secrets-Manager-Integration nicht aktiviert ist.

Weitere Informationen zum Verwenden der Bedingungsschlüssels in IAM-Richtlinien finden Sie unter Richtlinien-Bedingungsschlüssel für Aurora und Beispielrichtlinien: Verwenden von Bedingungsschlüsseln.

Verwaltung des Hauptbenutzerpassworts für einen DB-Cluster mit Secrets Manager

Sie können die Aurora-Verwaltung des Hauptbenutzerpassworts in Secrets Manager konfigurieren, wenn Sie die folgenden Aktionen ausführen:

- Erstellen eines Amazon Aurora-DB Clusters
- Ändern eines Amazon Aurora-DB-Clusters
- Migrieren von Daten aus einer externen MySQL-Datenbank zu einem Amazon-Aurora-MySQL-DB-Cluster

Sie können die RDS-Konsole AWS CLI, die oder die RDS-API verwenden, um diese Aktionen auszuführen.

Konsole

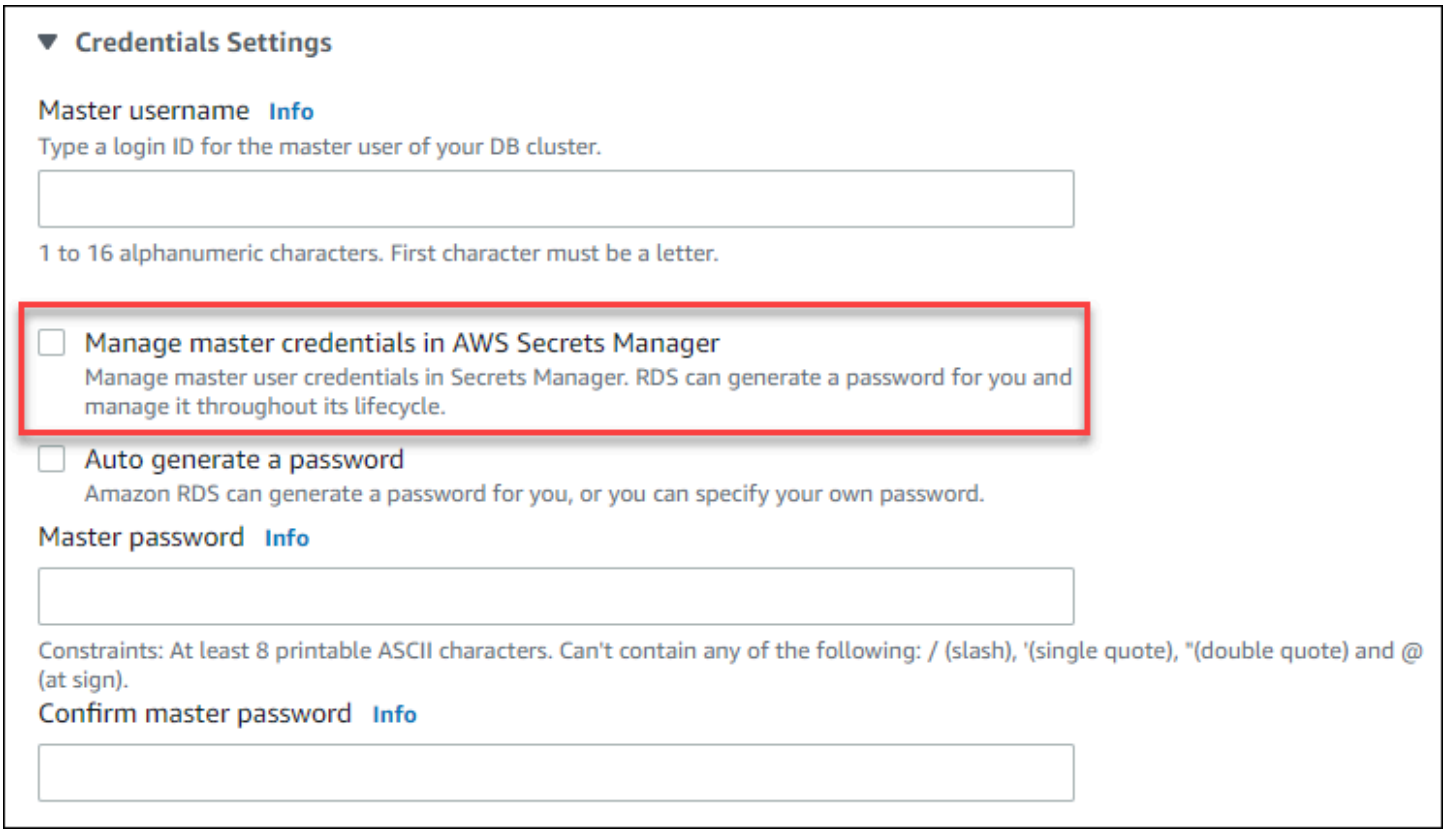
Folgen Sie den Anweisungen zum Erstellen oder Ändern eines DB-Clusters mit der RDS-Konsole:

- Erstellen eines DB-Clusters
- Ändern einer DB-Instance in einem DB-Cluster

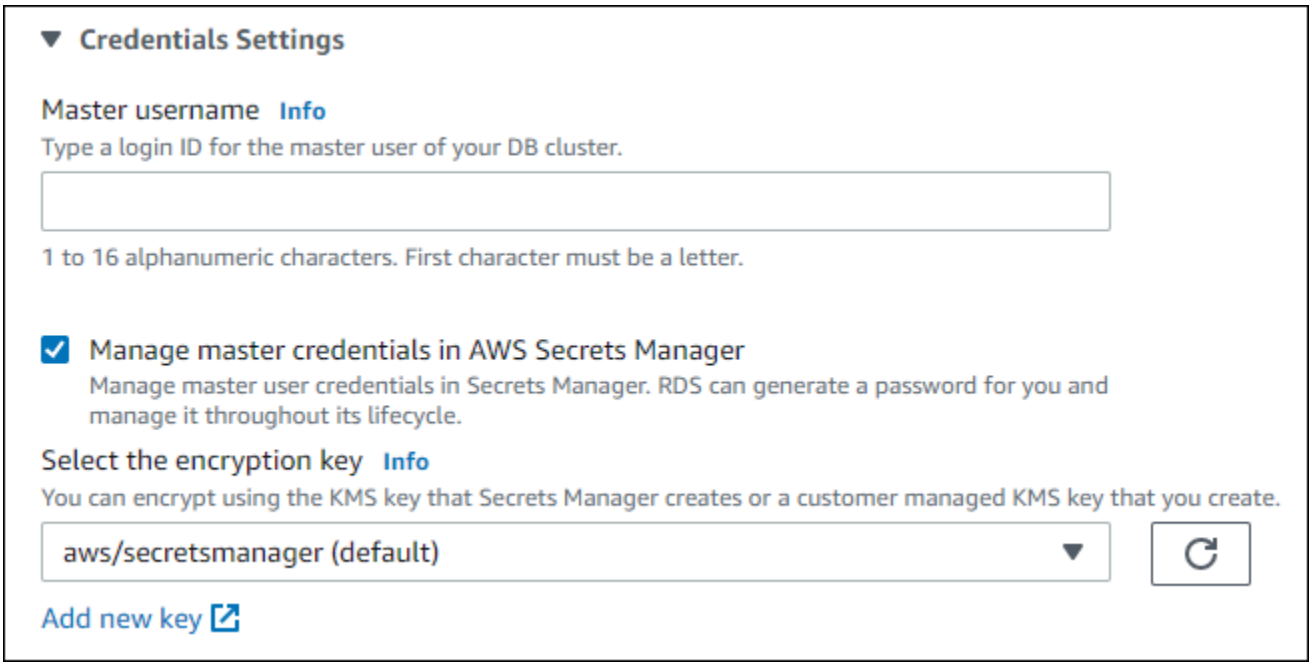
  In der RDS-Konsole können Sie jede DB-Instance ändern, um die Verwaltungseinstellungen für das Hauptbenutzerpasswort für den gesamten DB-Cluster anzugeben.
- Wiederherstellen eines Amazon Aurora-MySQL-DB-Clusters aus einem Amazon S3-Bucket

Wenn Sie die RDS-Konsole verwenden, um eine dieser Operationen auszuführen, können Sie angeben, dass das Hauptbenutzerpasswort von Aurora in Secrets Manager verwaltet wird. Wählen Sie dazu beim Erstellen oder Wiederherstellen eines DB-Clusters Hauptanmeldeinformationen in AWS Secrets Manager verwalten unter Anmeldeinformationseinstellungen aus. Wenn Sie einen DB-Cluster ändern, wählen Sie Hauptanmeldeinformationen in AWS Secrets Manager verwalten unter Einstellungen aus.

Die folgende Abbildung zeigt ein Beispiel für die Einstellung Hauptanmeldeinformationen in AWS Secrets Manager verwalten beim Erstellen oder Wiederherstellen eines DB-Clusters.



Wenn Sie diese Option auswählen, generiert Aurora das Hauptbenutzerpasswort und verwaltet es während seines gesamten Lebenszyklus in Secrets Manager.



Sie können wählen, ob Sie das Secret mit einem von Secrets Manager bereitgestellten KMS-Schlüssel oder mit einem von Ihnen erstellten kundenverwalteten Schlüssel verschlüsseln möchten. Nachdem Aurora die Datenbankanmeldeinformationen für einen DB-Cluster verwaltet hat, können Sie den KMS-Schlüssel, der zum Verschlüsseln des Secrets verwendet wird, nicht mehr ändern.

Sie können andere Einstellungen auswählen, die Ihren Anforderungen entsprechen.

Weitere Informationen zu den verfügbaren Einstellungen beim Erstellen eines DB-Clusters finden Sie unter Einstellungen für Aurora-DB-Cluster. Weitere Informationen zu den verfügbaren Einstellungen beim Ändern eines DB-Clusters finden Sie unter Einstellungen für Amazon Aurora.

AWS CLI

Wenn Sie angeben möchten, dass Aurora das Hauptbenutzerpasswort in Secrets Manager verwalten soll, geben Sie die `--manage-master-user-password`-Option in einem der folgenden Befehle an:

- create-db-cluster
- modify-db-cluster
- restore-db-cluster-from-s3

Wenn Sie die `--manage-master-user-password`-Option angeben, generiert Aurora das Hauptbenutzerpasswort und verwaltet es während seines gesamten Lebenszyklus in Secrets Manager.

Sie können auch einen kundenverwalteten Schlüssel angeben, um das Secret zu verschlüsseln, oder den KMS-Standardschlüssel verwenden, der von Secrets Manager bereitgestellt wird. Verwenden Sie die `--master-user-secret-kms-key-id`-Option, um einen kundenverwalteten Schlüssel anzugeben. Die AWS KMS-Schlüssel-ID ist der Schlüssel-ARN, die Schlüssel-ID, der Alias-ARN oder der Aliasname für den KMS-Schlüssel. Um einen KMS-Schlüssel in einem anderen zu verwenden AWS-Konto, geben Sie den Schlüssel-ARN oder den Alias-ARN an. Nachdem Aurora die Datenbankanmeldeinformationen für einen DB-Cluster verwaltet hat, können Sie den KMS-Schlüssel, der zum Verschlüsseln des Secrets verwendet wird, nicht mehr ändern.

Sie können andere Einstellungen auswählen, die Ihren Anforderungen entsprechen.

Weitere Informationen zu den verfügbaren Einstellungen beim Erstellen eines DB-Clusters finden Sie unter Einstellungen für Aurora-DB-Cluster. Weitere Informationen zu den verfügbaren Einstellungen beim Ändern eines DB-Clusters finden Sie unter Einstellungen für Amazon Aurora.

In diesem Beispiel wird ein -DB-Cluster erstellt und angegeben, dass Aurora das Passwort in Secrets Manager verwaltet. Das Secret wird mit dem KMS-Schlüssel verschlüsselt, der von Secrets Manager bereitgestellt wird.

Example

Für LinuxmacOS, oderUnix:

```
aws rds create-db-cluster \
     --db-cluster-identifier sample-cluster \
     --engine aurora-mysql \
     --engine-version 8.0 \
     --master-username admin \
     --manage-master-user-password
```

Windows:

```
aws rds create-db-cluster ^
     --db-cluster-identifier sample-cluster ^
     --engine aurora-mysql ^
     --engine-version 8.0 ^
```

```
    --master-username admin ^
    --manage-master-user-password
```

RDS-API

Wenn Sie angeben möchten, dass Aurora das Hauptbenutzerpasswort in Secrets Manager verwaltet, legen Sie den `ManageMasterUserPassword`-Parameter in einer der folgenden Operationen auf `true` fest:

- CreateDBCluster
- ModifyDBCluster
- DB S3 wiederhergestellt ClusterFrom

Wenn Sie den `ManageMasterUserPassword`-Parameter in einer dieser Operationen auf `true` festlegen, generiert Aurora das Hauptbenutzerpasswort und verwaltet es während seines gesamten Lebenszyklus in Secrets Manager.

Sie können auch einen kundenverwalteten Schlüssel angeben, um das Secret zu verschlüsseln, oder den KMS-Standardschlüssel verwenden, der von Secrets Manager bereitgestellt wird. Verwenden Sie den `MasterUserSecretKmsKeyId`-Parameter, um einen kundenverwalteten Schlüssel anzugeben. Die AWS KMS-Schlüssel-ID ist der Schlüssel-ARN, die Schlüssel-ID, der Alias-ARN oder der Aliasname für den KMS-Schlüssel. Geben Sie den Schlüssel-ARN oder Alias-ARN an, um einen KMS-Schlüssel in einem anderen AWS-Konto zu verwenden. Nachdem Aurora die Datenbankanmeldeinformationen für einen DB-Cluster verwaltet hat, können Sie den KMS-Schlüssel, der zum Verschlüsseln des Secrets verwendet wird, nicht mehr ändern.

Rotieren des Hauptbenutzerpasswort-Secrets für einen DB-Cluster

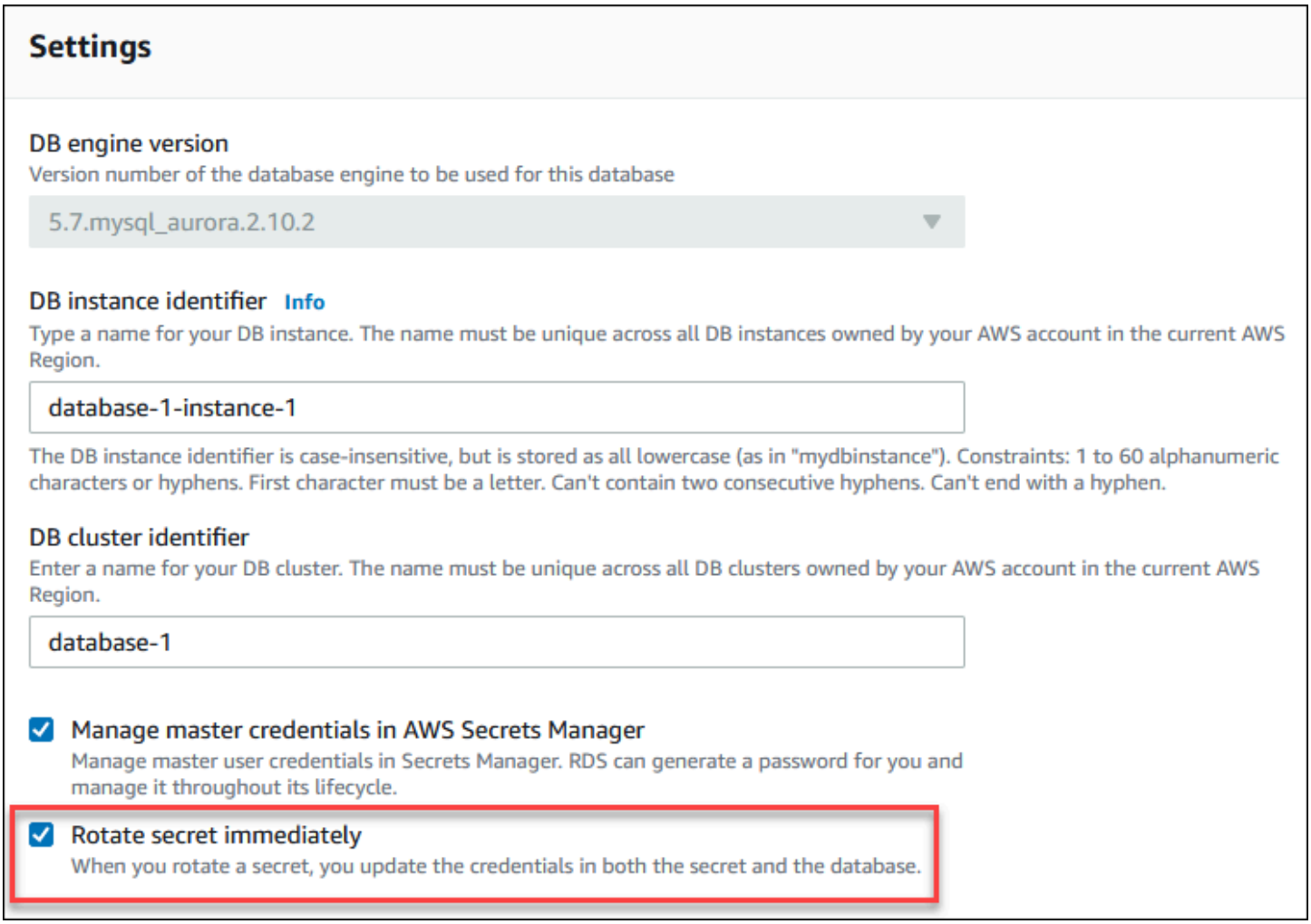
Wenn Aurora ein Hauptbenutzerpasswort-Secret rotiert, generiert Secrets Manager eine neue Secret-Version für das vorhandene Secret. Die neue Secret-Version enthält das neue Hauptbenutzerpasswort. Aurora ändert das Hauptbenutzerpasswort für den -DB-Cluster so, dass es mit dem Passwort für die neue Secret-Version übereinstimmt.

Sie können ein Secret sofort rotieren, anstatt auf eine geplante Rotation zu warten. Wenn Sie das Hauptbenutzerpasswort-Secret in Secrets Manager rotieren möchten, ändern Sie den DB-Cluster. Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Sie können das geheime Masterbenutzer-Passwort sofort mit der RDS-Konsole AWS CLI, der oder der RDS-API wechseln. Das neue Passwort ist immer 28 Zeichen lang und enthält mindestens einen Groß- und Kleinbuchstaben, eine Zahl und ein Satzzeichen.

Konsole

Wenn Sie das Hauptbenutzerpasswort-Secret mithilfe der RDS-Konsole rotieren möchten, ändern Sie den DB-Cluster und wählen Sie die Option Rotate secret immediately (Sofortige Secret-Drehung) unter Settings (Einstellungen) aus.



Folgen Sie den Anweisungen zum Ändern eines DB-Clusters mit der RDS-Konsole in Ändern des DB-Clusters über die Konsole, die CLI und die API. Sie müssen auf der Bestätigungsseite die Option Apply immediately (Sofort anwenden) auswählen.

AWS CLI

Verwenden Sie den modify-db-clusterBefehl und geben Sie die Option an AWS CLI, um das geheime Masterbenutzerpasswort mithilfe von zu ändern. `--rotate-master-user-password` Sie müssen die `--apply-immediately`-Option angeben, wenn Sie das Hauptpasswort rotieren.

In diesem Beispiel wird ein Hauptbenutzerpasswort-Secret rotiert.

Example

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --rotate-master-user-password \
    --apply-immediately
```

Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --rotate-master-user-password ^
    --apply-immediately
```

RDS-API

Sie können ein Hauptbenutzerpasswort-Secret mit der Operation ModifyDBCluster und der Einstellung des `RotateMasterUserPassword`-Parameters auf `true` rotieren. Sie müssen den `ApplyImmediately`-Parameter auf `true` festlegen, wenn Sie das Hauptpasswort rotieren.

Anzeigen der Details zu einem Secret für einen DB-Cluster

Sie können Ihre Secrets über die Konsole (https://console.aws.amazon.com/secretsmanager/) oder den AWS CLI (get-secret-valueSecrets Manager Manager-Befehl) abrufen.

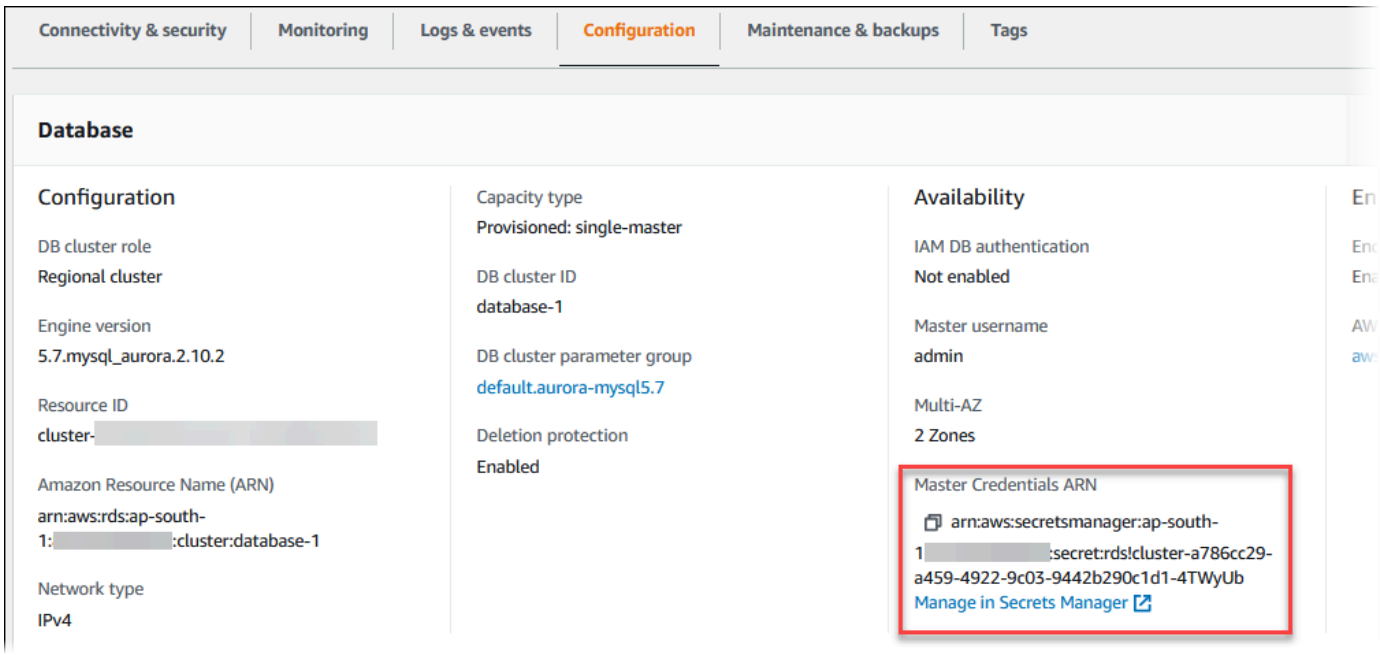
Sie finden den Amazon-Ressourcennamen (ARN) eines von Aurora verwalteten Secrets im Secrets Manager mit der RDS-Konsole AWS CLI, der oder der RDS-API.

Konsole

So zeigen Sie die Details zu einem von Aurora verwalteten Secret in Secrets Manager an

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den Namen des DB-Clusters aus, um dessen Details anzuzeigen.
4. Wählen Sie die Registerkarte Konfiguration aus.

   Unter Master Credentials ARN (ARN der Hauptanmeldeinformationen) können Sie den geheimen ARN einsehen.



   Sie können dem Link Manage in Secrets Manager (In Secrets Manager verwalten) folgen, um das Secret in der Secrets-Manager-Konsole anzuzeigen und zu verwalten.

AWS CLI

Sie können den AWS CLI describe-db-clustersBefehl RDS verwenden, um die folgenden Informationen zu einem Secret zu finden, das von Aurora in Secrets Manager verwaltet wird:

- `SecretArn` – Der ARN des Secrets
- `SecretStatus` – Der Status des Secrets

Mögliche Werte für den Status sind u. a. folgende:

- `creating` – Das Secret wird erstellt.
- `active` – Das Secret ist für den normalen Gebrauch und die Rotation verfügbar.
- `rotating` – Das Secret wird rotiert.
- `impaired` – Das Secret kann für den Zugriff auf Datenbankanmeldeinformationen verwendet werden, es kann jedoch nicht rotiert werden. Ein Secret kann diesen Status haben, wenn beispielsweise die Berechtigungen geändert werden, sodass RDS nicht mehr auf das Secret oder den KMS-Schlüssel für das Secret zugreifen kann.

  Wenn ein Secret diesen Status hat, können Sie die Bedingung korrigieren, die den Status verursacht hat. Wenn Sie die Bedingung korrigieren, die den Status verursacht hat, behält der Status bis zur nächsten Rotation den Wert `impaired`. Alternativ können Sie den DB-Cluster ändern, um die automatische Verwaltung von Datenbankanmeldeinformationen zu deaktivieren, und dann den DB-Cluster erneut ändern, um die automatische Verwaltung von Datenbankanmeldeinformationen zu aktivieren. Verwenden Sie die `--manage-master-user-password` Option im modify-db-clusterBefehl, um den DB-Cluster zu ändern.
- `KmsKeyId` – Der ARN des KMS-Schlüssels, der verwendet wird, um das Secret zu verschlüsseln

Geben Sie die `--db-cluster-identifier`-Option an, um die Ausgabe für einen bestimmten DB-Cluster anzuzeigen. Dieses Beispiel zeigt die Ausgabe für ein Secret, das von einem DB-Cluster verwendet wird.

Example

```
aws rds describe-db-clusters --db-cluster-identifier mydbcluster
```

Das folgende Beispiel zeigt die Ausgabe für ein Secret:

```
"MasterUserSecret": {
                "SecretArn": "arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
cluster-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx",
                "SecretStatus": "active",
                "KmsKeyId": "arn:aws:kms:eu-
west-1:123456789012:key/0987dcba-09fe-87dc-65ba-ab0987654321"
            }
```

Wenn Sie über den geheimen ARN verfügen, können Sie mit dem get-secret-valueSecrets Manager-CLI-Befehl Details zum Secret Manager anzeigen.

Dieses Beispiel zeigt die Details für das Secret in der vorherigen Beispielausgabe.

Example

Für LinuxmacOS, oderUnix:

```
aws secretsmanager get-secret-value \
    --secret-id 'arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
cluster-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx'
```

Windows:

```
aws secretsmanager get-secret-value ^
    --secret-id 'arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
cluster-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx'
```

RDS-API

Sie können den ARN, den Status und den KMS-Schlüssel für ein von Aurora verwaltetes Secret in Secrets Manager anzeigen, indem Sie die RDS-Operation DescribeDBClusters verwenden und den `DBClusterIdentifier`-Parameter auf eine DB-Instance-ID festlegen. Details zum Secret sind in der Ausgabe enthalten

Wenn Sie über den geheimen ARN verfügen, können Sie mithilfe des GetSecretValueSecrets Manager-Vorgangs Details zu dem Secret anzeigen.

Datenschutz in Amazon RDS

Das AWS Modell der geteilten Verantwortung wird auch auf den Datenschutz in Amazon Relational Database Service angewendet. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon RDS oder anderen AWS-Services über die Konsole, API, AWS CLI oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Themen

Datenschutz durch Verschlüsselung

Sie können die Verschlüsselung für Datenbankressourcen aktivieren. Sie können auch Verbindungen zu DB- Clustern verschlüsseln.

Themen

- Verschlüsseln von Amazon Aurora-Ressourcen
- AWS KMS key-Verwaltung
- Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer
- Rotieren Ihrer SSL/TLS-Zertifikate

Verschlüsseln von Amazon Aurora-Ressourcen

Amazon Aurora kann Ihre Amazon Aurora-DB-Cluster verschlüsseln. Daten, die im Ruhezustand verschlüsselt werden, umfassen den zugehörigen Speicherplatz von DB-Clustern sowie deren automatisierte Backups, Lesereplikate und Snapshots.

Amazon Aurora-verschlüsselte DB-Cluster verwenden den standardmäßig in der Branche verwendeten AES-256-Verschlüsselungsalgorithmus, um Ihre Daten auf dem Server zu verschlüsseln, der Ihre Amazon Aurora-DB-Cluster hostet. Sobald Sie die Daten verschlüsselt haben, übernimmt Amazon Aurora die Authentifizierung des Zugriffs und die Entschlüsselung Ihrer Daten auf transparente Art und Weise und mit minimaler Auswirkung auf die Leistung. Sie müssen Ihre Datenbank-Client-Anwendungen nicht ändern, um Verschlüsselung anzuwenden.

> **Note**
>
> Bei verschlüsselten und unverschlüsselten werden Daten, die zwischen der Quelle und den Read Replicas übertragen werden, verschlüsselt, auch wenn sie regionsübergreifend repliziert werden. AWS

Themen

- Übersicht über die Verschlüsselung von Amazon Aurora-Ressourcen
- Verschlüsseln eines Amazon-Aurora-DB-Clusters
- Bestimmen, ob die Verschlüsselung für einen DB-Cluster aktiviert ist
- Verfügbarkeit der Amazon Aurora-Verschlüsselung
- Verschlüsselung während der Übertragung
- Einschränkungen von Amazon Aurora-verschlüsselten DB-Clustern

Übersicht über die Verschlüsselung von Amazon Aurora-Ressourcen

Amazon Aurora-verschlüsselte DB-Cluster bieten zusätzlichen Datenschutz, indem Sie Ihre Daten vor unautorisiertem Zugriff auf den zugehörigen Speicherplatz sichern. Sie können die Amazon Aurora-Verschlüsselung verwenden, um den Datenschutz für Ihre in der Cloud bereitgestellten Anwendungen zu erhöhen und die Compliance-Anforderungen bei der Verschlüsselung von Daten im Ruhezustand zu erfüllen.

Bei einem mit Amazon Aurora verschlüsselten DB-Cluster werden alle DB-Instances, Protokolle, Backups und Snapshots verschlüsselt. Lesereplikate von Amazon-Aurora-verschlüsselten Clustern können ebenfalls verschlüsselt werden. Amazon Aurora verwendet einen AWS Key Management Service Schlüssel, um diese Ressourcen zu verschlüsseln. Weitere Informationen über KMS-Schlüssel finden Sie unter AWS KMS keys im Entwicklerhandbuch zu AWS Key Management Service und in AWS KMS key-Verwaltung. Jede DB-Instanz im DB-Cluster wird mit demselben KMS-Schlüssel wie der DB-Cluster verschlüsselt. Wenn Sie einen verschlüsselten Snapshot kopieren, können Sie zum Verschlüsseln des Ziel-Snapshots einen anderen KMS-Schlüssel verwenden als den, der zum Verschlüsseln des Quell-Snapshots verwendet wurde.

Sie können einen Von AWS verwalteter Schlüssel verwenden oder vom Kunden verwaltete Schlüssel erstellen. Zur Verwaltung der vom Kunden verwalteten Schlüssel, die für die Ver- und Entschlüsselung Ihrer Amazon Aurora-Ressourcen verwendet werden, verwenden Sie die AWS Key Management Service (AWS KMS). AWS KMS kombiniert sichere, hochverfügbare Hardware und Software, um ein für die Cloud skaliertes Schlüsselverwaltungssystem bereitzustellen. Mit AWS KMS dieser können Sie vom Kunden verwaltete Schlüssel erstellen und die Richtlinien definieren, die steuern, wie diese vom Kunden verwalteten Schlüssel verwendet werden können. AWS KMS unterstützt CloudTrail, sodass Sie die Verwendung von KMS-Schlüsseln überprüfen können, um sicherzustellen, dass vom Kunden verwaltete Schlüssel ordnungsgemäß verwendet werden. Sie können Ihre vom Kunden verwalteten Schlüssel mit Amazon Aurora und unterstützten AWS Diensten wie Amazon S3, Amazon EBS und Amazon Redshift verwenden. Eine Liste der Dienste, die integriert sind, finden Sie unter AWS KMSAWS Serviceintegration.

Verschlüsseln eines Amazon-Aurora-DB-Clusters

Wählen Sie Enable encryption (Verschlüsselung aktivieren) in der Konsole aus, um einen neuen DB-Cluster zu verschlüsseln. Weitere Informationen zum Erstellen eines DB-Clusters finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Wenn Sie den AWS CLI Befehl create-db-cluster verwenden, um einen verschlüsselten DB-Cluster zu erstellen, legen Sie den Parameter fest. `--storage-encrypted` Wenn Sie die API-Operation CreateDBCluster verwenden, legen Sie den Parameter `StorageEncrypted` auf „true“ fest.

Wenn Sie einen verschlüsselten DB-Cluster erstellen, können Sie einen vom Kunden verwalteten Schlüssel oder den Von AWS verwalteter Schlüssel für Amazon Aurora zur Verschlüsselung Ihres DB-Clusters wählen. Wenn Sie die Schlüssel-ID für einen vom Kunden verwalteten Schlüssel nicht angeben, verwendet Amazon Aurora die Von AWS verwalteter Schlüssel für Ihren neuen DB-Cluster. Amazon Aurora erstellt eine Von AWS verwalteter Schlüssel für Amazon Aurora für Ihr AWS Konto. Ihr AWS Konto hat Von AWS verwalteter Schlüssel für Amazon Aurora für jede AWS Region ein anderes.

Weitere Informationen über KMS-Schlüssel finden Sie unter AWS KMS keys im Entwicklerhandbuch zu AWS Key Management Service .

Sobald Sie einen verschlüsselten DB-Cluster erstellt haben, können Sie den von diesem DB-Cluster verwendeten KMS-Schlüssel nicht mehr ändern. Stellen Sie daher sicher, dass Sie Ihre KMS-Schlüsselanforderungen bestimmen, bevor Sie Ihren verschlüsselten DB-Cluster erstellen.

Wenn Sie den AWS CLI `create-db-cluster` Befehl verwenden, um einen verschlüsselten DB-Cluster mit einem vom Kunden verwalteten Schlüssel zu erstellen, setzen Sie den `--kms-key-id` Parameter auf eine beliebige Schlüssel-ID für den KMS-Schlüssel. Wenn Sie den Vorgang Amazon RDS API `CreateDBInstance` verwenden, setzen Sie den Parameter `KmsKeyId` auf einen beliebigen Schlüsselbezeichner für den KMS-Schlüssel. Um einen vom Kunden verwalteten Schlüssel in einem anderen AWS -Konto zu verwenden, geben Sie die Schlüssel-ARN oder Alias-ARN an.

> **Important**
>
> Amazon Aurora kann den Zugriff auf den KMS-Schlüssel für einen DB-Cluster verlieren, wenn Sie den KMS-Schlüssel deaktivieren. In diesen Fällen geht der verschlüsselte DB-Cluster in Kürze in den `inaccessible-encryption-credentials-recoverable` Status über. Der DB-Cluster verbleibt sieben Tage lang in diesem Zustand. Während dieser Zeit wird die Instance gestoppt. API-Aufrufe, die während dieser Zeit an den DB-Cluster getätigt wurden, sind möglicherweise nicht erfolgreich. Um den DB-Cluster wiederherzustellen, aktivieren Sie den KMS-Schlüssel und starten Sie diesen DB-Cluster neu. Aktivieren Sie den KMS-Schlüssel aus dem AWS Management Console. Starten Sie den DB-Cluster mit dem AWS CLI -Befehl start-db-cluster oder AWS Management Console neu.

Wenn der DB-Cluster nicht innerhalb von sieben Tagen wiederhergestellt wird, wechselt er in den `inaccessible-encryption-credentials` Terminalstatus. In diesem Zustand ist der DB-Cluster nicht mehr nutzbar und Sie können den DB-Cluster nur aus einem Backup wiederherstellen. Wir empfehlen dringend, dass Sie immer Backups für verschlüsselte DB-Cluster aktivieren, um den Verlust verschlüsselter Daten in Ihren Datenbanken zu verhindern. Während der Erstellung eines DB-Clusters prüft Aurora, ob der aufrufende Principal Zugriff auf den KMS-Schlüssel hat, und generiert aus dem KMS-Schlüssel einen Grant, den es für die gesamte Lebensdauer des DB-Clusters verwendet. Das Widerrufen des Zugriffs der aufrufenden Prinzipale auf den KMS-Schlüssel hat keine Auswirkungen auf eine laufende Datenbank. Wenn KMS-Schlüssel in kontoübergreifenden Szenarien verwendet werden, z. B. beim Kopieren eines Snapshots in ein anderes Konto, muss der KMS-Schlüssel mit dem anderen Konto geteilt werden. Wenn Sie aus dem Snapshot einen DB-Cluster erstellen, ohne einen anderen KMS-Schlüssel anzugeben, verwendet der neue Cluster den KMS-Schlüssel aus dem Quellkonto. Das Widerrufen des Zugriffs auf den Schlüssel nach der Erstellung des DB-Clusters hat keine Auswirkungen auf den Cluster. Die Deaktivierung des Schlüssels wirkt sich jedoch auf alle DB-Cluster aus, die mit diesem Schlüssel verschlüsselt wurden. Um dies zu verhindern, geben Sie während des Snapshot-Kopiervorgangs einen anderen Schlüssel an.

Bestimmen, ob die Verschlüsselung für einen DB-Cluster aktiviert ist

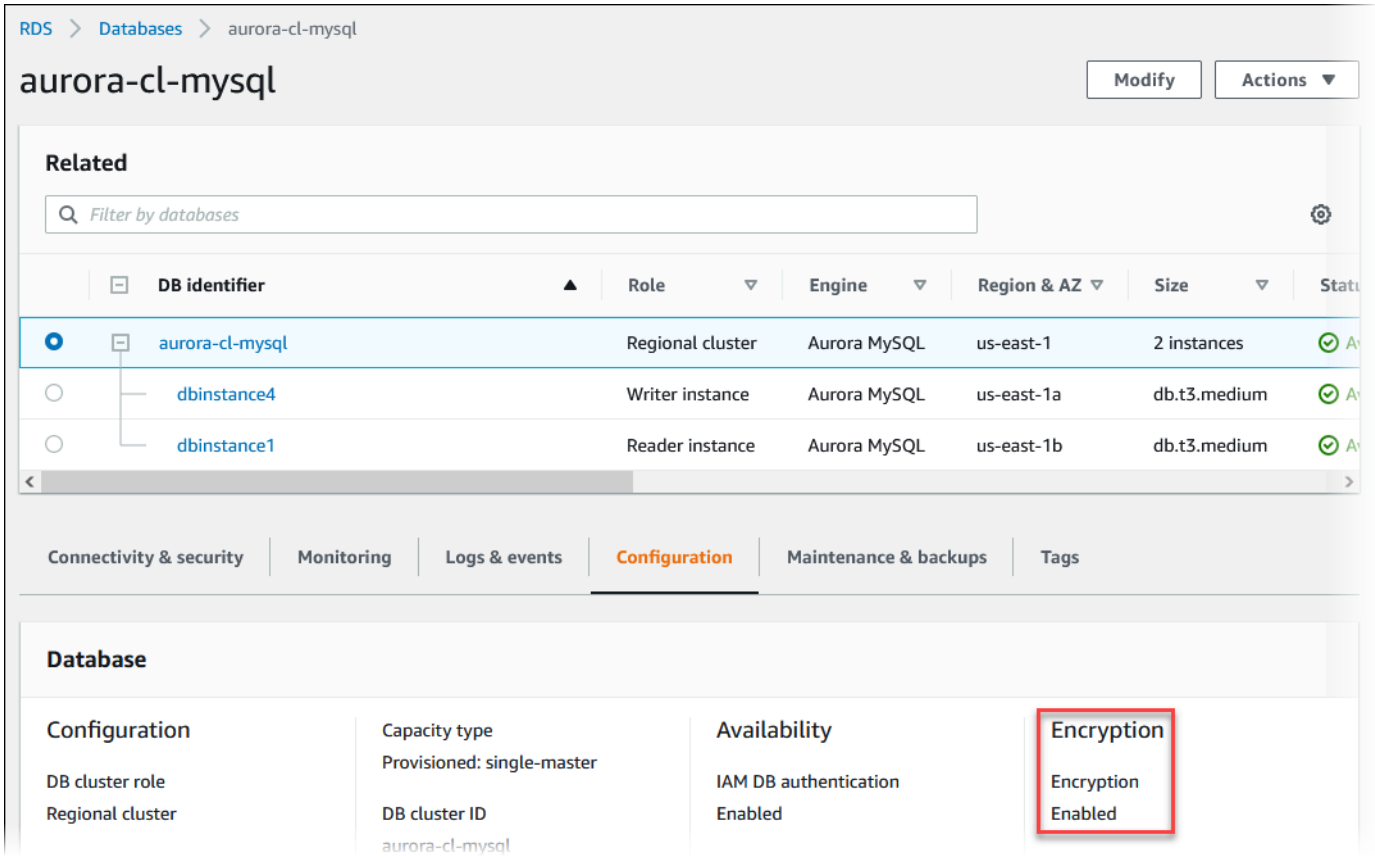
Sie können die AWS Management Console, oder RDS-API verwenden AWS CLI, um festzustellen, ob die Verschlüsselung im Ruhezustand für einen DB-Cluster aktiviert ist.

Konsole

So ermitteln Sie, ob die Verschlüsselung im Ruhezustand für einen DB-Cluster aktiviert ist

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie den Namen des DB-Clusters aus, den Sie überprüfen möchten, um dessen Details anzuzeigen.
4. Wählen Sie die Registerkarte Konfiguration aus und überprüfen Sie den Wert für die Verschlüsselung.

   Es zeigt entweder Aktiviert oder Nicht aktiviert.



AWS CLI

Rufen Sie den Befehl describe-db-clusters mit der folgenden Option auf, um festzustellen AWS CLI, ob die Verschlüsselung im Ruhezustand für einen DB-Cluster aktiviert ist:

- `--db-cluster-identifier` – der Name des DB-Clusters.

Im folgenden Beispiel wird eine Abfrage verwendet, um entweder `TRUE` oder `FALSE` bezüglich der Verschlüsselung im Ruhezustand für den `mydb` DB-Cluster zurückzugeben.

Example

```
aws rds describe-db-clusters --db-cluster-identifier mydb --query "*[].
{StorageEncrypted:StorageEncrypted}" --output text
```

RDS-API

Um zu ermitteln, ob die Verschlüsselung im Ruhezustand für einen DB-Cluster mithilfe der Amazon RDS-API aktiviert ist, rufen Sie die Operation DescribeDBClusters mit dem folgenden Parameter auf:

- `DBClusterIdentifier` – der Name des DB-Clusters.

Verfügbarkeit der Amazon Aurora-Verschlüsselung

Die Verschlüsselung von Amazon Aurora ist aktuell für alle Datenbank-Engines und Speichertypen verfügbar, .

> **Note**
>
> Die Amazon Aurora-Verschlüsselung ist für die DB-Instance-Klasse db.t2.micro nicht verfügbar.

Verschlüsselung während der Übertragung

AWS bietet sichere und private Konnektivität zwischen DB-Instances aller Typen. Darüber hinaus verwenden einige Instance-Typen die Offload-Funktionen der zugrunde liegenden Nitro-System-Hardware, um den Datenverkehr während der Übertragung zwischen Instances automatisch zu verschlüsseln. Diese Verschlüsselung verwendet AEAD-Algorithmen (Authenticated Encryption with Associated Data) mit 256-Bit-Verschlüsselung. Es gibt keine Auswirkungen auf die Netzwerkleistung. Um diese zusätzliche Verschlüsselung des Datenverkehrs während der Übertragung zwischen Instances zu unterstützen, müssen die folgenden Anforderungen erfüllt sein:

- Die Instances verwenden die folgenden Instance-Typen:
  - Allgemeiner Zweck: M6i, M6id, M6in, M6idn, M7g
  - Speicheroptimiert: R6i, R6id, R6in, R6idn, R7G, X2idn, X2iEDN, X2IEZn
- Die Instanzen AWS-Region befinden sich in derselben.
- Die Instances befinden sich in derselben VPC oder in per Peering verbundenen VPCs und der Datenverkehr wird nicht durch ein virtuelles Netzwerkgerät, z. B. einen Load Balancer oder ein Transit Gateway, geleitet.

Einschränkungen von Amazon Aurora-verschlüsselten DB-Clustern

Folgende Einschränkungen bestehen für Amazon Aurora-verschlüsselte DB-Cluster:

- Sie können die Verschlüsselung für einen verschlüsselten DB-Cluster nicht deaktivieren.
- Sie können keinen verschlüsselten Snapshot einer/eines unverschlüsselten DB-Clusters erstellen.

- Ein Snapshot eines verschlüsselten DB-clusters muss mit demselben KMS-Schlüssel verschlüsselt werden wie der DB-cluster.
- Unverschlüsselte DB-Cluster können nicht in verschlüsselte umgewandelt werden. Sie können jedoch einen unverschlüsselten Snapshot in einen verschlüsselten Aurora-DB-Cluster wiederherstellen. Geben Sie dazu bei der Wiederherstellung aus dem unverschlüsselten Snapshot einen KMS-Schlüssel an.
- Sie können keine verschlüsselte Aurora-Replica aus einem unverschlüsselten Aurora-DB-Cluster erstellen. Sie können keine unverschlüsselte Aurora-Replica aus einem verschlüsselten Aurora-DB-Cluster erstellen.
- Um einen verschlüsselten Snapshot von einer AWS Region in eine andere zu kopieren, müssen Sie den KMS-Schlüssel in der AWS Zielregion angeben. Dies liegt daran, dass KMS-Schlüssel für die AWS Region spezifisch sind, in der sie erstellt wurden.

  Der Quell-Snapshot bleibt den gesamten Kopiervorgang über verschlüsselt. Amazon Aurora verwendet Envelope-Verschlüsselung, um Daten während des Kopiervorgangs zu schützen. Weitere Informationen zur Envelope-Verschlüsselung finden Sie unter Envelope-Verschlüsselung im AWS Key Management Service -Entwicklerhandbuch.
- Sie können eine(n) verschlüsselte(n) DB-Cluster nicht entschlüsseln. Sie können jedoch Daten aus einer/einem verschlüsselten DB-Cluster exportieren und die Daten in eine(n) unverschlüsselte(n) DB-Cluster importieren.

AWS KMS key-Verwaltung

Amazon Aurora wird automatisch zur Schlüsselverwaltung in AWS Key Management Service (AWS KMS) integriert. Amazon Aurora verwendet eine Envelope-Verschlüsselung. Weitere Informationen zur Envelope-Verschlüsselung finden Sie unter Envelope-Verschlüsselung im AWS Key Management Service-Entwicklerhandbuch.

Sie können zwei Arten von AWS KMS-Schlüsseln verwenden, um Ihre DB-Cluster zu verschlüsseln.

- Wenn Sie die volle Kontrolle über einen KMS-Schlüssel haben möchten, müssen Sie einen vom Kunden verwalteten Schlüssel erstellen. Weitere Informationen über kundenverwaltete Schlüssel finden Sie unter Kundenverwaltete Schlüssel im AWS Key Management Service Developer Guide.

  Sie können einen Snapshot der verschlüsselt wurde, nicht mit dem Von AWS verwalteter Schlüssel der AWS Konten freigeben, die den Schnappschuss freigegeben haben.

- Von AWS verwaltete Schlüssel sind KMS-Schlüssel in Ihrem Konto, die in Ihrem Namen von einem AWS Dienst erstellt, verwaltet und verwendet werden, der mit AWS KMS. Standardmäßig wird der RDS-Von AWS verwalteter Schlüssel (`aws/rds`) für die Verschlüsselung verwendet. Sie können den RDS-Von AWS verwalteter Schlüssel nicht verwalten, rotieren oder löschen. Weitere Informationen zu Von AWS verwaltete Schlüssel finden Sie unter Von AWS verwaltete Schlüssel im AWS Key Management Service-Entwickler-Leitfaden.

Zur Verwaltung von KMS-Schlüsseln für verschlüsselte Amazon-Aurora-DB-Cluster verwenden Sie den AWS Key Management Service (AWS KMS) in der AWS KMS-Konsole, die AWS CLI- oder die AWS KMS-API. Verwenden Sie zur Anzeige von Audit-Protokollen für jede Aktion, die mit einem AWS-verwalteten oder kundenverwalteten Schlüssel durchgeführt wurde AWS CloudTrail. Weitere Informationen zum Rotieren der Schlüssel finden Sie unter Rotieren von AWS KMS-Schlüsseln.

> **Important**
>
> Wenn Sie Berechtigungen für einen KMS-Schlüssel deaktivieren oder widerrufen, der von einer RDS-Datenbank verwendet wird, versetzt RDS Ihre Datenbank in einen Terminalstatus, wenn Zugriff auf den KMS-Schlüssel erforderlich ist. Diese Änderung kann je nach Anwendungsfall, der Zugriff auf den KMS-Schlüssel erforderte, sofort oder verschoben werden. In diesem Fall ist der DB-Cluster nicht länger verfügbar und der aktuelle Zustand der Datenbank kann nicht mehr wiederhergestellt werden. Um den DB-Cluster wiederherzustellen, müssen Sie den Zugriff auf den KMS-Schlüssel für RDS erneut aktivieren und den DB-Cluster anschließend aus dem letzten Backup wiederherstellen.

Autorisieren der Verwendung eines kundenverwalteten Schlüssels

Wenn Aurora einen vom Kunden verwalteten Schlüssel für kryptografische Operationen verwendet, handelt es im Namen des Benutzers, der die Aurora-Ressource erstellt oder ändert.

Wenn Sie eine Aurora-Ressource mit einem vom Kunden verwalteten Schlüssel erstellen möchten, müssen Sie die Berechtigung haben, die folgenden Operationen für den vom Kunden verwalteten Schlüssel aufzurufen:

- kms:CreateGrant
- kms:DescribeKey

Sie können diese erforderlichen Berechtigungen in einer Schlüsselrichtlinie oder in einer IAM-Richtlinie angeben, wenn die Schlüsselrichtlinie dies zulässt.

Sie können die IAM-Richtlinie auf verschiedene Weise strikter gestalten. Um beispielsweise zu erlauben, dass der vom Kunden verwaltete Schlüssel nur für Anfragen verwendet wird, die von Aurora ausgehen, können Sie den kms:ViaService-Bedingungsschlüssel mit dem Wert `rds.<region>.amazonaws.com` verwenden. Sie können auch die Schlüssel oder Werte im Amazon-RDS-Verschlüsselungskontext als Bedingung für die Verwendung des vom Kunden verwalteten Schlüssels für die Verschlüsselung verwenden.

Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service-Entwicklerhandbuch und unter Schlüsselrichtlinien in AWS KMS.

Amazon-RDS-Verschlüsselungskontext

Wenn Aurora Ihren KMS-Schlüssel verwendet oder Amazon EBS den KMS-Schlüssel im Auftrag von Aurora verwendet, gibt der Service einen Verschlüsselungskontext an. Der Verschlüsselungskontext enthält zusätzliche authentifizierte Daten (AAD), anhand derer AWS KMS die Datenintegrität sicherstellt. Wenn für eine Verschlüsselungsoperation ein Verschlüsselungskontext angegeben wird, muss der Service denselben Verschlüsselungskontext auch für die Entschlüsselungsoperation angeben. Andernfalls schlägt die Entschlüsselung fehl. Der Verschlüsselungskontext wird zudem in Ihre AWS CloudTrail-Protokolle geschrieben, sodass Sie jederzeit nachvollziehen können, warum ein bestimmter KMS-Schlüssel verwendet wurde. Ihre CloudTrail-Protokolle können sehr viele Einträge zur Verwendung eines KMS-Schlüssels enthalten. Der Verschlüsselungskontext in den einzelnen Protokolleinträgen kann Ihnen jedoch helfen, herauszufinden, warum der KMS-Schlüssel zu einem gegebenen Zeitpunkt verwendet wurde.

Aurora gibt als Verschlüsselungskontext immer mindestens die ID der DB-Instance an, wie im folgenden JSON-Beispiel illustriert:

```
{ "aws:rds:db-id": "db-CQYSMDPBRZ7BPMH7Y3RTDG5QY" }
```

Anhand dieses Verschlüsselungskontexts können Sie herausfinden, für welche DB-Instance der KMS-Schlüssel verwendet wurde.

Wird Ihr KMS-Schlüssel für eine bestimmte DB-Instance und ein bestimmtes Amazon-EBS-Volume verwendet, werden sowohl die ID der DB-Instance als auch die ID des EBS-Volumes als Verschlüsselungskontext angegeben, wie im folgenden JSON-Beispiel zu sehen:

```
{
  "aws:rds:db-id": "db-BRG7VYS3SVIFQW7234EJQOM5RQ",
  "aws:ebs:id": "vol-ad8c6542"
}
```

Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer

Sie können Secure Socket Layer (SSL) oder Transport Layer Security (TLS) aus Ihrer Anwendung verwenden, um eine Verbindung zu einem DB-Cluster zu verschlüsseln, der mit Aurora MySQL oder Aurora PostgreSQL läuft.

Optional kann Ihre SSL/TLS-Verbindung eine Überprüfung der Serveridentität durchführen, indem das in Ihrer Datenbank installierte Serverzertifikat validiert wird. Gehen Sie wie folgt vor, um eine Überprüfung der Serveridentität vorzuschreiben:

1. Wählen Sie die Zertifizierungsstelle (Certificate Authority, CA) aus, die das DB-Serverzertifikat für Ihre Datenbank zertifiziert. Weitere Informationen zu Zertifizierungsstellen finden Sie unter Zertifizierungsstellen.
2. Laden Sie ein Zertifikatspaket herunter, das verwendet werden soll, wenn Sie eine Verbindung zur Datenbank herstellen. Informationen zum Herunterladen eines Zertifikatspakets finden Sie unter Zertifikatspakete für alle AWS-Regionen und Zertifikatspakete für bestimmte AWS-Regionen.

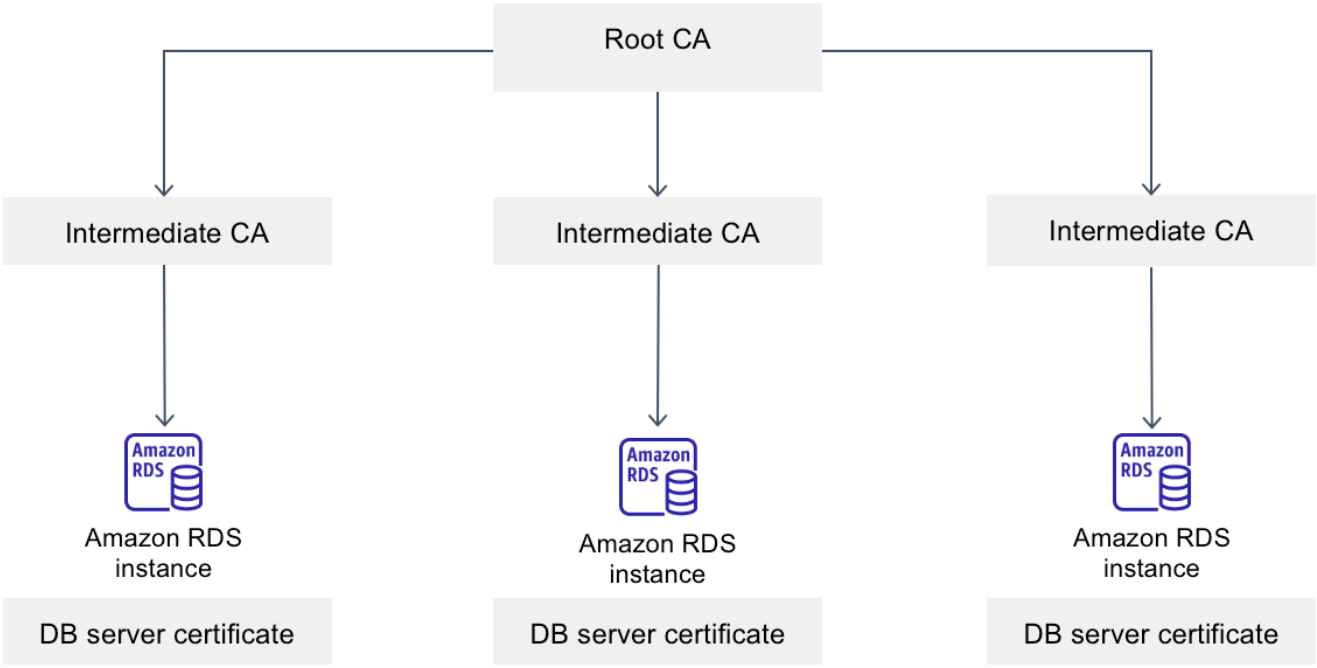
   > **Note**
   >
   > Alle Zertifikate stehen nur über SSL/TLS-Verbindungen zum Download zur Verfügung.

3. Stellen Sie anhand des Verfahrens Ihrer DB-Engine zur Implementierung von SSL/TLS-Verbindungen eine Verbindung zur Datenbank her. Jede DB-Engine hat einen eigenen Vorgang für die Implementierung von SSL/TLS. Verwenden Sie den entsprechenden Link für Ihre DB-Engine, um mehr über die Implementierung von SSL/TLS in Ihrer Datenbank zu erfahren:
   - Sicherheit in Amazon Aurora MySQL
   - Sicherheit in Amazon Aurora PostgreSQL

Zertifizierungsstellen

Die Zertifizierungsstelle (CA) ist das Zertifikat, das die Stamm-CA an der Spitze der Zertifikatskette identifiziert. Die CA signiert das DB-Serverzertifikat. Dies ist das Serverzertifikat, das auf jeder DB-

Instance installiert ist. Das DB-Serverzertifikat identifiziert die DB-Instance als vertrauenswürdigen Server.



Amazon RDS stellt die folgenden Zertifizierungsstellen bereit, um das DB-Serverzertifikat für eine Datenbank zu signieren.

Zertifizierungsstelle (Certificate authority, CA)	Beschreibung
rds-ca-2019	Verwendet eine Zertifizierungsstelle mit dem privaten Schlüsselalgorithmus RSA 2048 und dem SHA256-Signaturalgorithmus. Diese CA läuft 2024 ab und unterstützt keine automatische Rotation von Serverzertifikaten. Wenn Sie diese CA verwenden und den gleichen Standard beibehalten möchten, empfehlen wir Ihnen, zur rds-ca-rsa2048-g1-CA zu wechseln.
rds-ca-rsa2048-g1	Verwendet eine Zertifizierungsstelle mit dem privaten Schlüsselalgorithmus RSA 2048 und dem SHA256-Signaturalgorithmus in den meisten AWS-Regionen.

Zertifizierungsstelle (Certificate authority, CA)	Beschreibung
	In der AWS GovCloud (US) Regions verwendet diese CA eine Zertifizierungsstelle mit dem RSA 2048-Algorithmus für private Schlüssel und dem SHA384-Signaturalgorithmus. Diese CA bleibt länger gültig als die CA rds-ca-2019. Diese CA unterstützt die automatische Rotation von Serverzertifikaten.
rds-ca-rsa4096-g1	Verwendet eine Zertifizierungsstelle mit dem privaten Schlüsselalgorithmus RSA 4096 und dem SHA384-Signaturalgorithmus. Diese CA unterstützt die automatische Rotation von Serverzertifikaten.
rds-ca-ecc384-g1	Verwendet eine Zertifizierungsstelle mit dem privaten Schlüsselalgorithmus ECC 384 und dem SHA384-Signaturalgorithmus. Diese CA unterstützt die automatische Rotation von Serverzertifikaten.

> **Note**
>
> Wenn Sie das verwenden AWS CLI, können Sie die Gültigkeiten der oben aufgeführten Zertifizierungsstellen mithilfe von describe-certificates überprüfen.

Diese CA-Zertifikate sind im regionalen und globalen Zertifikat-Bundle enthalten. Wenn Sie die Zertifizierungsstelle rds-ca-rsa 2048-g1, rds-ca-rsa 4096-g1 oder rds-ca-ecc 384-g1 mit einer Datenbank verwenden, verwaltet RDS das DB-Serverzertifikat in der Datenbank. RDS rotiert das DB-Serverzertifikat automatisch, bevor es abläuft.

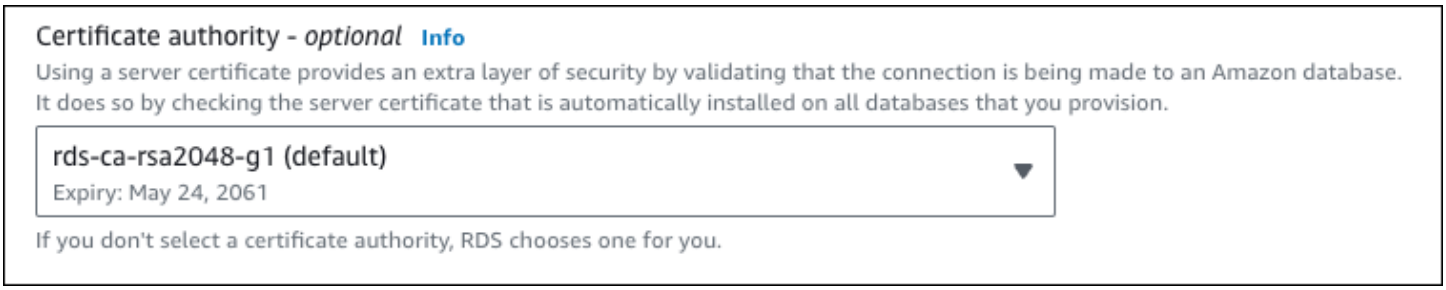
Einstellung der CA für Ihre Datenbank

Sie können die CA für eine Datenbank einstellen, wenn Sie die folgenden Aufgaben ausführen:

- Einen Aurora-DB-Cluster erstellen — Sie können die CA für eine DB-Instance in einem Aurora-Cluster festlegen, wenn Sie die erste DB-Instance im DB-Cluster mithilfe der AWS CLI oder RDS-API erstellen. Derzeit können Sie die CA für die DB-Instances in einem DB-Cluster nicht einstellen, wenn Sie den DB-Cluster über die RDS-Konsole erstellen. Anweisungen finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.
- Eine DB-Instance ändern – Sie können die CA für eine DB-Instance in einem DB-Cluster festlegen, indem Sie sie ändern. Anweisungen finden Sie unter Ändern einer DB-Instance in einem DB-Cluster.

> **Note**
>
> Die Standard-CA ist auf rds-ca-rsa 2048-g1 festgelegt. Sie können die Standard-CA für Sie überschreiben, AWS-Konto indem Sie den Befehl modify-certificates verwenden.

Die verfügbaren CAs hängen von der DB-Engine und der DB-Engine-Version ab. Wenn Sie die AWS Management Console verwenden, können Sie die CA mithilfe der Einstellung Certificate authority (Zertifizierungsstelle) auswählen, wie in der folgenden Abbildung gezeigt.



Die Konsole zeigt nur die CAs an, die für die DB-Engine und die DB-Engine-Version verfügbar sind. Wenn Sie die verwenden AWS CLI, können Sie die CA für eine DB-Instance mit dem create-db-instanceBefehl or festlegen. modify-db-instance

Wenn Sie den verwenden AWS CLI, können Sie die verfügbaren Zertifizierungsstellen für Ihr Konto mithilfe des Befehls describe-certificates einsehen. Dieser Befehl zeigt in der Ausgabe auch das Ablaufdatum für jede CA in `ValidTill` an. Mithilfe des Befehls können Sie die Zertifizierungsstellen finden, die für eine bestimmte DB-Engine und DB-Engine-Version verfügbar sind. describe-db-engine-versions

Das folgende Beispiel zeigt die CAs, die für die DB-Engine-Standardversion von RDS für PostgreSQL verfügbar sind.

```
aws rds describe-db-engine-versions --default-only --engine postgres
```

Ihre Ausgabe sieht Folgendem ähnlich. Die verfügbaren CAs sind unter `SupportedCACertificateIdentifiers` aufgeführt. Die Ausgabe zeigt auch, ob die Version der DB-Engine das Rotieren des Zertifikats ohne Neustart in `SupportsCertificateRotationWithoutRestart` unterstützt.

```
{
    "DBEngineVersions": [
        {
            "Engine": "postgres",
            "MajorEngineVersion": "13",
            "EngineVersion": "13.4",
            "DBParameterGroupFamily": "postgres13",
            "DBEngineDescription": "PostgreSQL",
            "DBEngineVersionDescription": "PostgreSQL 13.4-R1",
            "ValidUpgradeTarget": [],
            "SupportsLogExportsToCloudwatchLogs": false,
            "SupportsReadReplica": true,
            "SupportedFeatureNames": [
                "Lambda"
            ],
            "Status": "available",
            "SupportsParallelQuery": false,
            "SupportsGlobalDatabases": false,
            "SupportsBabelfish": false,
            "SupportsCertificateRotationWithoutRestart": true,
            "SupportedCACertificateIdentifiers": [
                "rds-ca-2019",
                "rds-ca-rsa2048-g1",
                "rds-ca-ecc384-g1",
                "rds-ca-rsa4096-g1"
            ]
        }
    ]
}
```

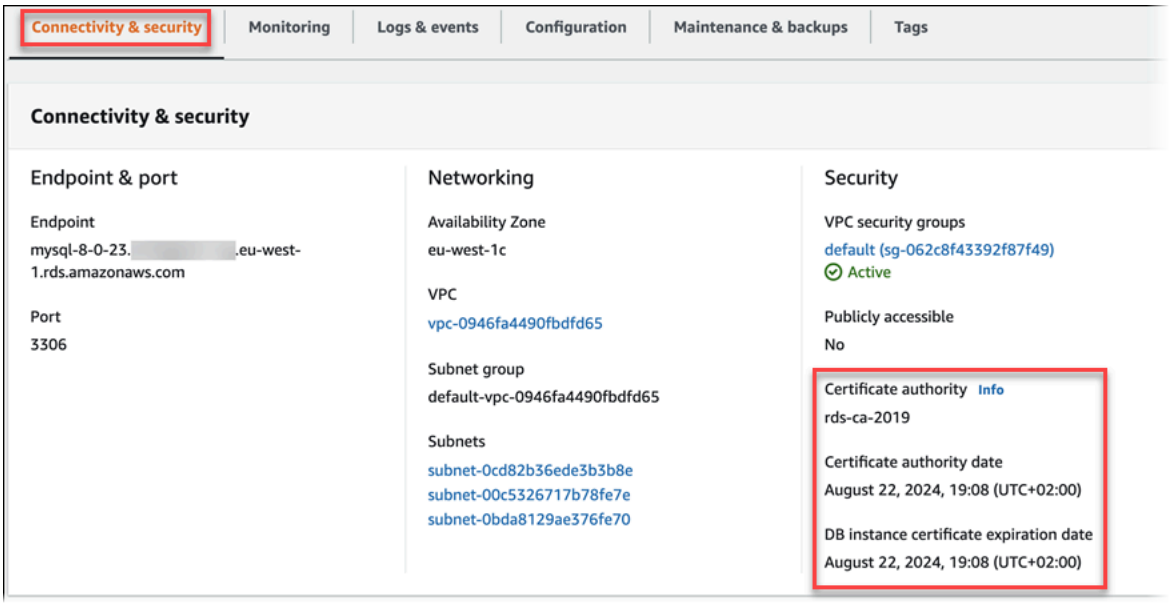
Gültigkeiten von DB-Serverzertifikaten

Die Gültigkeit des DB-Serverzertifikats hängt von der DB-Engine und der Version der DB-Engine ab. Wenn die Version der DB-Engine das Rotieren des Zertifikats ohne Neustart unterstützt, beträgt die Gültigkeit des DB-Serverzertifikats 1 Jahr. Andernfalls beträgt die Gültigkeit 3 Jahre.

Weitere Informationen zur Rotation des DB-Serverzertifikats finden Sie unter Automatische Rotation von Serverzertifikaten.

Die CA für Ihre DB-Instance anzeigen

Sie können die Details zur CA für eine Datenbank einsehen, indem Sie die Registerkarte Konnektivität und Sicherheit in der Konsole aufrufen, wie in der folgenden Abbildung dargestellt.



Wenn Sie die verwenden AWS CLI, können Sie die Details zur CA für eine DB-Instance mithilfe des describe-db-instancesBefehls anzeigen.

Verwenden Sie den folgenden Befehl, um den Inhalt Ihres CA-Zertifikatspakets zu überprüfen:

```
keytool -printcert -v -file global-bundle.pem
```

Zertifikatspakete für alle AWS-Regionen

Um ein Zertifikatspaket für alle zu erhalten AWS-Regionen, laden Sie es von https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem herunter.

Das Paket enthält sowohl das `rds-ca-2019` Zwischen- als auch das Stammzertifikat. Das Paket enthält auch die `rds-ca-ecc384-g1` CA-Stammzertifikate `rds-ca-rsa2048-g1rds-ca-rsa4096-g1`, und. Ihr Application Trust Store muss nur das Root-CA-Zertifikat registrieren.

Wenn Ihre Anwendung unter Microsoft Windows läuft und eine PKCS7-Datei benötigt, können Sie das PKCS7-Zertifikatspaket von https://truststore.pki.rds.amazonaws.com/global/global-bundle.p7b herunterladen.

> **Note**
>
> Amazon RDS Proxy and Zertifikate von AWS Certificate Manager (ACM). Wenn Sie RDS Proxy verwenden, müssen Sie keine Amazon RDS-Zertifikate herunterladen oder Anwendungen aktualisieren, die RDS-Proxy-Verbindungen verwenden. Weitere Informationen finden Sie unter Verwenden von TLS/SSL mit RDS Proxy.
> Wenn Sie Amazon RDS-Zertifikate verwendenAurora Serverless v1, ist das Herunterladen von Amazon RDS-Zertifikaten nicht erforderlich. Weitere Informationen finden Sie unter Verwenden von TLS/SSL mit Aurora Serverless v1.

Zertifikatspakete für bestimmte AWS-Regionen

Das Paket enthält sowohl die `rds-ca-2019` Zwischen- als auch die Stammzertifikate. Das Paket enthält auch die `rds-ca-ecc384-g1` CA-Stammzertifikate `rds-ca-rsa2048-g1rds-ca-rsa4096-g1`, und. Ihr Application Trust Store muss nur das Root-CA-Zertifikat registrieren.

Um ein Zertifikatspaket für ein zu erhalten AWS-Region, laden Sie es über den Link AWS-Region in der folgenden Tabelle herunter.

AWS Region	Zertifikat-Paket (PEM)	Zertifikat-Paket (PKCS7)
USA Ost (Nord-Virginia)	us-east-1-bundle.pem	us-east-1-bundle.p7b
US East (Ohio)	us-east-2-bundle.pem	us-east-2-bundle.p7b
USA West (Nordkalifornien)	us-west-1-bundle.pem	us-west-1-bundle.p7b
USA West (Oregon)	us-west-2-bundle.pem	us-west-2-bundle.p7b
Africa (Cape Town)	af-south-1-bundle.pem	af-south-1-bundle.p7b
Asia Pacific (Hong Kong)	ap-east-1-bundle.pem	ap-east-1-bundle.p7b
Asien-Pazifik (Hyderabad)	ap-south-2-bundle.pem	ap-south-2-bundle.p7b
Asien-Pazifik (Jakarta)	ap-southeast-3-bundle.pem	ap-southeast-3-bundle.p7b
Asien-Pazifik (Melbourne)	ap-southeast-4-bundle.pem	ap-southeast-4-bundle.p7b

AWS Region	Zertifikat-Paket (PEM)	Zertifikat-Paket (PKCS7)
Asien-Pazifik (Mumbai)	ap-south-1-bundle.pem	ap-south-1-bundle.p7b
Asia Pacific (Osaka)	ap-northeast-3-bundle.pem	ap-northeast-3-bundle.p7b
Asien-Pazifik (Tokio)	ap-northeast-1-bundle.pem	ap-northeast-1-bundle.p7b
Asia Pacific (Seoul)	ap-northeast-2-bundle.pem	ap-northeast-2-bundle.p7b
Asien-Pazifik (Singapur)	ap-southeast-1-bundle.pem	ap-southeast-1-bundle.p7b
Asien-Pazifik (Sydney)	ap-southeast-2-bundle.pem	ap-southeast-2-bundle.p7b
Canada (Central)	ca-central-1-bundle.pem	ca-central-1-bundle.p7b
Kanada West (Calgary)	ca-west-1-bundle.pem	ca-west-1-bundle.p7b
Europa (Frankfurt)	eu-central-1-bundle.pem	eu-central-1-bundle.p7b
Europa (Irland)	eu-west-1-bundle.pem	eu-west-1-bundle.p7b
Europe (London)	eu-west-2-bundle.pem	eu-west-2-bundle.p7b
Europe (Milan)	eu-south-1-bundle.pem	eu-south-1-bundle.p7b
Europe (Paris)	eu-west-3-bundle.pem	eu-west-3-bundle.p7b
Europa (Spain)	eu-south-2-bundle.pem	eu-south-2-bundle.p7b
Europa (Stockholm)	eu-north-1-bundle.pem	eu-north-1-bundle.p7b
Europa (Zürich)	eu-central-2-bundle.pem	eu-central-2-bundle.p7b
Israel (Tel Aviv)	il-central-1-bundle.pem	il-central-1-bundle.p7b
Naher Osten (Bahrain)	me-south-1-bundle.pem	me-south-1-bundle.p7b
Naher Osten (VAE)	me-central-1-bundle.pem	me-central-1-bundle.p7b
Südamerika (São Paulo)	sa-east-1-bundle.pem	sa-east-1-bundle.p7b

AWS GovCloud (US) -Zertifikate

Um ein Zertifikatspaket zu erhalten, das sowohl die Zwischen- als auch die Stammzertifikate für das AWS GovCloud (US) Region s enthält, laden Sie es von https://truststore.pki herunter. us-gov-west-1.rds.amazonaws.com/global/global-bundle.pem.

Wenn Ihre Anwendung unter Microsoft Windows läuft und eine PKCS7-Datei benötigt, können Sie das PKCS7-Zertifikatspaket von https://truststore.pki herunterladen. us-gov-west-1.rds.amazonaws.com/global/global-bundle.p7b.

Das Paket enthält sowohl das Zwischen- als auch das Stammzertifikat. `rds-ca-2019` Das Paket enthält auch die `rds-ca-ecc384-g1` CA-Stammzertifikate `rds-ca-rsa2048-g1rds-ca-rsa4096-g1`, und. Ihr Application Trust Store muss nur das Root-CA-Zertifikat registrieren.

Um ein Zertifikatspaket für ein zu erhalten AWS GovCloud (US) Region, laden Sie es über den Link AWS GovCloud (US) Region in der folgenden Tabelle herunter.

AWS GovCloud (US) Region	Zertifikat-Paket (PEM)	Zertifikat-Paket (PKCS7)
AWS GovCloud (US-Ost)	us-gov-east-1-bundle.pem	us-gov-east-1-Bundle.p7b
AWS GovCloud (US-West)	us-gov-west-1-bundle.pem	us-gov-west-1-Bundle.p7b

Rotieren Ihrer SSL/TLS-Zertifikate

Die Zertifikate der Amazon RDS Certificate Authority rds-ca-2019 laufen im August 2024 ab. Wenn Sie Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) mit Zertifikatsüberprüfung verwenden oder dies planen, um eine Verbindung zu Ihren RDS-DB-Instances herzustellen, sollten Sie die Verwendung eines der neuen CA-Zertifikate rds-ca-rsa 2048-g1, rds-ca-rsa 4096-g1 oder 384-g1 in Betracht ziehen. rds-ca-ecc Wenn Sie SSL/TLS derzeit nicht mit der Zertifikatüberprüfung verwenden, haben Sie dennoch möglicherweise ein abgelaufenes CA-Zertifikat und müssen dieses auf ein neues CA-Zertifikat aktualisieren, wenn Sie über SSL/TLS mit Zertifikatüberprüfung eine Verbindung zu Ihren RDS-Datenbanken herstellen möchten.

Befolgen Sie diese Anweisungen, um Ihre Updates abzuschließen. Bevor Sie Ihre DB-Instances für die Verwendung des neuen CA-Zertifikats aktualisieren, stellen Sie sicher, dass Sie Ihre Clients oder Anwendungen aktualisieren, die eine Verbindung zu Ihren RDS-Datenbanken herstellen.

Amazon RDS bietet neue CA-Zertifikate als bewährte AWS Sicherheitsmethode. Informationen zu den neuen Zertifikaten und den unterstützten AWS Regionen finden Sie unterVerwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

> **Note**
>
> Amazon RDS Proxy and Zertifikate von AWS Certificate Manager (ACM). Wenn Sie RDS Proxy verwenden, müssen Sie bei der Rotation Ihres SSL/TLS-Zertifikats keine Anwendungen aktualisieren, die RDS-Proxy-Verbindungen verwenden. Weitere Informationen finden Sie unter Verwenden von TLS/SSL mit RDS Proxy.
> Wenn Sie Amazon RDS-Zertifikate verwendenAurora Serverless v1, ist das Herunterladen von Amazon RDS-Zertifikaten nicht erforderlich. Weitere Informationen finden Sie unter Verwenden von TLS/SSL mit Aurora Serverless v1.

> **Note**
>
> Wenn Sie eine Go-Anwendung der Version 1.15 mit einer DB-Instance verwenden, das vor dem 28. Juli 2020 erstellt oder auf das rds-ca-2019-Zertifikat aktualisiert wurde, müssen Sie das Zertifikat erneut aktualisieren. Mit dem Befehl `describe-db-engine-versions` finden Sie die CAs, die für eine bestimmte DB-Engine und DB-Engine-Version verfügbar sind.
> Wenn Sie Ihre Datenbank nach dem 28. Juli 2020 erstellt oder ihr Zertifikat aktualisiert haben, sind keine Maßnahmen erforderlich. Weitere Informationen finden Sie in GitHub Go-Ausgabe #39568.

Themen

- Aktualisierung Ihres CA-Zertifikats durch Änderung Ihrer DB-Instance
- Aktualisieren des CA-Zertifikats durch Anwenden der Wartung
- Automatische Rotation von Serverzertifikaten
- Beispielskript für den Import von Zertifikaten in Ihren Trust Store

Aktualisierung Ihres CA-Zertifikats durch Änderung Ihrer DB-Instance

Im folgenden Beispiel wird Ihr CA-Zertifikat von rds-ca-2019 auf rds-ca-rsa2048-g1 aktualisiert. Sie können ein anderes Zertifikat wählen. Weitere Informationen finden Sie unter Zertifizierungsstellen.

Aktualisieren Sie Ihren Application Trust Store, um Ausfallzeiten im Zusammenhang mit der Aktualisierung Ihres CA-Zertifikats zu reduzieren. Weitere Informationen zu Neustarts im Zusammenhang mit der Rotation von CA-Zertifikaten finden Sie unterAutomatische Rotation von Serverzertifikaten.

So aktualisieren Sie Ihr CA-Zertifikat, indem Sie Ihre DB-Instance Ihren Cluster ändern

1. Laden Sie das neue SSL/TLS-Zertifikat herunter wie unter beschriebe Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .
2. Aktualisieren Sie Ihre Anwendungen zur Verwendung der neuen SSL/TLS-Zertifikate.

   Die Methoden zur Aktualisierung von Anwendungen für neue SSL/TLS-Zertifikate hängen von Ihren spezifischen Anwendungen ab. Arbeiten Sie mit Ihren Anwendungsentwicklern zusammen, um die SSL/TLS-Zertifikate für Ihre Anwendungen zu aktualisieren.

   Informationen zur Prüfung auf SSL/TLS-Verbindungen und die Aktualisierung von Anwendungen für jede DB_Engine finden Sie in den folgenden Themen:

   - Aktualisieren von Anwendungen, um Verbindungen mit DB-Clustern von Aurora MySQL mithilfe neuer TLS-Zertifikate herzustellen
   - Aktualisieren von Anwendungen für die Verbindung zu Aurora-PostgreSQL-DB-Clustern mit neuen SSL/TLS-Zertifikaten

   Ein Beispielskript, das einen Trust Store für ein Linux-Betriebssystem aktualisiert, finden Sie unter Beispielskript für den Import von Zertifikaten in Ihren Trust Store.

   > **Note**
   >
   > Das Zertifikat-Bundle enthält Zertifikate für die neue und die alte CA, damit Sie Ihre Anwendung sicher aktualisieren und die Verbindung während der Übergangsphase aufrecht erhalten können. Wenn Sie das verwenden, um eine Datenbank AWS Database Migration Service zu einer zu migrieren, empfehlen wir die Verwendung des Zertifikatspakets, um die Konnektivität während der Migration sicherzustellen.

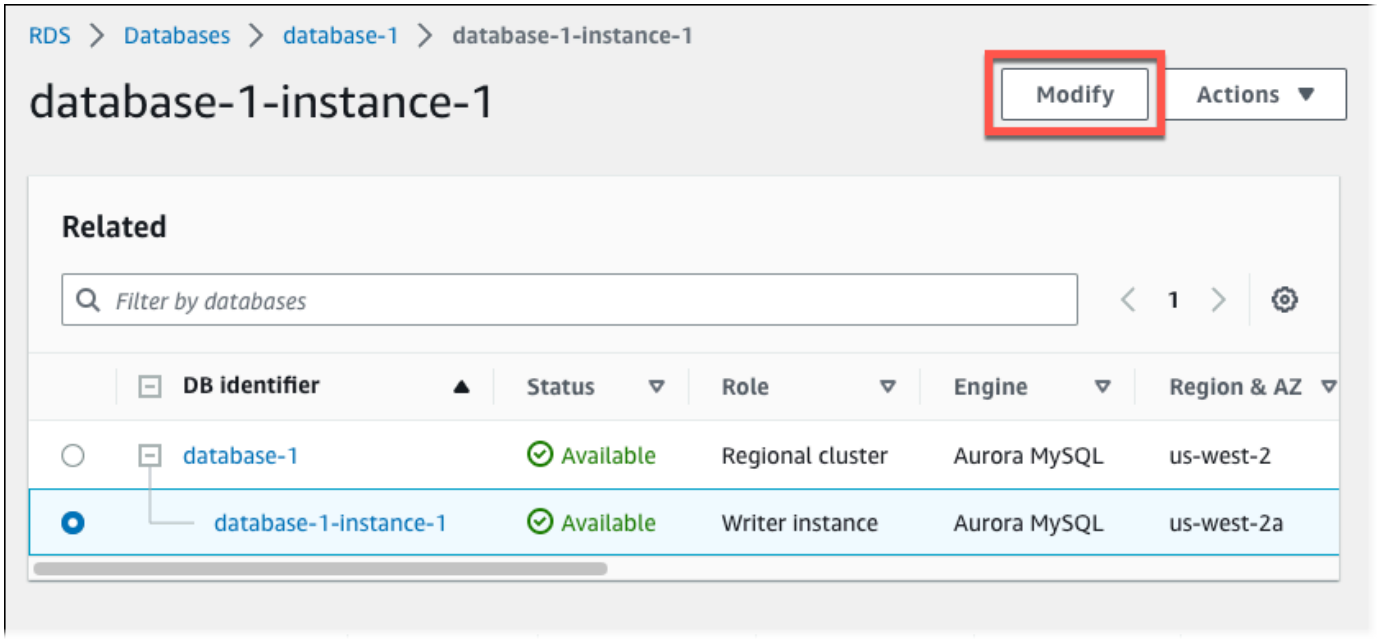
3. Ändern Sie die DB-Instance , um die CA von rds-ca-2019 auf rds-ca-rsa2048-g1 zu ändern. Verwenden Sie den Befehl describe-db-engine-versions und sehen Sie sich das Flag `SupportsCertificateRotationWithoutRestart` an, um zu überprüfen, ob Ihre Datenbank zum Aktualisieren der CA-Zertifikate neu gestartet werden muss.

> **Note**
>
> Starten Sie Ihren Babelfish-Cluster nach der Änderung neu, um das CA-Zertifikat zu aktualisieren.

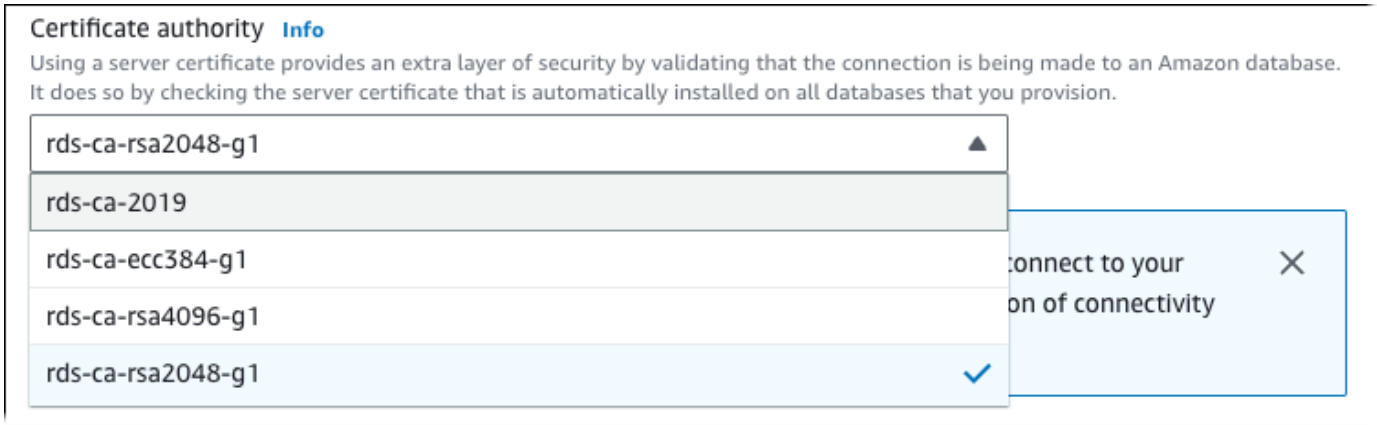
> **Important**
>
> Wenn nach dem Ablauf des Zertifikats Verbindungsprobleme auftreten, verwenden Sie die Option „Sofort anwenden“, indem Sie Sofort anwenden in der Konsole angeben oder die Option `--apply-immediately` mit der AWS CLI festlegen. Die Ausführung dieser Operation ist standardmäßig während Ihres nächsten Wartungsfensters eingeplant.
> Um eine Überschreibung für Ihre Cluster-CA festzulegen, die sich vom standardmäßigen RDS-CA unterscheidet, verwenden Sie den CLI-Befehl modify-certificates.

Konsole

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken und dann die DB-Instance aus, den Sie ändern möchten.
3. Wählen Sie Ändern aus.



4. Wählen Sie im Abschnitt Anbindung rds-ca-rsa2048-g1 aus.



5. Klicken Sie auf Weiter und überprüfen Sie die Zusammenfassung aller Änderungen.
6. Wählen Sie Sofort anwenden aus, um die Änderungen sofort anzuwenden.
7. Überprüfen Sie auf der Bestätigungsseite Ihre Änderungen. Wenn sie korrekt sind, wählen Sie „DB-Instance modifizieren“ “, um Ihre Änderungen zu speichern.

> **Important**
>
> Wenn Sie diese Operation planen, stellen Sie sicher, dass Sie zuvor Ihren clientseitigen Vertrauensspeicher aktualisiert haben.

Oder klicken Sie auf Zurück, um Ihre Änderungen zu bearbeiten, oder auf Abbrechen, um Ihre Änderungen zu verwerfen.

AWS CLI

AWS CLI Um die CA für eine DB-Instance oder einen Multi-AZ-DB-Cluster von rds-ca-2019 auf rds-ca-rsa2048-g1 zu ändern, rufen Sie den Befehl modify-db-instance modify-db-cluster auf. Geben DB-Instance- oder Cluster-ID und die Option an. `--ca-certificate-identifier`

Verwenden Sie den `--apply-immediately` Parameter, um das Update sofort anzuwenden. Die Ausführung dieser Operation ist standardmäßig während Ihres nächsten Wartungsfensters eingeplant.

> **Important**
>
> Wenn Sie diese Operation planen, stellen Sie sicher, dass Sie zuvor Ihren clientseitigen Vertrauensspeicher aktualisiert haben.

Example

Im folgenden Beispiel wird die Änderung vorgenommen, `mydbinstance` indem das CA-Zertifikat auf `rds-ca-rsa2048-g1` festgelegt wird.

Für LinuxmacOS, oderUnix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --ca-certificate-identifier rds-ca-rsa2048-g1
```

Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --ca-certificate-identifier rds-ca-rsa2048-g1
```

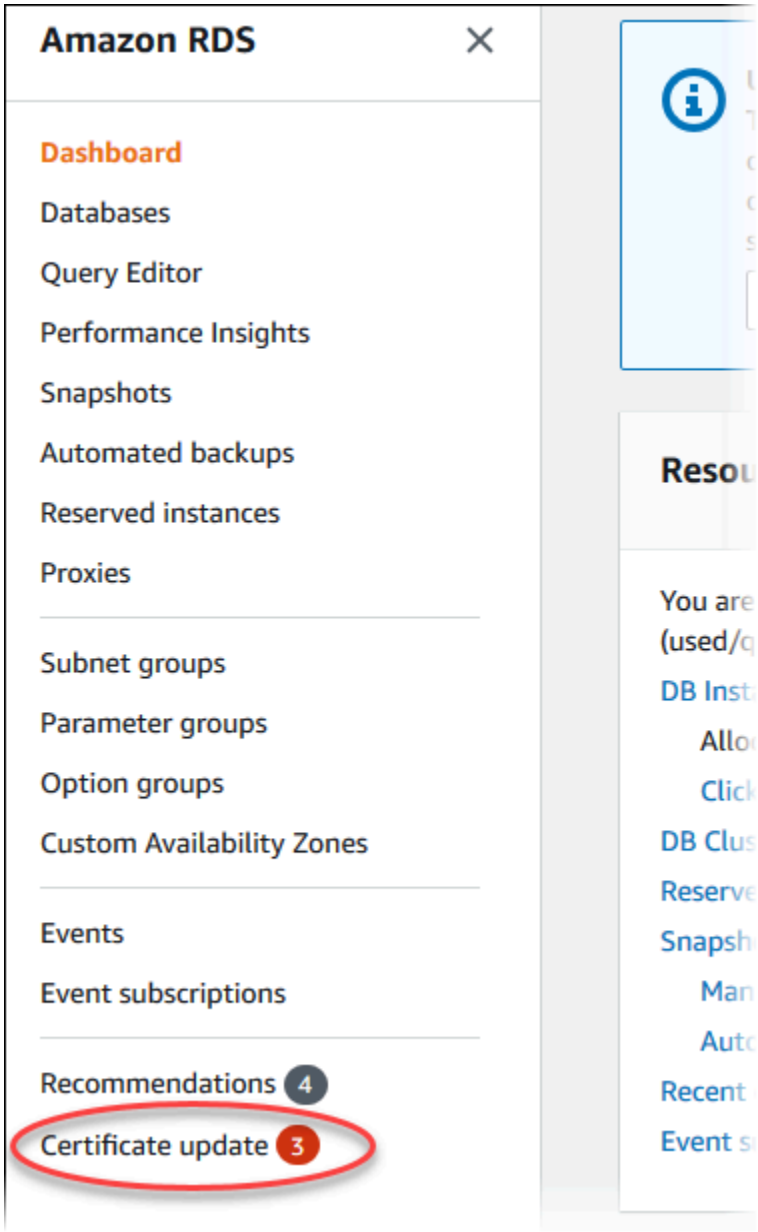
> **Note**
>
> Wenn Ihre Instance neu gestartet werden muss, können Sie den CLI-Befehl modify-db-instance verwenden und die Option angeben. `--no-certificate-rotation-restart`

Aktualisieren des CA-Zertifikats durch Anwenden der Wartung

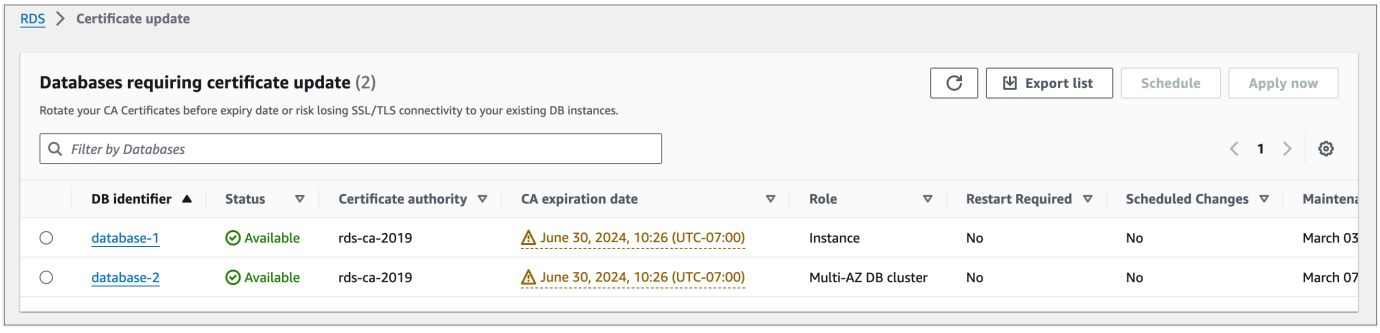
Führen Sie die folgenden Schritte aus, um Ihr CA-Zertifikat zu aktualisieren, indem Sie die Wartung durchführen.

Um Ihr CA-Zertifikat zu aktualisieren, indem Sie Wartungsarbeiten durchführen

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich die Option Certificate update aus.



Die Seite Datenbanken, die eine Zertifikataktualisierung erfordern wird angezeigt.



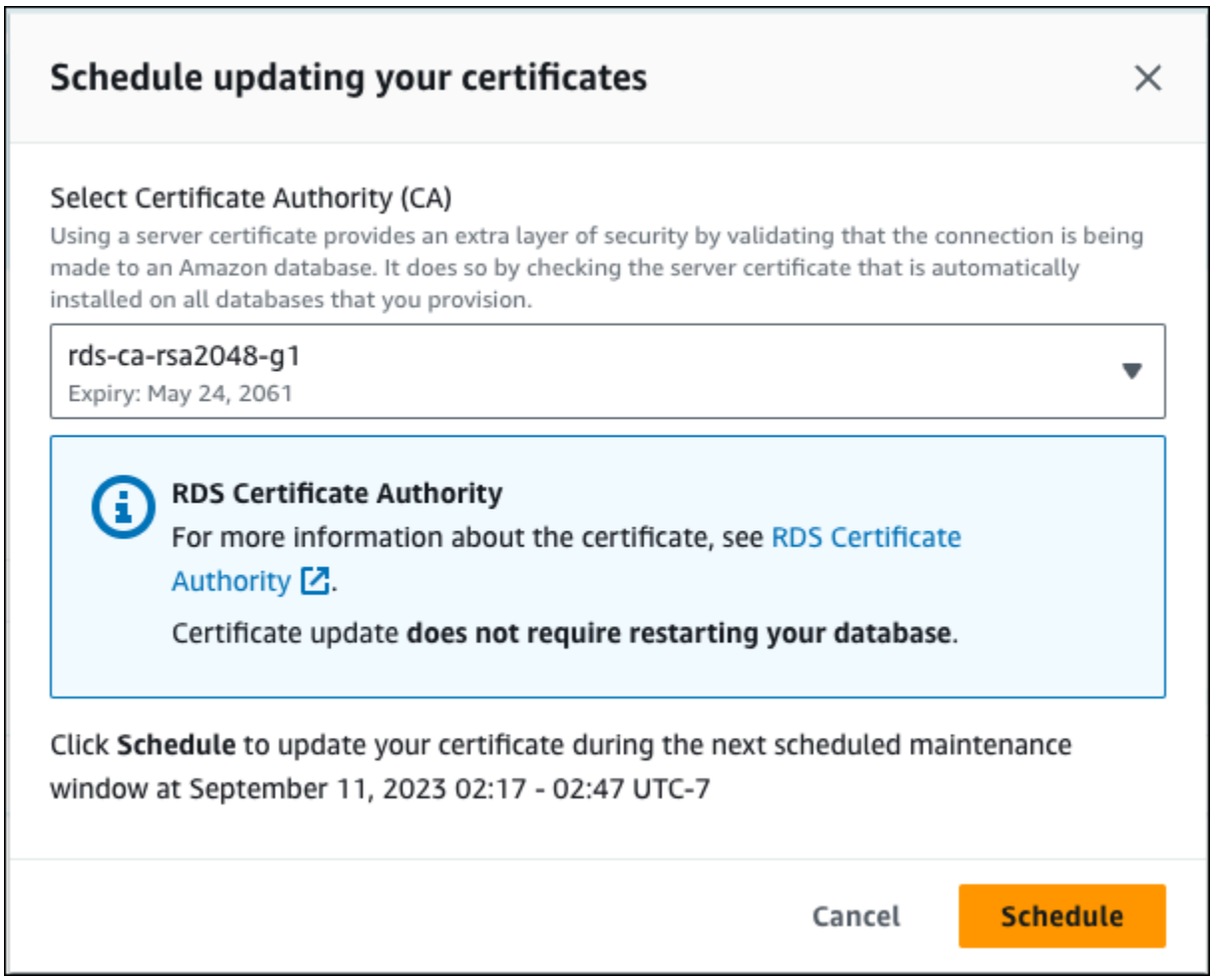
> **Note**
>
> Auf dieser Seite werden nur die aktuellen DB-Instances angezeigt AWS-Region. Wenn Sie Datenbanken in mehr als einer haben AWS-Region, überprüfen Sie diese Seite auf jeder Seite, AWS-Region um alle DB-Instances mit alten SSL/TLS-Zertifikaten zu sehen.

3. Wählen Sie die DB-Instance aus, den Sie aktualisieren möchten.

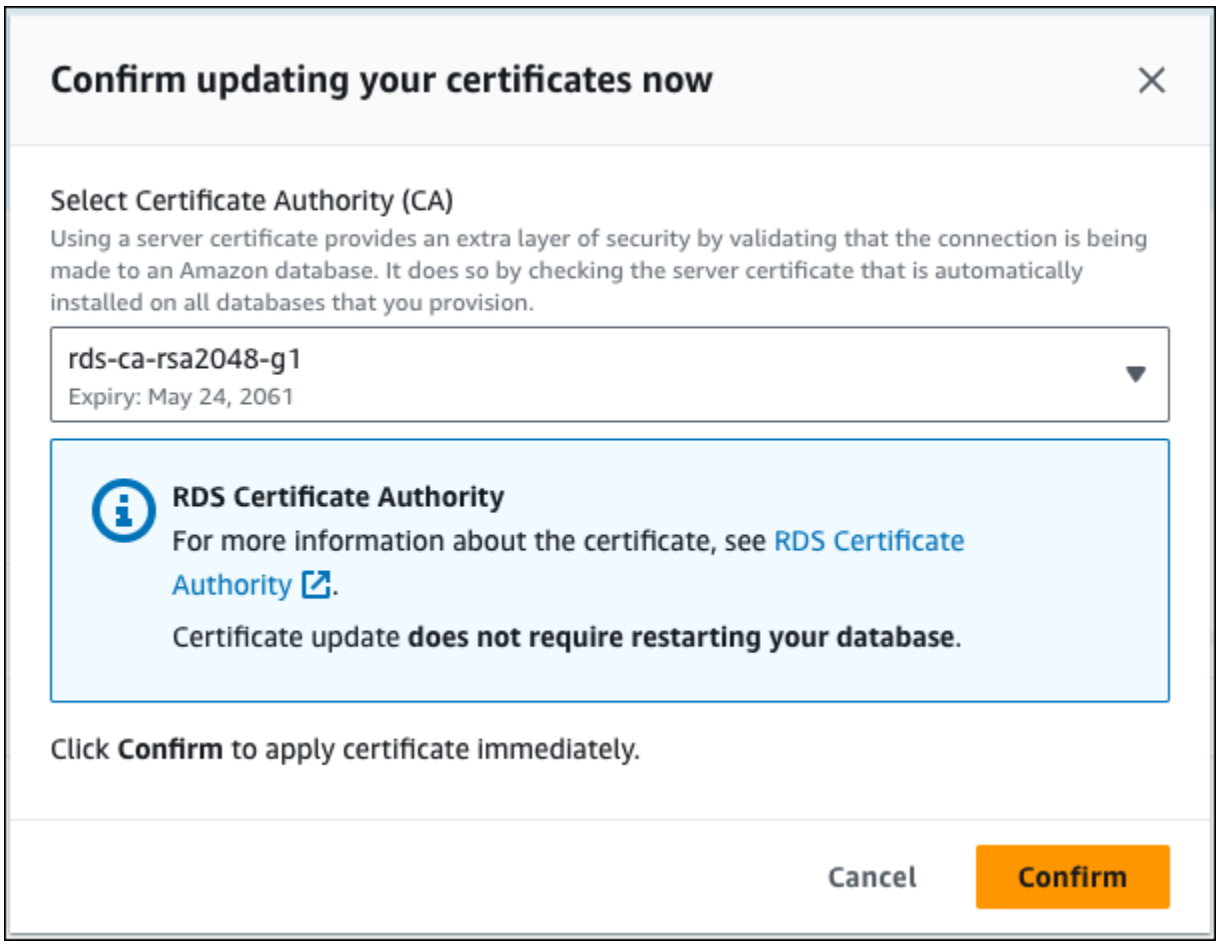
   Sie können die Zertifikatrotation für das nächste Wartungsfenster planen, indem Sie Zeitplan wählen. Wenden Sie die Rotation sofort an, indem Sie Jetzt anwenden wählen.

   > **Important**
   >
   > Wenn nach Ablauf des Zertifikats Verbindungsprobleme auftreten, verwenden Sie die Option Jetzt anwenden.

4. a. Wenn Sie Zeitplan wählen, werden Sie aufgefordert, die Rotation der CA-Zertifikate zu bestätigen. In dieser Aufforderung wird auch das geplante Fenster für das Update angegeben.



b. Wenn Sie Jetzt anwenden wählen, werden Sie aufgefordert, die Rotation der CA-Zertifikate zu bestätigen.



> **Important**
>
> Bevor Sie die Rotation des CA-Zertifikats in der Datenbank planen, aktualisieren Sie alle Clientanwendungen, die SSL/TLS und das Serverzertifikat verwenden, um eine Verbindung herzustellen. Diese Updates sind spezifisch für Ihre DB-Engine. Nachdem Sie diese Clientanwendungen aktualisiert haben, können Sie die Rotation des CA-Zertifikats bestätigen.

Aktivieren Sie das Kontrollkästchen und klicken Sie dann auf Confirm (Bestätigen), um fortzufahren.

5. Wiederholen Sie die Schritte 3 und 4 für jede DB-Instance , den Sie aktualisieren möchten.

Automatische Rotation von Serverzertifikaten

Wenn Ihre CA die automatische Rotation von Serverzertifikaten unterstützt, übernimmt RDS automatisch die Rotation des DB-Serverzertifikats. RDS verwendet dieselbe Stamm-CA für diese automatische Rotation, sodass Sie kein neues CA-Paket herunterladen müssen. Siehe Zertifizierungsstellen.

Die Rotation und Gültigkeit Ihres DB-Serverzertifikats hängen von Ihrer DB-Engine ab:

- Wenn Ihre DB-Engine die Rotation ohne Neustart unterstützt, rotiert RDS das DB-Serverzertifikat automatisch, ohne dass Sie etwas unternehmen müssen. RDS versucht, Ihr DB-Serverzertifikat in Ihrem bevorzugten Wartungsfenster nach der Halbwertszeit des DB-Serverzertifikats zu rotieren. Das neue DB-Serverzertifikat ist 12 Monate lang gültig.
- Wenn Ihre DB-Engine die Rotation ohne Neustart nicht unterstützt, benachrichtigt RDS Sie mindestens 6 Monate vor Ablauf des DB-Serverzertifikats über ein Wartungsereignis. Das neue DB-Serverzertifikat ist 36 Monate lang gültig.

Verwenden Sie den describe-db-engine-versionsBefehl und überprüfen Sie das `SupportsCertificateRotationWithoutRestart` Flag, um festzustellen, ob die DB-Engine-Version das Rotieren des Zertifikats ohne Neustart unterstützt. Weitere Informationen finden Sie unter Einstellung der CA für Ihre Datenbank.

Beispielskript für den Import von Zertifikaten in Ihren Trust Store

Nachfolgend sind Beispiel-Shell-Skripte aufgeführt, die das Zertifikatspaket in einen Vertrauensspeicher importieren.

Jedes Beispiel-Shell-Skript verwendet keytool, das Teil des Java Development Kits (JDK) ist. Weitere Informationen über die Installation von JDK finden Sie im JDK-Installationshandbuch.

Themen

- Beispielskript für den Import von Zertifikaten unter Linux
- Beispielskript zum Importieren von Zertifikaten unter macOS

Beispielskript für den Import von Zertifikaten unter Linux

Nachfolgend finden Sie ein Beispiel-Shell-Skript, das das Zertifikatpaket in einen Trust Store auf einem Linux-Betriebssystem importiert.

```
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
mkdir -p "${mydir}"
fi

truststore=${mydir}/rds-truststore.jks
storepassword=changeit

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem" >
 ${mydir}/global-bundle.pem
awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/ {split_after=1}
{print > "rds-ca-" n+1 ".pem"}' < ${mydir}/global-bundle.pem

for CERT in rds-ca-*; do
  alias=$(openssl x509 -noout -text -in $CERT | perl -ne 'next unless /Subject:/;
 s/.*(CN=|CN = )//; print')
  echo "Importing $alias"
  keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -keystore
 ${truststore} -noprompt
  rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep Alias | cut
 -d " " -f3- | while read alias
do
   expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword} -alias
 "${alias}" | grep Valid | perl -ne 'if(/until: (.*?)\n/) { print "$1\n"; }'`
   echo " Certificate ${alias} expires in '$expiry'"
done
```

Beispielskript zum Importieren von Zertifikaten unter macOS

Es folgt ein Beispiel für ein Shell-Skript, das das Zertifikatspaket in einen Vertrauensspeicher unter macOS importiert.

```
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
mkdir -p "${mydir}"
fi

truststore=${mydir}/rds-truststore.jks
storepassword=changeit

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem" >
 ${mydir}/global-bundle.pem
split -p "-----BEGIN CERTIFICATE-----" ${mydir}/global-bundle.pem rds-ca-

for CERT in rds-ca-*; do
  alias=$(openssl x509 -noout -text -in $CERT | perl -ne 'next unless /Subject:/;
 s/.*(CN=|CN = )//; print')
  echo "Importing $alias"
  keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -keystore
 ${truststore} -noprompt
  rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep Alias | cut
 -d " " -f3- | while read alias
do
   expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword} -alias
 "${alias}" | grep Valid | perl -ne 'if(/until: (.*?)\n/) { print "$1\n"; }'`
   echo " Certificate ${alias} expires in '$expiry'"
done
```

Richtlinie für den Datenverkehr zwischen Netzwerken

Verbindungen werden geschützt zwischen Amazon Aurora und On-Premises-Anwendungen sowie zwischen Amazon Aurora und anderen AWS-Ressourcen innerhalb derselben AWS-Region.

Datenverkehr zwischen Service und lokalen Clients und Anwendungen

Sie haben zwei Verbindungsoptionen zwischen Ihrem privaten Netzwerk und AWS:

- AWS Site-to-Site VPN-Verbindung Weitere Informationen finden Sie unter Was ist AWS Site-to-Site VPN?
- AWS Direct Connect-Verbindung Weitere Informationen finden Sie unter Was ist AWS Direct Connect?

Sie erhalten Zugriff auf Amazon Aurora über das Netzwerk, indem Sie von AWS veröffentlichte API-Operationen verwenden. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Identity and Access Management für Amazon Aurora

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren steuern, wer authenticated (angemeldet) und authorized (autorisiert) (im Besitz von Berechtigungen) ist, um Amazon-RDS-Ressourcen zu nutzen. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Aurora ausführen.

Service-Benutzer – Wenn Sie den Aurora-Service verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen bereit. Wenn Sie für Ihre Arbeit weitere Aurora-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle verstehen, kann Ihnen dies helfen, die richtigen Berechtigungen von Ihrem Administrator anzufordern. Unter Fehlerbehebung für Amazon Aurora-Identität und -Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in Aurora haben.

Service-Administrator – Wenn Sie in Ihrem Unternehmen die Verantwortung für Aurora-Ressourcen haben, haben Sie wahrscheinlich vollständigen Zugriff auf Aurora. Ihre Aufgabe besteht darin, die Aurora-Funktionen und -Ressourcen festzulegen, auf die Mitarbeiter zugreifen können sollten. Sie müssen anschließend bei Ihrem -Administrator entsprechende Änderungen für die Berechtigungen Ihrer Service-Benutzer anfordern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Aurora verwenden kann, finden Sie unter Funktionsweise von Amazon Aurora mit IAM.

Administrator – Wenn Sie als Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Aurora verfassen können. Beispiele für identitätsbasierte Aurora-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Amazon-Aurora-Richtlinien.

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-

Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS Konto (Root-Benutzer)

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen

wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

Sie können sich mit der IAM-Datenbankauthentifizierung bei Ihrem DB--Cluster authentifizieren.

Die IAM-Datenbank-Authentifizierung funktioniert mit Aurora. Weitere Informationen zur Authentifizierung bei Ihrem DB--Cluster mit IAM finden Sie unter IAM-Datenbankauthentifizierung.

IAM roles

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist mit einem Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Temporäre Benutzerberechtigungen – Ein Benutzer kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Verbundbenutzerzugriff: Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so

wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward-Access-Sitzungen — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem

Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen verwenden sollten, finden Sie unter Wann Sie eine IAM-Rolle (statt eines Benutzers) erstellen sollten im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an IAM-Identitäten oder -Ressourcen anhängen. AWS Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn eine Entität (Root-Benutzer, Benutzer oder IAM-Rolle) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Ein Administrator kann mithilfe von Richtlinien angeben, wer Zugriff auf AWS Ressourcen hat und welche Aktionen er mit diesen Ressourcen ausführen kann. Eine IAM-Entität (Berechtigungssatz oder Rolle) besitzt zunächst keine Berechtigungen. Anders ausgedrückt, können Benutzer standardmäßig keine Aktionen ausführen und nicht einmal ihr Passwort ändern. Um einem Benutzer die Berechtigung für eine Aktion zu erteilen, muss ein Administrator einem Benutzer eine Berechtigungsrichtlinie zuweisen. Alternativ kann der Administrator den Benutzer zu einer Gruppe hinzufügen, die über die gewünschten Berechtigungen verfügt. Wenn ein Administrator einer Gruppe Berechtigungen erteilt, erhalten alle Benutzer in dieser Gruppe diese Berechtigungen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. ein Berechtigungssatz oder eine Rolle. Diese Richtlinien steuern, welche Aktionen diese Identität für welche Ressourcen und unter welchen Bedingungen ausführen kann. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Berechtigungssatz oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Berechtigungssätzen und Rollen in Ihrem AWS Konto zuordnen können. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Informationen zu AWS verwalteten Richtlinien, die speziell für Aurora gelten, finden Sie unterAWS Von verwaltete Richtlinien für Amazon RDS.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (Berechtigungssatz oder Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die resultierenden Berechtigungen sind eine Schnittmenge der identitätsbasierten Richtlinien der Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Berechtigungssatz oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien

setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer AWS Konten, die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP beschränkt die Berechtigungen für Entitäten in Mitgliedskonten, einschließlich der einzelnen Konten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations - Benutzerhandbuch.
- Sitzungsrichtlinien:Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Berechtigungssatzes oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Funktionsweise von Amazon Aurora mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf Amazon Aurora verwenden, sollten Sie verstehen, welche IAM-Funktionen für die Verwendung mit Aurora verfügbar sind.

IAM-Funktionen, die Sie mit Amazon Aurora verwenden können

IAM-Feature	Unterstützung von Amazon Aurora
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein

IAM-Feature	Unterstützung von Amazon Aurora
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
Attributbasierte Zugriffssteuerung (Attribute-Based Access Control, ABAC) (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Zugriffssitzungen weiterleiten	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie , Amazon Aurora und andere AWS Services mit IAM zusammenarbeiten, finden Sie im IAM-Benutzerhandbuch unter AWS Services, die mit IAM funktionieren.

Themen

- Identitätsbasierte Aurora-Richtlinien
- Ressourcenbasierte Richtlinien in Aurora
- Richtlinienaktionen für Aurora
- Richtlinienressourcen für Aurora
- Richtlinien-Bedingungsschlüssel für Aurora
- Zugriffssteuerungslisten (ACLs) in Aurora
- Attributbasierte Zugriffssteuerung (Attribute-Based Access Control, ABAC) in Richtlinien mit Aurora-Tags
- Verwenden temporärer Anmeldeinformationen mit Aurora

- Zugriffssitzungen für Aurora weiterleiten
- Servicerollen für Aurora
- Serviceverknüpfte Rollen für Aurora

Identitätsbasierte Aurora-Richtlinien

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Aurora-Richtlinien

Beispiele für identitätsbasierte Aurora-Richtlinien finden Sie unter Beispiele für identitätsbasierte Amazon-Aurora-Richtlinien.

Ressourcenbasierte Richtlinien in Aurora

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein

bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für Aurora

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Aurora verwenden das folgende Präfix vor der Aktion: `rds:`. Um beispielsweise jemandem die Berechtigung zu erteilen, DB-Instances mit der API-Operation Amazon RDS `DescribeDBInstances` zu beschreiben, nehmen Sie die Aktion `rds:DescribeDBInstances` in die Richtlinie auf. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-

Element enthalten. Aurora definiert eine eigene Gruppe von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Um mehrere -Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie folgendermaßen durch Kommas.

```
"Action": [
      "rds:action1",
      "rds:action2"
```

Sie können auch Platzhalter (*) verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "rds:Describe*"
```

Um eine Liste von Aurora-Aktionen finden Sie unter Von Amazon RDS definierte Aktionen in der Service-Autorisierungs-Referenz

Richtlinienressourcen für Aurora

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Die DB-Instance-Ressource hat den folgenden Amazon-Ressourcennamen (ARN).

```
arn:${Partition}:rds:${Region}:${Account}:{ResourceType}/${Resource}
```

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs) and AWS Service Namespaces.

Wenn Sie beispielsweise die `dbtest`-DB-Instance in Ihrer Anweisung angeben möchten, verwenden Sie den folgenden ARN.

```
"Resource": "arn:aws:rds:us-west-2:123456789012:db:dbtest"
```

Wenn Sie alle DB-Instances angeben möchten, die einem bestimmten Konto angehören, verwenden Sie den Platzhalter (*).

```
"Resource": "arn:aws:rds:us-east-1:123456789012:db:*"
```

Einige RDS-API-Operationen, z. B. das Erstellen von Ressourcen, können nicht für eine bestimmte Ressource durchgeführt werden. Verwenden Sie in diesen Fällen den Platzhalter (*).

```
"Resource": "*"
```

Viele Amazon RDS-API-Operationen umfassen mehrere Ressourcen. `CreateDBInstance` erstellt beispielsweise eine DB-Instance. Sie können festlegen, dass ein -Benutzer beim Erstellen einer DB-Instance eine bestimmte Sicherheitsgruppe und Parametergruppe verwenden muss. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

```
"Resource": [
      "resource1",
      "resource2"
```

Um eine Liste von Aurora-Aktionen finden Sie unter Von Amazon RDS definierte Aktionen in der Service-Autorisierungs-Referenz Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Amazon RDS definierte Aktionen.

Richtlinien-Bedingungsschlüssel für Aurora

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Aurora definiert einen eigenen Satz von Bedingungsschlüsseln und unterstützt auch einige globale Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Alle RDS-API-Operationen unterstützen den Bedingungsschlüssel `aws:RequestedRegion`.

Um eine Liste von Aurora-Bedingungsschlüsseln finden Sie unter Bedingungsschlüssel für Amazon RDS in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und

Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon RDS definierte Aktionen.

Zugriffssteuerungslisten (ACLs) in Aurora

Unterstützt Zugriffssteuerungslisten (Access Control Lists, ACLs)	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffssteuerung (Attribute-Based Access Control, ABAC) in Richtlinien mit Aurora-Tags

Unterstützt Tags für die attributbasierte Zugriffssteuerung (Attribute-Based Access Control, ABAC) in Richtlinien	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen über das Markieren von Aurora-Ressourcen mit Tags finden Sie unter Festlegen von Bedingungen: Verwenden von benutzerdefinierten Tags. Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Tags dieser Ressource finden Sie unter Erteilen von Berechtigungen für Aktionen in einer Ressource mit einem bestimmten Tag und zwei verschiedenen Tag-Werten.

Verwenden temporärer Anmeldeinformationen mit Aurora

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Zugriffssitzungen für Aurora weiterleiten

Unterstützt Forward-Access-Sitzungen	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Aurora

Unterstützt Servicerollen	Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die Aurora-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Aurora dazu Anleitungen gibt.

Serviceverknüpfte Rollen für Aurora

Unterstützt serviceverknüpfte Rollen	Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Verwenden von serviceverknüpften Aurora-Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Aurora.

Beispiele für identitätsbasierte Amazon-Aurora-Richtlinien

Standardmäßig besitzen Berechtigungssätze und Rollen keine Berechtigungen zum Erstellen oder Ändern von Aurora-Ressourcen. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Berechtigungssätzen und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den Berechtigungssätzen oder Rollen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien können festlegen, ob jemand Amazon-RDS-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder daraus löschen kann. Dies kann zusätzliche Kosten für Ihr

verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren

Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Aurora-Konsole

Um auf die Amazon Aurora-Konsole zuzugreifen, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Aurora Aurora-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Um sicherzustellen, dass diese Entitäten weiterhin die Aurora-Konsole verwenden können, fügen Sie den Entitäten auch die folgende AWS verwaltete Richtlinie hinzu.

```
AmazonRDSReadOnlyAccess
```

Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Erlaubt einem Benutzer, DB-Instances in einem Konto zu erstellen AWS

Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die es dem Benutzer mit der ID ermöglicht, DB-Instances für Ihr AWS Konto `123456789012` zu erstellen. Die Richtlinie setzt voraus, dass der Name der DB-Instance mit beginn `test`. Die neue DB-Instance muss auch die MySQL-Datenbank-Engine und die DB-Instance-Klasse `db.t2.micro` verwenden. Zusätzlich muss die neue DB-Instance eine Optionsgruppe und eine DB-Parametergruppe verwenden, die mit `default` beginnt und die Subnetzgruppe `default` verwendet.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
```

```
        "Sid": "AllowCreateDBInstanceOnly",
        "Effect": "Allow",
        "Action": [
           "rds:CreateDBInstance"
        ],
        "Resource": [
           "arn:aws:rds:*:123456789012:db:test*",
           "arn:aws:rds:*:123456789012:og:default*",
           "arn:aws:rds:*:123456789012:pg:default*",
           "arn:aws:rds:*:123456789012:subgrp:default"
        ],
        "Condition": {
           "StringEquals": {
              "rds:DatabaseEngine": "mysql",
              "rds:DatabaseClass": "db.t2.micro"
           }
        }
     }
  ]
}
```

Die Richtlinie ist ein einzelnes Statement, das die folgenden Berechtigungen für den -Benutzer bestimmt:

- Die Richtlinie ermöglicht es dem Benutzer, eine DB-Instance mithilfe des API-Vorgangs CreateDBInstance zu erstellen (dies gilt auch für den Befehl AWS CLI create-db-instance und den). AWS Management Console
- Das Element `Resource` gibt an, dass der Benutzer auf oder mit Ressourcen Aktionen ausführen kann. Sie geben Ressourcen über einen Amazon Resources Name (ARN) an. Dieser ARN umfasst den Namen des Dienstes, zu dem die Ressource gehört (`rds`), die AWS Region (*gibt in diesem Beispiel eine beliebige Region an), die AWS Kontonummer (123456789012ist in diesem Beispiel die Kontonummer) und den Ressourcentyp. Weitere Informationen zum Erstellen von ARNs finden Sie unter Arbeiten mit Amazon-Ressourcennamen (ARN) in Amazon RDS.

  Das `Resource`-Element im Beispiel gibt für den Benutzer die folgenden richtlinienbezogenen Einschränkungen für die Ressourcen an:

  - Die DB-Instance-Kennung für die neue DB-Instance muss mit `test` beginnen (zum Beispiel `testCustomerData1`, `test-region2-data`).
  - Die Optionsgruppe für die neue DB-Instance muss mit beginne `default`.
  - Die DB-Parametergruppe für die neue DB-Instance muss mit beginne `default`.

  - Die Subnetzgruppe für die neue DB-Instance muss mit `default` beginnen.
- Das `Condition`-Element gibt an, dass die DB-Engine MySQL sein muss und die DB-Instance-Klasse `db.t2.micro` sein muss. Das `Condition`-Element bestimmt die Bedingungen, wann eine Richtlinie wirksam sein soll. Sie können zusätzliche Berechtigungen oder Einschränkungen hinzufügen, indem Sie das `Condition`-Element verwenden. Weitere Informationen zur Angabe von Bedingungen finden Sie unter Richtlinien-Bedingungsschlüssel für Aurora. Dieses Beispiel zeigt die Bedingungen `rds:DatabaseEngine` und `rds:DatabaseClass`. Informationen zu den gültigen Bedingungswerten für `rds:DatabaseEngine` finden Sie in der Liste unter dem Parameter `Engine` in CreateDBInstance. Informationen zu den gültigen Bedingungswerten für `rds:DatabaseClass` finden Sie unter Unterstützte DB-Engines für DB-Instance-Klassen.

Das Element `Principal` ist in der Richtlinie nicht angegeben, da in identitätsbasierten Richtlinien die Angabe des Prinzipals als Empfänger der Berechtigung nicht erforderlich ist. Wenn Sie einem Benutzer eine Richtlinie zuweisen, ist der Benutzer automatisch der Prinzipal. Wird die Berechtigungsrichtlinie einer IAM-Rolle zugewiesen, erhält der in der Vertrauensrichtlinie der Rolle angegebene Prinzipal die Berechtigungen.

Um eine Liste von Aurora-Aktionen finden Sie unter Von Amazon RDS definierte Aktionen in der Service-Autorisierungs-Referenz

Erforderliche Berechtigungen für die Verwendung der Konsole

Damit ein Benutzer mit der Konsole arbeiten kann, muss dieser Benutzer über einen Minimumsatz an Berechtigungen verfügen. Diese Berechtigungen ermöglichen es dem Benutzer, die Aurora Aurora-Ressourcen für sein AWS Konto zu beschreiben und andere verwandte Informationen bereitzustellen, einschließlich Amazon EC2-Sicherheits- und Netzwerkinformationen.

Wenn Sie eine IAM-Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Benutzer mit dieser IAM-Richtlinie. Um sicherzustellen, dass diese Benutzer die Konsole weiterhin verwenden können, fügen Sie dem Benutzer auch die verwaltete Richtlinie `AmazonRDSReadOnlyAccess` an. Einzelheiten dazu finden Sie unter Verwalten des Zugriffs mit Richtlinien.

Für Benutzer, die nur Aufrufe an die AWS CLI oder Amazon-RDS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen.

Die folgende Richtlinie gewährt vollen Zugriff auf alle Aurora Aurora-Ressourcen für das AWS Root-Konto:

```
AmazonRDSFullAccess
```

Einem Benutzer eine beliebige Beschreibungsaktion für eine beliebige RDS-Ressource erlauben

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen für einen Benutzer, alle Aktionen auszuführen, die mit beginne `Describe`. Diese Aktionen zeigen Informationen zu einer RDS-Ressource, z. B. eine DB-Instance. Das Platzhalterzeichen (*) im `Resource`-Element zeigt an, dass die Aktionen für alle Amazon Aurora-Ressourcen erlaubt sind, die dem Konto gehören.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowRDSDescribe",
         "Effect": "Allow",
         "Action": "rds:Describe*",
         "Resource": "*"
      }
   ]
}
```

Einem Benutzer erlauben, eine DB-Instance zu erstellen, die spezifische DB-Parametergruppe und Subnetzgruppe verwendet.

Die folgenden Berechtigungsrichtlinien erteilen einem Benutzer die Erlaubnis, ausschließlich eine DB-Instance mit der DB-Parametergruppe `mydbpg` und der DB-Subnetzgruppe `mydbsubnetgroup` zu erstellen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": "rds:CreateDBInstance",
         "Resource": [
            "arn:aws:rds:*:*:pg:mydbpg",
```

```
            "arn:aws:rds:*:*:subgrp:mydbsubnetgroup"
         ]
      }
   ]
}
```

Erteilen von Berechtigungen für Aktionen in einer Ressource mit einem bestimmten Tag und zwei verschiedenen Tag-Werten

Sie können in Ihrer identitätsbasierten Richtlinie Bedingungen für die Steuerung des Zugriffs auf Aurora-Ressourcen auf der Basis von Tags verwenden. Die folgende Richtlinie erteilt die Berechtigung, die API-Operation `CreateDBSnapshot` auf DB-Instances durchzuführen, bei denen das Tag `stage` entweder auf `development` oder `test` festgelegt ist.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowAnySnapshotName",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBSnapshot"
         ],
         "Resource":"arn:aws:rds:*:123456789012:snapshot:*"
      },
      {
         "Sid":"AllowDevTestToCreateSnapshot",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBSnapshot"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:*",
         "Condition":{
            "StringEquals":{
                "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
```

```
}
```

Die folgende Richtlinie erteilt die Berechtigung, die API-Operation `ModifyDBInstance` auf DB-Instances durchzuführen, bei denen das Tag `stage` entweder auf `development` oder `test` festgelegt ist.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowChangingParameterOptionSecurityGroups",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance"
         ],
         "Resource": [
            "arn:aws:rds:*:123456789012:pg:*",
            "arn:aws:rds:*:123456789012:secgrp:*",
            "arn:aws:rds:*:123456789012:og:*"
         ]
      },
      {
         "Sid":"AllowDevTestToModifyInstance",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:*",
         "Condition":{
            "StringEquals":{
                "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
}
```

Verhindern, dass ein Benutzer eine DB-Instance löscht

Die folgenden Berechtigungsrichtlinien erteilen Berechtigungen, um einen Benutzer davon abzuhalten, eine bestimmte DB-Instance zu löschen. Beispielsweise möchten Sie jedem Benutzer, der kein Administrator ist, verbieten, Ihre Produktions-DB-Instances zu löschen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "DenyDelete1",
         "Effect": "Deny",
         "Action": "rds:DeleteDBInstance",
         "Resource": "arn:aws:rds:us-west-2:123456789012:db:my-mysql-instance"
      }
   ]
}
```

Verweigern des gesamten Zugriffs auf eine Ressource

Sie können den Zugriff auf eine Ressource explizit verweigern. Verweigerungsrichtlinien haben Vorrang vor Zulassungsrichtlinien. Die folgende Richtlinie verweigert einem Benutzer explizit die Möglichkeit, eine Ressource zu verwalten:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": "rds:*",
         "Resource": "arn:aws:rds:us-east-1:123456789012:db:mydb"
      }
   ]
}
```

Beispielrichtlinien: Verwenden von Bedingungsschlüsseln

Im Folgenden finden Sie Beispiele für die Verwendung von Bedingungsschlüsseln in den IAM-Berechtigungsrichtlinien von Amazon Aurora.

Beispiel 1: Erteilen der Berechtigung zum Erstellen einer DB-Instance mit einer bestimmten DB-Engine ohne Multi-AZ-Bereitstellung

Die folgende Richtlinie nutzt einen RDS-Bedingungsschlüssel und legt fest, dass ein Benutzer nur DB-Instances erstellen darf, die die MySQL-Datenbank-Engine und keine Multi-AZ-Bereitstellung verwenden. Das Element `Condition` gibt die Voraussetzung an, dass es sich um eine MySQL-Datenbank-Engine handeln muss.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowMySQLCreate",
         "Effect": "Allow",
         "Action": "rds:CreateDBInstance",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "rds:DatabaseEngine": "mysql"
            },
            "Bool": {
               "rds:MultiAz": false
            }
         }
      }
   ]
}
```

Beispiel 2: Explizites Verweigern der Berechtigung, DB-Instances für bestimmte DB-Instance-Klassen sowie DB-Instances, die bereitgestellte IOPS verwenden, zu erstellen

Die folgende Richtlinie verweigert explizit die Berechtigung, DB-Instances für die DB-Instance-Klassen `r3.8xlarge` und `m4.10xlarge` zu erstellen, die zu den größten und teuersten DB-Instance-Klassen gehören. Diese Richtlinie hält Benutzer ebenfalls davon ab, DB-Instances zu erstellen, die bereitgestellte IOPS verwenden, durch die zusätzliche Kosten entstehen.

Eine explizit verweigerte Berechtigung überschreibt alle anderen erteilten Berechtigungen. So wird sichergestellt, dass Identitäten nicht aus Versehen eine Berechtigung erhalten, die Sie nie erteilen wollten.

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "DenyLargeCreate",
         "Effect": "Deny",
         "Action": "rds:CreateDBInstance",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "rds:DatabaseClass": [
                  "db.r3.8xlarge",
                  "db.m4.10xlarge"
               ]
            }
         }
      },
      {
         "Sid": "DenyPIOPSCreate",
         "Effect": "Deny",
         "Action": "rds:CreateDBInstance",
         "Resource": "*",
         "Condition": {
            "NumericNotEquals": {
               "rds:Piops": "0"
            }
         }
      }
   ]
}
```

Beispiel 3: Einschränken des Satzes von Tag-Schlüsseln und Werten, mit dem eine Ressource mit einem Tag versehen werden kann

Die folgende Richtlinie verwendet einen RDS-Bedingungsschlüssel und erlaubt es, ein Tag mit dem Schlüssel `stage` einer Ressource mit den Werten `test`, `qa` und `production` hinzuzufügen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "rds:AddTagsToResource",
```

```
            "rds:RemoveTagsFromResource"
         ],
         "Resource": "*",
         "Condition": {
            "streq": {
               "rds:req-tag/stage": [
                  "test",
                  "qa",
                  "production"
               ]
            }
         }
      }
   ]
}
```

Festlegen von Bedingungen: Verwenden von benutzerdefinierten Tags

Amazon Aurora bietet Unterstützung für das Festlegen von Bedingungen in einer IAM-Richtlinie mithilfe von benutzerdefinierten Tags.

Angenommen, Sie fügen Ihren DB-Instances ein Tag namens `environment` mit Werten wie `beta`, `staging`, `production` und so weiter hinzu. Wenn dies der Fall ist, können Sie eine Richtlinie erstellen, die bestimmte Benutzer basierend auf dem Tag-Wert `environment` auf DB-Instances beschränkt.

> **Note**
>
> Bei benutzerdefinierten Tag-Kennungen muss auf Groß- und Kleinschreibung geachtet werden.

In der folgenden Tabelle werden die RDS-Tag-Kennungen aufgeführt, die Sie in einem `Condition`-Element verwenden können.

RDS-Tag-ID	Gilt für
`db-tag`	DB-Instances einschließlich Lesereplikaten
`snapshot-tag`	DB-Snapshots

RDS-Tag-ID	Gilt für
`ri-tag`	Reservierte DB-Instances
`og-tag`	DB-Optionsgruppen
`pg-tag`	DB-Parametergruppen
`subgrp-tag`	DB-Subnetzgruppen
`es-tag`	Ereignisabonnements
`cluster-tag`	DB-Cluster
`cluster-pg-tag`	DB-Cluster-Parametergruppen
`cluster-snapshot-tag`	DB-Cluster-Snapshots

Die Syntax für eine benutzerdefinierte Tag-Bedingung sieht wie folgt aus:

```
"Condition":{"StringEquals":{"rds:rds-tag-identifier/tag-name":
["value"]} }
```

Beispielsweise gilt das folgende `Condition`-Element für DB-Instances mit dem Tag `environment` und dem Tag-Wert `production`.

```
"Condition":{"StringEquals":{"rds:db-tag/environment": ["production"]} }
```

Weitere Informationen über die Erstellung von Tags finden Sie unter Markieren von Amazon RDS-Ressourcen.

> **Important**
>
> Wenn Sie den Zugriff auf Ihre RDS-Ressourcen mithilfe von Tags verwalten, empfehlen wir, den Zugriff auf die Tags Ihrer RDS-Ressourcen zu sichern. Sie können den Zugriff auf Tags verwalten, indem Sie Richtlinien für die Aktionen `AddTagsToResource` und `RemoveTagsFromResource` erstellen. Beispielsweise verweigert die folgende Richtlinie den Benutzern das Hinzufügen und Entfernen von Tags für alle Ressourcen. Sie können anschließend Richtlinien erstellen, die es bestimmten Benutzern ermöglichen, Tags hinzuzufügen oder zu entfernen.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyTagUpdates",
         "Effect":"Deny",
         "Action":[
            "rds:AddTagsToResource",
            "rds:RemoveTagsFromResource"
         ],
         "Resource":"*"
      }
   ]
}
```

Um eine Liste von Aurora-Aktionen finden Sie unter Von Amazon RDS definierte Aktionen in der Service-Autorisierungs-Referenz

Beispielrichtlinien: Verwenden von benutzerdefinierten Tags

Im Folgenden finden Sie Beispiele für die Verwendung von benutzerdefinierten Tags in den IAM-Berechtigungsrichtlinien in Amazon Aurora. Weitere Informationen zum Hinzufügen von Tags zu einer Amazon Aurora-Ressource finden Sie unter Arbeiten mit Amazon-Ressourcennamen (ARN) in Amazon RDS.

> **Note**
>
> In allen Beispielen werden die Region „us-west-2” und fiktive Konto-IDs verwendet.

Beispiel 1: Erteilen von Berechtigungen für Aktionen in einer Ressource mit einem bestimmten Tag und zwei verschiedenen Tag-Werten

Die folgende Richtlinie erteilt die Berechtigung, die API-Operation `CreateDBSnapshot` auf DB-Instances durchzuführen, bei denen das Tag `stage` entweder auf `development` oder `test` festgelegt ist.

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowAnySnapshotName",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBSnapshot"
         ],
         "Resource":"arn:aws:rds:*:123456789012:snapshot:*"
      },
      {
         "Sid":"AllowDevTestToCreateSnapshot",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBSnapshot"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:*",
         "Condition":{
            "StringEquals":{
                "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
}
```

Die folgende Richtlinie erteilt die Berechtigung, die API-Operation `ModifyDBInstance` auf DB-Instances durchzuführen, bei denen das Tag `stage` entweder auf `development` oder `test` festgelegt ist.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowChangingParameterOptionSecurityGroups",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance"
         ],
         "Resource":" [
```

```
            "arn:aws:rds:*:123456789012:pg:*",
            "arn:aws:rds:*:123456789012:secgrp:*",
            "arn:aws:rds:*:123456789012:og:*"
         ]
      },
      {
         "Sid":"AllowDevTestToModifyInstance",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:*",
         "Condition":{
            "StringEquals":{
                "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
}
```

Bespiel 2: Explizites Verweigern der Berechtigung zum Erstellen einer DB-Instance, die bestimmte DB-Parametergruppen verwendet

Die folgende Richtlinie verweigert explizit die Berechtigung, eine DB-Instance zu erstellen, die DB-Parametergruppen mit bestimmten Tag-Werten verwendet. Sie können diese Richtlinie anwenden, wenn stets eine bestimmte kundenseitig erstellte DB-Parametergruppe beim Erstellen von DB-Instances verwendet werden muss. Die Richtlinien mit `Deny` werden meist genutzt, um den von einer allgemeineren Richtlinie erteilten Zugriff einzuschränken.

Eine explizit verweigerte Berechtigung überschreibt alle anderen erteilten Berechtigungen. So wird sichergestellt, dass Identitäten nicht aus Versehen eine Berechtigung erhalten, die Sie nie erteilen wollten.

```
{
   "Version":"2012-10-17",
   "Statement":[
```

```
      {
         "Sid":"DenyProductionCreate",
         "Effect":"Deny",
         "Action":"rds:CreateDBInstance",
         "Resource":"arn:aws:rds:*:123456789012:pg:*",
         "Condition":{
            "StringEquals":{
               "rds:pg-tag/usage":"prod"
            }
         }
      }
   ]
}
```

Beispiel 3: Erteilen von Berechtigungen für Aktionen auf einer DB-Instance mit einem Instance-Namen, der den Benutzernamen als Präfix enthält

Die folgende Richtlinie erteilt die Berechtigung, eine beliebige API (mit Ausnahme von `AddTagsToResource` oder `RemoveTagsFromResource`) auf einer DB-Instance aufzurufen, deren Instance-Name den Benutzernamen als Präfix aufweist und das Tag `stage` mit dem Wert `devo` oder kein Tag `stage` enthält.

Die Zeile `Resource` in der Richtlinie kennzeichnet eine Ressource durch den Amazon-Ressourcennamen (ARN). Weitere Informationen zur Verwendung von ARNs mit Amazon Aurora-Ressourcen finden Sie unter Arbeiten mit Amazon-Ressourcennamen (ARN) in Amazon RDS.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowFullDevAccessNoTags",
         "Effect":"Allow",
         "NotAction":[
            "rds:AddTagsToResource",
            "rds:RemoveTagsFromResource"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:${aws:username}*",
         "Condition":{
            "StringEqualsIfExists":{
               "rds:db-tag/stage":"devo"
            }
         }
```

```
        }
    ]
}
```

AWS Von verwaltete Richtlinien für Amazon RDS

Um Berechtigungen zu Berechtigungssätzen und Rollen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere von AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu von AWS verwalteten Richtlinien finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS-Services AWS verwaltete Richtlinien pflegen und aktualisieren. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Berechtigungssätze und Rollen), denen die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am wahrscheinlichsten, wenn eine neue Funktion gestartet wird oder wenn neue Vorgänge verfügbar werden. Services entfernen keine Berechtigungen aus einer von AWS verwalteten Richtlinie, sodass Richtlinienaktualisierungen Ihre vorhandenen Berechtigungen nicht beeinträchtigen.

Darüber hinaus AWS unterstützt verwaltete Richtlinien für Auftragsfunktionen, die sich über mehrere Services erstrecken. Die von `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS-Services und Ressourcen. Wenn ein Service ein neues Feature startet, AWS fügt schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Themen

AWS Von verwaltete Richtlinie: AmazonRDSReadOnlyAccess

Diese Richtlinie gewährt schreibgeschützten Zugriff auf Amazon RDS über die AWS Management Console.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `rds` – Ermöglicht es Prinzipalen, Amazon-RDS-Ressourcen zu beschreiben und die Tags für Amazon-RDS-Ressourcen aufzulisten.
- `cloudwatch` – Ermöglicht es Prinzipalen, Amazon- CloudWatch Metrikstatistiken abzurufen.
- `ec2` – Ermöglicht es Prinzipalen, Availability Zones und Netzwerkressourcen zu beschreiben.
- `logs` – Ermöglicht es Prinzipalen, CloudWatch Protokollstreams von Protokollgruppen zu beschreiben und CloudWatch Protokollereignisse abzurufen.
- `devops-guru` – Ermöglicht es Prinzipalen, Ressourcen mit Amazon- DevOpsGuru-Abdeckung zu beschreiben, die entweder durch CloudFormation Stack-Namen oder Ressourcen-Tags angegeben wird.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments, finden Sie unter AmazonRDSReadOnlyAccess im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonRDSFullAccess

Diese Richtlinie bietet vollen Zugriff auf Amazon RDS über die AWS Management Console.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `rds` – Ermöglicht Prinzipalen Vollzugriff auf alle Amazon RDS.
- `application-autoscaling` – Ermöglicht es Prinzipalen, Ziele und Richtlinien zur Skalierung der automatischen Anwendungsskalierung zu beschreiben und zu verwalten.
- `cloudwatch` – Ermöglicht es Prinzipalen, CloudWatch Metrik-Statiken abzurufen und CloudWatch Alarme zu verwalten.
- `ec2` – Ermöglicht es Prinzipalen, Availability Zones und Netzwerkressourcen zu beschreiben.
- `logs` – Ermöglicht es Prinzipalen, CloudWatch Protokollstreams von Protokollgruppen zu beschreiben und CloudWatch Protokollereignisse abzurufen.

- `outposts` – Ermöglicht es Prinzipalen, AWS Outposts Instance-Typen abzurufen.
- `pi` – Ermöglicht es Prinzipalen, Performance-Insights-Metriken abzurufen.
- `sns` – Ermöglicht es Prinzipalen, Amazon Simple Notification Service (Amazon SNS)-Abonnements und -Themen zu abonnieren und Amazon-SNS-Nachrichten zu veröffentlichen.
- `devops-guru` – Ermöglicht es Prinzipalen, Ressourcen mit Amazon- DevOpsGuru-Abdeckung zu beschreiben, die entweder durch CloudFormation Stack-Namen oder Ressourcen-Tags angegeben wird.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments, finden Sie unter AmazonRDSFullAccess im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonRDSDataFullAccess

Diese Richtlinie ermöglicht vollen Zugriff auf die Verwendung der Daten-API und des Abfrage-Editors auf Aurora Serverless Clustern in einer bestimmten AWS-Konto. Diese Richtlinie ermöglicht es dem AWS-Konto , den Wert eines Secrets von abzurufen AWS Secrets Manager.

Sie können die `AmazonRDSDataFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `dbqms` – Ermöglicht es Prinzipalen, auf Abfragen zuzugreifen, Abfragen zu erstellen, zu löschen, zu beschreiben und zu aktualisieren. Der Database Query Metadata Service (`dbqms`) ist ein reiner Dienst für interne Daten. Es stellt Ihre aktuellen und gespeicherten Abfragen für den Abfrage-Editor auf AWS Management Console für mehrere bereit AWS-Services, einschließlich Amazon RDS.
- `rds-data` – Ermöglicht es Prinzipalen, SQL-Anweisungen in Aurora Serverless-Datenbanken auszuführen.
- `secretsmanager` – Ermöglicht es Prinzipalen, den Wert eines Secrets von abzurufen AWS Secrets Manager.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments, finden Sie unter AmazonRDSDataFullAccess im AWS Referenzhandbuch zu verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonRDSEnhancedMonitoringRole

Diese Richtlinie bietet Zugriff auf Amazon CloudWatch Logs für Amazon RDS Enhanced Monitoring.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `logs` – Ermöglicht es Prinzipalen, CloudWatch Protokollgruppen und Aufbewahrungsrichtlinien zu erstellen und CloudWatch Protokollstreams von Protokollgruppen zu erstellen und zu beschreiben. Außerdem können Prinzipale CloudWatch Protokollereignisse ablegen und abrufen.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments, finden Sie unter AmazonRDSEnhancedMonitoringRole im AWS Referenzhandbuch zu verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonRDSPerformanceInsightsReadOnly

Diese Richtlinie bietet schreibgeschützten Zugriff auf Amazon RDS Performance Insights für Amazon-RDS-DB-Instances und Amazon-Aurora-DB-Cluster.

Die Richtlinie enthält jetzt `Sid` (Anweisungs-ID) als Bezeichner für die Richtlinienanweisung.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `rds` – Ermöglicht es Prinzipalen, Amazon-RDS-DB-Instances und Amazon-Aurora-DB-Cluster zu beschreiben.
- `pi` – Ermöglicht es Prinzipalen, Aufrufe an die Amazon-RDS-Performance-Insights-API zu tätigen und auf Performance-Insights-Metriken zuzugreifen

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments, finden Sie unter AmazonRDSPerformanceInsightsReadOnly im AWS Referenzhandbuch zu verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonRDSPerformanceInsightsFullAccess

Diese Richtlinie bietet Vollzugriff auf Erkenntnisse zur Amazon-RDS-Leistung für DB-Instances von Amazon RDS und DB-Clustern von Amazon Aurora.

Die Richtlinie enthält jetzt `Sid` (Anweisungs-ID) als Bezeichner für die Richtlinienanweisung.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `rds` – Ermöglicht es Prinzipalen, Amazon-RDS-DB-Instances und Amazon-Aurora-DB-Cluster zu beschreiben.
- `pi` – Ermöglicht es Prinzipalen, die API von Erkenntnissen zur Amazon-RDS-Leistung aufzurufen und Leistungsanalyseberichte zu erstellen, anzusehen und zu löschen.
- `cloudwatch` – Ermöglicht es Prinzipalen, alle Amazon- CloudWatch Metriken aufzulisten und Metrikdaten und Statistiken abzurufen.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments, finden Sie unter AmazonRDSPerformanceInsightsFullAccess im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonRDSDirectoryServiceAccess

Diese Richtlinie ermöglicht es Amazon RDS, Aufrufe an AWS Directory Service zu tätigen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgende Berechtigung:

- `ds` – Ermöglicht es Prinzipalen, AWS Directory Service Verzeichnisse zu beschreiben und die Autorisierung für AWS Directory Service Verzeichnisse zu steuern.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments, finden Sie unter AmazonRDSDirectoryServiceAccess im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonRDSServiceRolePolicy

Sie können die `AmazonRDSServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist mit einer servicegebundenen Rolle verknüpft, die es Amazon RDS ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Berechtigungen von serviceverknüpften Rollen für Amazon Aurora.

Amazon RDS-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon RDS an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Amazon-RDS-Dokumentverlauf-Seite.

Änderung	Beschreibung	Datum
AWS Von verwaltete Richtlinien für Amazon RDS – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat `AmazonRDSCustomServiceRolePolicy` der `AWSServiceRoleForRDSCustom` serviceverknüpften Rolle eine neue Berechtigung hinzugefügt, damit RDS Custom for SQL Server den zugrunde liegenden Datenbank-Host-Instance-Typ ändern kann. RDS hat außerdem die `ec2:DescribeInstanceTypes` Berechtigung hinzugefügt, Informationen zum Instance-Typ für den Datenbank-Host abzurufen. Weitere Informationen finden Sie unter AWS Von verwaltete Richtlinien für Amazon RDS.	8. April 2024
AWS Von verwaltete Richtlinien für Amazon RDS – Neue Richtlinie.	Amazon RDS hat eine neue verwaltete Richtlinie hinzugefügt`AmazonRDSCustomInstanceProfileRolePolicy` , mit der RDS Custom Automatisierungsaktionen und Datenbank	27. Februar 2024

Änderung	Beschreibung	Datum
	verwaltungsaufgaben über ein EC2-Instance-Profil ausführen kann. Weitere Informationen finden Sie unter AWS Von verwaltete Richtlinien für Amazon RDS.	
Berechtigungen von serviceverknüpften Rollen für Amazon Aurora – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat der `AmazonRDSServiceRolePolicy` `AWSServiceRoleForRDS` serviceverknüpften Rolle neue Kontoausweis-IDs hinzugefügt. Weitere Informationen finden Sie unter Berechtigungen von serviceverknüpften Rollen für Amazon Aurora.	19. Januar 2024

Änderung	Beschreibung	Datum
AWS Von verwaltete Richtlinien für Amazon RDS – Aktualisierung auf bestehende Richtlinien	Die von `AmazonRDSPerformanceInsightsReadOnly` und `AmazonRDSPerformanceInsightsFullAccess` verwalteten Richtlinien enthalten jetzt `Sid` (Statement-ID) als Bezeichner in der Richtlinienerklärung. Weitere Informationen finden Sie unter AWS Von verwaltete Richtlinie: AmazonRDSPerformanceInsightsReadOnly und AWS Von verwaltete Richtlinie: AmazonRDSPerformanceInsightsFullAccess	23. Oktober 2023

Änderung	Beschreibung	Datum
AWS Von verwaltete Richtlinien für Amazon RDS – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat der verwalteten `AmazonRDSFullAccess` -Richtlinie neue Berechtigungen hinzugefügt. Mit den Berechtigungen können Sie den Leistungsanalysebericht für einen bestimmten Zeitraum erstellen, anzeigen und löschen. Weitere Informationen zur Konfiguration von Zugriffsrichtlinien für Performance Insights finden Sie unter Konfigurieren von Zugriffsrichtlinien für Performance Insights.	17. August 2023

Änderung	Beschreibung	Datum
AWS Von verwaltete Richtlinien für Amazon RDS – Neue Richtlinie und Aktualisierung der bestehenden Richtlinie	Amazon RDS hat der verwalteten `AmazonRDSPerformanceInsightsReadOnly` -Richtlinie neue Berechtigungen und eine neue verwaltete Richtlinie mit dem Namen `AmazonRDSPerformanceInsightsFullAccess` hinzugefügt. Diese Berechtigungen ermöglichen es Ihnen, Performance Insights für einen bestimmten Zeitraum zu analysieren, sich die Analyseergebnisse zusammen mit den Empfehlungen anzusehen und die Berichte zu löschen. Weitere Informationen zur Konfiguration von Zugriffsrichtlinien für Performance Insights finden Sie unter Konfigurieren von Zugriffsrichtlinien für Performance Insights.	16. August 2023

Änderung	Beschreibung	Datum
AWS Von verwaltete Richtlinien für Amazon RDS – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat einen neuen CloudWatch Amazon-Namespace `ListMetrics` zu `AmazonRDSFullAccess` und `AmazonRDSReadOnlyAccess` hinzugefügt. Dieser Namespace ist erforderlich, damit Amazon RDS spezifische Metriken zur Ressourcennutzung auflisten kann. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre CloudWatch Ressourcen.	4. April 2023

Änderung	Beschreibung	Datum
Berechtigungen von serviceverknüpften Rollen für Amazon Aurora – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat der `AmazonRDSServiceRolePolicy` `AWSServiceRoleForRDS` serviceverknüpften Rolle neue Berechtigungen für die Integration mit AWS Secrets Manager hinzugefügt. RDS erfordert die Integration mit Secrets Manager für die Verwaltung von Hauptbenutzerpasswörtern in Secrets Manager. Das Secret verwendet eine reservierte Namenskonvention und schränkt Kundenaktualisierungen ein. Weitere Informationen finden Sie unter Passwortverwaltung mit , Amazon Aurora und AWS Secrets Manager.	22. Dezember 2022

Änderung	Beschreibung	Datum
AWS Von verwaltete Richtlinien für Amazon RDS – Aktualisierung auf bestehende Richtlinien	Amazon RDS hat den `AmazonRDSFullAccess` `AmazonRDSReadOnlyAccess` verwalteten Richtlinien eine neue Berechtigung hinzugefügt, mit der Sie Amazon DevOps Guru in der RDS-Konsole aktivieren können. Diese Berechtigung ist erforderlich, um zu überprüfen, ob DevOps Guru aktiviert ist. Weitere Informationen finden Sie unter Konfiguration von IAM-Zugriffsrichtlinien für Guru for RDS DevOps.	19. Dezember 2022

Änderung	Beschreibung	Datum
Berechtigungen von serviceverknüpften Rollen für Amazon Aurora – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat einen neuen CloudWatch Amazon-Namespace zu `AmazonRDSPreviewServiceRolePolicy` for `PutMetricData` hinzugefügt. Dieser Namespace ist erforderlich, damit Amazon RDS Metriken zur Ressourcennutzung veröffentlichen kann. Weitere Informationen finden Sie unter Bedingungsschlüssel verwenden, um den Zugriff auf CloudWatch Namespaces zu beschränken im CloudWatch Amazon-Benutzerhandbuch.	7. Juni 2022

Änderung	Beschreibung	Datum
Berechtigungen von servicever knüpften Rollen für Amazon Aurora – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat einen neuen CloudWatch Amazon-Na mespace zu `AmazonRDS BetaServiceRolePol icy` for `PutMetricData` hinzugefügt. Dieser Namespace ist erforderlich, damit Amazon RDS Metriken zur Ressource nnutzung veröffentlichen kann. Weitere Informationen finden Sie unter Bedingungsschlüssel verwenden, um den Zugriff auf CloudWatch Namespaces zu beschränken im CloudWatch Amazon-Benutzerhandbuch.	7. Juni 2022

Änderung	Beschreibung	Datum
Berechtigungen von serviceverknüpften Rollen für Amazon Aurora – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat einen neuen CloudWatch Amazon-Namespace zu `AWSServiceRoleForRDS` for `PutMetricData` hinzugefügt. Dieser Namespace ist erforderlich, damit Amazon RDS Metriken zur Ressourcennutzung veröffentlichen kann. Weitere Informationen finden Sie unter Bedingungsschlüssel verwenden, um den Zugriff auf CloudWatch Namespaces zu beschränken im CloudWatch Amazon-Benutzerhandbuch.	22. April 2022
AWS Von verwaltete Richtlinien für Amazon RDS – Neue Richtlinie.	Amazon RDS hat eine neue verwaltete Richtlinie hinzugefügt`AmazonRDSPerformanceInsightsReadOnly`, die es Amazon RDS ermöglicht, AWS Dienste im Namen Ihrer DB-Instances aufzurufen. Weitere Informationen zur Konfiguration von Zugriffsrichtlinien für Performance Insights finden Sie unter Konfigurieren von Zugriffsrichtlinien für Performance Insights.	10. März 2022

Änderung	Beschreibung	Datum
Berechtigungen von serviceverknüpften Rollen für Amazon Aurora – Aktualisierung auf eine bestehende Richtlinie	Amazon RDS hat neue CloudWatch Amazon-Namespaces zu for hinzugefügt. `AWSServiceRoleForRDS` `PutMetricData` Diese Namespaces sind erforderlich, damit Amazon DocumentDB (mit MongoDB-Kompatibilität) und Amazon Neptune Metriken veröffentlichen können. CloudWatch Weitere Informationen finden Sie unter Bedingungsschlüssel verwenden, um den Zugriff auf CloudWatch Namespaces zu beschränken im CloudWatch Amazon-Benutzerhandbuch.	4. März 2022
Amazon RDS hat mit der Verfolgung von Änderungen begonnen	Amazon RDS begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	26. Oktober 2021

Vermeidung des dienstübergreifenden Confused-Deputy-Problems

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine Entität, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine Entität mit größeren Rechten zwingen kann, die Aktion auszuführen. In AWS kann der dienstübergreifende Identitätswechsel zu Confused-Deputy-Problem führen.

Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben. Weitere Informationen finden Sie unter Das Problem des verwirrten Stellvertreters im IAM-Benutzerhandbuch.

Wir empfehlen die Verwendung der globalen Bedingungskontextschlüssel `aws:SourceArn` und `aws:SourceAccount` in ressourcenbasierten Richtlinien, um die Berechtigungen, die Amazon RDS einem anderen Service erteilt, auf eine bestimmte Ressource zu beschränken.

In einigen Fällen enthält der `aws:SourceArn`-Wert nicht die Konto-ID, z. B. wenn Sie den Amazon-Ressourcennamen (ARN) für einen Amazon-S3-Bucket verwenden. Stellen Sie in diesen Fällen sicher, dass Sie beide globalen Kontextschlüssel für die Bedingung verwenden, um Berechtigungen einzuschränken. In einigen Fällen verwenden Sie beide globalen Bedingungskontextschlüssel und der `aws:SourceArn`-Wert enthält die Konto-ID. Stellen Sie in diesen Fällen sicher, dass der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn` dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden. Wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten, verwenden Sie `aws:SourceArn`. Wenn Sie zulassen möchten, dass Ressourcen im angegebenen AWS-Konto mit der betriebsübergreifenden Verwendung verknüpft werden, verwenden Sie `aws:SourceAccount`.

Stellen Sie sicher, dass der Wert von `aws:SourceArn` ein ARN für einen Amazon-RDS-Ressourcentyp ist. Weitere Informationen finden Sie unter Arbeiten mit Amazon-Ressourcennamen (ARN) in Amazon RDS.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontextschlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. In einigen Fällen kennen Sie möglicherweise den vollständigen ARN der Ressource nicht oder Sie geben möglicherweise mehrere Ressourcen an. Verwenden Sie in diesen Fällen die

globalen `aws:SourceArn`-Kontextbedingungsschlüssel mit Platzhaltern (*) für die unbekannten Teile des ARN. Ein Beispiel ist `arn:aws:rds:*:123456789012:*`.

Das folgende Beispiel zeigt, wie Sie die globalen Bedingungskontextschlüssel `aws:SourceArn` und `aws:SourceAccount` für Amazon RDS verwenden können, um das Confused-Deputy-Problem zu verhindern.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "rds.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:rds:us-east-1:123456789012:db:mydbinstance"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Weitere Beispiele für Richtlinien, die die globalen Bedingungskontextschlüssel `aws:SourceArn` und `aws:SourceAccount` verwenden, finden Sie in den folgenden Abschnitten:

- Erteilen von Berechtigungen zum Veröffentlichen von Benachrichtigungen in einem Amazon-SNS-Thema
- Einrichten des Zugriffs auf einen Amazon S3-Bucket (PostgreSQL-Import)
- Einrichten des Zugriffs auf einen Amazon S3-Bucket (PostgreSQL-Export)

IAM-Datenbankauthentifizierung

Sie können sich bei Ihrem mithilfe der AWS Identity and Access Management (IAM-) Datenbankauthentifizierung authentifizieren. Die IAM-Datenbankauthentifizierung funktioniert mit Aurora MySQL und Aurora PostgreSQL. Mit dieser Authentifizierungsmethode benötigen Sie kein Passwort, um eine Verbindung mit einer DB-Cluster herzustellen. Stattdessen verwenden Sie ein Authentifizierungstoken.

Ein Authentifizierungstoken ist eine eindeutige Zeichenfolge, die von Amazon Aurora auf Anforderung erzeugt wird. Authentifizierungstoken werden mit AWS Signature Version 4 generiert. Jedes Token verfällt 15 Minuten nach seiner Erzeugung. Da die Authentifizierung mithilfe von IAM extern verwaltet wird, ist es nicht erforderlich, Benutzeranmeldeinformationen in der Datenbank zu speichern. Sie können weiterhin auch die Standard-Datenbank-Authentifizierung verwenden. Das Token wird nur zur Authentifizierung verwendet und wirkt sich nicht auf die Sitzung aus, nachdem es eingerichtet wurde.

Die IAM-Datenbank-Authentifizierung bietet die folgenden Vorteile:

- Der Netzwerkverkehr zur und von der Datenbank wird mit Secure Socket Layer (SSL) oder Transport Layer Security (TLS) verschlüsselt. Weitere Informationen zur Verwendung von SSL/TLS mit Amazon Aurora finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .
- Sie können IAM verwenden, um den Zugriff auf Ihre Datenbankressourcen zentral zu verwalten, anstatt den Zugriff individuell auf jedem DB-Cluster zu verwalten.
- Für Anwendungen, die auf Amazon EC2 laufen, können Sie die der EC2-Instance eigenen Profil-Anmeldeinformationen anstatt eines Passworts verwenden, um auf Ihre Datenbank zuzugreifen. Dies erhöht die Sicherheit.

Erwägen Sie im Allgemeinen, die IAM-Datenbankauthentifizierung zu verwenden, wenn Ihre Anwendungen weniger als 200 Verbindungen pro Sekunde erstellen und Sie Benutzernamen und Passwörter nicht direkt in Ihrem Anwendungscode verwalten möchten.

Der Amazon Web Services (AWS) JDBC-Treiber unterstützt die IAM-Datenbankauthentifizierung. Weitere Informationen finden Sie unter AWS IAM-Authentifizierungs-Plug-In im Amazon Web Services (AWS) JDBC-Treiber-Repository. GitHub

Der Amazon Web Services (AWS) Python-Treiber unterstützt die IAM-Datenbankauthentifizierung. Weitere Informationen finden Sie unter AWS IAM-Authentifizierungs-Plug-In im GitHubPython-Treiber-Repository von Amazon Web Services (AWS).

Themen

Verfügbarkeit von Regionen und Versionen

Die Verfügbarkeit von Funktionen und der Support variieren zwischen bestimmten Versionen der einzelnen Aurora-Datenbank-Engines und in allen AWS-Regionen. Weitere Informationen zur Verfügbarkeit von Versionen und Regionen mit Aurora- und IAM-Datenbankauthentifizierung finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für die IAM-Datenbankauthentifizierung.

Für Aurora MySQL unterstützen alle unterstützten DB-Instance-Klassen die IAM-Datenbank-Authentifizierung, mit Ausnahme von db.t2.small und db.t3.small. Informationen zu den unterstützten DB-Instance-Klassen finden Sie unter Unterstützte DB-Engines für DB-Instance-Klassen.

CLI- und SDK-Unterstützung

Die IAM-Datenbankauthentifizierung ist für die AWS CLIund für die folgenden AWS sprachspezifischen SDKs verfügbar:

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby

Einschränkungen der IAM-Datenbank-Authentifizierung

Beachten Sie bei der Verwendung der IAM-Datenbankauthentifizierung die folgenden Einschränkungen:

- Die IAM-Datenbankauthentifizierung drosselt Verbindungen in den folgenden Szenarien:
  - Mit Authentifizierungstoken, die jeweils mit einer anderen IAM-Identität signiert sind, überschreiten Sie 20 Verbindungen pro Sekunde.
  - Sie überschreiten 200 Verbindungen pro Sekunde mit unterschiedlichen Authentifizierungstoken.

  Verbindungen, die dasselbe Authentifizierungstoken verwenden, werden nicht gedrosselt. Wir empfehlen, dass Sie Authentifizierungstoken nach Möglichkeit wiederverwenden.
- Derzeit unterstützt die IAM-Datenbankauthentifizierung nicht alle globalen Bedingungskontextschlüssel.

  Weitere Informationen über globale Bedingungskontextschlüssel finden Sie unter Globale AWS - Bedingungskontextschlüssel im IAM-Benutzerhandbuch.
- Wenn die IAM-Rolle (`rds_iam`) einem Benutzer (einschließlich RDS-Hauptbenutzer) hinzugefügt wird, hat bei PostgreSQL die IAM-Authentifizierung Vorrang vor der Passwort-Authentifizierung, so dass sich der Benutzer als IAM-Benutzer anmelden muss.
- Für Aurora PostgreSQL können Sie die IAM-Authentifizierung nicht verwenden, um eine Replikationsverbindung herzustellen.
- Sie können keinen benutzerdefinierten Route-53-DNS-Datensatz anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.
- CloudWatch und protokollieren Sie die IAM-Authentifizierung CloudTrail nicht. Diese Dienste verfolgen keine `generate-db-auth-token` API-Aufrufe, die die IAM-Rolle autorisieren, eine Datenbankverbindung zu aktivieren. Weitere Informationen finden Sie unter Erzielen Sie Überprüfbarkeit mit der Amazon RDS-IAM-Authentifizierung mithilfe der attributebasierten Zugriffskontrolle.

Empfehlungen für die IAM-Datenbankauthentifizierung

Bei Verwendung der IAM-Datenbankauthentifizierung empfehlen wir Folgendes:

- Verwenden Sie die IAM-Datenbankauthentifizierung, wenn Ihre Anwendung weniger als 200 neue IAM-Datenbankauthentifizierungsverbindungen pro Sekunde benötigt.

Die Datenbank-Engines, die mit Amazon Aurora kompatibel sind, setzen den Authentifizierungsversuchen pro Sekunde keine Grenzen. Wenn Sie jedoch die IAM-Datenbank-Authentifizierung verwenden, muss Ihre Anwendung ein Authentifizierungstoken erzeugen. Ihre Anwendung verwendet dann dieses Token, um eine Verbindung mit dem DB-Cluster herzustellen. Wenn Sie die Höchstanzahl neuer Verbindungen pro Sekunde überschreiten, kann der zusätzliche Overhead der IAM-Datenbankauthentifizierung zur Verbindungsablehnung führen.

Erwägen Sie die Verwendung von Verbindungspooling in Ihren Anwendungen, um den ständigen Verbindungsaufbau zu begrenzen. Dadurch lässt sich der Aufwand für die IAM-DB-Authentifizierung reduzieren und Ihre Anwendungen können bestehende Verbindungen wiederverwenden. Erwägen Sie alternativ die Verwendung von RDS-Proxy für diese Anwendungsfälle. RDS-Proxy ist mit zusätzlichen Kosten verbunden. Weitere Informationen finden Sie unter RDS-Proxy – Preise.

- Die Größe eines IAM-Datenbankauthentifizierungstokens hängt von vielen Faktoren ab, einschließlich der Anzahl der IAM-Tags, IAM-Servicerichtlinien, ARN-Längen sowie andere IAM- und Datenbankeigenschaften. Die Mindestgröße dieses Tokens beträgt im Allgemeinen etwa 1 KB, kann aber durchaus größer sein. Da dieses Token bei der IAM-Authentifizierung als Passwort in der Verbindungszeichenfolge zur Datenbank verwendet wird, sollten Sie sicherstellen, dass Ihr Datenbanktreiber (z. B. ODBC) und/oder andere Tools dieses Token aufgrund seiner Größe nicht beschränken oder auf andere Weise kürzen. Ein verkürztes Token führt dazu, dass die von der Datenbank und IAM durchgeführte Authentifizierungsüberprüfung fehlschlägt.
- Wenn Sie beim Erstellen eines IAM-Datenbank-Authentifizierungstokens temporäre Anmeldeinformationen verwenden, müssen die temporären Anmeldeinformationen weiterhin gültig sein, wenn Sie das IAM-Datenbank-Authentifizierungstoken für eine Verbindungsanforderung verwenden.

Kontext-Schlüssel für globale Bedingungen werden nicht unterstützt AWS

Die IAM-Datenbankauthentifizierung unterstützt die folgende Teilmenge der AWS globalen Bedingungskontextschlüssel nicht.

- `aws:Referer`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`

- `aws:UserAgent`
- `aws:VpcSourceIp`

Weitere Informationen finden Sie unter Globale AWS -Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung

Die IAM-Datenbank-Authentifizierung ist für DB-Cluster standardmäßig deaktiviert. Sie können die IAM-Datenbankauthentifizierung mithilfe der AWS Management Console, AWS CLI oder der API aktivieren (oder wieder deaktivieren).

Sie können die IAM-Datenbankauthentifizierung aktivieren, wenn Sie eine der folgenden Aktionen ausführen:

- Informationen zum Erstellen eines neuen DB-Clusters mit aktivierter IAM-Datenbankauthentifizierung finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.
- Informationen zum Ändern eines DB-Clusters zur Aktivierung der IAM-Datenbankauthentifizierung finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.
- Informationen zum Wiederherstellen eines DB-Clusters aus einem Snapshot mit aktivierter IAM-Datenbankauthentifizierung finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot.
- Informationen zum Wiederherstellen eines DB-Clusters zu einem Zeitpunkt mit aktivierter IAM-Datenbankauthentifizierung finden Sie unter Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit.

Konsole

Jeder Erstellungs- oder Änderungsworkflow verfügt über einen Abschnitt Database authentification (Datenbankauthentifizierung), in dem Sie die IAM-Datenbankauthentifizierung aktivieren oder deaktivieren können. Wählen Sie in diesem Abschnitt Password and IAM database authentication (Passwort- und IAM-Datenbankauthentifizierung), um die IAM-Datenbankauthentifizierung zu aktivieren.

So aktivieren bzw. deaktivieren die IAM-Datenbankauthentifizierung für eine vorhandene DB-einen vorhandenen DB-Cluster:

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie den DB-Cluster aus, die Sie ändern möchten.

> **Note**
>
> Sie können die IAM-Authentifizierung nur aktivieren, wenn alle DB-Instances im Cluster mit IAM kompatibel sind. Überprüfen Sie die Kompatibilitätsanforderungen in Verfügbarkeit von Regionen und Versionen.

4. Wählen Sie Modify aus.
5. Wählen Sie in diesem Abschnitt Datenbankauthentifizierung Password and IAM database authentication (Passwort- und IAM-Datenbankauthentifizierung), um die IAM-Datenbankauthentifizierung zu aktivieren. Wählen Sie Passwort-Authentifizierung oder Passwort- und Kerberos-Authentifizierung aus, um die IAM-Authentifizierung zu deaktivieren.
6. Klicken Sie auf Continue.
7. Um die Änderungen sofort anzuwenden, wählen Sie im Abschnitt Scheduling of modifications (Planen von Änderungen) die Option Immediately (Sofort).
8. Wählen Sie Cluster ändern.

AWS CLI

Verwenden Sie den Befehl AWS CLI, um mithilfe der `create-db-cluster` einen neuen DB-Cluster mit IAM-Authentifizierung zu erstellen. Legen Sie die Option `--enable-iam-database-authentication` fest.

Um einen bestehenden DB-Cluster mit oder ohne IAM-Authentifizierung zu aktualisieren, verwenden Sie den AWS CLI-Befehl `modify-db-cluster`. Sie müssen entweder die Option `--enable-iam-database-authentication` oder `--no-enable-iam-database-authentication` angeben.

> **Note**
>
> Sie können die IAM-Authentifizierung nur aktivieren, wenn alle DB-Instances im Cluster mit IAM kompatibel sind. Überprüfen Sie die Kompatibilitätsanforderungen in Verfügbarkeit von Regionen und Versionen.

Standardmäßig führt Aurora die Änderung während des nächsten Wartungsfensters durch. Wenn Sie diese Einstellung übergehen und die IAM-DB-Authentifizierung schnellstmöglich aktivieren möchten, verwenden Sie den Parameter `--apply-immediately`.

Verwenden Sie zum Wiederherstellen eines DB-Clusters einen der folgenden AWS CLI-Befehle:

- `restore-db-cluster-to-point-in-time`
- `restore-db-cluster-from-db-snapshot`

Die Voreinstellung der IAM-Datenbank-Authentifizierung entspricht der Einstellung des Quell-Snapshot. Wählen Sie die entsprechende Option `--enable-iam-database-authentication` oder `--no-enable-iam-database-authentication` aus.

RDS-API

Verwenden Sie die API-Operation , um mithilfe der API eine neue DB-Instance mit IAM-Authentifizierung zu erstellen `CreateDBCluster`. Stellen Sie den Parameter `EnableIAMDatabaseAuthentication` auf `true` ein.

Um einen bestehenden DB-Cluster mit oder ohne IAM-Authentifizierung zu aktualisieren, verwenden Sie die API-Operation `ModifyDBCluster`. Setzen Sie den Parameter `EnableIAMDatabaseAuthentication` auf `true`, um die IAM-Authentifizierung zu aktivieren, oder auf `false`, um sie zu deaktivieren.

> **Note**
>
> Sie können die IAM-Authentifizierung nur aktivieren, wenn alle DB-Instances im Cluster mit IAM kompatibel sind. Überprüfen Sie die Kompatibilitätsanforderungen in Verfügbarkeit von Regionen und Versionen.

Verwenden Sie eine der folgenden API-Operationen, wenn Sie einen DB--Cluster wiederherstellen.

- `RestoreDBClusterFromSnapshot`
- `RestoreDBClusterToPointInTime`

Die Voreinstellung der IAM-Datenbank-Authentifizierung entspricht der Einstellung des Quell-Snapshot. Zum Ändern dieser Einstellung setzen Sie den Parameter

`EnableIAMDatabaseAuthentication` auf `true`, um die IAM-Authentifizierung zu aktivieren, oder auf `false`, um sie zu deaktivieren.

Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff

Sie müssen eine IAM-Richtlinie erstellen, um einem Benutzer oder einer Rolle zu erlauben, eine Verbindung mit Ihrem DB-Cluster herzustellen. Anschließend fügen Sie die Richtlinie an einen Berechtigungssatz oder eine Rolle an.

> **Note**
>
> Weitere Informationen zu IAM-Richtlinien finden Sie unter Identity and Access Management für Amazon Aurora.

Die folgende Beispielrichtlinie erlaubt einem Benutzer, eine Verbindung mit einem DB-Cluster mithilfe der IAM-Datenbank-Authentifizierung herzustellen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
             "arn:aws:rds-db:us-east-2:1234567890:dbuser:cluster-ABCDEFGHIJKL01234/
db_user"
         ]
      }
   ]
}
```

> **Important**
>
> Ein Benutzer mit Administratorberechtigungen kann auf DB-Cluster zugreifen, ohne über eine IAM-Richtlinie explizite Berechtigungen zu erhalten. Wenn Sie den Administratorzugriff

auf DB--Cluster einschränken möchten, können Sie eine IAM-Rolle mit geeigneten, weniger privilegierten Berechtigungen erstellen und diese dem Administrator zuweisen.

> **Note**
>
> Verwechseln Sie das Präfix `rds-db:` nicht mit anderen RDS-API-Operationspräfixen, die mit `rds:` beginnen. Das Präfix `rds-db:` und die Aktion `rds-db:connect` werden nur zur IAM-Datenbank-Authentifizierung verwendet. Sie sind in keinem anderen Kontext gültig.

Die Beispielrichtlinie enthält eine einzige Anweisung mit den folgenden Elementen:

- `Effect` – Geben Sie `Allow` an, um den Zugriff auf den DB-Cluster zu gewähren. Wenn Sie den Zugriff nicht ausdrücklich erlauben, wird er automatisch verweigert.
- `Action` – Geben Sie `rds-db:connect` an, um Verbindungen mit dem DB-Cluster zu erlauben.
- `Resource` – Geben Sie einen Amazon-Ressourcennamen (ARN) an, der ein Datenbankkonto auf einem DB-Cluster beschreibt. Das ARN-Format lautet folgendermaßen.

```
arn:aws:rds-db:region:account-id:dbuser:DbClusterResourceId/db-user-name
```

  Ersetzen Sie in diesem Format Folgendes:

  - *`region`* ist die AWS-Region für die DB-Cluster. In der Beispielrichtlinie lautet die AWS-Region `us-east-2`.
  - *`account-id`* bezeichnet die AWS-Kontonummer für die DB- Cluster In der Beispielrichtlinie lautet die Kontonummer `1234567890`. Der Benutzer muss dasselbe Konto wie das Konto für die/den DB-Cluster haben.

    Um einen kontoübergreifenden Zugriff durchzuführen, erstellen Sie eine IAM-Rolle mit der oben angegebenen Richtlinie im Konto für die/den DB-Cluster und erlauben Sie Ihrem anderen Konto, die Rolle zu übernehmen.
  - *`DbClusterResourceId`* ist die Kennung des DB-Clusters. Diese Kennung ist für eineAWS-Region eindeutig und unveränderlich. In dieser Beispielrichtlinie lautet die Kennung `cluster-ABCDEFGHIJKL01234`.

Um die Ressourcen-ID eines DB-Clusters in der AWS Management Console für Amazon Aurora zu ermitteln, wählen Sie den DB-Cluster zum Anzeigen von Details aus. Wechseln Sie zur Registerkarte Konfiguration. Die Resource ID (Ressourcen-ID) wird im Abschnitt Configuration Details (Konfigurationsdetails) angezeigt.

Alternativ können Sie den AWS CLI-Befehl verwenden, um die Kennungen und Ressourcen-IDs für alle Ihre DB-Cluster in der aktuellen AWS-Region aufzulisten, wie nachstehend aufgeführt.

```
aws rds describe-db-clusters --query "DBClusters[*].
[DBClusterIdentifier,DbClusterResourceId]"
```

> **Note**
>
> Wenn Sie über den RDS-Proxy eine Verbindung zu einer Datenbank herstellen, geben Sie die Proxy-Ressourcen-ID an, z. B. `prx-ABCDEFGHIJKL01234`. Hinweise zur Verwendung der IAM-Datenbankauthentifizierung mit RDS-Proxy finden Sie unter Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung.

- *`db-user-name`* ist der Name des mit der IAM-Authentifizierung zu verknüpfenden Datenbankkontos. In der Beispielrichtlinie lautet das Datenbankkonto `db_user`.

Sie können andere ARN erstellen, um mehrere Zugriffsmuster zu unterstützen. Die folgende Richtlinie erlaubt den Zugriff auf zwei verschiedene Datenbankkonten auf einem DB-Cluster.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
             "arn:aws:rds-db:us-east-2:123456789012:dbuser:cluster-ABCDEFGHIJKL01234/
jane_doe",
```

```
            "arn:aws:rds-db:us-east-2:123456789012:dbuser:cluster-ABCDEFGHIJKL01234/
mary_roe"
         ]
      }
   ]
}
```

Die nachstehende Richtlinie verwendet das Zeichen "*", um alle DB-Cluster und Datenbankkonten eines bestimmten AWS-Kontos und in einer bestimmten AWS-Region freizugeben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds-db:connect"
            ],
            "Resource": [
                "arn:aws:rds-db:us-east-2:1234567890:dbuser:*/*"
            ]
        }
    ]
}
```

Die nachstehende Richtlinie gleicht alle DB-Cluster eines bestimmten AWS-Kontos und in einer bestimmten AWS-Region ab. Allerdings gewährt die Richtlinie nur den Zugriff auf DB-Cluster, die über ein `jane_doe`-Datenbankkonto verfügen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
```

```
            "arn:aws:rds-db:us-east-2:123456789012:dbuser:*/jane_doe"
         ]
      }
   ]
}
```

Der Benutzer oder die Rolle hat nur auf jene Datenbanken Zugriff, auf die der Datenbankbenutzer zugreifen kann. Nehmen wir beispielsweise an, dass Ihr DB-Cluster über eine Datenbank mit dem Namen dev und eine weitere Datenbank mit dem Namen test verfügt. Wenn der Datenbankbenutzer `jane_doe` nur auf dev zugreifen kann, haben auch alle anderen Benutzer oder Rollen, die auf diesen DB-Cluster mit dem Benutzer `jane_doe` zugreifen, lediglich die Berechtigung für den Zugriff auf dev. Diese Zugriffsbeschränkung gilt auch für andere Datenbankobjekte, wie z. B. Tabellen, Ansichten usw.

Ein Administrator muss IAM-Richtlinien erstellen, die Entitäten die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den Berechtigungssätzen oder Rollen anfügen, die diese Berechtigungen benötigen. Beispiele für Richtlinien finden Sie unter Beispiele für identitätsbasierte Amazon-Aurora-Richtlinien.

Anfügen einer IAM-Richtlinie an einen Berechtigungssatz oder eine Rolle

Nachdem Sie eine IAM-Richtlinie erstellt haben, um die Datenbank-Authentifizierung zu erlauben, müssen Sie die Richtlinie an einen Berechtigungssatz oder eine Rolle anfügen. Eine praktische Anleitung zu diesem Thema finden Sie unter Erstellen und Anfügen Ihrer ersten vom Kunden verwalteten Richtlinie im IAM-Benutzerhandbuch.

Wenn Sie die praktischen Anleitung durchgehen, können Sie eine der in diesem Abschnitt aufgeführten Beispielrichtlinien als Ausgangsbasis verwenden und auf Ihre Bedürfnisse anpassen. Am Ende des Tutorials verfügen Sie über einen Berechtigungssatz mit einer angefügten Richtlinie, der zur Durchführung der Aktion `rds-db:connect` berechtigt ist.

> **Note**
>
> Sie können mehrere Berechtigungssätze oder Rollen mit demselben Datenbank-Benutzerkonto verknüpfen. Nehmen wir beispielsweise an, dass Ihre IAM-Richtlinie folgenden Ressourcen-ARN enthält.

```
arn:aws:rds-db:us-east-2:123456789012:dbuser:cluster-12ABC34DEFG5HIJ6KLMNOP78QR/
jane_doe
```

Wenn Sie die Richtlinie an Jane, Bob und Diego anfügen, sind diese Benutzer in der Lage, eine Verbindung mit dem angegebenen DB-Cluster mithilfe des Datenbankkontos `jane_doe` herzustellen.

Erstellen eines Datenbankkontos mithilfe der IAM-Authentifizierung

Mit der IAM-Datenbank-Authentifizierung müssen Sie den von Ihnen erstellten Benutzerkonten keine Datenbankpasswörter zuweisen. Wenn Sie einen mit dem Datenbankkonto verknüpften Benutzer entfernen, sollten Sie auch das Datenbankkonto mit der Anweisung `DROP USER` entfernen.

> **Note**
>
> Der für die IAM-Authentifizierung verwendete Benutzername muss mit der Schreibweise des Benutzernamens in der Datenbank übereinstimmen.

Themen

- Verwenden der IAM-Authentifizierung mit Aurora MySQL
- Verwenden der IAM-Authentifizierung mit Aurora PostgreSQL

Verwenden der IAM-Authentifizierung mit Aurora MySQL

Mit Aurora MySQL erfolgt die Authentifizierung durch `AWSAuthenticationPlugin` – ein von AWS bereitgestelltes Plug-In, das reibungslos mit IAM zur Authentifizierung Ihrer Benutzer funktioniert. Stellen Sie als Hauptbenutzer oder als anderer Benutzer, der Benutzer erstellen und Berechtigungen gewähren kann, eine Verbindung mit dem DB-Cluster her. Geben Sie die `CREATE USER`-Anweisung aus, wie im folgenden Beispiel dargestellt.

```
CREATE USER jane_doe IDENTIFIED WITH AWSAuthenticationPlugin AS 'RDS';
```

Die Klausel `IDENTIFIED WITH` ermöglicht Aurora MySQL die Verwendung von `AWSAuthenticationPlugin`, um das Datenbankkonto (`jane_doe`) zu authentifizieren. Die

`AS 'RDS'`-Klausel bezieht sich auf die Authentifizierungsmethode. Stellen Sie sicher, dass der angegebene Datenbankbenutzername mit einer Ressource in der IAM-Richtlinie für den IAM-Datenbankzugriff identisch ist. Weitere Informationen finden Sie unter Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff.

> **Note**
>
> Wenn folgende Meldung erscheint, ist das von AWS bereitgestellte Plug-In für den aktuellen DB-Cluster nicht verfügbar.
> `ERROR 1524 (HY000): Plugin 'AWSAuthenticationPlugin' is not loaded`
> Stellen Sie sicher, dass Sie eine unterstützte Konfiguration verwenden und die IAM-Datenbankauthentifizierung auf Ihrem DB-Cluster aktiviert haben, um den Fehler zu beheben. Weitere Informationen erhalten Sie unter Verfügbarkeit von Regionen und Versionen und Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung.

Nachdem Sie ein Konto mithilfe von `AWSAuthenticationPlugin` erstellt haben, können Sie es in der gleichen Weise wie sonstige Datenbankkonten verwalten. Sie können beispielsweise Kontoberechtigungen mit den Anweisungen `GRANT` und `REVOKE` oder mehrere Kontoattribute mit der Anweisung `ALTER USER` ändern.

Der Datenbank-Netzwerkverkehr wird bei Verwendung von IAM mit SSL/TLS verschlüsselt. Ändern Sie mit dem folgenden Befehl das Benutzerkonto, um SSL-Verbindungen zuzulassen.

```
ALTER USER 'jane_doe'@'%' REQUIRE SSL;
```

Verwenden der IAM-Authentifizierung mit Aurora PostgreSQL

Wenn Sie die IAM-Authentifizierung mit Aurora PostgreSQL verwenden möchten, stellen Sie als Hauptbenutzer oder als anderer Benutzer, der Benutzer erstellen und Berechtigungen gewähren kann, eine Verbindung mit dem DB-Cluster her. Nachdem die Verbindung hergestellt wurde, erstellen Sie Datenbankbenutzer und weisen ihnen die `rds_iam`-Rolle zu, wie im folgenden Beispiel dargestellt.

```
CREATE USER db_userx;
GRANT rds_iam TO db_userx;
```

Stellen Sie sicher, dass der angegebene Datenbankbenutzername mit einer Ressource in der IAM-Richtlinie für den IAM-Datenbankzugriff identisch ist. Weitere Informationen finden Sie unter Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff.

Beachten Sie, dass ein PostgreSQL-Datenbankbenutzer entweder die IAM- oder Kerberos-Authentifizierung verwenden kann, jedoch nicht beides, so dass dieser Benutzer nicht auch über die `rds_ad`-Rolle verfügen kann. Dies gilt auch für verschachtelte Mitgliedschaften. Weitere Informationen finden Sie unter Schritt 7: Erstellen von PostgreSQL-Benutzern für Ihre Kerberos-Prinzipale .

Herstellen einer Verbindung zu Ihrem DB--Cluster mithilfe der IAM-Authentifizierung

Bei einer IAM-Datenbankauthentifizierung verwenden Sie ein Authentifizierungstoken, wenn Sie sich mit Ihrem DB-Cluster verbinden. Ein Authentifizierungstoken ist eine Zeichenfolge, die Sie anstelle eines Passworts verwenden. Nachdem Sie ein Authentifizierungstoken erzeugt haben, ist es 15 Minuten lang gültig. Wenn Sie versuchen, sich mit einem verfallenen Token zu verbinden, wird die Verbindungsabfrage abgelehnt.

Jedes Authentifizierungstoken muss eine gültige Signatur unter Verwendung von AWS Signature Version 4 enthalten. (Weitere Informationen finden Sie unter Signaturvorgang für Signature Version 4 in der Allgemeine AWS-Referenz.) Das AWS CLI und ein AWS SDK, z. B. das AWS SDK for Java oder AWS SDK for Python (Boto3), können jedes von Ihnen erstellte Token automatisch signieren.

Sie können ein Authentifizierungstoken verwenden, wenn Sie von einem anderen AWS Service aus eine Verbindung zu Amazon Aurora AWS Lambda herstellen, z. Durch Verwendung eines Tokens können Sie vermeiden, ein Passwort in Ihrem Code angeben zu müssen. Alternativ können Sie ein AWS SDK verwenden, um ein Authentifizierungstoken programmgesteuert zu erstellen und programmgesteuert zu signieren.

Nachdem Sie über ein signiertes IAM-Authentifizierungstoken verfügen, können Sie eine Verbindung mit einem Aurora-DB-Cluster herstellen. Im Folgenden erfahren Sie, wie Sie dies entweder mit einem Befehlszeilentool oder einem AWS SDK, wie dem oder, tun können. AWS SDK for Java AWS SDK for Python (Boto3)

Weitere Informationen finden Sie in den folgenden Blogeinträgen:

- IAM-Authentifikation zum Verbinden mit von SQL Workbench/J mit Aurora MySQL oder Amazon RDS for MySQL verwenden
- Verwenden der IAM-Authentifizierung zum Verbinden mit pgAdmin Amazon Aurora PostgreSQL oder Amazon RDS for PostgreSQL

Voraussetzungen

Die folgenden Voraussetzungen gelten für die Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung:

- Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung
- Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff
- Erstellen eines Datenbankkontos mithilfe der IAM-Authentifizierung

Themen

- Herstellen einer Verbindung zu Ihrem mithilfe der IAM-Authentifizierung mit den Treibern AWS
- Herstellen einer Verbindung zu Ihrem mithilfe der IAM-Authentifizierung über die Befehlszeile: AWS CLI und MySQL-Client
- Herstellen einer Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung von der Befehlszeile aus: AWS CLI und psql-Client
- Herstellen einer Verbindung zu Ihrem DB--Cluster mithilfe der IAM-Authentifizierung und AWS SDK for .NET
- Herstellen einer Verbindung zu Ihrem DB--Cluster mithilfe der IAM-Authentifizierung und AWS SDK for Go
- Herstellen einer Verbindung zu Ihrem mithilfe der IAM-Authentifizierung und der AWS SDK for Java
- Herstellen einer Verbindung zu Ihrem DB--Cluster mithilfe der IAM-Authentifizierung und AWS SDK for Python (Boto3)

Herstellen einer Verbindung zu Ihrem mithilfe der IAM-Authentifizierung mit den Treibern AWS

Die AWS Treibersuite wurde so konzipiert, dass sie schnellere Switchover- und Failover-Zeiten sowie Authentifizierung mit AWS Secrets Manager, AWS Identity and Access Management (IAM) und Federated Identity unterstützt. Die AWS Treiber sind darauf angewiesen, den Status der des DB-Clusters zu überwachen und die Cluster-Instance-Topologie zu kennen, um den Writer zu ermitteln. Dieser Ansatz reduziert die Switchover- und Failover-Zeiten auf einstellige Sekunden, verglichen mit mehreren zehn Sekunden bei Open-Source-Treibern.

Weitere Informationen zu den AWS Treibern finden Sie im entsprechenden Sprachtreiber für Ihren Aurora MySQL- oder Aurora PostgreSQL-DB-Cluster.

Herstellen einer Verbindung zu Ihrem mithilfe der IAM-Authentifizierung über die Befehlszeile: AWS CLI und MySQL-Client

Sie können von der Befehlszeile aus eine Verbindung zu einem Aurora-DB-Cluster der herstellen, indem Sie das `mysql` Befehlszeilentool AWS CLI und verwenden, wie im Folgenden beschrieben.

Voraussetzungen

Die folgenden Voraussetzungen gelten für die Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung:

- Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung
- Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff
- Erstellen eines Datenbankkontos mithilfe der IAM-Authentifizierung

> **Note**
>
> Informationen zum Herstellen einer Verbindung mit Ihrer Datenbank mithilfe von SQL Workbench/J mit IAM-Authentifizierung finden Sie im Blogbeitrag IAM-Authentifikation zum Verbinden von SQL Workbench/J Aurora MySQL oder Amazon RDS for MySQL verwenden.

Themen

- Generieren eines IAM-Authentifizierungstokens
- Herstellen der Verbindung zu einem DB--Cluster

Generieren eines IAM-Authentifizierungstokens

Im folgenden Beispiel wird gezeigt, wie Sie ein signiertes Authentifizierungstoken mithilfe der erhalte AWS CLI.

```
aws rds generate-db-auth-token \
   --hostname rdsmysql.123456789012.us-west-2.rds.amazonaws.com \
   --port 3306 \
   --region us-west-2 \
   --username jane_doe
```

In diesem Beispiel lauten die Parameter folgendermaßen:

- `--hostname` – Der Hostname des DB--Clusters, auf den Sie zugreifen möchten.
- `--port` – Die Nummer des Ports, der für die Verbindung mit dem DB--Cluster verwendet wird.
- `--region`— Die AWS Region, in der der läuft
- `--username` – Das Datenbankkonto, auf das Sie zugreifen möchten.

Die ersten Zeichen des Tokens sehen folgendermaßen aus.

```
rdsmysql.123456789012.us-west-2.rds.amazonaws.com:3306/?
Action=connect&DBUser=jane_doe&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

> **Note**
>
> Sie können keinen benutzerdefinierten Route-53-DNS-Eintrag oder einen benutzerdefinierten Aurora-Endpunkt anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.

Herstellen der Verbindung zu einem DB--Cluster

Das allgemeine Format zur Herstellung einer Verbindung wird nachfolgend dargestellt.

```
mysql --host=hostName --port=portNumber --ssl-ca=full_path_to_ssl_certificate --enable-
cleartext-plugin --user=userName --password=authToken
```

Dabei werden die folgenden Parameter verwendet:

- `--host` – Der Hostname des DB--Clusters, auf den Sie zugreifen möchten.
- `--port` – Die Nummer des Ports, der für die Verbindung mit dem DB--Cluster verwendet wird.
- `--ssl-ca` – Die SSL-Zertifikatsdatei, die den öffentlichen Schlüssel enthält

  Weitere Informationen finden Sie unter Verwenden von TLS mit DB-Clustern von Aurora MySQL.

  Zum Download eines SSL-Zertifikats siehe Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .
- `--enable-cleartext-plugin` – Ein Wert, der angibt, dass `AWSAuthenticationPlugin` für diese Verbindung zu verwenden ist.

Wenn Sie einen MariaDB-Client verwenden, ist die `--enable-cleartext-plugin` Option nicht erforderlich.

- `--user` – Das Datenbankkonto, auf das Sie zugreifen möchten.
- `--password` – Ein signiertes IAM-Authentifizierungstoken.

Das Authentifizierungstoken besteht aus hunderten von Zeichen. Dessen Handhabung in der Befehlszeile kann unhandlich sein. Eine Möglichkeit zur Umgehung dieses Problems besteht darin, das Token in einer Umgebungsvariable zu speichern und dann bei der Verbindungsherstellung diese Variable zu verwenden. Im folgenden Beispiel ist eine Möglichkeit dargestellt, um dieses Problem zu umgehen. Im Beispiel ist *`/sample_dir/`* der vollständige Pfad zur SSL-Zertifikatsdatei, die den öffentlichen Schlüssel enthält.

```
RDSHOST="mysqlcluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
TOKEN="$(aws rds generate-db-auth-token --hostname $RDSHOST --port 3306 --region us-
west-2 --username jane_doe )"

mysql --host=$RDSHOST --port=3306 --ssl-ca=/sample_dir/global-bundle.pem --enable-
cleartext-plugin --user=jane_doe --password=$TOKEN
```

Wenn Sie die Verbindung mithilfe von `AWSAuthenticationPlugin` herstellen, wird die Verbindung mit SSL geschützt. Geben Sie an der `mysql>`-Eingabeaufforderung Folgendes ein, um dies zu überprüfen.

```
show status like 'Ssl%';
```

In den folgenden Linien in der Ausgabe finden Sie weitere Details.

```
+---------------+-------------+
| Variable_name | Value

                                                                    |

+---------------+-------------+
| ...           | ...
| Ssl_cipher    | AES256-SHA

                                                                    |

| ...           | ...
```

```
| Ssl_version   | TLSv1.1

                                                                    |
| ...           | ...
+-----------------------------+
```

Informationen dazu, wie Sie über einen Proxy eine Verbindung mit einem DB-Cluster herstellen, finden Sie unter Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung.

Herstellen einer Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung von der Befehlszeile aus: AWS CLI und psql-Client

Sie können über die Befehlszeile eine Verbindung mit einem Aurora-PostgreSQL-DB-Cluster mit der AWS CLI und dem psql-Befehlszeilen-Tool herstellen, wie nachfolgend beschrieben.

Voraussetzungen

Die folgenden Voraussetzungen gelten für die Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung:

- Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung
- Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff
- Erstellen eines Datenbankkontos mithilfe der IAM-Authentifizierung

> **Note**
>
> Informationen zum Herstellen einer Verbindung mit Ihrer Datenbank mithilfe von pgAdmin mit IAM-Authentifizierung finden Sie im Blogbeitrag Using IAM authentication to connect with pgAdmin Amazon Aurora PostgreSQL or Amazon RDS for PostgreSQL.

Themen

- Generieren eines IAM-Authentifizierungstokens
- Verbinden mit einem und einem Aurora PostgreSQL-Cluster

Generieren eines IAM-Authentifizierungstokens

Das Authentifizierungstoken besteht aus hunderten von Zeichen, wodurch es in der Befehlszeile unhandlich wird. Eine Möglichkeit zur Umgehung dieses Problems besteht darin, das Token in

einer Umgebungsvariable zu speichern und dann bei der Verbindungsherstellung diese Variable zu verwenden. Im folgenden Beispiel wird gezeigt, wie Sie die AWS CLI verwenden, um ein signiertes Authentifizierungstoken mithilfe des `generate-db-auth-token`-Befehls zu erzeugen und dieses anschließend in einer `PGPASSWORD`-Umgebungsvariablen zu speichern.

```
export RDSHOST="mypostgres-cluster.cluster-123456789012.us-west-2.rds.amazonaws.com"
export PGPASSWORD="$(aws rds generate-db-auth-token --hostname $RDSHOST --port 5432 --
region us-west-2 --username jane_doe )"
```

In diesem Beispiel lauten die Parameter für den `generate-db-auth-token`-Befehl folgendermaßen:

- `--hostname`– Der Hostname des DB--Clusters (Cluster-Endpunkt), auf den Sie zugreifen möchten.
- `--port` – Die Nummer des Ports, der für die Verbindung mit dem DB--Cluster verwendet wird.
- `--region` – Die AWS-Region, in der der DB-Cluster ausgeführt wird.
- `--username` – Das Datenbankkonto, auf das Sie zugreifen möchten.

Die ersten Zeichen des generierten Tokens sehen folgendermaßen aus.

```
mypostgres-cluster.cluster-123456789012.us-west-2.rds.amazonaws.com:5432/?
Action=connect&DBUser=jane_doe&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

> **Note**
>
> Sie können keinen benutzerdefinierten Route-53-DNS-Eintrag oder einen benutzerdefinierten Aurora-Endpunkt anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.

Verbinden mit einem und einem Aurora PostgreSQL-Cluster

Das allgemeine Format zur Herstellung einer Verbindung mithilfe von psql wird nachfolgend dargestellt.

```
psql "host=hostName port=portNumber sslmode=verify-full
 sslrootcert=full_path_to_ssl_certificate dbname=DBName user=userName
 password=authToken"
```

Dabei werden die folgenden Parameter verwendet:

- `host`– Der Hostname des DB--Clusters (Cluster-Endpunkt), auf den Sie zugreifen möchten.
- `port` – Die Nummer des Ports, der für die Verbindung mit dem DB--Cluster verwendet wird.
- `sslmode` – Der zu verwendende SSL-Modus.

  Wenn Sie `sslmode=verify-full` verwenden, prüft die SSL-Verbindung den Endpunkt des DB-Clusters gegen den Endpunkt des SSL-Zertifikats.
- `sslrootcert` – Die SSL-Zertifikatsdatei, die den öffentlichen Schlüssel enthält

  Weitere Informationen finden Sie unter Sicherung von Aurora-PostgreSQL-Daten mit SSL/TLS.

  Zum Download eines SSL-Zertifikats siehe Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .
- `dbname` – Die Datenbank, auf die Sie zugreifen möchten.
- `user` – Das Datenbankkonto, auf das Sie zugreifen möchten.
- `password` – Ein signiertes IAM-Authentifizierungstoken.

> **Note**
>
> Sie können keinen benutzerdefinierten Route-53-DNS-Eintrag oder einen benutzerdefinierten Aurora-Endpunkt anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.

Das folgende Beispiel zeigt die Verwendung von psql für die Verbindung. Im Beispiel verwendet psql die Umgebungsvariable `RDSHOST` für den Host und die Umgebungsvariable `PGPASSWORD` für das generierte Token. Zudem ist */sample_dir/* der vollständige Pfad zur SSL-Zertifikatsdatei, die den öffentlichen Schlüssel enthält.

```
export RDSHOST="mypostgres-cluster.cluster-123456789012.us-west-2.rds.amazonaws.com"
export PGPASSWORD="$(aws rds generate-db-auth-token --hostname $RDSHOST --port 5432 --
region us-west-2 --username jane_doe )"
```

```
psql "host=$RDSHOST port=5432 sslmode=verify-full sslrootcert=/sample_dir/global-
bundle.pem dbname=DBName user=jane_doe password=$PGPASSWORD"
```

Informationen dazu, wie Sie über einen Proxy eine Verbindung mit einem DB-Cluster herstellen, finden Sie unter Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung.

Herstellen einer Verbindung zu Ihrem DB--Cluster mithilfe der IAM-Authentifizierung und AWS SDK for .NET

Sie können sich mit dem AWS SDK for .NET wie nachfolgend beschrieben mit einer Aurora-MySQL- oder Aurora-PostgreSQL-DB-Cluster verbinden.

Voraussetzungen

Die folgenden Voraussetzungen gelten für die Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung:

- Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung
- Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff
- Erstellen eines Datenbankkontos mithilfe der IAM-Authentifizierung

Beispiele

In den folgenden Beispielcodes wird gezeigt, wie Sie ein Authentifizierungstoken erzeugen und anschließend zum Verbinden mit einem DB-Cluster verwenden.

Um dieses Codebeispiel auszuführen, benötigen Sie das AWS SDK for .NET, das sich auf der AWS-Seite befindet. Die `AWSSDK.CORE`- und die `AWSSDK.RDS`-Pakete sind erforderlich. Um eine Verbindung mit einer DB-Cluster herzustellen, verwenden Sie den .NET-Datenbankkonnektor für die DB-Engine, z. B. MySqlConnector für MariaDB oder MySQL oder Npgsql für PostgreSQL.

Dieser Code stellt eine Verbindung mit einem Aurora MySQL DB-Cluster her. Ändern Sie die Werte der folgenden Parameter nach Bedarf.

- `server` – Der Endpunkt des DB--Clusters, auf den Sie zugreifen möchten.
- `user` – Das Datenbankkonto, auf das Sie zugreifen möchten.
- `database` – Die Datenbank, auf die Sie zugreifen möchten.

- `port` – Die Nummer des Ports, der für die Verbindung mit dem DB--Cluster verwendet wird.
- `SslMode` – Der zu verwendende SSL-Modus.

  Wenn Sie `SslMode=Required` verwenden, prüft die SSL-Verbindung den Endpunkt des DB-Clusters gegen den Endpunkt des SSL-Zertifikats.
- `SslCa` – Der vollständige Pfad zum SSL-Zertifikat für Amazon Aurora

  Informationen zum Download eines Zertifikats finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

> **Note**
>
> Sie können keinen benutzerdefinierten Route-53-DNS-Eintrag oder einen benutzerdefinierten Aurora-Endpunkt anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.

```
using System;
using System.Data;
using MySql.Data;
using MySql.Data.MySqlClient;
using Amazon;

namespace ubuntu
{
  class Program
  {
    static void Main(string[] args)
    {
      var pwd =
 Amazon.RDS.Util.RDSAuthTokenGenerator.GenerateAuthToken(RegionEndpoint.USEast1,
 "mysqlcluster.cluster-123456789012.us-east-1.rds.amazonaws.com", 3306, "jane_doe");
      // for debug only Console.Write("{0}\n", pwd);  //this verifies the token is
 generated

      MySqlConnection conn = new
 MySqlConnection($"server=mysqlcluster.cluster-123456789012.us-
east-1.rds.amazonaws.com;user=jane_doe;database=mydB;port=3306;password={pwd};SslMode=Required;
      conn.Open();
```

```
      // Define a query
      MySqlCommand sampleCommand = new MySqlCommand("SHOW DATABASES;", conn);

      // Execute a query
      MySqlDataReader mysqlDataRdr = sampleCommand.ExecuteReader();

      // Read all rows and output the first column in each row
      while (mysqlDataRdr.Read())
        Console.WriteLine(mysqlDataRdr[0]);

      mysqlDataRdr.Close();
      // Close connection
      conn.Close();
    }
  }
}
```

Dieser Code stellt eine Verbindung mit einem Aurora PostgreSQL DB-Cluster her.

Ändern Sie die Werte der folgenden Parameter nach Bedarf.

- `Server` – Der Endpunkt des DB--Clusters, auf den Sie zugreifen möchten.
- `User ID` – Das Datenbankkonto, auf das Sie zugreifen möchten.
- `Database` – Die Datenbank, auf die Sie zugreifen möchten.
- `Port` – Die Nummer des Ports, der für die Verbindung mit dem DB--Cluster verwendet wird.
- `SSL Mode` – Der zu verwendende SSL-Modus.

  Wenn Sie `SSL Mode=Required` verwenden, prüft die SSL-Verbindung den Endpunkt des DB-Clusters gegen den Endpunkt des SSL-Zertifikats.
- `Root Certificate` – Der vollständige Pfad zum SSL-Zertifikat für Amazon Aurora

  Informationen zum Download eines Zertifikats finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

> **Note**
>
> Sie können keinen benutzerdefinierten Route-53-DNS-Eintrag oder einen benutzerdefinierten Aurora-Endpunkt anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.

```
using System;
using Npgsql;
using Amazon.RDS.Util;

namespace ConsoleApp1
{
    class Program
    {
        static void Main(string[] args)
        {
            var pwd =
 RDSAuthTokenGenerator.GenerateAuthToken("postgresmycluster.cluster-123456789012.us-
east-1.rds.amazonaws.com", 5432, "jane_doe");
// for debug only Console.Write("{0}\n", pwd);  //this verifies the token is generated

            NpgsqlConnection conn = new
 NpgsqlConnection($"Server=postgresmycluster.cluster-123456789012.us-
east-1.rds.amazonaws.com;User Id=jane_doe;Password={pwd};Database=mydb;SSL
 Mode=Require;Root Certificate=full_path_to_ssl_certificate");
            conn.Open();

            // Define a query
                   NpgsqlCommand cmd = new NpgsqlCommand("select count(*) FROM
 pg_user", conn);

            // Execute a query
            NpgsqlDataReader dr = cmd.ExecuteReader();

            // Read all rows and output the first column in each row
            while (dr.Read())
                Console.Write("{0}\n", dr[0]);

            // Close connection
            conn.Close();
        }
    }
}
```

Informationen dazu, wie Sie über einen Proxy eine Verbindung mit einem DB-Cluster herstellen, finden Sie unter Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung.

Herstellen einer Verbindung zu Ihrem DB--Cluster mithilfe der IAM-Authentifizierung und AWS SDK for Go

Sie können sich mit dem AWS SDK for Go wie nachfolgend beschrieben mit einer Aurora-MySQL- oder Aurora-PostgreSQL-DB-Cluster verbinden.

Voraussetzungen

Die folgenden Voraussetzungen gelten für die Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung:

- Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung
- Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff
- Erstellen eines Datenbankkontos mithilfe der IAM-Authentifizierung

Beispiele

Um diese Codebeispiele auszuführen, benötigen Sie das AWS SDK for Go, das sich auf der AWS-Site befindet.

Ändern Sie die Werte der folgenden Parameter nach Bedarf.

- `dbName` – Die Datenbank, auf die Sie zugreifen möchten.
- `dbUser` – Das Datenbankkonto, auf das Sie zugreifen möchten.
- `dbHost` – Der Endpunkt des DB--Clusters, auf den Sie zugreifen möchten.

> **Note**
>
> Sie können keinen benutzerdefinierten Route-53-DNS-Eintrag oder einen benutzerdefinierten Aurora-Endpunkt anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.

- `dbPort` – Die Nummer des Ports, der für die Verbindung mit dem DB--Cluster verwendet wird.
- `region` – Die AWS-Region, in der der DB-Cluster ausgeführt wird.

Stellen Sie außerdem sicher, dass die importierten Bibliotheken im Beispielcode auf Ihrem System vorhanden sind.

Important

Die Beispiele in diesem Abschnitt verwenden den folgenden Code, um Anmeldeinformationen bereitzustellen, die von einer lokalen Umgebung aus auf eine Datenbank zugreifen:

```
creds := credentials.NewEnvCredentials()
```

Wenn Sie von einem AWS-Service wie Amazon EC2 oder Amazon ECS auf eine Datenbank zugreifen, können Sie den Code durch den folgenden Code ersetzen:

```
sess := session.Must(session.NewSession())
creds := sess.Config.Credentials
```

Wenn Sie diese Änderung vornehmen, stellen Sie sicher, dass Sie den folgenden Import hinzufügen:

```
"github.com/aws/aws-sdk-go/aws/session"
```

Themen

Herstellen einer Verbindung mit IAM-Authentifizierung und AWS SDK for Go V2

Sie können mithilfe der IAM-Authentifizierung und der AWS SDK for Go V2 eine Verbindung zu einem herstellen.

In den folgenden Beispielcodes wird gezeigt, wie Sie ein Authentifizierungstoken erzeugen und anschließend zum Verbinden mit einem DB-Cluster verwenden.

Dieser Code stellt eine Verbindung mit einem Aurora MySQL DB-Cluster her.

```
package main

import (
     "context"
     "database/sql"
     "fmt"

     "github.com/aws/aws-sdk-go-v2/config"
     "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
     _ "github.com/go-sql-driver/mysql"
)
```

```
func main() {

     var dbName string = "DatabaseName"
     var dbUser string = "DatabaseUser"
     var dbHost string = "mysqlcluster.cluster-123456789012.us-
east-1.rds.amazonaws.com"
     var dbPort int = 3306
     var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
     var region string = "us-east-1"

    cfg, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
     panic("configuration error: " + err.Error())
    }

    authenticationToken, err := auth.BuildAuthToken(
     context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
    if err != nil {
     panic("failed to create authentication token: " + err.Error())
    }

    dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
        dbUser, authenticationToken, dbEndpoint, dbName,
    )

    db, err := sql.Open("mysql", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

Dieser Code stellt eine Verbindung mit einem Aurora PostgreSQL DB-Cluster her.

```
package main

import (
     "context"
```

```
     "database/sql"
     "fmt"

     "github.com/aws/aws-sdk-go-v2/config"
     "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
     _ "github.com/lib/pq"
)

func main() {

     var dbName string = "DatabaseName"
     var dbUser string = "DatabaseUser"
     var dbHost string = "postgresmycluster.cluster-123456789012.us-
east-1.rds.amazonaws.com"
     var dbPort int = 5432
     var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
     var region string = "us-east-1"

    cfg, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
     panic("configuration error: " + err.Error())
    }

    authenticationToken, err := auth.BuildAuthToken(
     context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
    if err != nil {
     panic("failed to create authentication token: " + err.Error())
    }

    dsn := fmt.Sprintf("host=%s port=%d user=%s password=%s dbname=%s",
        dbHost, dbPort, dbUser, authenticationToken, dbName,
    )

    db, err := sql.Open("postgres", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

Informationen dazu, wie Sie über einen Proxy eine Verbindung mit einem DB-Cluster herstellen, finden Sie unter Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung.

Herstellen einer Verbindung mit IAM-Authentifizierung und AWS SDK for Go V1.

Sie können mithilfe der IAM-Authentifizierung und der AWS SDK for Go V1 eine Verbindung zu einem herstellen

In den folgenden Beispielcodes wird gezeigt, wie Sie ein Authentifizierungstoken erzeugen und anschließend zum Verbinden mit einem DB-Cluster verwenden.

Dieser Code stellt eine Verbindung mit einem Aurora MySQL DB-Cluster her.

```
package main

import (
    "database/sql"
    "fmt"
    "log"

    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/service/rds/rdsutils"
    _ "github.com/go-sql-driver/mysql"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "mysqlcluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
    dbPort := 3306
    dbEndpoint := fmt.Sprintf("%s:%d", dbHost, dbPort)
    region := "us-east-1"

    creds := credentials.NewEnvCredentials()
    authToken, err := rdsutils.BuildAuthToken(dbEndpoint, region, dbUser, creds)
    if err != nil {
        panic(err)
    }

    dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
        dbUser, authToken, dbEndpoint, dbName,
    )
```

```
    db, err := sql.Open("mysql", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

Dieser Code stellt eine Verbindung mit einem Aurora PostgreSQL DB-Cluster her.

```
package main

import (
 "database/sql"
 "fmt"

 "github.com/aws/aws-sdk-go/aws/credentials"
 "github.com/aws/aws-sdk-go/service/rds/rdsutils"
 _ "github.com/lib/pq"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "postgresmycluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
    dbPort := 5432
    dbEndpoint := fmt.Sprintf("%s:%d", dbHost, dbPort)
    region := "us-east-1"

    creds := credentials.NewEnvCredentials()
    authToken, err := rdsutils.BuildAuthToken(dbEndpoint, region, dbUser, creds)
    if err != nil {
        panic(err)
    }

    dsn := fmt.Sprintf("host=%s port=%d user=%s password=%s dbname=%s",
        dbHost, dbPort, dbUser, authToken, dbName,
    )

    db, err := sql.Open("postgres", dsn)
```

```
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

Informationen dazu, wie Sie über einen Proxy eine Verbindung mit einem DB-Cluster herstellen, finden Sie unter Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung.

Herstellen einer Verbindung zu Ihrem mithilfe der IAM-Authentifizierung und der AWS SDK for Java

Sie können wie im Folgenden beschrieben eine Verbindung zu einer mit Aurora MySQL oder Aurora PostgreSQL DB-Cluster herstellen. AWS SDK for Java

Voraussetzungen

Die folgenden Voraussetzungen gelten für die Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung:

- Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung
- Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff
- Erstellen eines Datenbankkontos mithilfe der IAM-Authentifizierung
- Richten Sie das AWS SDK for Java ein

Beispiele zur Verwendung des SDK for Java 2.x finden Sie unter Amazon RDS-Beispiele mit SDK for Java 2.x.

Themen

- Generieren eines IAM-Authentifizierungstokens
- Manuelles Erzeugen eines IAM-Authentifizierungstokens
- Herstellen der Verbindung zu einem DB--Cluster

Generieren eines IAM-Authentifizierungstokens

Wenn Sie Programme mit dem schreiben AWS SDK for Java, können Sie mithilfe der Klasse ein signiertes Authentifizierungstoken abrufen. `RdsIamAuthTokenGenerator` Für die Verwendung dieser Klasse müssen Sie AWS Anmeldeinformationen angeben. Dazu erstellen Sie eine Instanz der `DefaultAWSCredentialsProviderChain` Klasse. `DefaultAWSCredentialsProviderChain`verwendet den ersten AWS Zugriffsschlüssel und den ersten geheimen Schlüssel, den es in der standardmäßigen Anbieterkette für Anmeldeinformationen findet. Weitere Informationen über AWS -Zugriffsschlüssel finden Sie unter Verwalten von Zugriffsschlüsseln für Benutzer.

> **Note**
>
> Sie können keinen benutzerdefinierten Route-53-DNS-Eintrag oder einen benutzerdefinierten Aurora-Endpunkt anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.

Nachdem Sie eine Instance von `RdsIamAuthTokenGenerator` erstellt haben, können Sie das `getAuthToken`-Verfahren aufrufen, um ein signiertes Token zu erhalten. Geben Sie die AWS -Region, den Hostnamen, die Portnummer und den Benutzernamen an. Der folgende Beispielcode veranschaulicht diese Vorgehensweise.

```
package com.amazonaws.codesamples;

import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.services.rds.auth.GetIamAuthTokenRequest;
import com.amazonaws.services.rds.auth.RdsIamAuthTokenGenerator;

public class GenerateRDSAuthToken {

    public static void main(String[] args) {

     String region = "us-west-2";
     String hostname = "rdsmysql.123456789012.us-west-2.rds.amazonaws.com";
     String port = "3306";
     String username = "jane_doe";

     System.out.println(generateAuthToken(region, hostname, port, username));
    }
```

```
    static String generateAuthToken(String region, String hostName, String port, String
 username) {

     RdsIamAuthTokenGenerator generator = RdsIamAuthTokenGenerator.builder()
      .credentials(new DefaultAWSCredentialsProviderChain())
      .region(region)
      .build();

     String authToken = generator.getAuthToken(
      GetIamAuthTokenRequest.builder()
      .hostname(hostName)
      .port(Integer.parseInt(port))
      .userName(username)
      .build());

     return authToken;
    }

}
```

Manuelles Erzeugen eines IAM-Authentifizierungstokens

Der einfachste Weg in Java, um ein Authentifizierungstoken zu erzeugen, ist die Verwendung von `RdsIamAuthTokenGenerator`. Diese Klasse erstellt ein Authentifizierungstoken für Sie und signiert es dann mit der AWS Signaturversion 4. Weitere Informationen finden Sie unter Signaturprozess mit Signaturversion 4 im Allgemeine AWS-Referenz.

Sie können allerdings das Authentifizierungstoken auch manuell erstellen und signieren, wie im folgenden Beispielcode dargestellt.

```
package com.amazonaws.codesamples;

import com.amazonaws.SdkClientException;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.auth.SigningAlgorithm;
import com.amazonaws.util.BinaryUtils;
import org.apache.commons.lang3.StringUtils;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.nio.charset.Charset;
import java.security.MessageDigest;
import java.text.SimpleDateFormat;
```

```
import java.util.Date;
import java.util.SortedMap;
import java.util.TreeMap;

import static com.amazonaws.auth.internal.SignerConstants.AWS4_TERMINATOR;
import static com.amazonaws.util.StringUtils.UTF8;

public class CreateRDSAuthTokenManually {
    public static String httpMethod = "GET";
    public static String action = "connect";
    public static String canonicalURIParameter = "/";
    public static SortedMap<String, String> canonicalQueryParameters = new TreeMap();
    public static String payload = StringUtils.EMPTY;
    public static String signedHeader = "host";
    public static String algorithm = "AWS4-HMAC-SHA256";
    public static String serviceName = "rds-db";
    public static String requestWithoutSignature;

    public static void main(String[] args) throws Exception {

        String region = "us-west-2";
        String instanceName = "rdsmysql.123456789012.us-west-2.rds.amazonaws.com";
        String port = "3306";
        String username = "jane_doe";

        Date now = new Date();
        String date = new SimpleDateFormat("yyyyMMdd").format(now);
        String dateTimeStamp = new
 SimpleDateFormat("yyyyMMdd'T'HHmmss'Z'").format(now);
       DefaultAWSCredentialsProviderChain creds = new
 DefaultAWSCredentialsProviderChain();
    String awsAccessKey = creds.getCredentials().getAWSAccessKeyId();
    String awsSecretKey = creds.getCredentials().getAWSSecretKey();
       String expiryMinutes = "900";

       System.out.println("Step 1:  Create a canonical request:");
       String canonicalString = createCanonicalString(username, awsAccessKey, date,
 dateTimeStamp, region, expiryMinutes, instanceName, port);
       System.out.println(canonicalString);
       System.out.println();

       System.out.println("Step 2:  Create a string to sign:");
       String stringToSign = createStringToSign(dateTimeStamp, canonicalString,
 awsAccessKey, date, region);
```

```
        System.out.println(stringToSign);
        System.out.println();

        System.out.println("Step 3:  Calculate the signature:");
        String signature = BinaryUtils.toHex(calculateSignature(stringToSign,
newSigningKey(awsSecretKey, date, region, serviceName)));
        System.out.println(signature);
        System.out.println();

        System.out.println("Step 4:  Add the signing info to the request");

        System.out.println(appendSignature(signature));
        System.out.println();

    }

    //Step 1: Create a canonical request date should be in format YYYYMMDD and dateTime
should be in format YYYYMMDDTHHMMSSZ
    public static String createCanonicalString(String user, String accessKey, String
date, String dateTime, String region, String expiryPeriod, String hostName, String
port) throws Exception {
        canonicalQueryParameters.put("Action", action);
        canonicalQueryParameters.put("DBUser", user);
        canonicalQueryParameters.put("X-Amz-Algorithm", "AWS4-HMAC-SHA256");
        canonicalQueryParameters.put("X-Amz-Credential", accessKey + "%2F" + date +
"%2F" + region + "%2F" + serviceName + "%2Faws4_request");
        canonicalQueryParameters.put("X-Amz-Date", dateTime);
        canonicalQueryParameters.put("X-Amz-Expires", expiryPeriod);
        canonicalQueryParameters.put("X-Amz-SignedHeaders", signedHeader);
        String canonicalQueryString = "";
        while(!canonicalQueryParameters.isEmpty()) {
            String currentQueryParameter = canonicalQueryParameters.firstKey();
            String currentQueryParameterValue =
canonicalQueryParameters.remove(currentQueryParameter);
            canonicalQueryString = canonicalQueryString + currentQueryParameter + "=" +
currentQueryParameterValue;
            if (!currentQueryParameter.equals("X-Amz-SignedHeaders")) {
                canonicalQueryString += "&";
            }
        }
        String canonicalHeaders = "host:" + hostName + ":" + port + '\n';
        requestWithoutSignature = hostName + ":" + port + "/?" + canonicalQueryString;

        String hashedPayload = BinaryUtils.toHex(hash(payload));
```

```
        return httpMethod + '\n' + canonicalURIParameter + '\n' + canonicalQueryString
 + '\n' + canonicalHeaders + '\n' + signedHeader + '\n' + hashedPayload;

    }

    //Step 2: Create a string to sign using sig v4
    public static String createStringToSign(String dateTime, String canonicalRequest,
 String accessKey, String date, String region) throws Exception {
        String credentialScope = date + "/" + region + "/" + serviceName + "/
aws4_request";
        return algorithm + '\n' + dateTime + '\n' + credentialScope + '\n' +
 BinaryUtils.toHex(hash(canonicalRequest));

    }

    //Step 3: Calculate signature
    /**
     * Step 3 of the &AWS; Signature version 4 calculation. It involves deriving
     * the signing key and computing the signature. Refer to
     * http://docs.aws.amazon
     * .com/general/latest/gr/sigv4-calculate-signature.html
     */
    public static byte[] calculateSignature(String stringToSign,
                                            byte[] signingKey) {
        return sign(stringToSign.getBytes(Charset.forName("UTF-8")), signingKey,
                SigningAlgorithm.HmacSHA256);
    }

    public static byte[] sign(byte[] data, byte[] key,
                          SigningAlgorithm algorithm) throws SdkClientException {
        try {
            Mac mac = algorithm.getMac();
            mac.init(new SecretKeySpec(key, algorithm.toString()));
            return mac.doFinal(data);
        } catch (Exception e) {
            throw new SdkClientException(
                    "Unable to calculate a request signature: "
                            + e.getMessage(), e);
        }
    }

    public static byte[] newSigningKey(String secretKey,
                                   String dateStamp, String regionName, String
 serviceName) {
```

```
        byte[] kSecret = ("AWS4" + secretKey).getBytes(Charset.forName("UTF-8"));
        byte[] kDate = sign(dateStamp, kSecret, SigningAlgorithm.HmacSHA256);
        byte[] kRegion = sign(regionName, kDate, SigningAlgorithm.HmacSHA256);
        byte[] kService = sign(serviceName, kRegion,
                SigningAlgorithm.HmacSHA256);
        return sign(AWS4_TERMINATOR, kService, SigningAlgorithm.HmacSHA256);
    }

    public static byte[] sign(String stringData, byte[] key,
                      SigningAlgorithm algorithm) throws SdkClientException {
        try {
            byte[] data = stringData.getBytes(UTF8);
            return sign(data, key, algorithm);
        } catch (Exception e) {
            throw new SdkClientException(
                    "Unable to calculate a request signature: "
                            + e.getMessage(), e);
        }
    }

    //Step 4: append the signature
    public static String appendSignature(String signature) {
        return requestWithoutSignature + "&X-Amz-Signature=" + signature;
    }

    public static byte[] hash(String s) throws Exception {
        try {
            MessageDigest md = MessageDigest.getInstance("SHA-256");
            md.update(s.getBytes(UTF8));
            return md.digest();
        } catch (Exception e) {
            throw new SdkClientException(
                    "Unable to compute hash while signing request: "
                            + e.getMessage(), e);
        }
    }
}
```

Herstellen der Verbindung zu einem DB--Cluster

Im folgenden Codebeispiel wird gezeigt, wie Sie ein Authentifizierungstoken erzeugen und anschließend zum Verbinden mit einem Cluster für die Ausführung mit Aurora MySQL verwenden können.

Um dieses Codebeispiel auszuführen, benötigen Sie den AWS SDK for Java, der auf der AWS Site zu finden ist. Außerdem benötigen Sie Folgendes:

- MySQL Connector/J. Dieses Codebeispiel wurde mit `mysql-connector-java-5.1.33-bin.jar` getestet.
- Ein Zwischenzertifikat für Amazon Aurora, das für eine AWS Region spezifisch ist. (Weitere Informationen finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .) Während der Laufzeit sucht der Class Loader das Zertifikat in demselben Verzeichnis, in dem sich dieser Java-Beispielcode befindet, damit er es finden kann.
- Ändern Sie die Werte der folgenden Parameter nach Bedarf.
  - `RDS_INSTANCE_HOSTNAME` – Der Hostname des DB--Clusters, auf den Sie zugreifen möchten.
  - `RDS_INSTANCE_PORT` – Die Nummer des Ports, der für die Verbindung zum PostgreSQL-DB-Cluster verwendet wird.
  - `REGION_NAME`— Die AWS Region, in der der ausgeführt wird.
  - `DB_USER` – Das Datenbankkonto, auf das Sie zugreifen möchten.
  - `SSL_CERTIFICATE`— Ein SSL-Zertifikat für Amazon Aurora, das für eine AWS Region spezifisch ist.

    Informationen zum Herunterladen eines Zertifikats für Ihre AWS -Region finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer . Speichern Sie das SSL-Zertifikat in demselben Verzeichnis wie diese Java-Programmdatei ab, damit der Class Loader das Zertifikat während der Laufzeit finden kann.

In diesem Codebeispiel werden AWS Anmeldeinformationen aus der standardmäßigen Anbieterkette für Anmeldeinformationen abgerufen.

> **Note**
>
> Geben Sie aus Sicherheitsgründen für `DEFAULT_KEY_STORE_PASSWORD` ein anderes Passwort als hier angegeben an.

```
package com.amazonaws.samples;

import com.amazonaws.services.rds.auth.RdsIamAuthTokenGenerator;
import com.amazonaws.services.rds.auth.GetIamAuthTokenRequest;
```

```
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.auth.AWSStaticCredentialsProvider;

import java.io.File;
import java.io.FileOutputStream;
import java.io.InputStream;
import java.security.KeyStore;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.Statement;
import java.util.Properties;

import java.net.URL;

public class IAMDatabaseAuthenticationTester {
    //&AWS; Credentials of the IAM user with policy enabling IAM Database Authenticated
 access to the db by the db user.
    private static final DefaultAWSCredentialsProviderChain creds = new
 DefaultAWSCredentialsProviderChain();
    private static final String AWS_ACCESS_KEY =
 creds.getCredentials().getAWSAccessKeyId();
    private static final String AWS_SECRET_KEY =
 creds.getCredentials().getAWSSecretKey();

    //Configuration parameters for the generation of the IAM Database Authentication
 token
    private static final String RDS_INSTANCE_HOSTNAME = "rdsmysql.123456789012.us-
west-2.rds.amazonaws.com";
    private static final int RDS_INSTANCE_PORT = 3306;
    private static final String REGION_NAME = "us-west-2";
    private static final String DB_USER = "jane_doe";
    private static final String JDBC_URL = "jdbc:mysql://" + RDS_INSTANCE_HOSTNAME +
 ":" + RDS_INSTANCE_PORT;

    private static final String SSL_CERTIFICATE = "rds-ca-2019-us-west-2.pem";

    private static final String KEY_STORE_TYPE = "JKS";
    private static final String KEY_STORE_PROVIDER = "SUN";
```

```
    private static final String KEY_STORE_FILE_PREFIX = "sys-connect-via-ssl-test-
cacerts";
    private static final String KEY_STORE_FILE_SUFFIX = ".jks";
    private static final String DEFAULT_KEY_STORE_PASSWORD = "changeit";

    public static void main(String[] args) throws Exception {
        //get the connection
        Connection connection = getDBConnectionUsingIam();

        //verify the connection is successful
        Statement stmt= connection.createStatement();
        ResultSet rs=stmt.executeQuery("SELECT 'Success!' FROM DUAL;");
        while (rs.next()) {
             String id = rs.getString(1);
            System.out.println(id); //Should print "Success!"
        }

        //close the connection
        stmt.close();
        connection.close();

        clearSslProperties();

    }

    /**
     * This method returns a connection to the db instance authenticated using IAM
 Database Authentication
     * @return
     * @throws Exception
     */
    private static Connection getDBConnectionUsingIam() throws Exception {
        setSslProperties();
        return DriverManager.getConnection(JDBC_URL, setMySqlConnectionProperties());
    }

    /**
     * This method sets the mysql connection properties which includes the IAM Database
 Authentication token
     * as the password. It also specifies that SSL verification is required.
     * @return
     */
    private static Properties setMySqlConnectionProperties() {
        Properties mysqlConnectionProperties = new Properties();
```

```
        mysqlConnectionProperties.setProperty("verifyServerCertificate","true");
        mysqlConnectionProperties.setProperty("useSSL", "true");
        mysqlConnectionProperties.setProperty("user",DB_USER);
        mysqlConnectionProperties.setProperty("password",generateAuthToken());
        return mysqlConnectionProperties;
    }

    /**
     * This method generates the IAM Auth Token.
     * An example IAM Auth Token would look like follows:
     * btusi123.cmz7kenwo2ye.rds.cn-north-1.amazonaws.com.cn:3306/?
Action=connect&DBUser=iamtestuser&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20171003T010726Z&X-Amz-SignedHeaders=host&X-Amz-Expires=899&X-Amz-
Credential=AKIAPFXHGVDI5RNFO4AQ%2F20171003%2Fcn-north-1%2Frds-db%2Faws4_request&X-Amz-
Signature=f9f45ef96c1f770cdad11a53e33ffa4c3730bc03fdee820cfdf1322eed15483b
     * @return
     */
    private static String generateAuthToken() {
        BasicAWSCredentials awsCredentials = new BasicAWSCredentials(AWS_ACCESS_KEY,
 AWS_SECRET_KEY);

        RdsIamAuthTokenGenerator generator = RdsIamAuthTokenGenerator.builder()
                .credentials(new
 AWSStaticCredentialsProvider(awsCredentials)).region(REGION_NAME).build();
        return generator.getAuthToken(GetIamAuthTokenRequest.builder()

 .hostname(RDS_INSTANCE_HOSTNAME).port(RDS_INSTANCE_PORT).userName(DB_USER).build());
    }

    /**
     * This method sets the SSL properties which specify the key store file, its type
 and password:
     * @throws Exception
     */
    private static void setSslProperties() throws Exception {
        System.setProperty("javax.net.ssl.trustStore", createKeyStoreFile());
        System.setProperty("javax.net.ssl.trustStoreType", KEY_STORE_TYPE);
        System.setProperty("javax.net.ssl.trustStorePassword",
 DEFAULT_KEY_STORE_PASSWORD);
    }

    /**
     * This method returns the path of the Key Store File needed for the SSL
 verification during the IAM Database Authentication to
```

```
     * the db instance.
     * @return
     * @throws Exception
     */
    private static String createKeyStoreFile() throws Exception {
        return createKeyStoreFile(createCertificate()).getPath();
    }

    /**
     *  This method generates the SSL certificate
     * @return
     * @throws Exception
     */
    private static X509Certificate createCertificate() throws Exception {
        CertificateFactory certFactory = CertificateFactory.getInstance("X.509");
        URL url = new File(SSL_CERTIFICATE).toURI().toURL();
        if (url == null) {
            throw new Exception();
        }
        try (InputStream certInputStream = url.openStream()) {
            return (X509Certificate) certFactory.generateCertificate(certInputStream);
        }
    }

    /**
     * This method creates the Key Store File
     * @param rootX509Certificate - the SSL certificate to be stored in the KeyStore
     * @return
     * @throws Exception
     */
    private static File createKeyStoreFile(X509Certificate rootX509Certificate) throws
Exception {
        File keyStoreFile = File.createTempFile(KEY_STORE_FILE_PREFIX,
KEY_STORE_FILE_SUFFIX);
        try (FileOutputStream fos = new FileOutputStream(keyStoreFile.getPath())) {
            KeyStore ks = KeyStore.getInstance(KEY_STORE_TYPE, KEY_STORE_PROVIDER);
            ks.load(null);
            ks.setCertificateEntry("rootCaCertificate", rootX509Certificate);
            ks.store(fos, DEFAULT_KEY_STORE_PASSWORD.toCharArray());
        }
        return keyStoreFile;
    }

    /**
```

```
     * This method clears the SSL properties.
     * @throws Exception
     */
    private static void clearSslProperties() throws Exception {
           System.clearProperty("javax.net.ssl.trustStore");
           System.clearProperty("javax.net.ssl.trustStoreType");
           System.clearProperty("javax.net.ssl.trustStorePassword");
    }

}
```

Informationen dazu, wie Sie über einen Proxy eine Verbindung mit einem DB-Cluster herstellen, finden Sie unter Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung.

Herstellen einer Verbindung zu Ihrem DB--Cluster mithilfe der IAM-Authentifizierung und AWS SDK for Python (Boto3)

Sie können sich mit dem AWS SDK for Python (Boto3) wie nachfolgend beschrieben mit einer Aurora-MySQL- oder Aurora-PostgreSQL-DB-Cluster verbinden.

Voraussetzungen

Die folgenden Voraussetzungen gelten für die Verbindung mit Ihrem DB--Cluster mithilfe der IAM-Authentifizierung:

- Aktivieren und Deaktivieren der IAM-Datenbank-Authentifizierung
- Erstellen und Verwenden einer IAM-Richtlinie für den IAM-Datenbankzugriff
- Erstellen eines Datenbankkontos mithilfe der IAM-Authentifizierung

Stellen Sie außerdem sicher, dass die importierten Bibliotheken im Beispielcode auf Ihrem System vorhanden sind.

Beispiele

Die Codebeispiele verwenden Profile für freigegebene Anmeldeinformationen. Informationen zum Angeben von Anmeldeinformationen finden Sie unter Anmeldeinformationen in der AWS SDK for Python (Boto3)-Dokumentation.

In den folgenden Beispielcodes wird gezeigt, wie Sie ein Authentifizierungstoken erzeugen und anschließend zum Verbinden mit einem DB-Cluster verwenden.

Um dieses Codebeispiel auszuführen, benötigen Sie das AWS SDK for Python (Boto3), das sich auf der AWS-Seite befindet.

Ändern Sie die Werte der folgenden Parameter nach Bedarf.

- `ENDPOINT` – Der Endpunkt des DB--Clusters, auf den Sie zugreifen möchten.
- `PORT` – Die Nummer des Ports, der für die Verbindung mit dem DB--Cluster verwendet wird.
- `USER` – Das Datenbankkonto, auf das Sie zugreifen möchten.
- `REGION` – Die AWS-Region, in der der DB-Cluster ausgeführt wird.
- `DBNAME` – Die Datenbank, auf die Sie zugreifen möchten.
- `SSLCERTIFICATE` – Der vollständige Pfad zum SSL-Zertifikat für Amazon Aurora

  Geben Sie für `ssl_ca` ein SSL-Zertifikat an. Zum Download eines SSL-Zertifikats siehe Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einer .

> **Note**
>
> Sie können keinen benutzerdefinierten Route-53-DNS-Eintrag oder einen benutzerdefinierten Aurora-Endpunkt anstelle des DB-Cluster-Endpunkts verwenden, um das Authentifizierungstoken zu generieren.

Dieser Code stellt eine Verbindung mit einem Aurora MySQL DB-Cluster her.

Bevor Sie diesen Code ausführen, installieren Sie den PyMySQL-Treiber, indem Sie die Anweisungen im Python-Paketindex befolgen.

```
import pymysql
import sys
import boto3
import os

ENDPOINT="mysqlcluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
PORT="3306"
USER="jane_doe"
REGION="us-east-1"
DBNAME="mydb"
os.environ['LIBMYSQL_ENABLE_CLEARTEXT_PLUGIN'] = '1'
```

```
#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='default')
client = session.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USER,
 Region=REGION)

try:
    conn =  pymysql.connect(host=ENDPOINT, user=USER, passwd=token, port=PORT,
 database=DBNAME, ssl_ca='SSLCERTIFICATE')
    cur = conn.cursor()
    cur.execute("""SELECT now()""")
    query_results = cur.fetchall()
    print(query_results)
except Exception as e:
    print("Database connection failed due to {}".format(e))
```

Dieser Code stellt eine Verbindung mit einem Aurora PostgreSQL DB-Cluster her.

Bevor Sie diesen Code ausführen, installieren Sie `psycopg2`, indem Sie die Anweisungen in der Psycopg-Dokumentation befolgen.

```
import psycopg2
import sys
import boto3
import os

ENDPOINT="postgresmycluster.cluster-123456789012.us-east-1.rds.amazonaws.com"
PORT="5432"
USER="jane_doe"
REGION="us-east-1"
DBNAME="mydb"

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
client = session.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USER,
 Region=REGION)

try:
```

```
    conn = psycopg2.connect(host=ENDPOINT, port=PORT, database=DBNAME, user=USER,
 password=token, sslrootcert="SSLCERTIFICATE")
    cur = conn.cursor()
    cur.execute("""SELECT now()""")
    query_results = cur.fetchall()
    print(query_results)
except Exception as e:
    print("Database connection failed due to {}".format(e))
```

Informationen dazu, wie Sie über einen Proxy eine Verbindung mit einem DB-Cluster herstellen, finden Sie unter Herstellen einer Verbindung mit einem Proxy mithilfe der IAM-Authentifizierung.

Fehlerbehebung für Amazon Aurora-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit Aurora und IAM auftreten könnten.

Themen

- Ich bin nicht autorisiert, eine Aktion in Aurora auszuführen
- Ich bin nicht zum Durchführen von iam:PassRole berechtigt
- Ich möchte Personen außerhalb meines AWS-Kontos Zugriff auf meine Aurora-Ressourcen erteilen

Ich bin nicht autorisiert, eine Aktion in Aurora auszuführen

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der Benutzer `mateojackson` versucht, die Konsole zum Anzeigen von Details zu einem *`Widget`* zu verwenden, jedoch nicht über `rds:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 rds:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `rds:`*`GetWidget`* zugreifen zu können.

Ich bin nicht zum Durchführen von iam:PassRole berechtigt

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der Aktion `iam:PassRole` autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt. Bitten Sie diese Person um die Aktualisierung Ihrer Richtlinien, um eine Rolle an Aurora übergeben zu können.

Einige AWS-Services gewähren Ihnen die Berechtigung zur Übergabe einer vorhandenen Rolle an diesen Service, statt eine neue Service-Rolle oder serviceverknüpfte Rolle erstellen zu müssen. Hierfür benötigen Sie Berechtigungen zur Übergabe der Rolle an den Service.

Der folgende Beispielfehler tritt auf, wenn ein Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Aurora auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Service-Rolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall bittet Mary ihren Administrator um die Aktualisierung ihrer Richtlinien, um die Aktion `iam:PassRole` ausführen zu können.

Ich möchte Personen außerhalb meines AWS-Kontos Zugriff auf meine Aurora-Ressourcen erteilen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen finden Sie hier:

- Informationen dazu, ob Aurora diese Funktionen unterstützt, finden Sie unter Funktionsweise von Amazon Aurora mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konten im IAM-Benutzerhandbuch.

- Informationen dazu, wie Sie AWS-Drittkonten Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Protokollieren und Überwachen in Amazon Aurora

Die Überwachung ist ein wichtiger Teil der Aufrechterhaltung von Zuverlässigkeit, Verfügbarkeit und Performance von Amazon Aurora und Ihren AWS-Lösungen. Sammeln Sie Überwachungsdaten aller Bestandteile Ihrer AWS-Lösung, damit Sie Ausfälle an mehreren Punkten leichter debuggen können. AWS bietet mehrere Tools für die Überwachung Ihrer Amazon-Aurora-Ressourcen und die Reaktion auf mögliche Vorfälle:

Amazon- CloudWatch Alarme

Mithilfe von Amazon- CloudWatch Alarmen überwachen Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum. Wenn die Metrik einen bestimmten Schwellenwert überschreitet, wird eine Benachrichtigung an ein Amazon SNS-Thema oder eine AWS Auto Scaling Richtlinie gesendet. CloudWatch Alarme rufen keine Aktionen auf, da sie sich in einem bestimmten Status befinden. Der Status muss sich stattdessen geändert haben und für eine festgelegte Anzahl an Zeiträumen aufrechterhalten worden sein.

AWS CloudTrail-Protokolle

CloudTrail bietet eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem -AWSService in Amazon Aurora durchgeführten Aktionen. CloudTrail erfasst alle API-Aufrufe für Amazon Aurora als Ereignisse, einschließlich Aufrufen von der Konsole und von Code-Aufrufen an Amazon-RDS-API-Operationen. Anhand der von CloudTrailgesammelten Informationen können Sie die an Amazon Aurora gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora-API-Aufrufen in AWS CloudTrail.

Enhanced Monitoring (Erweiterte Überwachung)

Amazon Aurora stellt in Echtzeit Metriken für das Betriebssystem (BS) bereit, auf dem Ihr DB-Cluster ausgeführt wird. Sie können die Metriken für Ihre DB DB-Cluster über die Konsole anzeigen oder die Enhanced Monitoring JSON-Ausgabe von Amazon CloudWatch Logs in einem Überwachungssystem Ihrer Wahl verwenden. Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Enhanced Monitoring“·(Erweiterte·Überwachung).

Amazon RDS Performance Insights

Performance Insights lässt sich auf vorhandene Amazon Aurora-Überwachungsfunktionen erweitern, damit Sie die Performance Ihrer Datenbank darstellen und mögliche Probleme analysieren können. Mit dem Performance Insights-Dashboard können Sie die Datenbankauslastung visualisieren und die Auslastung nach Wartezeiten, SQL-Anweisungen, Hosts oder Benutzern filtern. Weitere Informationen finden Sie unter Überwachung mit Performance Insights auf .

Datenbankprotokolle

Sie können Datenbankprotokolle mithilfe der AWS Management Console, AWS CLI oder RDS-API anzeigen, herunterladen und ansehen. Weitere Informationen finden Sie unter Überwachen von Amazon Aurora-Protokolldateien.

Amazon Aurora-Empfehlungen

Amazon Aurora bietet automatisierte Empfehlungen für Datenbankressourcen. Diese Empfehlungen bieten Anleitungen nach bewährten Methoden, indem sie die Konfigurations-, Nutzungs- und Performance-Daten des DB-Clusters analysieren. Weitere Informationen finden Sie unter Anzeigen und Beantworten von Amazon-Aurora-Empfehlungen.

Amazon Aurora-Ereignisbenachrichtigung

Amazon Aurora verwendet Amazon Simple Notification Service (Amazon SNS), um Benachrichtigungen zu senden, wenn ein Amazon Aurora-Ereignis stattfindet. Diese Benachrichtigungen können jedes von Amazon SNS für eine AWS-Region unterstützte Format aufweisen, wie zum Beispiel eine E-Mail, eine SMS oder ein Anruf an einen HTTP-Endpunkt. Weitere Informationen finden Sie unter Arbeiten mit Amazon-RDS-Ereignisbenachrichtigungen.

AWS Trusted Advisor

Trusted Advisor stützt sich auf bewährte Methoden, die sich während der gesamten Betriebsgeschichte der Betreuung vieler Hunderttausend AWS-Kunden ergeben haben. Trusted Advisor überprüft Ihre AWS-Umgebung und gibt dann Empfehlungen, sobald sich Möglichkeiten

ergeben, Kosten zu senken, die Systemleistung zu verbessern oder Schwachstellen zu schließen. Alle AWS-Kunden haben Zugriff auf fünf Trusted Advisor-Prüfungen. Kunden mit dem „Business“- oder „Enterprise“-Support-Plan können alle Trusted Advisor-Prüfungen anzeigen.

Trusted Advisor bietet die folgenden Amazon-Aurora-bezogenen Prüfungen:

- Amazon Aurora-DB-Instances im Leerlauf
- Zugriffsrisiko für Amazon Aurora-Sicherheitsgruppen
- Amazon Aurora-Backups
- Amazon Aurora-Multi-AZ
- Barrierefreiheit von Aurora-DB-Instances

Weitere Informationen zu diesen Prüfungen finden Sie unter Trusted Advisor – bewährte Methoden (Prüfungen).

Datenbankaktivitäts-Streams

Datenbankaktivitäts-Streams schützen Ihre Datenbanken vor internen Bedrohungen durch Kontrolle des DBA-Zugriffs auf die Datenbankaktivitäts-Streams. Die DBAs, die die Datenbank verwalten, haben folglich keine Zugriffsrechte für die Erfassung, Übertragung, Speicherung und nachfolgende Verarbeitung des Datenbankaktivitäts-Streams. Datenbankaktivitäts-Streams können Sicherheitsmaßnahmen für Ihre Datenbank bereitstellen und die Compliance-Anforderungen und behördlichen Vorgaben erfüllen. Weitere Informationen finden Sie unter Überwachung von Amazon Aurora mithilfe von Datenbankaktivitätsstreams.

Weitere Informationen zur Überwachung von Aurora finden Sie unter Überwachung von Metriken in einem Amazon-Aurora-Cluster.

Compliance-Validierung für Amazon Aurora

Externe Auditoren bewerten im Rahmen verschiedener AWS-Compliance-Programme die Sicherheit und Compliance von Amazon Aurora. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS-Services, die in den Geltungsbereich bestimmter Compliance-Programme fallen, finden Sie auf der Seite AWS-Services in Scope nach Compliance-Programm. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Die Auditberichte von Drittanbietern lassen sich mit herunterlade AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS Artifact.

Ihre Compliance-Verantwortung bei der Verwendung von Amazon Aurora wird durch die Sensibilität Ihrer Daten, die Compliance-Ziele Ihrer Organisation und die geltenden Gesetze und Vorschriften bestimmt. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden finden Sie wichtige Überlegungen zur Architektur sowie die einzelnen Schritte zur Bereitstellung von sicherheits- und Compliance-orientierten Basisumgebungen in AWS.
- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen können.
- AWS-Compliance-Ressourcen – Diese Sammlung von Arbeitsmappen und Leitfäden könnte für Ihre Branche und Ihren Standort interessant sein.
- AWS Config – Dieser AWS-Service bewertet, zu welchem Grad die Konfiguration Ihrer Ressourcen den internen Vorgehensweisen, Branchenrichtlinien und Vorschriften entspricht.
- AWS Security Hub – Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS-Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.

Ausfallsicherheit in Amazon Aurora

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und Availability Zones (Verfügbarkeitszonen, AZs). AWS Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die mit Netzwerken mit geringer Latenz, hohem Durchsatz und hochredundanten Vernetzungen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und -Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Neben der globalen AWS-Infrastruktur stellt Aurora Funktionen bereit, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden.

Backup und Backup

Aurora sichert Ihr Cluster-Volume automatisch und bewahrt die Wiederherstellungsdaten für die Länge des Aufbewahrungszeitraums für Backups auf. Aurora-Backups sind kontinuierlich und inkrementell, sodass Sie schnell eine Backup auf einen beliebigen Punkt im Aufbewahrungszeitraum für Backups durchführen können. Es gibt keine Auswirkungen auf die Leistungsfähigkeit oder Unterbrechung von Datenbank-Services, während Backup-Daten geschrieben werden. Sie können einen Aufbewahrungszeitraum für Backups von 1 bis 35 Tagen festlegen, wenn Sie Ihr DB-Cluster erstellen oder ändern.

Wenn Sie ein Backup nach dem eingestellten Aufbewahrungszeitraum behalten möchten, können Sie auch einen Snapshot der Daten Ihres Cluster-Volumes machen. Aurora bewahrt für den gesamten Aufbewahrungszeitraum für Backups inkrementelle Wiederherstellungsdaten auf. Daher müssen Sie einen Snapshot nur für Daten erstellen, die Sie über die Aufbewahrungsfrist hinaus aufbewahren möchten. Sie können ein neues DB-Cluster aus dem Snapshot erstellen.

Sie können Ihre Daten wiederherstellen, indem Sie ein neues Aurora-DB-Cluster aus den von Aurora aufbewahrten Sicherungsdaten oder aus einem von Ihnen gespeicherten DB-Cluster-Snapshot erstellen. Sie können aus den Sicherungsdaten zu einem beliebigen Zeitpunkt während Ihrer Aufbewahrungsfrist schnell eine neue Kopie eines DB-Clusters erstellen. Das Prinzip der fortlaufenden und ansteigenden Aurora-Backups während des Aufbewahrungszeitraums für

Backups bedeutet, dass Sie keine häufigen Snapshots Ihrer Daten machen müssen, um die Wiederherstellungszeiten zu optimieren.

Weitere Informationen finden Sie unter Sichern und Wiederherstellen eines Amazon-Aurora-DB-Clusters.

Replikation

Aurora-Replicas sind unabhängige Endpunkte in einem Aurora-DB-Cluster, die die beste Methode für das Skalieren von Leseoperationen und Erhöhen der Verfügbarkeit darstellen. Es können bis zu 15 Aurora-Replikate über die Availability Zones verteilt werden, über die sich ein DB-Cluster innerhalb einer AWS-Region erstreckt. Das DB-Cluster-Volume besteht aus mehreren Kopien der Daten für den DB-Cluster. Die Daten im Cluster-Volume werden jedoch als ein einzelnes logisches Volume der primären DB-Instance und der Aurora Replicas im DB-Cluster dargestellt. Wenn die primäre DB-Instance ausfällt, wird ein Aurora-Replica zur primären DB-Instance hochgestuft.

Aurora unterstützt außerdem für Aurora MySQL und Aurora PostgreSQL spezifische Replikationsoptionen.

Weitere Informationen finden Sie unter Replikation mit Amazon Aurora.

Failover

Aurora speichert Kopien der Daten in einem DB-Cluster über mehrere Availability Zones in einer einzigen AWS-Region. Dieser Speichervorgang erfolgt unabhängig davon, ob die DB-Instances im DB-Cluster mehrere Availability Zones umfassen. Wenn Sie Aurora Replicas über mehrere Availability Zones hinweg erstellen, stellt Aurora diese automatisch bereit und verwaltet sie synchron. Die primäre DB-Instance wird synchron über mehrere Availability Zones zu einer Aurora Replica repliziert, um für Datenredundanz zu sorgen, das Einfrieren von I/O-Vorgängen zu vermeiden und Latenzspitzen im Verlauf von Systemsicherungen zu minimieren. Wenn Sie einen DB-Cluster mit hoher Verfügbarkeit ausführen, kann dies die Verfügbarkeit bei geplanten Systemwartungen verbessern. Außerdem kann dies Ihre Datenbanken bei Ausfällen und bei Nichtverfügbarkeit von Availability Zones schützen.

Weitere Informationen finden Sie unter Hohe Verfügbarkeit für Amazon Aurora.

Sicherheit der Infrastruktur in Amazon Aurora

Als verwalteter Service ist Amazon Relational Database Service durch die globale Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon RDS zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Darüber hinaus bietet Aurora Funktionen zur Unterstützung der Infrastruktursicherheit.

Sicherheitsgruppen

Sicherheitsgruppen kontrollieren die Zugriffsaktivitäten von eingehendem und ausgehendem Datenverkehr in einem DB-Cluster. Standardmäßig ist der Netzwerkzugriff auf einen DB-Cluster deaktiviert. Sie können Regeln in einer Sicherheitsgruppe angeben, die den Zugriff aus einem IP-Adressbereich, über einen Port oder für eine Sicherheitsgruppe zulassen. Nach der Konfiguration von ingress-Regeln gelten diese für alle DB-Cluster, die dieser Sicherheitsgruppe zugeordnet sind.

Weitere Informationen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen.

Public accessibility (Öffentliche Zugänglichkeit)

Wenn Sie eine DB-Instance innerhalb einer Virtual Private Cloud (VPC) basierend auf dem Amazon VPC-Service starten, können Sie die öffentliche Zugriffsmöglichkeit für diese DB-Instance ein- oder ausschalten. Um festzulegen, ob die von Ihnen erstellte DB-Instance einen DNS-Namen hat, der

in eine öffentliche IP-Adresse aufgelöst wird, verwenden Sie den Parameter Public Accessibility (Öffentliche Erreichbarkeit). Mit diesem Parameter können Sie festlegen, ob ein öffentlicher Zugriff auf die DB-Instance besteht. Sie können eine DB-Instance ändern und die öffentliche Zugänglichkeit im Parameter Öffentlicher Zugriff aktivieren und deaktivieren.

Weitere Informationen finden Sie unter Ausblenden einer DB-Clusters in einer VPC vor dem Internet.

> **Note**
>
> Wenn sich Ihre DB-Instance in einer VPC befindet, aber nicht öffentlich zugänglich ist, können Sie auch eine AWS-Site-to-Site-VPN-Verbindung oder eine AWS Direct Connect-Verbindung verwenden, um von einem privaten Netzwerk aus darauf zuzugreifen. Weitere Informationen finden Sie unter Richtlinie für den Datenverkehr zwischen Netzwerken.

Amazon-RDS-API und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und Amazon-RDS-API-Endpunkten herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt erstellen. Schnittstellenendpunkte werden von unterstütz AWS PrivateLink.

AWS PrivateLink ermöglicht Ihnen den privaten Zugriff auf Amazon RDS-API-Operationen ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder AWS Direct Connect Verbindung. DB-Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen für die Kommunikation mit Amazon-RDS-API-Endpunkten, um DB-Instances und DB-Cluster zu starten, zu ändern oder zu beenden. Ihre DB-Instances benötigen auch keine öffentlichen IP-Adressen, um beliebige der verfügbaren RDS-API-Operationen zu verwenden. Der Datenverkehr zwischen der VPC und Amazon RDS verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt. Weitere Informationen zu Elastic Network-Schnittstellen finden Sie unter Elastic Network-Schnittstellen im Amazon EC2 Benutzerhandbuch.

Weitere Informationen zu VPC-Endpunkten finden Sie unter Interface VPC Endpoints (AWS PrivateLink) im Amazon VPC-Benutzerhandbuch. Weitere Informationen zu RDS-API-Operationen finden Sie in der Amazon-RDS-API-Referenz.

Sie benötigen keinen Schnittstellen-VPC-Endpunkt, um eine Verbindung zu einer DB-Cluster herzustellen. Weitere Informationen finden Sie unter Szenarien für den Zugriff auf eine DB-Cluster in einer VPC.

Überlegungen zu VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Amazon RDS-API-Endpunkte einrichten, stellen Sie sicher, dass Sie die Eigenschaften und Einschränkungen des Schnittstellenendpunkts im Amazon VPC Benutzerhandbuch einsehen.

Alle RDS-API-Operationen, die für die Verwaltung von Amazon-Aurora-Ressourcen relevant sind, sind mit AWS PrivateLinküber Ihre VPC verfügbar.

VPC-Endpunktrichtlinien werden für RDS-API-Endpunkte unterstützt. Standardmäßig ist der vollständige Zugriff auf RDS-API-Operationen über den Endpunkt zulässig. Weitere Informationen

finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon VPC Benutzerhandbuch.

Verfügbarkeit

Die Amazon RDS-API unterstützt derzeit VPC-Endpunkte in den folgenden Regionen: AWS

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Kanada West (Calgary)
- China (Peking)
- China (Ningxia)
- Europa (Frankfurt)
- Europa (Zürich)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- Europa (Milan)
- Israel (Tel Aviv)

- Naher Osten (Bahrain)
- Südamerika (São Paulo)
- AWS GovCloud (US-Ost)
- AWS GovCloud (US-West)

Erstellen eines Schnittstellen-VPC-Endpunkts für die Amazon RDS-API

Sie können einen VPC-Endpunkt für die Amazon RDS-API entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Amazon VPC Benutzerhandbuch.

Erstellen Sie einen VPC-Endpunkt für die Amazon RDS-API unter Verwendung des Servicenamens `com.amazonaws.region.rds`.

Mit Ausnahme von AWS Regionen in China können Sie, wenn Sie privates DNS für den Endpunkt aktivieren, API-Anfragen an Amazon RDS mit dem VPC-Endpunkt stellen, indem Sie beispielsweise `rds.us-east-1.amazonaws.com` dessen Standard-DNS-Namen für die AWS Region verwenden. Für die AWS Regionen China (Peking) und China (Ningxia) können Sie API-Anfragen mit dem VPC-Endpunkt jeweils mit `rds-api.cn-north-1.amazonaws.com.cn` und `rds-api.cn-northwest-1.amazonaws.com.cn` stellen.

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Amazon VPC Benutzerhandbuch.

Erstellen einer VPC-Endpunktrichtlinie für die Amazon RDS-API

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf die Amazon RDS-API steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon VPC Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Amazon RDS-API-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für die Amazon RDS-API. Wenn diese Richtlinie an einen Endpunkt angefügt wird, gewährt sie Zugriff auf die aufgelisteten Amazon RDS-API-Aktionen für alle Prinzipale auf allen Ressourcen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBInstance",
            "rds:ModifyDBInstance",
            "rds:CreateDBSnapshot"
         ],
         "Resource":"*"
      }
   ]
}
```

Beispiel: VPC-Endpunktrichtlinie, die jeglichen Zugriff von einem bestimmten Konto aus verweigert AWS

Die folgende VPC-Endpunktrichtlinie verweigert dem AWS Konto 123456789012 jeglichen Zugriff auf Ressourcen, die den Endpunkt verwenden. Die Richtlinie erlaubt alle Aktionen von anderen Konten.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": { "AWS": [ "123456789012" ] }
     }
   ]
}
```

Bewährte Methoden für die Sicherheit in Amazon Aurora

Verwenden Sie AWS Identity and Access Management (IAM-) Konten, um den Zugriff auf Amazon RDS-API-Operationen zu kontrollieren, insbesondere auf Operationen, die Aurora erstellen, ändern oder löschen. Zu solchen Ressourcen gehören DB- Cluster, Sicherheitsgruppen und Parametergruppen. Verwenden Sie zudem IAM zur Steuerung der Aktionen, die allgemeine administrative Aktionen wie die Sicherung und Wiederherstellung von DB-Clustern ausführen.

- Erstellen Sie einen individuellen Benutzer für jede Person, die Ressourcen von Amazon Aurora verwaltet, einschließlich Sie selbst. Verwenden Sie keine AWS Root-Anmeldeinformationen, um Aurora Aurora-Ressourcen zu verwalten.
- Gewähren Sie jedem Benutzer nur den Mindestsatz an Berechtigungen, die für die Ausführung seiner Aufgaben erforderlich sind.
- Verwenden Sie IAM-Gruppen, um Berechtigungen für mehrere Benutzer effektiv zu verwalten.
- Wechseln Sie regelmäßig die IAM-Anmeldeinformationen.
- Konfigurieren AWS Secrets Manager Sie so, dass die Secrets für Aurora automatisch rotiert werden. Weitere Informationen finden Sie unter Rotation Ihrer AWS Secrets Manager Geheimnisse im AWS Secrets Manager Benutzerhandbuch. Sie können die Anmeldeinformationen auch AWS Secrets Manager programmgesteuert von abrufen. Weitere Informationen finden Sie unter Abrufen des Secret-Wertes im AWS Secrets Manager -Benutzerhandbuch.

Weitere Informationen zur Sicherheit von Amazon Aurora finden Sie unter Sicherheit in Amazon Aurora. Weitere Informationen zu IAM finden Sie unter AWS Identity and Access Management. Informationen zu den bewährten Methoden für IAM finden Sie unter Bewährte Methoden für IAM.

AWS Security Hub verwendet Sicherheitskontrollen, um Ressourcenkonfigurationen und Sicherheitsstandards zu bewerten und Sie bei der Einhaltung verschiedener Compliance-Frameworks zu unterstützen. Weitere Informationen zur Verwendung von Security Hub zur Evaluierung von RDS-Ressourcen finden Sie unter Amazon Relational Database Service Controls im AWS Security Hub Benutzerhandbuch.

Sie können Ihre Nutzung von RDS in Bezug auf bewährte Sicherheitsmethoden mithilfe von Security Hub überwachen. Weitere Informationen finden Sie unter Was ist AWS Security Hub? .

Verwenden Sie die AWS Management Console AWS CLI, die oder die RDS-API, um das Passwort für Ihren Masterbenutzer zu ändern. Falls Sie zum Ändern des Hauptbenutzerpassworts ein anderes

Tool verwenden, beispielsweise einen SQL-Client, werden dem Benutzer unter Umständen ohne Absicht seine Berechtigungen entzogen.

Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der verschiedene Datenquellen analysiert und verarbeitet, einschließlich Amazon RDS-Anmeldeaktivitäten. Er verwendet Feeds mit Bedrohungsinformationen und maschinelles Lernen, um unerwartetes, potenziell nicht autorisiertes, verdächtiges Anmeldeverhalten und böswillige Aktivitäten in Ihrer AWS Umgebung zu identifizieren.

Wenn Amazon GuardDuty RDS Protection einen potenziell verdächtigen oder anomalen Anmeldeversuch erkennt, der auf eine Bedrohung für Ihre Datenbank hinweist, GuardDuty generiert Amazon RDS Protection ein neues Ergebnis mit Details über die potenziell gefährdete Datenbank. Weitere Informationen finden Sie unter Überwachung von Bedrohungen mit Amazon GuardDuty RDS Protection.

Zugriffskontrolle mit Sicherheitsgruppen

VPC-Sicherheitsgruppen kontrollieren die Zugriffsaktivitäten von eingehendem und ausgehendem Datenverkehr in einem DB-Cluster. Standardmäßig ist der Netzwerkzugriff auf einen DB-Cluster deaktiviert. Sie können Regeln in einer Sicherheitsgruppe angeben, die den Zugriff aus einem IP-Adressbereich, über einen Port oder für eine Sicherheitsgruppe zulassen. Nach der Konfiguration von ingress-Regeln gelten diese für alle DB-Cluster, die dieser Sicherheitsgruppe zugeordnet sind. Sie können bis zu 20 Regeln in einer Sicherheitsgruppe angeben.

Überblick über VPC-Sicherheitsgruppen

Jede VPC-Sicherheitsgruppenregel ermöglicht einer bestimmten Quelle den Zugriff auf einen DB-Cluster in einer VPC, die dieser VPC-Sicherheitsgruppe zugeordnet ist. Die Quelle kann ein Adressenbereich (zum Beispiel: 203.0.113.0/24) oder eine andere VPC-Sicherheitsgruppe sein. Wenn Sie eine VPC-Sicherheitsgruppe als Quelle festlegen, erlauben Sie eingehenden Datenverkehr von allen Instances (typischerweise Anwendungsserver), die Quell-VPC-Sicherheitsgruppe verwenden. VPC-Sicherheitsgruppen können über Regeln verfügen, die den eingehenden und ausgehenden Datenverkehr regulieren. Die Regeln für ausgehenden Datenverkehr gelten jedoch normalerweise nicht für DB-Cluster. Die Regeln für den ausgehenden Datenverkehr gelten nur, wenn der DB-Cluster als Client agiert. Sie müssen die Amazon EC2-API oder die Option Security Group (Sicherheitsgruppe) in der VPC-Konsole verwenden, um VPC-Sicherheitsgruppen zu erstellen.

Wenn Sie Regeln für Ihre VPC-Sicherheitsgruppe erstellen, die den Zugriff auf Cluster in Ihrer VPC erlauben, müssen Sie einen Port für jeden Adressbereich bestimmen, für den die Regel Zugriff

zulässt. Wenn Sie beispielsweise SSH-Zugriff auf Instances in der VPC aktivieren möchten, dann erstellen Sie eine Regel, die Zugriff auf TCP-Port 22 für den bestimmten Adressbereich zulässt.

Sie können mehrere VPC-Sicherheitsgruppen konfigurieren, die Zugriff auf verschiedenen Ports für verschiedenen Instances in Ihrer VPC zulassen. Beispielsweise können Sie eine VPC-Sicherheitsgruppe erstellen, die den Zugriff auf TCP-Port 80 für Webserver in Ihrer VPC ermöglicht. Sie können dann eine andere VPC-Sicherheitsgruppe erstellen, die den Zugriff auf TCP-Port 3306 für Aurora MySQL-DB-Instances in Ihrer VPC ermöglicht.

> **Note**
>
> In einem Aurora-DB-Cluster ist die VPC-Sicherheitsgruppe, die mit dem DB-Cluster verknüpft ist, auch mit allen anderen DB-Instances im DB-Cluster verknüpft. Wenn Sie die VPC-Sicherheitsgruppe für den DB-Cluster oder die DB-Instance ändern, wird die Änderung automatisch für alle DB-Instances im DB-Cluster übernommen.

Weitere Informationen zu VPC-Sicherheitsgruppen finden Sie unter Sicherheitsgruppen im Amazon Virtual Private Cloud-Benutzerhandbuch.

> **Note**
>
> Wenn sich Ihr in einer VPC befindet, aber nicht öffentlich zugänglich ist, können Sie auch eine AWS Site-to-Site-VPN-Verbindung oder eine Verbindung verwenden, um von einem AWS Direct Connect privaten Netzwerk aus darauf zuzugreifen. Weitere Informationen finden Sie unter Richtlinie für den Datenverkehr zwischen Netzwerken.

Sicherheitsgruppenszenario

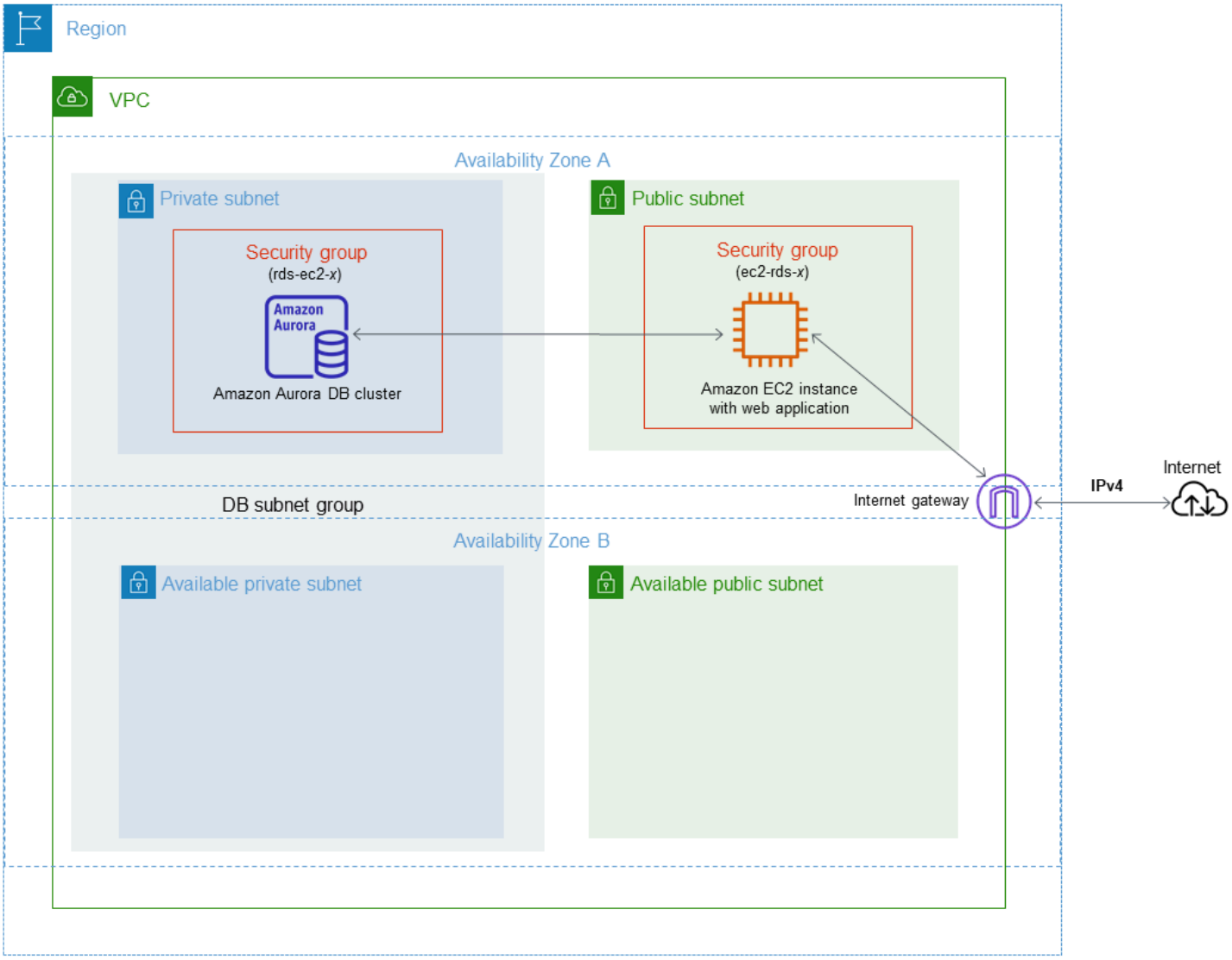
Eine häufige Verwendung von DB-Clustern in einer VPC ist das Teilen von Daten mit einem Anwendungsserver. Dieser wird in einer Amazon-EC2-Instance ausgeführt, die sich in derselben VPC befindet, auf die eine Clientanwendung von außerhalb der VPC zugreift. Für dieses Szenario verwenden Sie die RDS- und VPC-Seiten der AWS Management Console oder die RDS- und EC2-API-Operationen, um die notwendigen Instances und Sicherheitsgruppen zu erstellen:

1. Erstellen einer VPC-Sicherheitsgruppe (zum Beispiel `sg-0123ec2example`) und Definieren von eingehenden Regeln, welche die IP-Adressen der Client-Anwendung als Quelle verwenden.

Diese Sicherheitsgruppe erlaubt Ihrer Client-Anwendung, sich mit EC2-Instances in einer VPC zu verbinden, die diese Sicherheitsgruppe verwendet.

2. Erstellen Sie eine EC2-Instance für eine Anwendung und fügen Sie dieser EC2-Instance eine VPC-Sicherheitsgruppe (`sg-0123ec2example`) hinzu, die Sie im vorherigen Schritt erstellt haben.
3. Erstellen Sie eine zweite VPC-Sicherheitsgruppe (zum Beispiel `sg-6789rdsexample`) und erstellen Sie eine neue Regel durch Festlegen der VPC-Sicherheitsregel, die Sie in Schritt 1 (`sg-0123ec2example`) als Quelle erstellt haben.
4. Erstellen Sie einen neuen DB-Cluster und fügen Sie den DB-Cluster der VPC-Sicherheitsgruppe (`sg-6789rdsexample`) hinzu, die Sie im vorherigen Schritt erstellt haben. Wenn Sie einen DB-Cluster erstellen, verwenden Sie dieselbe Portnummer, die für die VPC-Sicherheitsgruppenregel (`sg-6789rdsexample`) festgelegt ist, die Sie in Schritt 3 erstellt haben.

Im folgenden Diagramm wird dieses Szenario veranschaulicht.



Ausführliche Anweisungen zum Konfigurieren einer VPC für dieses Szenario finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4). Weitere Informationen zur Verwendung einer VPC finden Sie unter Amazon VPCs und Amazon Aurora.

Erstellen einer VPC-Sicherheitsgruppe

Sie können unter Verwendung der VPC-Konsole eine VPC-Sicherheitsgruppe für eine DB-Instance erstellen. Weitere Informationen zum Erstellen einer Sicherheitsgruppe finden Sie unter Ermöglichen des Zugriffs auf den DB-Cluster in der VPC durch Erstellen einer Sicherheitsgruppe und Sicherheitsgruppen im Amazon Virtual Private Cloud-Benutzerhandbuch.

Verknüpfen einer Sicherheitsgruppe mit einem DB-Cluster

Sie können eine Sicherheitsgruppe mit einem DB-Cluster verknüpfen, indem Sie die Option Cluster modifizieren auf der RDS-Konsole, die `ModifyDBCluster` Amazon RDS-API oder den `modify-db-cluster` AWS CLI Befehl verwenden.

Das folgende CLI-Beispiel ordnet eine bestimmte VPC-Gruppe zu und entfernt DB-Sicherheitsgruppen aus dem DB-Cluster

```
aws rds modify-db-cluster --db-cluster-identifier dbName --vpc-security-group-ids sg-ID
```

Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Berechtigungen von Hauptbenutzerkonten

Wenn Sie einen neuen DB-Cluster erstellen, erhält der Standardbenutzer, den Sie verwenden, bestimmte Sonderrechte für diesen DB-Cluster. Sie können den Master-Benutzernamen nicht ändern, nachdem die DB-Cluster erstellt wurde.

> **Important**
>
> Wir empfehlen Ihnen, den Hauptbenutzer nicht direkt in Ihren Anwendungen zu verwenden. Bleiben Sie stattdessen bei der bewährten Methode, einen Datenbankbenutzer zu verwenden, der mit den Mindestberechtigungen erstellt wurde, die für Ihre Anwendung erforderlich sind.

> **Note**
>
> Wenn Sie die Berechtigungen für den Hauptbenutzer aus Versehen gelöscht haben, können Sie diese wiederherstellen, indem Sie den DB--Cluster ändern und ein neues Passwort für den Hauptbenutzer festlegen. Weitere Informationen über das Ändern eines DB--Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Die folgende Tabelle zeigt die Sonderrechte und Datenbankrollen, die der Hauptbenutzer in jeder der Datenbank-Engines erhält.

Datenban-Engine	Systemberechtigung	Datenbankrolle
Aurora MySQL	Version 2: `ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE USER, CREATE VIEW, DELETE, DROP, EVENT, EXECUTE, GRANT OPTION, INDEX, INSERT, LOAD FROM S3, LOCK TABLES, PROCESS, REFERENCES , RELOAD, REPLICATION CLIENT , REPLICATION SLAVE , SELECT, SELECT INTO S3, SHOW DATABASES , SHOW VIEW, TRIGGER, UPDATE`	—
	Version 3: `ALTER, APPLICATION_PASSWORD_ADMIN , ALTER ROUTINE, CONNECTION_ADMIN , CREATE, CREATE ROLE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE USER, CREATE VIEW, DELETE, DROP, DROP ROLE, EVENT, EXECUTE, INDEX, INSERT, LOCK TABLES, PROCESS, REFERENCES , RELOAD, REPLICATION CLIENT , REPLICATION SLAVE , ROLE_ADMIN , SET_USER_ID , SELECT, SHOW DATABASES , SHOW_ROUTINE` (Aurora-MySQL-Version 3.04 und höher), `SHOW VIEW, TRIGGER, UPDATE, XA_RECOVER_ADMIN`	`rds_superuser_role` Weitere Informationen zur rds_superuser_role finden Sie unter Rollenbasiertes Berechtigungsmodell.
Aurora PostgreSQL	`LOGIN, NOSUPERUSER , INHERIT, CREATEDB, CREATEROLE , NOREPLICATION , VALID UNTIL 'infinity'`	`RDS_SUPERUSER` Weitere Informationen zu RDS_SUPERUSER finden Sie unter Grundlegendes zu PostgreSQL-Rollen und -Berechtigungen.

Verwenden von serviceverknüpften Rollen für Amazon Aurora

Amazon Aurora nutzt von AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Amazon Aurora verknüpft ist. Serviceverknüpfte Rollen werden von Amazon Aurora vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle macht die Nutzung von Amazon Aurora einfacher, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon Aurora definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur Amazon Aurora seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können die Rollen nur nach dem Löschen der zugehörigen Ressourcen löschen. Dies schützt Ihre Amazon Aurora-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-Linked Role (Serviceverknüpfte Rolle) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Amazon Aurora

Amazon Aurora verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForRDS– damit Amazon RDS -AWSServices im Namen Ihrer DB-clusters aufrufen kann.

Die servicegebundene Rolle AWSServiceRoleForRDS vertraut den folgenden Services, die diese Rolle übernehmen:

- `rds.amazonaws.com`

Dieser dienstgebundenen Rolle ist eine Berechtigungsrichtlinie namens `AmazonRDSServiceRolePolicy` zugeordnet, die ihr Berechtigungen für den Betrieb in Ihrem Konto erteilt. Die Rollenberechtigungsrichtlinie erlaubt Amazon Aurora die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments, finden Sie unter AmazonRDSServiceRolePolicy im Referenzleitfaden zur AWS-verwalteten Richtlinie.

> **Note**
>
> Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Wenn Sie die folgende Fehlermeldung erhalten:
> Unable to create the resource. Überprüfen Sie, ob Sie die Berechtigung haben, eine serviceverknüpfte Rolle zu erstellen. Andernfalls warten Sie und versuchen Sie es später noch einmal.
> Stellen Sie sicher, dass Sie die folgenden Berechtigungen für Sie aktiviert sind:
>
> ```
> {
>     "Action": "iam:CreateServiceLinkedRole",
>     "Effect": "Allow",
>     "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
> AWSServiceRoleForRDS",
>     "Condition": {
>         "StringLike": {
>             "iam:AWSServiceName":"rds.amazonaws.com"
>         }
>     }
> }
> ```
>
> Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Amazon Aurora

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen DB-Cluster erstellen, erstellt Amazon Aurora die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Wenn Sie Amazon Aurora bereits vor dem 1. Dezember 2017 verwendet haben, bevor der Service serviceverknüpfte Rollen unterstützt hat, hat Amazon Aurora die Rolle

AWSServiceRoleForRDS in Ihrem Konto erstellt. Weitere Informationen finden Sie unter In meinem AWS-Konto wird eine neue Rolle angezeigt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie einen DB-Cluster erstellen, erstellt Amazon Aurora wieder die serviceverknüpfte Rolle für Sie.

Bearbeiten einer serviceverknüpften Rolle für Amazon Aurora

Amazon Aurora erlaubt es Ihnen nicht, die serviceverknüpfte Rolle AWSServiceRoleForRDS zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon Aurora

Wenn Sie eine Funktion oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch all Ihre DB-Cluster löschen, bevor Sie die serviceverknüpfte Rolle löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor Sie mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie sich zunächst vergewissern, dass die Rolle über keine aktiven Sitzungen verfügt, und alle Ressourcen entfernen, die von der Rolle verwendet werden.

So überprüfen Sie in der IAM-Konsole, ob die serviceverknüpfte Rolle über eine aktive Sitzung verfügt

1. Melden Sie sich bei der AWS Management Console an, und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM Console Roles aus. Wählen Sie dann den Namen (nicht das Kontrollkästchen) der Rolle AWSServiceRoleForRDS aus.
3. Wählen Sie auf der Seite Summary (Zusammenfassung) für die ausgewählte Rolle die Registerkarte Access Advisor (Advisor aufrufen) aus.

4. Überprüfen Sie auf der Registerkarte Access Advisor die jüngsten Aktivitäten für die serviceverknüpfte Rolle.

> **Note**
>
> Wenn Sie sich nicht sicher sind, ob Amazon Aurora die Rolle AWSServiceRoleForRDS verwendet, können Sie versuchen, die Rolle zu löschen. Wenn der Service die Rolle verwendet, schlägt die Löschung fehl und Sie können die AWS-Regionen anzeigen, in denen die Rolle verwendet wird. Wenn die Rolle verwendet wird, müssen Sie warten, bis die Sitzung beendet wird, bevor Sie die Rolle löschen können. Die Sitzung für eine serviceverknüpfte Rolle können Sie nicht widerrufen.

Wenn Sie die Rolle AWSServiceRoleForRDS entfernen wollen, müssen Sie zunächst alle DB-Cluster löschen.

Löschen aller Ihrer Cluster

Verwenden Sie eines der folgenden Verfahren, um einen einzelnen Cluster zu löschen. Wiederholen Sie dieses Verfahren für jeden der Cluster.

So löschen Sie einen Cluster (Konsole)

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der Liste Databases (Datenbanken) den Cluster aus, den Sie löschen möchten.
3. Wählen Sie bei Cluster Actions (Cluster-Aktionen) die Option Delete (Löschen).
4. Wählen Sie Delete (Löschen).

So löschen Sie einen Cluster (CLI)

Siehe `delete-db-cluster` in der AWS CLI-Befehlsreferenz.

So löschen Sie einen Cluster (API)

Weitere Informationen finden Sie im Amazon RDS API Reference unter `DeleteDBCluster`.

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die serviceverknüpfte Rolle AWSServiceRoleForRDS zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Amazon VPCs und Amazon Aurora

Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie AWS-Ressourcen, wie z. B. Aurora-DB-Cluster, in einer Virtual Private Cloud (VPC) starten.

Wenn Sie eine VPC verwenden, haben Sie die Kontrolle über Ihre virtuelle Netzwerkumgebung. Sie können Ihren eigenen IP-Adressbereich auswählen, Subnetze erstellen sowie Routing-Tabellen und Zugriffskontrolllisten konfigurieren. Es fallen keine zusätzlichen Kosten für das Ausführen einer DB-Cluster in einer VPC an.

Konten haben eine Standard-VPC. Alle neuen DB-Cluster werden in der Standard-VPC erstellt, außer Sie ändern die Einstellungen.

Themen

Im Folgenden finden Sie eine Diskussion über VPC-Funktionalität, die relevant ist für Amazon Aurora-DB-Cluster. Weitere Informationen zu Amazon VPC finden Sie unter Amazon-VPC-Handbuch „Erste Schritte“ und Amazon-VPC-Benutzerhandbuch.

Arbeiten mit einer DB-Cluster in einer VPC

Ihr DB-Cluster befindet sich in einer Virtual Private Cloud (VPC). Eine VPC ist ein virtuelles Netzwerk, das von anderen virtuellen Netzwerken in der AWS-Cloud logisch isoliert ist. Mit Amazon VPC können Sie AWS Ressourcen, wie z. B. einen Amazon Aurora DB-Cluster oder eine Amazon-EC2-Instance, in einer VPC starten. Bei der VPC kann es sich um die mit Ihrem Konto verknüpfte Standard-VPC oder eine von Ihnen erstellte VPC handeln. Alle VPCs sind mit Ihrem AWS-Konto verknüpft.

Die Standard-VPC besitzt drei Subnetze, mit denen Sie Ressourcen innerhalb der VPC separieren können. Zudem verfügt die Standard-VPC über ein Internet-Gateway, mit dem Sie den externen Zugriff auf Ressourcen in der VPC gewähren können.

Eine Liste von Szenarien mit Amazon Aurora DB-Clusters in einer VPC finden Sie unter Szenarien für den Zugriff auf eine DB-Cluster in einer VPC.

Themen

In den folgenden Tutorials lernen Sie, eine VPC zu erstellen, die Sie für ein gängiges Amazon-Aurora-Szenario verwenden können:

Arbeiten mit einer DB-Cluster in einer VPC

Hier sind einige Tipps für das Arbeiten mit einer DB-Cluster in einer VPC:

- Ihre VPC muss mindestens zwei Subnetze besitzen. Diese Subnetze müssen sich in zwei unterschiedlichen Availability Zones in der AWS-Region befinden, in der Sie Ihre DB-Cluster bereitstellen möchten. Ein Subnetz ist ein Segment des IP-Adressbereichs einer VPC, das Sie angeben können und das Sie zur Gruppierung von DB-Clustern auf der Grundlage Ihrer Sicherheits- und Betriebsanforderungen verwenden können.
- Wenn Sie möchten, dass Ihr DB-Cluster in der VPC öffentlich zugänglich ist, stellen Sie sicher, dass Sie die VPC-Attribute DNS-Hostnamen und DNS-Auflösung aktivieren.
- Sie müssen für Ihre VPC eine DB-Sicherheitsgruppe erstellen. Sie erstellen eine DB-Subnetzgruppe, indem Sie die Subnetze angeben, die Sie erstellt haben. Amazon Aurora wählt ein Subnetz und eine IP-Adresse innerhalb dieses Subnetzes, die mit der primären DB-Instance in Ihrem DB-Cluster verknüpft wird. Die primäre DB-Instance verwendet die Availability Zone, die das Subnetz enthält.
- Ihre VPC muss über eine VPC-Sicherheitsgruppe verfügen, die den Zugriff auf die DB-Cluster zulässt.

  Weitere Informationen finden Sie unter Szenarien für den Zugriff auf eine DB-Cluster in einer VPC.

- Die CIDR-Blöcke in jedem Subnetz müssen groß genug sein, um freie IP-Adressen für Amazon Aurora unterzubringen, die während der Wartungsarbeiten genutzt werden können, einschließlich Failover und Skalierung. Beispielsweise ist ein Bereich wie 10.0.0.0/24 und 10.0.1.0/24 normalerweise groß genug.
- Eine VPC kann über das Attribut instance tenancy mit dem Wert default oder dedicated verfügen. Bei allen Standard-VPCs ist das Attribut "instance tenancy" auf den Standardwert gesetzt; und eine Standard-VPC kann eine beliebige DB-Instance-Klasse unterstützen.

  Wenn Ihre DB-Cluster in einer dedizierten VPC ist und das Attribut „instance tenancy“ den Wert „dedicated“ aufweist, muss die DB-Instance-Klasse Ihrer DB-Cluster einem der zulässigen Dedicated-Instance-Typen von Amazon EC2 entsprechen. Zum Beispiel entspricht die EC2–Dedicated Instance r5.large der DB-Instance-Klasse db.r5.large. Informationen über die Instance-Tenancy in einer VPC finden Sie unter Dedicated Instances im Amazon Elastic Compute Cloud-Benutzerhandbuch.

  Weitere Informationen zu Instance-Typen, die in einer Dedicated Instance enthalten sein dürfen, finden Sie unter Amazon EC2 Dedicated Instances auf der EC2-Preis-Seite.

  > **Note**
  >
  > Wenn Sie das Attribut instance tenancy für einen DB-Cluster auf „dedicated“ setzen, garantiert dies nicht, dass der DB-Cluster auf einem dedizierten Host läuft.

Arbeiten mit DB-Subnetzgruppen

Subnetze sind Segmente eines IP-Adressbereichs der VPC, die Sie festlegen und mit denen Sie basierend auf Ihren Sicherheits- und Betriebsanforderungen Ressourcen gruppieren können. Eine DB-Subnetzgruppe ist eine Sammlung von Subnetzen (in der Regel private Subnetze), die Sie in einer VPC erstellen und anschließend Ihrer DB-Clusters zuweisen. Durch die Verwendung einer DB-Subnetzgruppe können Sie eine bestimmte VPC angeben, wenn Sie DB-Cluster mit der AWS CLI oder RDS-API erstellen. Wenn Sie die Konsole verwenden, können Sie die VPC und Subnetze auswählen, die Sie verwenden möchten.

Jede DB-Subnetzgruppe sollte über Subnetze in mindestens zwei Availability Zones in einer bestimmten AWS-Region verfügen. Beim Erstellen einer DB-Cluster in einer VPC müssen Sie eine DB-Subnetzgruppe dafür auswählen. Aus der DB-Subnetzgruppe wählt Amazon Aurora ein Subnetz

und eine IP-Adresse innerhalb dieses Subnetzes aus, um es mit der primären DB-Instance in Ihrem DB-Cluster zu verbinden. Die DB verwendet die Availability Zone, die das Subnetz enthält.

Die Subnetze in einer DB-Subnetzgruppe sind entweder öffentlich oder privat. Die Subnetze sind öffentlich oder privat, abhängig von der Konfiguration, die Sie für die Netzwerkzugriffskontrolllisten (Netzwerk-ACLs) und Routingtabellen festgelegt haben. Damit öffentlich auf eine DB-Cluster zugegriffen werden kann, müssen alle Subnetze in der entsprechenden DB-Subnetzgruppe öffentlich sein. Wenn ein Subnetz, das mit einer öffentlich zugänglichen DBCluster verknüpft ist, von öffentlich in privat geändert wird, kann dies die Verfügbarkeit der DB-Cluster beeinträchtigen.

Wenn Sie eine DB-Subnetzgruppe erstellen möchten, die den Dual-Stack-Modus unterstützt, stellen Sie sicher, dass jedem Subnetz, das Sie der DB-Subnetzgruppe hinzufügen, ein CIDR-Block der Internetprotokollversion 6 (IPv6) zugeordnet ist. Weitere Informationen finden Sie unter Amazon-Aurora-IP-Adressierung und Migrieren zu IPv6 im Amazon VPC-Benutzerhandbuch.

Wenn Amazon Aurora eine DB-Cluster in einer VPC erstellt, wird Ihrer DB-Cluster mithilfe einer IP-Adresse aus Ihrer DB-Subnetzgruppe eine Netzwerkschnittstelle zugewiesen. Wir empfehlen jedoch dringend, den DNS-Namen (Domain Name System) für die Verbindung zu Ihrem DB-Cluster zu verwenden. Wir empfehlen dies, da sich die zugrunde liegende IP-Adresse während des Failovers ändert.

> **Note**
>
> Für jede DB-Cluster, die Sie in einer VPC ausführen, stellen Sie sicher, mindestens eine Adresse in jedem Subnetz der DB-Subnetzgruppe für Wiederherstellungsmaßnahmen von Amazon Aurora zu reservieren.

Gemeinsam genutzte Subnetze

Sie können eine(n) DB-Cluster in einer gemeinsam genutzten VPC erstellen.

Einige Aspekte, die Sie bei der Verwendung gemeinsam genutzter VPCs beachten sollten:

- Sie können eine(n) DB-Cluster von einem gemeinsam genutzten VPC-Subnetz in ein nicht gemeinsam genutztes VPC-Subnetz verschieben und umgekehrt.
- Teilnehmer in einer gemeinsam genutzten VPC müssen eine Sicherheitsgruppe in der VPC erstellen, damit sie eine(n) DB-Cluster erstellen können.

- Besitzer und Teilnehmer in einer gemeinsam genutzten VPC können mithilfe von SQL-Abfragen auf die Datenbank zugreifen. Allerdings kann nur der Ersteller einer Ressource beliebige API-Aufrufe für die Ressource tätigen.

Amazon-Aurora-IP-Adressierung

IP-Adressen ermöglichen es Ressourcen in Ihrer VPC untereinander und mit Ressourcen im Internet zu kommunizieren. Amazon Aurora unterstützt sowohl IPv4- als auch IPv6-Adressierungsprotokolle. Standardmäßig verwenden Amazon Aurora und Amazon VPC das IPv4-Adressierungsprotokoll. Sie können dieses Standardverhalten nicht deaktivieren. Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 CIDR-Block (einen privaten IPv4-Adressenbereich) angeben. Optional können Sie Ihrer VPC und den Subnetzen einen IPv6 CIDR-Block zuordnen und den Clustern in Ihrem Subnetz IPv6-Adressen von diesem Block zuweisen.

Durch die Unterstützung des IPv6-Protokolls wird die Anzahl der unterstützten IP-Adressen erweitert. Durch die Verwendung des IPv6-Protokolls stellen Sie sicher, dass Sie über ausreichende verfügbare Adressen für das künftige Wachstum des Internets verfügen. Neue und vorhandene RDS-Ressourcen können IPv4- und IPv6-Adressen innerhalb Ihrer VPC verwenden. Das Konfigurieren, Sichern und Übersetzen des Netzwerkverkehrs zwischen den beiden Protokollen, die in verschiedenen Teilen einer Anwendung verwendet werden, können den Betriebsaufwand erhöhen. Sie können das IPv6-Protokoll für Amazon RDS-Ressourcen standardisieren, um Ihre Netzwerkkonfiguration zu vereinfachen.

Themen

- IPv4-Adressen
- IPv6-Adressen
- Dual-Stack-Modus

IPv4-Adressen

Beim Erstellen einer VPC müssen Sie für diese einen IPv4-Adressbereich in Form eines CIDR-Blocks wie `10.0.0.0/16` festlegen. Eine DB-Subnetzgruppe definiert den Bereich der IP-Adressen in diesem CIDR-Block, den eine DB-Cluster verwenden kann. Diese IP-Adressen können privat oder öffentlich sein.

Eine private IPv4-Adresse ist eine IP-Adresse, die nicht über das Internet erreichbar ist. Sie können private IPv4-Adressen zur Kommunikation zwischen Ihrem DB-Cluster und anderen Ressourcen, wie

Amazon-EC2-Instances, in derselben VPC verwenden. Jeder DB-Cluster hat eine private IP-Adresse für die Kommunikation in der VPC.

Eine öffentliche IP-Adresse ist eine IPv4-Adresse, die über das Internet erreichbar ist. Sie können öffentliche Adressen zur Kommunikation zwischen Ihrem DB-Cluster und Ressourcen im Internet, wie ein SQL-Client, verwenden. Anhand der folgenden Schritte können Sie kontrollieren, ob Ihr DB-Cluster eine öffentliche IP-Adresse erhält:

Weitere Informationen zum Erstellen einer VPC nur mit privaten IPv4-Adressen, die Sie mit einem gängigen Amazon Aurora-Szenario verwenden können, finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4).

IPv6-Adressen

Optional können Sie Ihrer VPC und den Subnetzen einen IPv6 CIDR-Block zuordnen und den Ressourcen in Ihrer VPC IPv6-Adressen von diesem Block zuweisen. Jede IPv6-Adresse ist global eindeutig.

Der IPv6 CIDR-Block für Ihre VPC wird automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können den Bereich nicht selbst auswählen.

Stellen Sie beim Herstellen einer Verbindung mit einer IPv6-Adresse sicher, dass die folgenden Bedingungen erfüllt sind:

- Der Client ist so konfiguriert, dass der Datenverkehr zwischen Client und Datenbank über IPv6 erlaubt ist.
- RDS-Sicherheitsgruppen, die von der DB-Instance verwendet werden, sind korrekt konfiguriert, sodass der Datenverkehr zwischen Client und Datenbank über IPv6 erlaubt ist.
- Der Clientbetriebssystem-Stack erlaubt Datenverkehr an der IPv6-Adresse und Betriebssystemtreiber und Bibliotheken sind so konfiguriert, dass sie den richtigen Standardendpunkt der DB-Instance auswählen (entweder IPv4 oder IPv6).

Weitere Informationen über IPv6 finden Sie unter IP-Adresszuweisung im Amazon VPC Benutzerhandbuch.

Dual-Stack-Modus

Wenn ein DB-Cluster sowohl über die IPv4- als auch die IPv6-Adressierungsprotokolle kommunizieren kann, erfolgt die Ausführung im Dual-Stack-Modus. So können Ressourcen

mit dem DB-Cluster über IPv4, IPv6 oder beides kommunizieren. RDS deaktiviert den Internet-Gateway-Zugriff für IPv6-Endpunkte privater DB-Instances im Dual-Stack-Modus. RDS tut dies, um sicherzustellen, dass Ihre IPv6-Endpunkte privat und nur von Ihrer VPC aus zugänglich sind.

Themen

- Dual-Stack-Modus und DB-Subnetzgruppen
- Arbeiten mit DB-Instances im Dual-Stack-Modus
- Ändern von reinen IPv4-DB-Clusters zur Verwendung des Dual-Stack-Modus
- Verfügbarkeit von Dual-Stack-Netzwerk-DB-Cluster
- Einschränkungen für Dual-Stack-Netzwerk-DB-Cluster

Weitere Informationen zum Erstellen einer VPC sowohl mit IPv4- als auch IPv6-Adressen, die Sie mit einem gängigen Amazon-Aurora-Szenario verwenden können, finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einer DB–einem DB-Cluster (Dual-Stack-Modus).

Dual-Stack-Modus und DB-Subnetzgruppen

Zur Verwendung des Dual-Stack-Modus stellen Sie sicher, dass jedem Subnetz in der DB-Subnetzgruppe, das Sie mit dem DB-Cluster verknüpfen, ein IPv6-CIDR-Block zugeordnet ist. Sie können eine neue DB-Subnetzgruppe erstellen oder eine vorhandene DB-Subnetzgruppe ändern, um diese Anforderung zu erfüllen. Nachdem ein DB-Cluster in den Dual-Stack-Modus gewechselt ist, können sich Clients normal damit verbinden. Stellen Sie sicher, dass Client-Sicherheits-Firewalls und Sicherheitsgruppen der RDS-DB-Instance präzise konfiguriert sind, um Datenverkehr über IPv6 zuzulassen. Zum Herstellen einer Verbindung verwenden Clients den Endpunkt der primären Instance des DB-Clusters. Clientanwendungen können angeben, welches Protokoll bevorzugt wird, wenn eine Verbindung mit einer Datenbank hergestellt wird. Im Dual-Stack-Modus erkennt der DB-Cluster das bevorzugte Netzwerkprotokoll des Clients, entweder IPv4 oder IPv6, und verwendet dieses Protokoll für die Verbindung.

Wenn eine DB-Subnetzgruppe den Dual-Stack-Modus aufgrund der Löschung des Subnetzes oder der CIDR-Trennung nicht mehr unterstützt, besteht die Gefahr eines inkompatiblen Netzwerkstatus für DB-Instances, die mit der DB-Subnetzgruppe verknüpft sind. Sie können die DB-Subnetzgruppe auch nicht verwenden, wenn Sie einen neuen DB-Cluster im Dual-Stack-Modus erstellen.

Wenn Sie mit der AWS Management Console ermitteln möchten, ob eine DB-Subnetzgruppe den Dual-Stack-Modus unterstützt, sehen Sie sich Network type (Netzwerktyp) auf der Detailseite der DB-Subnetzgruppe an. Um mithilfe der zu ermitteln, ob eine DB-Subnetzgruppe den Dual-Stack-

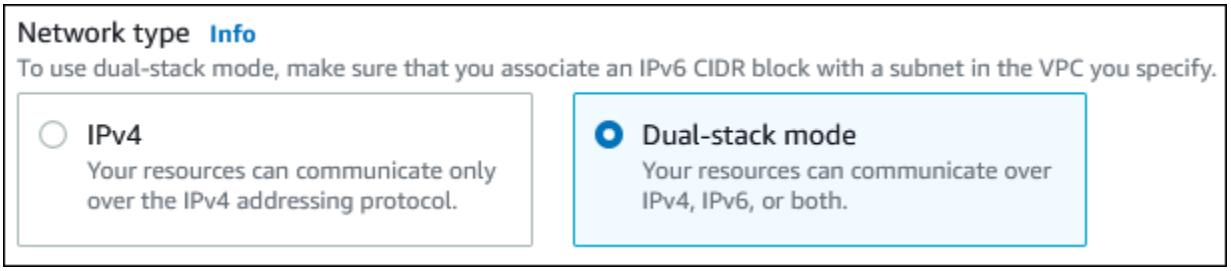
Modus unterstütztAWS CLI, führen Sie den describe-db-subnet-groups Befehl aus und zeigen Sie `SupportedNetworkTypes` in der Ausgabe an.

Lesereplikate werden als unabhängige DB-Instances behandelt und können einen anderen Netzwerktyp haben als die primäre DB-Instance. Wenn Sie den Netzwerktyp der primären DB-Instance eines Lesereplikats ändern, ist das Lesereplikat nicht betroffen. Wenn Sie eine DB-Instance wiederherstellen, können Sie sie auf jedem unterstützten Netzwerktyp wiederherstellen.

Arbeiten mit DB-Instances im Dual-Stack-Modus

Wenn Sie einen DB-Cluster erstellen oder ändern, können Sie den Dual-Stack-Modus angeben, damit Ihre Ressourcen mit Ihrer Ihrem DB-Cluster über IPv4, IPv6 oder beidem kommunizieren können.

Wenn Sie die AWS Management Console zum Erstellen oder Ändern einer DB-Instance verwenden, können Sie den Dual-Stack-Modus im Abschnitt Network type (Netzwerktyp) angeben. Die folgende Abbildung zeigt den Abschnitt Network type (Netzwerktyp) in der Konsole.



Wenn Sie die AWS CLI zum Erstellen oder Ändern eines DB-Clusters verwenden, legen Sie die Option `--network-type` auf `DUAL` fest, um den Dual-Stack-Modus zu verwenden. Wenn Sie die RDS API zum Erstellen oder Ändern eines DB-Clusters verwenden, legen Sie den Parameter `NetworkType` auf `DUAL` fest, um den Dual-Stack-Modus zu verwenden. Wenn Sie den Netzwerktyp einer DB-Instance ändern, sind Ausfallzeiten möglich. Wenn der Dual-Stack-Modus von der angegebenen DB-Engine-Version oder der DB-Subnetzgruppe nicht unterstützt wird, wird der Fehler `NetworkTypeNotSupported` zurückgegeben.

Weitere Informationen zum Erstellen eines DB-Clusters finden Sie unter Erstellen eines Amazon Aurora-DB Clusters. Weitere Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

Um festzustellen, ob sich ein DB-Cluster im Dual-Stack-Modus befindet, sehen Sie sich den Netzwerktyp auf der Registerkarte Connectivity & security (Konnektivität & Sicherheit) für den DB-Cluster an.

Ändern von reinen IPv4-DB-Clusters zur Verwendung des Dual-Stack-Modus

Sie können eine reine IPv4-DB-Cluster zur Verwendung des Dual-Stack-Modus ändern. Dazu ändern Sie den Netzwerktyp der DB-Cluster. Die Änderung kann zu Ausfallzeiten führen.

Es wird empfohlen, den Netzwerktyp Ihrer Amazon-Aurora-DB-Cluster während eines Wartungsfensters zu ändern. Das Festlegen des Netzwerktyps neuer Instances auf den Dual-Stack-Modus wird derzeit nicht unterstützt. Sie können den Netzwerktyp manuell festlegen, indem Sie den Befehl `modify-db-cluster` verwenden.

Bevor Sie eine DB-Cluster zur Verwendung des Dual-Stack-Modus ändern, stellen Sie sicher, dass ihre DB-Subnetzgruppe den Dual-Stack-Modus unterstützt. Wenn die mit der DB-Cluster verknüpfte DB-Subnetzgruppe den Dual-Stack-Modus nicht unterstützt, geben Sie eine andere DB-Subnetzgruppe an, die DB-Cluster unterstützt, wenn Sie sie ändern. Das Ändern der DB-Subnetzgruppe eines DB-Clusters kann zu Ausfallzeiten führen.

Wenn Sie die DB-Subnetzgruppe eines DB-Clusters ändern, bevor Sie den DB-Cluster zur Verwendung des Dual-Stack-Modus ändern, stellen Sie sicher, dass die DB-Subnetzgruppe vor und nach der Änderung für den DB-Cluster gültig ist.

Wir empfehlen, die modify-db-cluster API nur mit dem `---network-type`Parameter mit dem Wert auszuführen`DUAL`, um das Netzwerk eines Amazon-Aurora-Clusters in den Dual-Stack-Modus zu ändern. Das Hinzufügen anderer Parameter zusammen mit dem Parameter `--network-type` in demselben API-Aufruf kann zu Ausfallzeiten führen.

Wenn Sie nach der Änderung keine Verbindung mit dem DB-Cluster herstellen können, stellen Sie sicher, dass die Firewalls und Routing-Tabellen für die Client- und Datenbanksicherheit genau konfiguriert sind, um Datenverkehr zur Datenbank im ausgewählten Netzwerk (entweder IPv4 oder IPv6) zuzulassen. Möglicherweise müssen Sie auch Betriebssystemparameter, Bibliotheken oder Treiber ändern, um eine Verbindung mithilfe einer IPv6-Adresse herzustellen.

Ändern Sie eine reine IPv4-DB-Cluster zur Verwendung des Dual-Stack-Modus wie folgt

1. Ändern Sie eine DB-Subnetzgruppe, um den Dual-Stack-Modus zu unterstützen, oder erstellen Sie eine DB-Subnetzgruppe, die den Dual-Stack-Modus unterstützt:

   a. Ordnen Sie Ihrer VPC einen IPv6-CIDR-Block zu.

      Weitere Informationen finden Sie unter Hinzufügen eines IP6-CIDR-Blocks zu Ihrem VPC im Amazon-VPC-Benutzerhandbuch.

b. Fügen Sie den IPv6 CIDR-Block allen Subnetzen in der DB-Subnetzgruppe an.

   Weitere Informationen finden Sie unter Hinzufügen eines IP6-CIDR-Blocks zu Ihrem Subnetz im Amazon-VPC-Benutzerhandbuch.

c. Vergewissern Sie sich, dass die DB-Subnetzgruppe den Dual-Stack-Modus unterstützt.

   Wenn Sie die AWS Management Console verwenden, wählen Sie die DB-Subnetzgruppe aus und stellen Sie sicher, dass der Wert Supported network types (Unterstützte Netzwerktypen) Dual, IPv4 lautet.

   Wenn Sie die verwendenAWS CLI, führen Sie den describe-db-subnet-groups Befehl aus und stellen Sie sicher, dass der `SupportedNetworkType` Wert für die DB-Instance lautet`Dual, IPv4`.

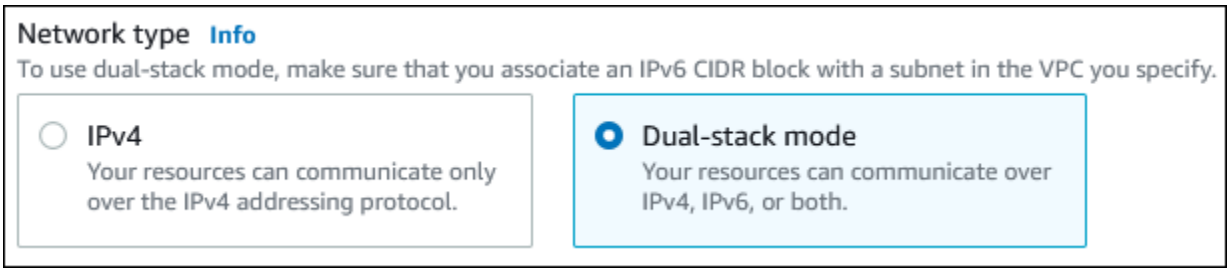
2. Ändern Sie die mit der DB-Cluster verknüpfte Sicherheitsgruppe, um IPv6-Verbindungen mit der Datenbank zuzulassen, oder erstellen Sie eine neue Sicherheitsgruppe, die IPv6-Verbindungen zulässt.

   Eine Anleitung dazu finden Sie unter Sicherheitsgruppenregeln im Amazon-VPC-Benutzerhandbuch.

3. Ändern der DB-Cluster zur Unterstützung des Dual-Stack-Modus. Setzen Sie hierzu den Netzwerk-Typ auf Dual-Stack-Modus.

   Wenn Sie die Konsole verwenden, stellen Sie sicher, dass die folgenden Einstellungen korrekt sind:

   - Network type (Netzwerktyp) – Dual-stack mode (Dual-Stack-Modus)

   - DB-Subnet group (Subnetzgruppe) – Die DB-Subnetzgruppe, die Sie in einem vorherigen Schritt konfiguriert haben
   - Security group (Sicherheitsgruppe) – Die Sicherheitsgruppe, die Sie in einem vorherigen Schritt konfiguriert haben

Wenn Sie die AWS CLI verwenden, stellen Sie sicher, dass die folgenden Einstellungen korrekt sind:

- `--network-type` – `dual`
- `--db-subnet-group-name` – Die DB-Subnetzgruppe, die Sie in einem vorherigen Schritt konfiguriert haben
- `--vpc-security-group-ids` – Die VPC-Sicherheitsgruppe, die Sie in einem vorherigen Schritt konfiguriert haben

Beispielsweise:

```
aws rds modify-db-cluster --db-cluster-identifier my-cluster --network-type "DUAL"
```

4. Vergewissern Sie sich, dass die DB-Cluster den Dual-Stack-Modus unterstützt.

   Wenn Sie die Konsole verwenden, wählen Sie die Registerkarte Konfiguration für die DB-Cluster. Stellen Sie auf dieser Registerkarte sicher, dass der Wert des Netzwerk-TypsDual-Stack-Modus ist.

   Wenn Sie die verwendenAWS CLI, führen Sie den describe-db-clusters Befehl aus und stellen Sie sicher, dass der `NetworkType` Wert für den DB-Cluster lautet`dual`.

   Führen Sie den `dig`-Befehl auf dem Writer-Endpunkt der DB-Instance aus, um die damit verknüpfte IPv6-Adresse zu kennzeichnen.

   ```
   dig db-instance-endpoint AAAA
   ```

   Verwenden Sie den Writer-DB-Instance-Endpunkt, nicht die IPv6-Adresse, um sich mit dem DB-Cluster zu verbinden.

Verfügbarkeit von Dual-Stack-Netzwerk-DB-Cluster

Die folgenden DB-Engine-Versionen unterstützen Dual-Stack-Netzwerk-DB-Cluster, außer in den Regionen Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Kanada West (Calgary), Europa (Spanien), Europa (Zürich), Israel (Tel Aviv) und Naher Osten (VAE):

- Aurora-MySQL-Versionen:

  - 3.02 und höhere 3-Versionen
  - 2.09.1 und höhere 2-Versionen

  Weitere Informationen über Aurora MySQL-Versionen finden Sie in den Release Notes für Aurora MySQL.
- Aurora-PostgreSQL-Versionen:
  - 14.3 und höhere 14-Versionen
  - 13.7 und höhere 13-Versionen

  Weitere Informationen zu Aurora-PostgreSQL-Versionen finden Sie unter Versionshinweise für Aurora PostgreSQL.

Einschränkungen für Dual-Stack-Netzwerk-DB-Cluster

Die folgenden Einschränkungen gelten für Dual-Stack-Netzwerk-DB-Cluster:

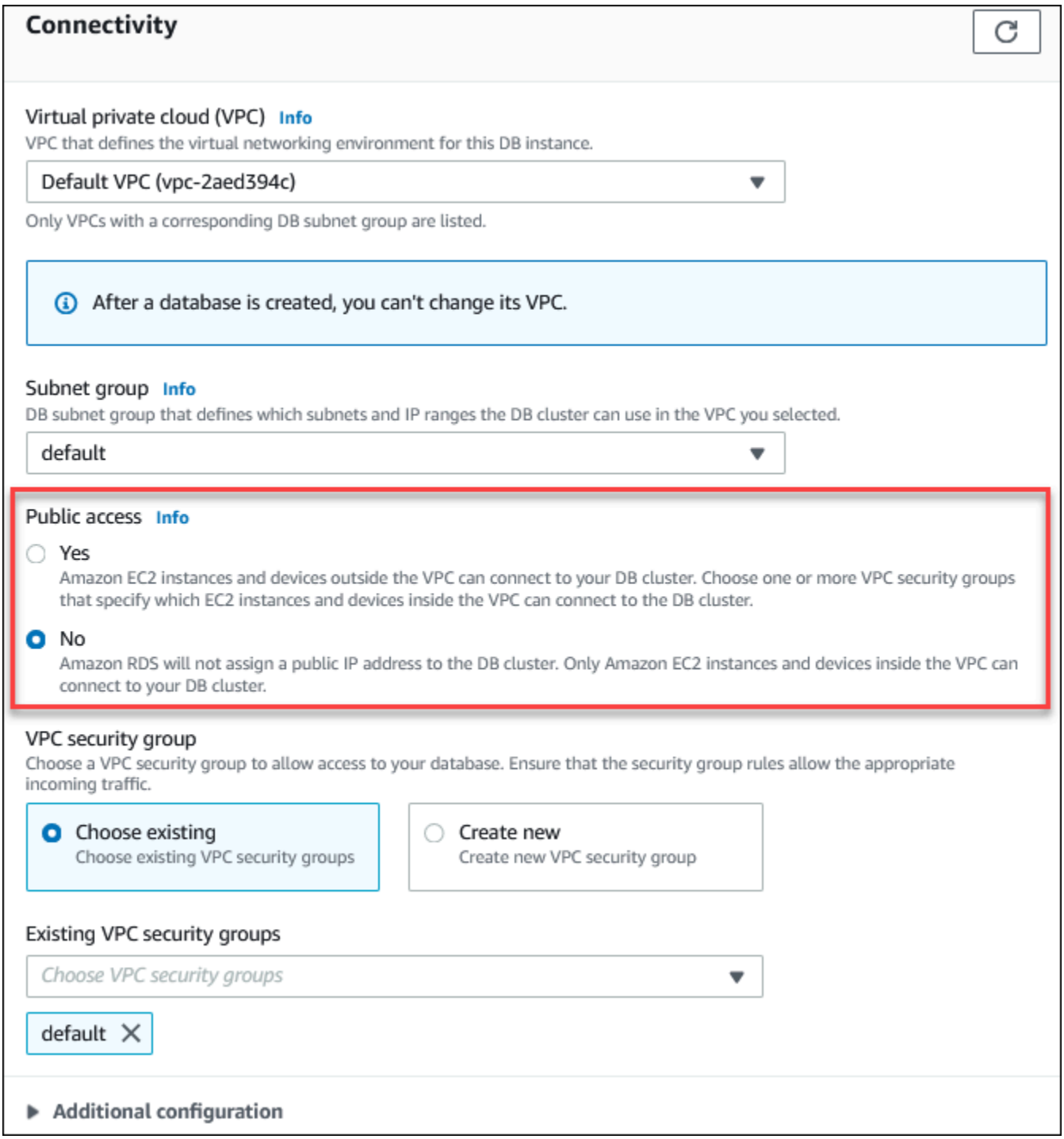
- DB-Cluster können das IPv6-Protokoll nicht ausschließlich verwenden. Sie können ausschließlich IPv4 oder das IPv4- und das IPv6-Protokoll (Dual-Stack-Modus) verwenden.
- Amazon RDS unterstützt keine nativen IPv6-Subnetze.
- DB-Cluster, die den Dual-Stack-Modus verwenden, müssen privat sein. Sie dürfen nicht öffentlich zugänglich sein.
- Der Dual-Stack-Modus unterstützt die DB-Instance-Klassen db.r3 nicht.
- Sie können RDS Proxy nicht mit DB-Cluster im Dual-Stack-Modus verwenden.

Ausblenden einer DB-Clusters in einer VPC vor dem Internet

Ein häufiges Amazon Aurora-Szenario ist eine VPC, in der Sie eine EC2-Instance mit einer öffentlich zugänglichen Webanwendung und einen DB-Cluster mit einer nicht öffentlich zugänglichen Datenbank haben. Sie können beispielsweise eine VPC mit einem öffentlichen und einem privaten Subnetz erstellen. Amazon-EC2-Instances, die als Webserver verwendet werden, können im öffentlichen Subnetz bereitgestellt werden. Die DB-Cluster werden im privaten Subnetz bereitgestellt. Bei einer solchen Bereitstellung haben nur die Webserver Zugang zu den DB-Cluster. Eine bildliche Darstellung dieses Szenarios finden Sie unter Ein DB- luster in einer VPC, auf den eine EC2-Instance in derselben VPC zugreift.

Wenn Sie eine DB-Cluster innerhalb einer VPC starten, verfügt die DB-Cluster über eine private IP-Adresse für den Datenverkehr innerhalb der VPC. Diese private IP-Adresse ist nicht öffentlich zugänglich. Mit der Option Public access (Öffentlicher Zugriff) können Sie festlegen, ob die DB-Cluster neben der privaten IP-Adresse auch eine öffentliche IP-Adresse hat. Wenn die DB-Cluster als öffentlich zugänglich bezeichnet wird, wird ihr DNS-Endpunkt innerhalb der VPC in die private IP-Adresse aufgelöst. Es wird in die öffentliche IP-Adresse von außerhalb der VPC aufgelöst. Zugriff auf die DB-Cluster wird letztendlich von der Sicherheitsgruppe kontrolliert, die sie verwendet. Dieser öffentliche Zugang ist nicht erlaubt, wenn die dem DB-Cluster zugewiesene Sicherheitsgruppe keine eingehenden Regeln enthält, die ihn erlauben. Damit ein DB-Cluster öffentlich zugänglich ist, müssen die Subnetze in seiner DB-Subnetzgruppe außerdem über ein Internet-Gateway verfügen. Weitere Informationen finden Sie unter Verbindung zur Amazon RDS-DB-Instance kann nicht hergestellt werden

Sie können eine DB-Cluster ändern und die öffentliche Zugänglichkeit mit der Option Public access (Öffentlicher Zugriff) aktivieren und deaktivieren. Die folgende Abbildung zeigt die Option Public access (Öffentlicher Zugriff) im Abschnitt Additional connectivity configuration (Zusätzliche Konnektivitätskonfiguration) . Um die Option festzulegen, öffnen Sie den Abschnitt Additional connectivity configuration (Zusätzliche Konnektivitätskonfiguration) im Abschnitt Connectivity (Konnektivität) .



Hinweise zum Ändern einer DB-Instance zum Festlegen der Option Public access (Öffentlicher Zugriff) finden Sie unter Ändern einer DB-Instance in einem DB-Cluster.

Erstellen einer DB-Cluster in einer VPC

In den folgenden Verfahren wird das Erstellen einer DB-Cluster in einer VPC veranschaulicht. Um die Standard-VPC zu verwenden, können Sie mit Schritt 2 beginnen und die VPC- und DB-Subnetzgruppe verwenden, die bereits für Sie erstellt wurden. Wenn Sie eine zusätzliche VPC erstellen möchten, können Sie eine neue VPC erstellen.

> **Note**
>
> Wenn Sie möchten, dass Ihr DB-Cluster in der VPC öffentlich zugänglich ist, müssen Sie die DNS-Informationen für die VPC aktualisieren, indem Sie die VPC-Attribute DNS-Hostnamen und DNS-Auflösung aktivieren. Weitere Informationen zum Aktualisieren der DNS-Informationen für eine VPC-Instance finden Sie unter Aktualisieren des DNS-Supports für Ihre VPC.

Gehen Sie wie folgt vor, um eine DB-Instance in einer VPC zu erstellen:

- Schritt 1: Erstellen einer VPC
- Schritt 2: Erstellen einer DB-Subnetzgruppe
- Schritt 3: Erstellen einer VPC-Sicherheitsgruppe
- Schritt 4: Erstellen einer DB-Instance in der VPC

Schritt 1: Erstellen einer VPC

Erstellen Sie eine VPC mit Subnetzen in mindestens zwei Availability Zones. Diese Subnetze verwenden Sie, wenn Sie eine DB-Subnetzgruppe erstellen. Wenn Sie eine Standard-VPC verwenden, wird automatisch ein Subnetz in jeder Availability Zone der AWS-Region für Sie erstellt.

Weitere Informationen finden Sie unter Erstellen einer VPC mit privaten und öffentlichen Subnetzen oder unter Create a VPC (VPC erstellen) im Amazon VPC Benutzerhandbuch.

Schritt 2: Erstellen einer DB-Subnetzgruppe

Eine DB-Subnetzgruppe ist eine Sammlung von Subnetzen (in der Regel private Subnetze), die Sie für eine VPC erstellen und anschließend Ihren DB-Cluster zuweisen. Mit einer DB-Subnetzgruppe können Sie eine bestimmte VPC definieren, wenn Sie DB-Cluster mit der AWS CLI oder der RDS API

erstellen. Wenn Sie die Konsole verwenden, können Sie einfach die VPC und Subnetze auswählen, die Sie verwenden möchten. Jede DB-Subnetzgruppe muss über mindestens ein Subnetz in mindestens zwei Availability Zones der AWS-Region verfügen. Jede DB-Subnetzgruppe sollte über mindestens ein Subnetz für jede Availability Zone in einer bestimmten AWS-Region verfügen.

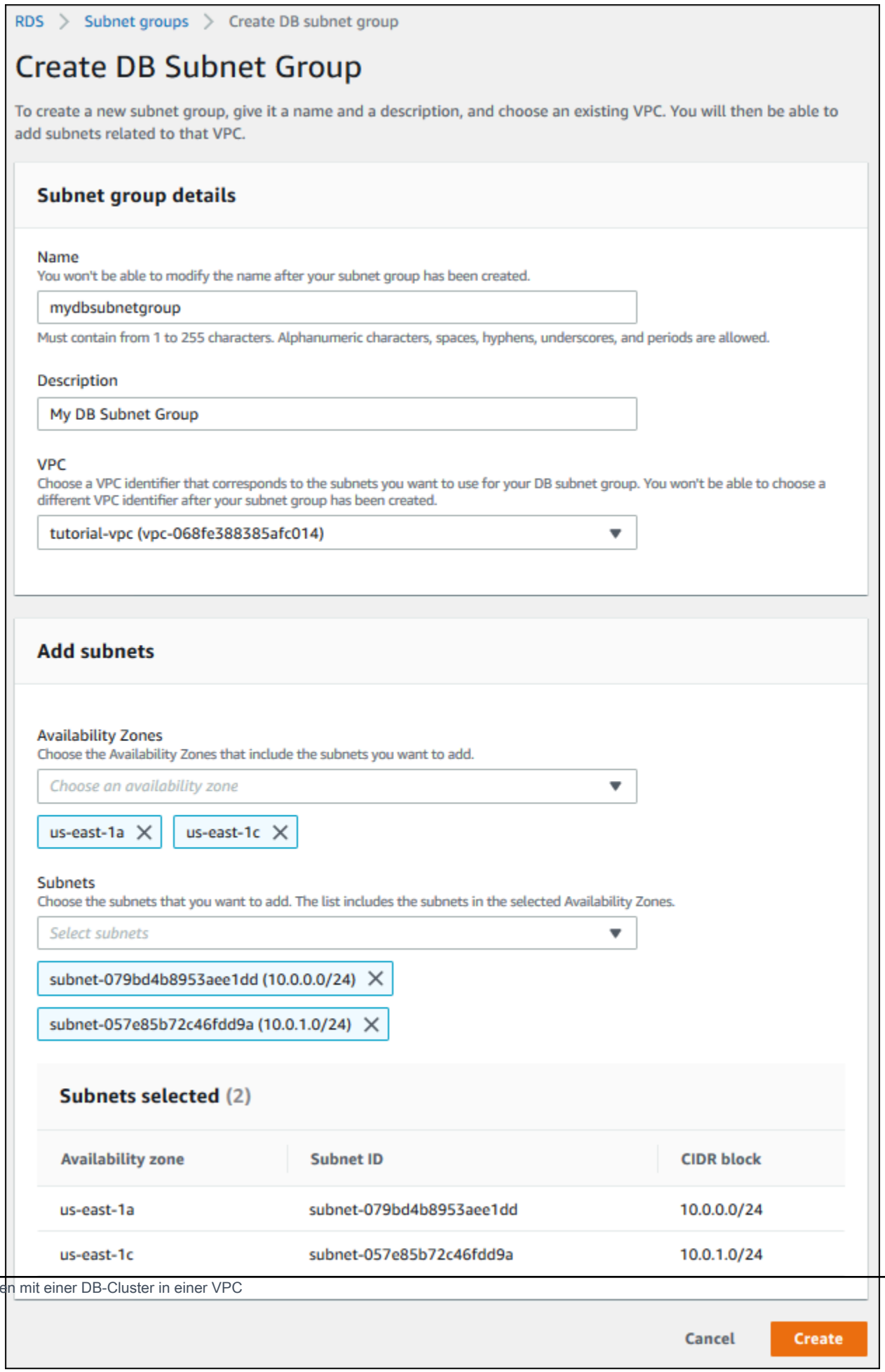
Damit öffentlich auf eine DB-Cluster zugegriffen werden kann, müssen die Subnetze in der DB-Subnetzgruppe über ein Internet-Gateway verfügen. Weitere Informationen zu Internet-Gateways für Subnetze finden Sie unter Verbinden mit dem Internet durch einen Internet-Gateway im Amazon VPC Benutzerhandbuch.

Beim Erstellen einer DB-Cluster in einer VPC müssen Sie eine DB-Subnetzgruppe auswählen. Amazon Aurora wählt ein Subnetz und eine IP-Adresse innerhalb dieses Subnetzes, um es mit Ihrem DB-Cluster zu verbinden. Wenn keine DB-Subnetzgruppen existieren, erstellt Amazon Aurora eine Standard-Subnetzgruppe, wenn Sie einen DB-Cluster erstellen. Amazon Aurora erstellt und ordnet Ihrer DB-Cluster eine Elastic-Network-Schnittstelle mit dieser IP-Adresse zu. Die DB-Cluster verwendet die Availability Zone, die das Subnetz enthält.

In diesem Schritt erstellen Sie eine DB-Subnetzgruppe und fügen die Subnetze hinzu, die Sie für Ihre VPC erstellt haben.

Erstellen einer DB-Sicherheitsgruppe

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Subnetzgruppe aus.
3. Wählen Sie DB-Subnetzgruppe erstellen aus.
4. Geben Sie im Feld Name den Namen Ihrer DB-Subnetzgruppe ein.
5. Geben Sie unter Beschreibung eine Beschreibung für Ihre DB-Subnetzgruppe ein.
6. Für VPC wählen Sie die Standard-VPC oder die zuvor erstellte VPC aus.
7. Wählen Sie im Abschnitt Subnetze hinzufügen die Availability Zones aus, die die Subnetze aus Availability Zones enthalten, und wählen Sie dann die Subnetze aus Subnetze aus.


RDS > Subnet groups > Create DB subnet group
Create DB Subnet Group
To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.
Subnet group details
Name
You won't be able to modify the name after your subnet group has been created.
mydbsubnetgroup
Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.
Description
My DB Subnet Group
VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.
tutorial-vpc (vpc-068fe388385afc014)
Add subnets
Availability Zones
Choose the Availability Zones that include the subnets you want to add.
Choose an availability zone
us-east-1a
us-east-1c
Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.
Select subnets
subnet-079bd4b8953aee1dd (10.0.0.0/24)
subnet-057e85b72c46fdd9a (10.0.1.0/24)
Subnets selected (2)
Availability zone
Subnet ID
CIDR block
us-east-1a
subnet-079bd4b8953aee1dd
10.0.0.0/24
us-east-1c
subnet-057e85b72c46fdd9a
10.0.1.0/24
Cancel
Create

8. Wählen Sie Create (Erstellen) aus.

   Ihre neue DB-Subnetzgruppe wird in der Liste der DB-Subnetzgruppen in der RDS-Konsole angezeigt. Sie können die DB-Subnetzgruppe auswählen und unten im Detailbereich ausführliche Informationen einschließlich aller Subnetze für diese Gruppe anzeigen.

Schritt 3: Erstellen einer VPC-Sicherheitsgruppe

Vor der DB-Cluster müssen Sie eine VPC-Sicherheitsgruppe erstellen, die Ihrer DB-Cluster zugeordnet wird. Wenn Sie keine VPC-Sicherheitsgruppe erstellen, können Sie die Standardsicherheitsgruppe beim Erstellen einer DB-Cluster verwenden. Eine Anleitung zum Erstellen einer Sicherheitsgruppe für Ihren DB-Cluster finden Sie unter Erstellen einer VPC-Sicherheitsgruppe für einen privaten DB-Cluster, oder unter Control traffic to resources using security groups (Kontrolle des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen) im Amazon VPC Benutzerhandbuch.

Schritt 4: Erstellen einer DB-Instance in der VPC

In diesem Schritt erstellen Sie eine DB-Cluster und verwenden den VPC-Namen, die DB-Subnetzgruppe und die VPC-Sicherheitsgruppe, die Sie in den vorherigen Schritten erstellt haben.

> **Note**
>
> Wenn Sie möchten, dass Ihr DBCluster in der VPC öffentlich zugänglich ist, müssen Sie die VPC-Attribute DNS-Hostnamen und DNS-Auflösung aktivieren. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Weitere Informationen zum Erstellen eines DB-Clusters finden Sie unter Erstellen eines Amazon Aurora-DB Clusters.

Wenn Sie im Abschnitt Konnektivität dazu aufgefordert werden, geben Sie den VPC-Namen, die DB-Subnetzgruppe und die VPC-Sicherheitsgruppe ein.

> **Note**
>
> Das Aktualisieren von VPCs wird aktuell für Aurora-DB-Cluster nicht unterstützt.

Szenarien für den Zugriff auf eine DB-Cluster in einer VPC

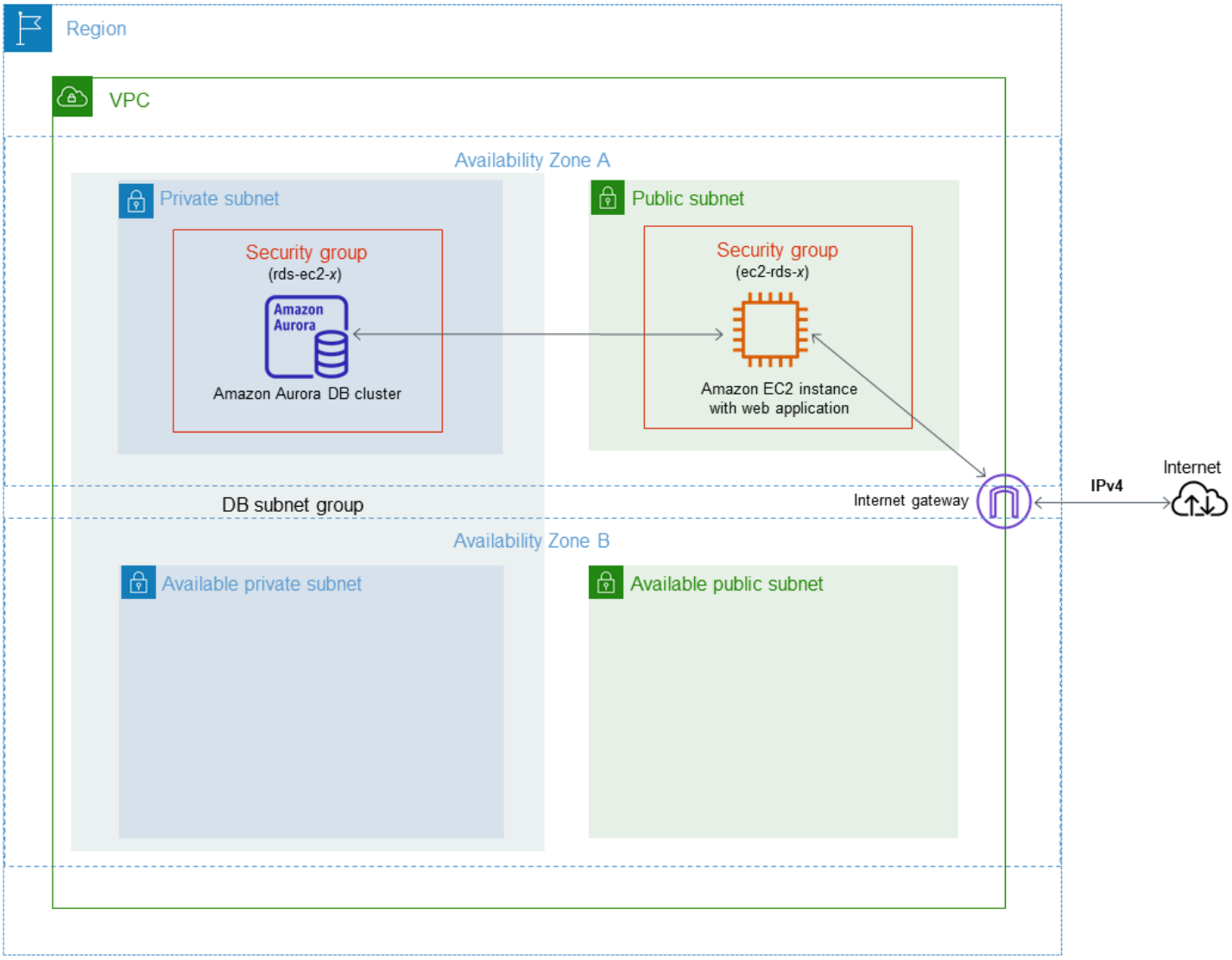
Amazon Aurora unterstützt die folgenden Szenarien für den Zugriff auf eine DB- Cluster in einer VPC:

- Eine EC2-Instance in derselben VPC
- Eine EC2-Instance in einer anderen VPC
- Eine Client-Anwendung über das Internet
- Ein Privates Netzwerk

Ein DB- luster in einer VPC, auf den eine EC2-Instance in derselben VPC zugreift

Häufig wird eine DB- Cluster in einer VPC genutzt, um Daten mit einem Anwendungsserver zu teilen, der auf einer EC2-Instance in derselben VPC ausgeführt wird.

Im folgenden Diagramm wird dieses Szenario veranschaulicht.



Nachfolgend finden Sie den einfachsten Weg für die Verwaltung des Zugriffs zwischen EC2-Instances und DB- Cluster in derselben VPC:

- Erstellen Sie eine VPC-Sicherheitsgruppe, in der sich Ihre DB- Cluster befinden sollen. Diese Sicherheitsgruppe kann verwendet werden, um den Zugriff auf DB- Cluster zu beschränken. Sie können beispielsweise eine benutzerdefinierte Regel für diese Sicherheitsgruppe erstellen. Dies kann den TCP-Zugriff über den Port ermöglichen, den Sie dem DB- Cluster bei der Erstellung zugewiesen haben, sowie eine IP-Adresse, die Sie für den Zugriff auf den DB- Cluster für Entwicklungs- oder andere Zwecke verwenden.
- Erstellen Sie eine VPC-Sicherheitsgruppe, der sich Ihre EC2-Instances (Webserver und Clients) befinden. Mithilfe dieser Sicherheitsgruppe können Sie bei Bedarf den Internetzugriff auf die EC2-

Instance über die Routing-Tabelle der VPC zulassen. Sie können beispielsweise Regeln für diese Sicherheitsgruppe festlegen, damit der TCP-Zugriff auf die EC2-Instance über Port 22 möglich ist.

- Erstellen Sie in der Sicherheitsgruppe benutzerdefinierte Regeln für Ihre DB- Cluster, um Verbindungen von der (für die EC2-Instances) erstellten Sicherheitsgruppe zuzulassen. Diese Regeln können jedem Mitglied der Sicherheitsgruppe den Zugang zu den DB- Clustern ermöglichen.

Es gibt ein zusätzliches öffentliches und privates Subnetz in einer separaten Availability Zone. Eine RDS-DB-Subnetzgruppe erfordert ein Subnetz in mindestens zwei Availability Zones. Das zusätzliche Subnetz erleichtert den Wechsel zu einer Multi-AZ-DB-Instance-Bereitstellung in der future.

Ein Tutorial mit einer Anleitung zum Erstellen einer VPC mit öffentlichen und privaten Subnetzen für dieses Szenario finden Sie unter Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4).

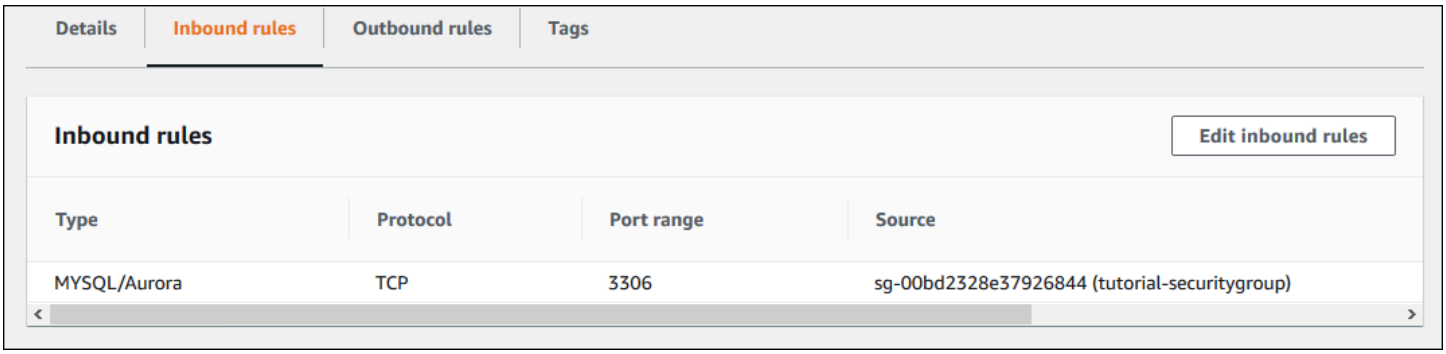
> **Tip**
>
> Sie können die Netzwerkkonnektivität zwischen einer Amazon-EC2-Instance und einem DB-Cluster automatisch beim Erstellen des DB-Clusters einrichten. Weitere Informationen finden Sie unter Automatische Netzwerkkonnektivität mit einer EC2-Instance konfigurieren .

Führen Sie folgende Schritte aus, um eine Regel in einer VPC-Sicherheitsgruppe zu erstellen, die Verbindungen von einer anderen Sicherheitsgruppe zulässt:

1. Melden Sie sich bei der Amazon VPC-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/vpc.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Erstellen oder wählen Sie eine Sicherheitsgruppe aus, der Sie den Zugriff zu Teilen einer anderen Sicherheitsgruppe erlauben möchten. Im vorhergehenden Szenario ist dies die Sicherheitsgruppe, die Sie für Ihre DB- Cluster verwenden. Wählen Sie die Registerkarte Inbound Rules (Eingehende Regeln) und anschließend Edit Inbound Rules (Eingehende Regeln bearbeiten) aus.
4. Wählen Sie auf der Seite Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) die Option Add Rule (Regel hinzufügen).
5. Wählen Sie für Typ den Eintrag, der dem Port entspricht, den Sie bei der Erstellung Ihres DB-Clusters verwendet haben, z. B. MYSQL/Aurora.

6. Geben Sie im Feld Source (Quelle) die ID der Sicherheitsgruppe ein. Anschließend werden die übereinstimmenden Sicherheitsgruppen auflistet. Wählen Sie die Sicherheitsgruppe mit den Mitgliedern aus, die Zugriff auf die durch diese Sicherheitsgruppe geschützten Ressourcen erhalten sollen. Im vorhergehenden Szenario ist dies die Sicherheitsgruppe, die Sie für Ihre EC2-Instance verwenden.
7. Wiederholen Sie die Schritte für das TCP-Protokoll, indem Sie eine Regel mit All TCP (Alle TCP) als Type (Typ) und Ihrer Sicherheitsgruppe im Feld Source (Quelle) erstellen. Wenn Sie das UDP-Protokoll verwenden möchten, erstellen Sie eine Regel mit Alle UDP als Typ und Ihrer Sicherheitsgruppe im Quelle.
8. Wählen Sie Save rules (Regeln speichern) aus.

Der folgende Bildschirm zeigt eine eingehende Regel mit einer Sicherheitsgruppe für ihre Quelle.

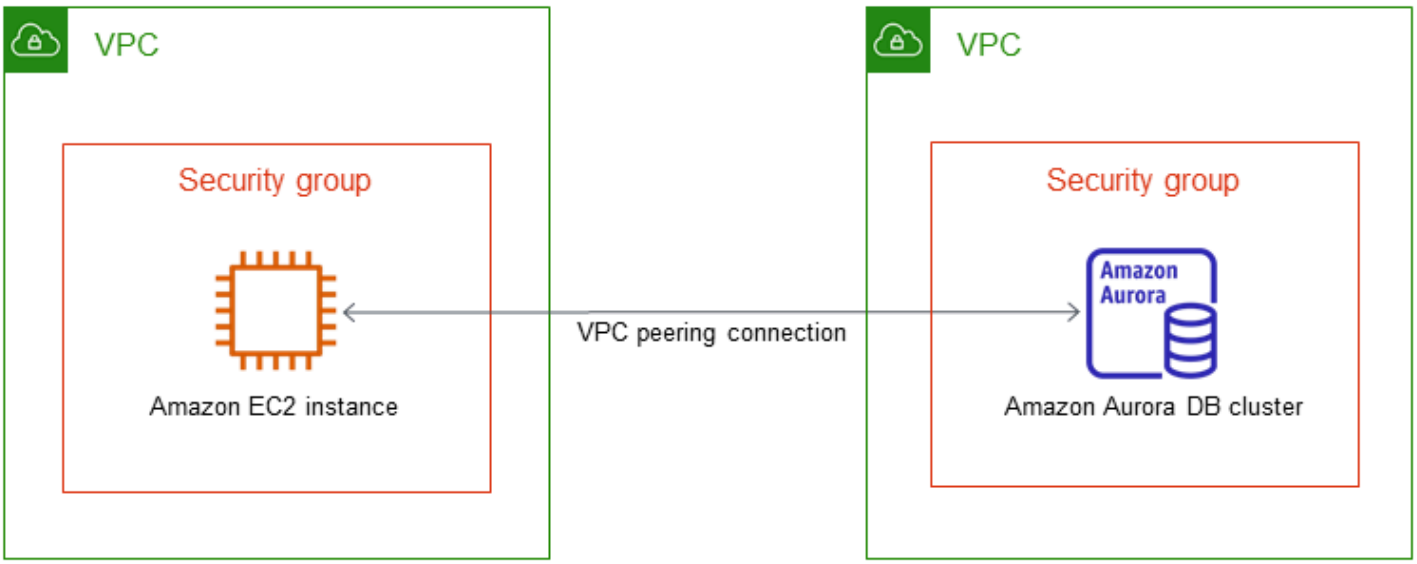


Weitere Informationen zum Herstellen einer Verbindung mit dem DB-Cluster von Ihrer EC2-Instance aus finden Sie unter Herstellen einer Verbindung mit einem Amazon Aurora-DB-Cluster.

Ein DB-Cluster in einer VPC, auf den eine EC2-Instanz in einer anderen VPC zugreift

Wenn sich Ihre DB- Cluster in einer anderen VPC als die für den Zugriff darauf verwendete EC2-Instance befindet, können Sie per VPC Peering auf die DB- Cluster zugreifen.

Im folgenden Diagramm wird dieses Szenario veranschaulicht.

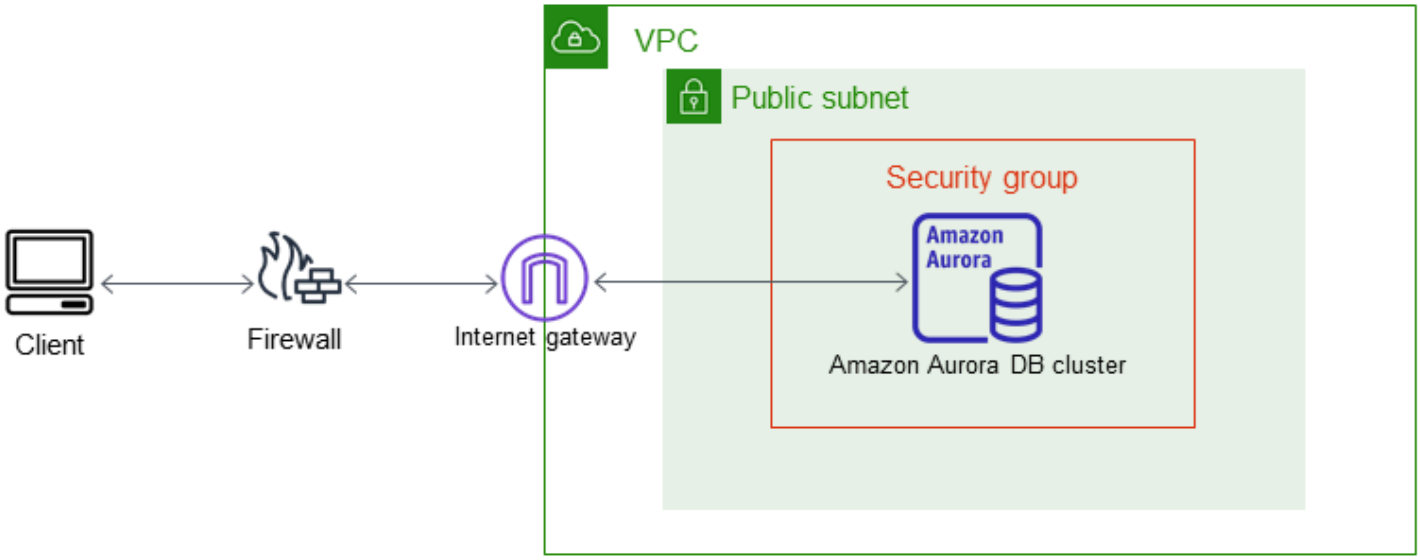


Peering: Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs. Diese ermöglicht die Weiterleitung des Datenverkehrs zwischen den VPCs mithilfe von privaten IP-Adressen. Ressourcen in jeder der VPCs können so miteinander kommunizieren, als befänden sie sich im selben Netzwerk. Sie können eine VPC-Peering-Verbindung zwischen Ihren eigenen VPCs, mit einer VPC in einem anderen AWS Konto oder mit einer VPC in einem anderen Konto herstellen. AWS-Region Weitere Informationen über VPC-Peering finden Sie unter VPC-Peering im Amazon Virtual Private Cloud-Benutzerhandbuch.

Zugriff auf eine DB-Cluster in einer VPC durch eine Client-Anwendung über das Internet

Damit eine Client-Anwendung über das Internet auf eine DB- Cluster in einer VPC zugreifen kann, konfigurieren Sie eine VPC mit einem einzelnen öffentlichen Subnetz und ein Internet-Gateway für die Kommunikation über das Internet.

Im folgenden Diagramm wird dieses Szenario veranschaulicht.



Wir empfehlen die folgende Konfiguration:

- Eine VPC der Größe /16 (z. B. CIDR: 10.0.0.0/16). Diese Größe bietet 65.536 private IP-Adressen.
- Ein Subnetz der Größe /24 (z. B. CIDR: 10.0.0.0/24). Diese Größe bietet 256 private IP-Adressen.
- Ein DB-Cluster von Amazon Aurora mit Zuordnung zur VPC und zum Subnetz. Amazon RDS weist Ihrer DB- Cluster eine IP-Adresse im Subnetz zu.
- Ein Internet-Gateway, das die VPC mit dem Internet und mit anderen AWS -Produkten verbindet.
- Eine Sicherheitsgruppe, die der DB- Cluster zugeordnet ist. Die Regeln für eingehenden Datenverkehr der Sicherheitsgruppe erlauben der Clientanwendung den Zugriff auf die DB- Cluster.

Informationen zum Erstellen einer DB- Cluster in einer VPC finden Sie unter Erstellen einer DB-Cluster in einer VPC.

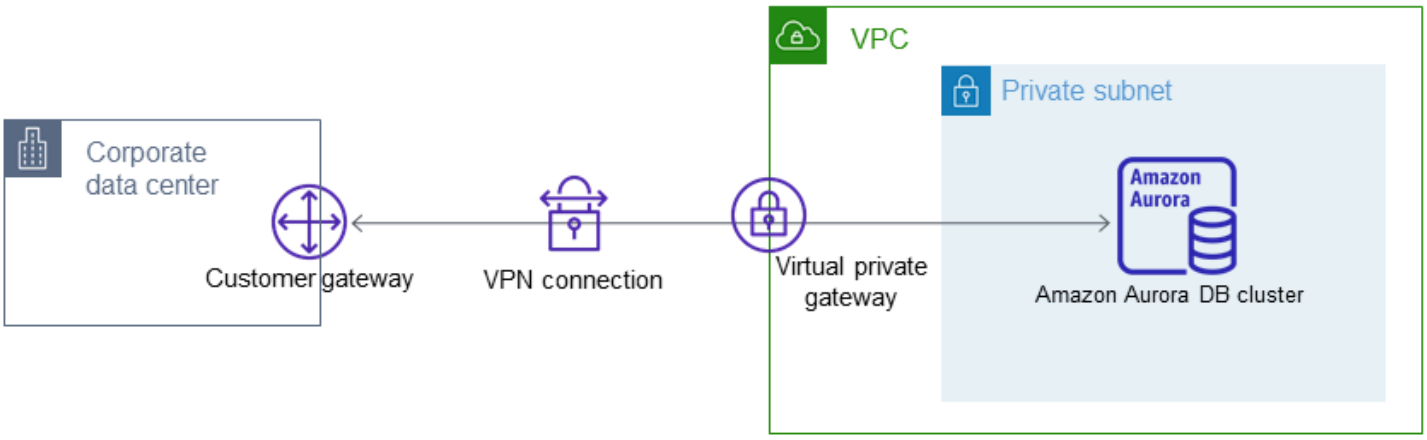
Eine DB-Cluster in einer VPC, auf die von einem privaten Netzwerk zugegriffen wird

Wenn Ihre DB- Cluster nicht öffentlich zugänglich ist, haben Sie die folgenden Optionen, um von einem privaten Netzwerk aus darauf zuzugreifen:

- Eine AWS Site-to-Site-VPN-Verbindung. Weitere Informationen finden Sie unter Was ist AWS Site-to-Site VPN?
- Eine Verbindung. AWS Direct Connect Weitere Informationen finden Sie unter Was ist AWS Direct Connect?

- Eine AWS Client VPN Verbindung. Weitere Informationen finden Sie unter Was ist AWS Client VPN?

Das folgende Diagramm zeigt ein Szenario mit einer AWS Site-to-Site-VPN-Verbindung.

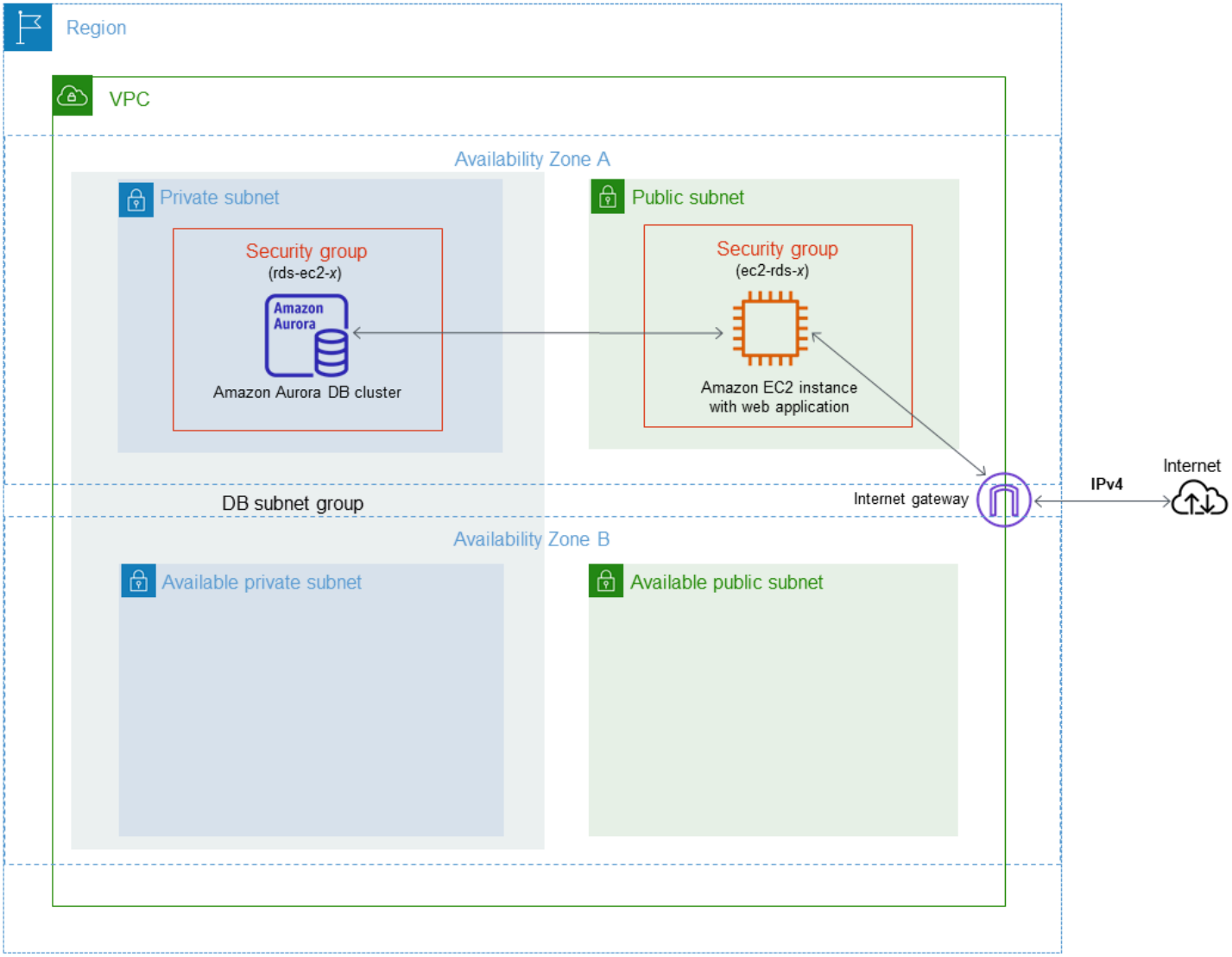


Weitere Informationen finden Sie unter Richtlinie für den Datenverkehr zwischen Netzwerken.

Tutorial: Erstellen einer VPC zur Verwendung mit einem DB-Cluster (nur IPv4)

Ein häufiges Szenario umfasst einen DB-Cluster in einer Virtual Private Cloud (VPC), die auf dem Amazon-VPC-Service basiert. Diese VPC teilt Daten mit einem Webserver, der in derselben VPC ausgeführt wird. In diesem Tutorial erstellen Sie die VPC für dieses Szenario.

Im folgenden Diagramm wird dieses Szenario veranschaulicht. Weitere Informationen zu anderen Szenarien finden Sie unter Szenarien für den Zugriff auf eine DB-Cluster in einer VPC.



Ihr DB-Cluster braucht nur für Ihren Webserver verfügbar zu sein und muss nicht vom öffentlichen Internet aus erreichbar sein. Daher erstellen Sie eine VPC sowohl mit öffentlichen als auch mit privaten Subnetzen. Der Webserver wird im öffentlichen Subnetz gehostet, damit er im öffentlichen

Internet erreicht werden kann. Der DB-Cluster wird in einem privaten Subnetz gehostet. Der Webserver kann eine Verbindung mit dem DB-Cluster herstellen, da das Hosten innerhalb derselben VPC erfolgt. Der DB-Cluster ist jedoch nicht für das öffentliche Internet verfügbar und bietet so mehr Sicherheit.

In diesem Tutorial wird ein zusätzliches öffentliches und ein privates Subnetz in einer separaten Availability Zone konfiguriert. Diese Subnetze werden im Tutorial nicht verwendet. Eine RDS-DB-Subnetzgruppe erfordert ein Subnetz in mindestens zwei Availability Zones. Das zusätzliche Subnetz erleichtert die Konfiguration von mehr als einer Aurora-DB-Instance.

In diesem Tutorial wird das Konfigurieren einer VPC für Amazon Aurora-DB-Cluster beschrieben. Ein Tutorial, das Ihnen veranschaulicht, wie Sie einen Webserver für dieses VPC-Szenario erstellen, finden Sie unter Tutorial: Erstellen eines Webservers und einer eines Amazon Aurora-DB-Clusters. Weitere Informationen zu Amazon VPC finden Sie unter Amazon-VPC-Handbuch „Erste Schritte“ und Amazon-VPC-Benutzerhandbuch.

> **Tip**
>
> Sie können die Netzwerkkonnektivität zwischen einer Amazon-EC2-Instance und einem DB-Cluster automatisch einrichten, wenn Sie den DB-Cluster erstellen. Die Netzwerkkonfiguration ähnelt der in diesem Tutorial beschriebenen Konfiguration. Weitere Informationen finden Sie unter Automatische Netzwerkkonnektivität mit einer EC2-Instance konfigurieren.

Erstellen einer VPC mit privaten und öffentlichen Subnetzen

Verwenden sie die folgenden Vorgänge, um eine VPC sowohl mit öffentlichen als auch mit privaten Subnetzen zu erstellen.

So erstellen Sie eine VPC und Subnetze

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie oben rechts in der AWS Management Console die Region aus, in der Sie Ihre VPC erstellen möchten. In diesem Beispiel wird die Region USA West (Oregon) verwendet.
3. Wählen Sie links oben die Option VPC-Dashboard aus. Wählen Sie Create VPC (VPC erstellen) aus, um mit dem Erstellen einer VPC zu beginnen.
4. Wählen Sie unter VPC Settings (VPC-Einstellungen) für Resources to create (Zu erstellende Ressourcen) VPC and more (VPC und mehr) aus.

5. Legen Sie für VPC settings (VPC-Einstellungen) folgende Werte fest:

   - Name tag auto-generation (Namens-Tag automatisch erstellen) – **`tutorial`**
   - IPv4 CIDR block (IPv4-CIDR-Block) – **`10.0.0.0/16`**
   - IPv6 CIDR block (IPv6-CIDR-Block) – No IPv6 CIDR block (Kein IPv6-CIDR-Block)
   - Tenancy – Default (Standard)
   - Number of Availability Zones (AZs) (Anzahl der Availability Zones (AZs) – 2
   - Customize AZs (AZs anpassen) – Übernehmen Sie die Standardwerte.
   - Number of public subnet (Anzahl der öffentlichen Subnetze) – 2
   - Number of private subnets (Anzahl der privaten Subnetze) – 2
   - Customize subnets CIDR blocks (CIDR-Blöcke für Subnetze anpassen) – Übernehmen Sie die Standardwerte.
   - NAT gateways ($) (NAT-Gateways ($)) – None (Keine)
   - VPC endpoints (VPC-Endpunkte) – None (Keine)
   - DNS options (DNS-Optionen) – Übernehmen Sie die Standardwerte.

6. Wählen Sie Create VPC aus.

Erstellen einer VPC-Sicherheitsgruppe für einen öffentlichen Webserver

Als Nächstes erstellen Sie eine Sicherheitsgruppe für öffentlichen Zugriff. Wenn Sie eine Verbindung mit öffentlichen EC2-Instances in Ihrer VPC herstellen möchten, fügen Sie Ihrer VPC-Sicherheitsgruppe Regeln für eingehenden Datenverkehr hinzu. Diese ermöglichen die Verbindung des Datenverkehrs aus dem Internet.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC Dashboard (VPC-Dashboard), Security Groups (Sicherheitsgruppen) und anschließend Create security group (Sicherheitsgruppe erstellen).
3. Legen Sie auf der Seite Create security group (Sicherheitsgruppe erstellen) die folgenden Werte fest:

   - Security group name (Name der Sicherheitsgruppe: **`tutorial-securitygroup`**
   - Description (Beschreibung: **`Tutorial Security Group`**

- VPC: Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-***identifier*** (tutorial-vpc)

4. Fügen Sie der Sicherheitsgruppe Regeln für den eingehenden Datenverkehr hinzu.

   a. Legen Sie die IP-Adresse fest, die für die Verbindung mit EC2-Instances in Ihrer VPC mit Secure Shell (SSH) verwendet werden soll. Um Ihre öffentliche IP-Adresse zu ermitteln, können Sie in einem anderen Browserfenster oder einer anderen Registerkarte den Service unter https://checkip.amazonaws.com verwenden. Ein Beispiel für eine IP-Adresse ist `203.0.113.25/32`.

      In vielen Fällen können Sie eine Verbindung über einen Internetdienstanbieter (ISP) oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen. Suchen Sie in diesem Fall den Bereich der IP-Adressen, die von Client-Computern verwendet werden.

      > **Warning**
      >
      > Wenn Sie `0.0.0.0/0` für SSH-Zugriff verwenden, ermöglichen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen Instances. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Für die Produktion wird nur eine bestimmte IP-Adresse bzw. ein bestimmter Adressbereich für den Zugriff auf Ihre Instances autorisiert.

   b. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

   c. Legen Sie die folgenden Werte für Ihre neue eingehende Regel fest, um SSH den Zugriff auf Ihre Amazon-EC2-Instance zu erlauben. Dann können Sie eine Verbindung mit Ihrer Amazon-EC2-Instance herstellen, um den Webserver und andere Hilfsprogramme zu installieren. Außerdem stellen Sie eine Verbindung mit Ihrer EC2-Instance her, um Inhalte für Ihren Webserver hochzuladen.

      - Typ: **`SSH`**
      - Quelle: Die IP-Adresse bzw. der IP-Bereich aus Schritt a, zum Beispiel: **`203.0.113.25/32`**.

   d. Wählen Sie Add rule.

   e. Stellen Sie die folgenden Werte für Ihre neue eingehende Regel ein, um HTTP-Zugriff auf Ihren Webserver zuzulassen:

      - Typ: **`HTTP`**

- Quelle: **`0.0.0.0/0`**

5. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus, um die Sicherheitsgruppe zu erstellen.

   Notieren Sie sich die Sicherheitsgruppen-ID, da Sie sie später in diesem Tutorial benötigen.

Erstellen einer VPC-Sicherheitsgruppe für einen privaten DB-Cluster

Erstellen Sie eine zweite Sicherheitsgruppe für privaten Zugriff, um Ihren DB-Cluster privat zu halten. Um eine Verbindung mit privaten DB-Clustern in Ihrer VPC herzustellen, fügen Sie eingehende Regeln zu Ihrer VPC-Sicherheitsgruppe hinzu, die ausschließlich Verbindungen von Ihrem Webserver zulassen.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC Dashboard (VPC-Dashboard), Security Groups (Sicherheitsgruppen) und anschließend Create security group (Sicherheitsgruppe erstellen).
3. Legen Sie auf der Seite Create security group (Sicherheitsgruppe erstellen) die folgenden Werte fest:

   - Security group name (Name der Sicherheitsgruppe: **`tutorial-db-securitygroup`**
   - Description (Beschreibung: **`Tutorial DB Instance Security Group`**
   - VPC: Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-***`identifier`*** (tutorial-vpc)

4. Fügen Sie der Sicherheitsgruppe Regeln für den eingehenden Datenverkehr hinzu.

   a. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

   b. Legen Sie die folgenden Werte für Ihre neue eingehende Regel fest, um MySQL-Datenverkehr von Ihrer Amazon-EC2-Instance an Port 3306 zuzulassen. In diesem Fall können Sie von Ihrem Webserver eine Verbindung mit Ihrem DB-Cluster herstellen. Auf diese Weise können Sie Daten aus Ihrer Webanwendung in Ihre Datenbank abrufen und dort speichern.

      - Typ: **`MySQL/Aurora`**
      - Source (Quelle): Die Kennung der Sicherheitsgruppe tutorial-securitygroup, die Sie zuvor in diesem Tutorial erstellt haben, z. B. sg-9edd5cfb.

5. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus, um die Sicherheitsgruppe zu erstellen.

Erstellen einer DB-Subnetzgruppe

Eine DB-Subnetzgruppe ist eine Sammlung von Subnetzen, die Sie in einer VPC erstellen und anschließend den DB-Clustern zuweisen. Mithilfe einer DB-Subnetzgruppe können Sie beim Erstellen von DB-Clustern eine bestimmte VPC festlegen.

Erstellen einer DB-Sicherheitsgruppe

1. Identifizieren Sie die privaten Subnetze für Ihre Datenbank in der VPC.

   a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
   b. Wählen Sie VPC Dashboard (VPC-Dashboard) und dann Subnets (Subnetze) aus.
   c. Beachten Sie die Subnetz-IDs der Subnetze mit den Namen tutorial-subnet-private1-us-west-2a und tutorial-subnet-private2-us-west-2b.

      Sie benötigen die Subnetz-IDs, wenn Sie Ihre DB-Subnetzgruppe erstellen.
2. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

   Stellen Sie sicher, dass Sie eine Verbindung mit der Amazon-RDS-Konsole herstellen, nicht mit der Amazon-VPC-Konsole.
3. Wählen Sie im Navigationsbereich Subnetzgruppe aus.
4. Wählen Sie Create DB subnet group (DB-Subnetzgruppe erstellen) aus.
5. Legen Sie auf der Seite DB-Subnetzgruppe erstellen unter Subnetzgruppendetails die folgenden Werte fest:

   - Name (Name: **`tutorial-db-subnet-group`**
   - Description (Beschreibung: **`Tutorial DB Subnet Group`**
   - VPC: tutorial-vpc (vpc-***`identifier`***)
6. Wählen Sie im Abschnitt Subnetze hinzufügen die Availability Zones und Subnetze aus.

   Wählen Sie für dieses Tutorial us-west-2a und us-west-2b als Availability Zones aus. Wählen Sie für Subnets (Subnetze) die privaten Subnetze aus, die Sie im vorherigen Schritt identifiziert haben.
7. Wählen Sie Create (Erstellen) aus.

Ihre neue DB-Subnetzgruppe wird in der Liste der DB-Subnetzgruppen in der RDS-Konsole angezeigt. Sie können die DB-Subnetzgruppe auswählen und unten im Detailbereich ausführliche Informationen anzeigen. Diese Informationen umfassen alle Subnetze, die der Gruppe zugeordnet sind.

> **Note**
>
> Wenn Sie diese VPC zum Vervollständigen von Tutorial: Erstellen eines Webservers und einer eines Amazon Aurora-DB-Clusters erstellt haben, erstellen Sie den DB-Cluster, indem Sie die Anweisungen unter Erstellen eines Amazon Aurora-DB-Clusters befolgen.

Löschen der VPC

Nachdem Sie die VPC und andere Ressourcen für dieses Tutorial erstellt haben, können Sie sie löschen, wenn sie nicht mehr benötigt werden.

> **Note**
>
> Wenn Sie in der VPC, die Sie für dieses Tutorial erstellt haben, Ressourcen hinzugefügt haben, müssen Sie diese möglicherweise löschen, bevor Sie die VPC löschen können. Zu diesen Ressourcen können beispielsweise Amazon-EC2-Instances oder DB-Cluster von Amazon RDS. Weitere Informationen finden Sie unter Löschen Ihrer VPC im Amazon VPC User Guide.

So löschen Sie eine VPC und zugehörige Ressourcen

1. Löschen Sie die DB-Subnetzgruppe.
   a. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
   b. Wählen Sie im Navigationsbereich Subnetzgruppe aus.
   c. Wählen Sie die DB-Subnetzgruppe aus, die Sie löschen möchten.tutorial-db-subnet-groupaus.
   d. Wählen Sie Löschen, und wählen Sie dann im Bestätigungsfenster Löschen.
2. Notieren Sie die VPC ID.

a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
b. Wählen Sie VPC Dashboard und dann VPCs.
c. Suchen Sie in der Liste die von Ihnen erstellte VPC, z. B.tutorial-vpc.
d. Notieren Sie die VPC ID (VPC-ID) der VPC, die Sie erstellt haben. Sie benötigen die VPC-ID in späteren Schritten.

3. Löschen der Sicherheitsgruppe.

a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
b. Wählen Sie VPC Dashboard und dann Sicherheitsgruppen.
c. Wählen Sie die Sicherheitsgruppe für die Amazon RDS-DB-Instance aus, z. B.tutorial-db-securitygroupaus.
d. Wählen Sie unter Actions (Aktionen) Delete security groups (Sicherheitsgruppen löschen) und dann Delete (Löschen) auf der Bestätigungsseite aus.
e. Klicken Sie auf derSicherheitsgruppendie Sicherheitsgruppe für die Amazon EC2 Instance aus, z. B.tutorial-securitygroupaus.
f. Wählen Sie unter Actions (Aktionen) Delete security groups (Sicherheitsgruppen löschen) und dann Delete (Löschen) auf der Bestätigungsseite aus.

4. Löschen der VPC.

a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
b. Wählen Sie VPC Dashboard und dann VPCs.
c. Wählen Sie die VPC aus, die Sie löschen möchten, z. B.tutorial-vpcaus.
d. Wählen Sie unter Actions (Aktionen) die Option Delete VPC (VPC löschen) aus.

   Auf der Bestätigungsseite werden weitere Ressourcen angezeigt, die der VPC zugeordnet sind, die ebenfalls gelöscht werden, einschließlich der damit verknüpften Subnetze.
e. Geben Sie auf der Bestätigungsseite **`delete`** ein, und wählen Sie die Option Delete (Löschen) aus.

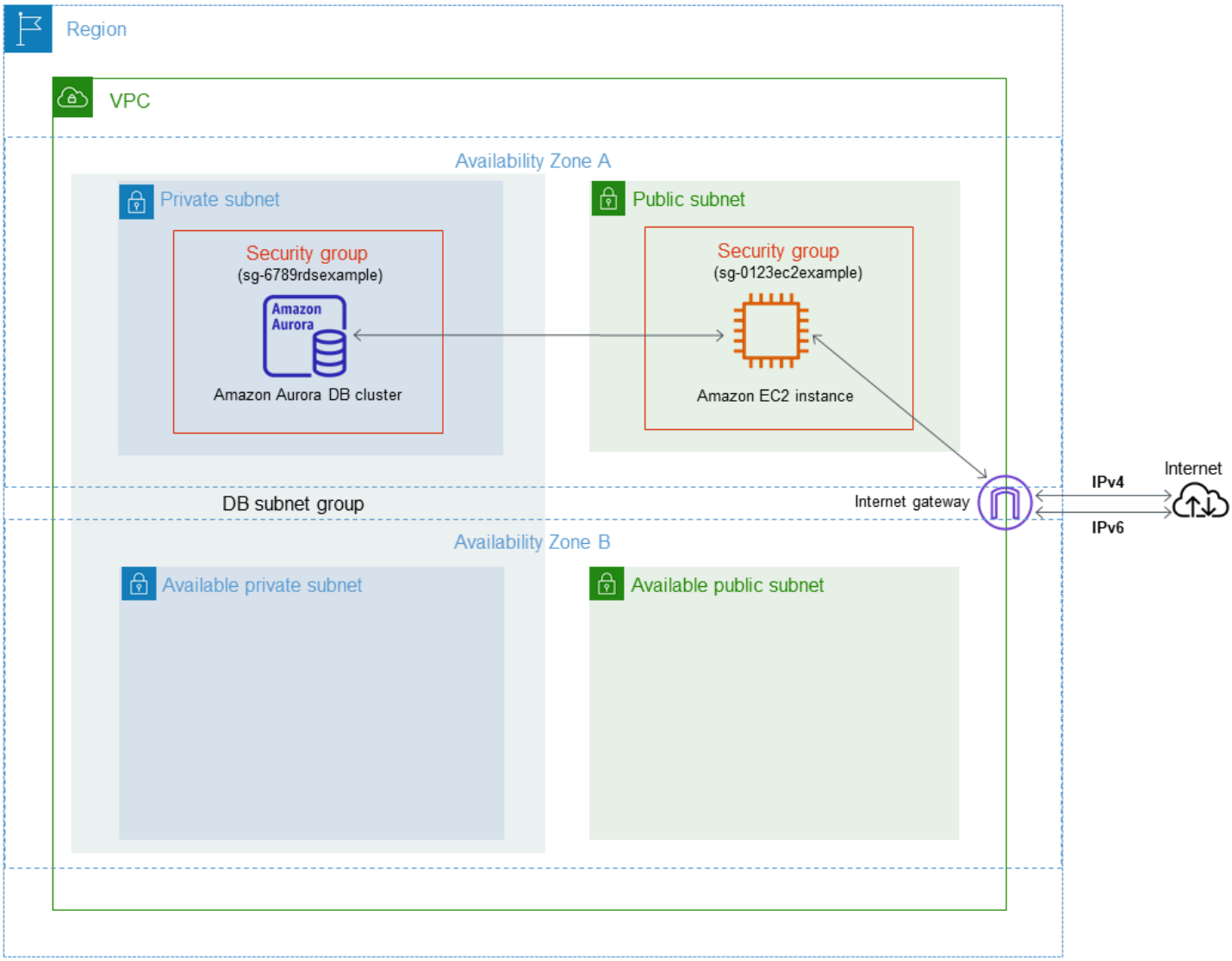
Tutorial: Erstellen einer VPC zur Verwendung mit einer DB–einem DB-Cluster (Dual-Stack-Modus)

Ein häufiges Szenario umfasst einen DB-Cluster in einer Virtual Private Cloud (VPC), die auf dem Amazon-VPC-Service basiert. Diese VPC teilt Daten mit einer öffentlichen Amazon-EC2-Instance, die in derselben VPC ausgeführt wird.

In diesem Tutorial erstellen Sie die VPC für dieses Szenario, die mit einer Datenbank arbeitet, die im Dual-Stack-Modus ausgeführt wird. Dual-Stack-Modus, um eine Verbindung über das IPv6-Adressierungsprotokoll zu ermöglichen. Weitere Informationen über die IP-Adressierung finden Sie unter Amazon-Aurora-IP-Adressierung.

Dual-Stack-Netzwerk-Cluster werden in den meisten Regionen unterstützt. Weitere Informationen finden Sie unter Verfügbarkeit von Dual-Stack-Netzwerk-DB-Cluster. Informationen zu den Einschränkungen des Dual-Stack-Modus finden Sie unter Einschränkungen für Dual-Stack-Netzwerk-DB-Cluster.

Im folgenden Diagramm wird dieses Szenario veranschaulicht.



Weitere Informationen zu anderen Szenarien finden Sie unter [Szenarien für den Zugriff auf eine DB-Cluster in einer VPC](#).

Ihr DB-Cluster muss nur für Ihre Amazon-EC2-Instance verfügbar sein und nicht im öffentlichen Internet. Daher erstellen Sie eine VPC sowohl mit öffentlichen als auch mit privaten Subnetzen. Die Amazon-EC2-Instance wird im öffentlichen Subnetz gehostet, damit sie im öffentlichen Internet erreicht werden kann. Der DB-Cluster wird in einem privaten Subnetz gehostet. Die Amazon-EC2-Instance kann eine Verbindung mit dem DB-Cluster herstellen, da sie innerhalb derselben VPC gehostet wird. Der DB-Cluster ist jedoch nicht für das öffentliche Internet verfügbar und bietet so mehr Sicherheit.

In diesem Tutorial wird ein zusätzliches öffentliches und ein privates Subnetz in einer separaten Availability Zone konfiguriert. Diese Subnetze werden im Tutorial nicht verwendet. Eine RDS DB-

Subnetzgruppe erfordert ein Subnetz in mindestens zwei Availability Zones. Das zusätzliche Subnetz erleichtert die Konfiguration von mehr als einer Aurora-DB-Instance.

Zum Erstellen eines DB-Clusters, der den Dual-Stack-Modus verwendet, geben Sie Dual-stack mode (Dual-Stack-Modus) für die Einstellung Network type (Netzwerktyp) ein. Sie können einen DB-Cluster mit der gleichen Einstellung auch ändern. Weitere Informationen zum Erstellen eines DB-Clusters finden Sie unter Erstellen eines Amazon Aurora-DB Clusters. Weitere Informationen über das Ändern eines DB-Clusters finden Sie unter Ändern eines Amazon Aurora-DB-Clusters.

In diesem Tutorial wird das Konfigurieren einer VPC für Amazon Aurora-DB-Cluster beschrieben. Weitere Informationen zur Amazon VPC-Sicherheit finden Sie im Amazon VPC-Benutzerhandbuch.

Erstellen einer VPC mit privaten und öffentlichen Subnetzen

Verwenden sie die folgenden Vorgänge, um eine VPC sowohl mit öffentlichen als auch mit privaten Subnetzen zu erstellen.

So erstellen Sie eine VPC und Subnetze

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie in der oberen rechten Ecke von die Region aus AWS Management Console, in der Sie Ihre VPC erstellen möchten. In diesem Beispiel wird die Region USA Ost (Ohio) verwendet.
3. Wählen Sie links oben die Option VPC-Dashboard aus. Wählen Sie Create VPC (VPC erstellen) aus, um mit dem Erstellen einer VPC zu beginnen.
4. Wählen Sie unter VPC Settings (VPC-Einstellungen) für Resources to create (Zu erstellende Ressourcen) VPC and more (VPC und mehr) aus.
5. Legen Sie für die übrigen VPC settings (VPC-Einstellungen) folgende Werte fest:

   - Name tag auto-generation (Namens-Tag automatisch erstellen) – **`tutorial-dual-stack`**
   - IPv4 CIDR block (IPv4-CIDR-Block) – **`10.0.0.0/16`**
   - IPv6 CIDR block (IPv6-CIDR-Block) – Amazon-provided IPv6 CIDR block (Von Amazon bereitgestellter IPv6-CIDR-Block)
   - Tenancy – Default (Standard)
   - Number of Availability Zones (AZs) (Anzahl der Availability Zones (AZs) – 2
   - Customize AZs (AZs anpassen) – Übernehmen Sie die Standardwerte.
   - Number of public subnet (Anzahl der öffentlichen Subnetze) – 2
   - Number of private subnets (Anzahl der privaten Subnetze) – 2

- Customize subnets CIDR blocks (CIDR-Blöcke für Subnetze anpassen) – Übernehmen Sie die Standardwerte.
- NAT gateways ($) (NAT-Gateways ($)) – None (Keine)
- Egress only internet gateway (Internet-Gateway nur für ausgehenden Datenverkehr) – No (Nein)
- VPC endpoints (VPC-Endpunkte) – None (Keine)
- DNS options (DNS-Optionen) – Übernehmen Sie die Standardwerte.

> **Note**
>
> Amazon RDS erfordert mindestens zwei Subnetze in zwei verschiedenen Availability Zones, um Multi-AZ-Bereitstellungen von DB-Instances zu unterstützen. In diesem Tutorial wird eine Single-AZ-Bereitstellung erstellt, aber die Anforderung erleichtert die spätere Konvertierung in eine Multi-AZ-Bereitstellung von DB-Instances.

6. Wählen Sie VPC erstellen aus.

Erstellen einer VPC-Sicherheitsgruppe für eine öffentliche Amazon-EC2-Instance

Als Nächstes erstellen Sie eine Sicherheitsgruppe für öffentlichen Zugriff. Wenn Sie eine Verbindung mit öffentlichen EC2-Instances in Ihrer VPC herstellen möchten, fügen Sie Ihrer VPC-Sicherheitsgruppe eingehende Regeln hinzu, die Verbindungen aus dem Internet zulassen.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC Dashboard (VPC-Dashboard), Security Groups (Sicherheitsgruppen) und anschließend Create security group (Sicherheitsgruppe erstellen).
3. Legen Sie auf der Seite Create security group (Sicherheitsgruppe erstellen) die folgenden Werte fest:

   - Security group name (Name der Sicherheitsgruppe: **`tutorial-dual-stack-securitygroup`**
   - Description (Beschreibung: **`Tutorial Dual-Stack Security Group`**

- VPC: Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-***identifier*** (tutorial-dual-stack-vpc)

4. Fügen Sie der Sicherheitsgruppe Regeln für den eingehenden Datenverkehr hinzu.

   a. Legen Sie die IP-Adresse fest, die für die Verbindung mit EC2-Instances in Ihrer VPC mit Secure Shell (SSH) verwendet werden soll.

      Ein Beispiel für eine Internet Protocol Version 4 (IPv4)-Adresse ist `203.0.113.25/32`. Ein Beispiel für einen Internet Protocol Version 6 (IPv6)-Adressbereich ist `2001:db8:1234:1a00::/64`.

      In vielen Fällen können Sie eine Verbindung über einen Internetdienstanbieter (ISP) oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen. Suchen Sie in diesem Fall den Bereich der IP-Adressen, die von Client-Computern verwendet werden.

      > **Warning**
      >
      > Wenn Sie `0.0.0.0/0` für IPv4 oder `::0` für IPv6 verwenden, lassen Sie für alle IP-Adressen den Zugriff auf Ihre öffentlichen Instances mit SSH zu. Dieser Ansatz ist zwar für kurze Zeit in einer Testumgebung zulässig, aber für Produktionsumgebungen sehr unsicher. Autorisieren Sie in Produktionsumgebungen nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre Instances.

   b. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

   c. Legen Sie die folgenden Werte für Ihre neue eingehende Regel fest, um Secure Shell (SSH) den Zugriff auf Ihre Amazon-EC2-Instance zu erlauben. In diesem Fall können Sie eine Verbindung mit Ihrer EC2-Instance herstellen, um SQL-Clients und andere Anwendungen zu installieren. Geben Sie eine IP-Adresse an, damit Sie auf Ihre EC2-Instance zugreifen können:

      - Typ: **SSH**
      - Source (Quelle): Die IP-Adresse bzw. der IP-Bereich aus Schritt a. Ein Beispiel für eine IPv4-IP-Adresse ist **203.0.113.25/32**. Ein Beispiel für eine IPv6-IP-Adresse ist **2001:DB8::/32**.

5. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus, um die Sicherheitsgruppe zu erstellen.

Notieren Sie sich die Sicherheitsgruppen-ID, da Sie sie später in diesem Tutorial benötigen.

Erstellen einer VPC-Sicherheitsgruppe für einen privaten DB-Cluster

Erstellen Sie eine zweite Sicherheitsgruppe für privaten Zugriff, um Ihren DB-Cluster privat zu halten. Um eine Verbindung mit privaten DB-Clustern in Ihrer VPC herzustellen, fügen Sie Regeln für eingehenden Datenverkehr zu Ihrer VPC-Sicherheitsgruppe hinzu. Diese lassen ausschließlich Datenverkehr von Ihrer Amazon-EC2-Instance zu.

So erstellen Sie eine VPC-Sicherheitsgruppe

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC Dashboard (VPC-Dashboard), Security Groups (Sicherheitsgruppen) und anschließend Create security group (Sicherheitsgruppe erstellen).
3. Legen Sie auf der Seite Create security group (Sicherheitsgruppe erstellen) die folgenden Werte fest:

   - Security group name (Name der Sicherheitsgruppe: **`tutorial-dual-stack-db-securitygroup`**
   - Description (Beschreibung: **`Tutorial Dual-Stack DB Instance Security Group`**
   - VPC: Wählen Sie die VPC aus, die Sie zuvor erstellt haben, zum Beispiel: vpc-***`identifier`*** (tutorial-dual-stack-vpc)
4. Fügen Sie der Sicherheitsgruppe Regeln für den eingehenden Datenverkehr hinzu:

   a. Wählen Sie im Abschnitt Eingehende Regeln die Option Regel hinzufügen aus.

   b. Legen Sie die folgenden Werte für Ihre neue eingehende Regel fest, um MySQL-Datenverkehr von Ihrer Amazon-EC2-Instance an Port 3306 zuzulassen. In diesem Fall können Sie von Ihrer EC2-Instance eine Verbindung mit Ihrem DB-Cluster herstellen. Dies bedeutet, dass Sie Daten aus Ihrer EC2-Instance an Ihre Datenbank senden können.

      - Type (Typ) MySQL/Aurora
      - Source (Quelle): Die Kennung der Sicherheitsgruppe tutorial-dual-stack-securitygroup, die Sie zuvor in diesem Tutorial erstellt haben, z. B. sg-9edd5cfb.
5. Um die Sicherheitsgruppe zu erstellen, wählen Sie Sicherheitsgruppe erstellen aus.

Erstellen einer DB-Subnetzgruppe

Eine DB-Subnetzgruppe ist eine Sammlung von Subnetzen, die Sie in einer VPC erstellen und anschließend den DB-Clustern zuweisen. Mit einer DB-Subnetzgruppe können Sie beim Erstellen von DB-Clustern eine bestimmte VPC angeben. Wenn Sie eine DB-Sicherheitsgruppe erstellen möchten, die mit DUAL kompatibel ist, müssen alle Subnetze mit DUAL kompatibel sein. Um mit DUAL kompatibel zu sein, muss einem Subnetz ein IPv6 CIDR zugeordnet sein.

Erstellen einer DB-Sicherheitsgruppe

1. Identifizieren Sie die privaten Subnetze für Ihre Datenbank in der VPC.

   a. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.

   b. Wählen Sie VPC Dashboard (VPC-Dashboard) und dann Subnets (Subnetze) aus.

   c. Beachten Sie die Subnetz-IDs der Subnetze mit den Namen tutorial-dual-stack-subnet-private1-us-west-2a und tutorial-dual-stack-subnet-private2-us-west-2b.

      Sie benötigen die Subnetz-IDs, wenn Sie Ihre DB-Subnetzgruppe erstellen.

2. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

   Stellen Sie sicher, dass Sie eine Verbindung mit der Amazon-RDS-Konsole herstellen, nicht mit der Amazon-VPC-Konsole.

3. Wählen Sie im Navigationsbereich Subnetzgruppe aus.

4. Wählen Sie Create DB subnet group (DB-Subnetzgruppe erstellen) aus.

5. Legen Sie auf der Seite DB-Subnetzgruppe erstellen unter Subnetzgruppendetails die folgenden Werte fest:

   - Name (Name: **`tutorial-dual-stack-db-subnet-group`**
   - Description (Beschreibung: **`Tutorial Dual-Stack DB Subnet Group`**
   - VPC: tutorial-dual-stack-vpc ***`(vpc-Kennung)`***

6. Wählen Sie im Abschnitt Add subnets (Subnetze hinzufügen) Werte für die Availability Zones und Subnets (Subnetze) aus.

   Wählen Sie für dieses Tutorial us-east-2a und us-east-2b als Availability Zones aus. Wählen Sie für Subnets (Subnetze) die privaten Subnetze aus, die Sie im vorherigen Schritt identifiziert haben.

7. Wählen Sie Create (Erstellen) aus.

Ihre neue DB-Subnetzgruppe wird in der Liste der DB-Subnetzgruppen in der RDS-Konsole angezeigt. Sie können die DB-Subnetzgruppe auswählen, um ihre Details anzuzeigen. Dazu gehören die unterstützten Adressierungsprotokolle und alle Subnetze, die mit der Gruppe verknüpft sind, sowie der von der DB-Subnetzgruppe unterstützte Netzwerktyp.

Erstellen einer Amazon-EC2-Instance im Dual-Stack-Modus

Um eine Amazon EC2 EC2-Instance zu erstellen, folgen Sie den Anweisungen unter Starten einer Instance mithilfe des Assistenten zum Starten einer Instance im Amazon EC2 EC2-Benutzerhandbuch.

Legen Sie auf der Seite Configure Instance Details (Konfigurieren von Instance-Detail)s wie im Folgenden gezeigt die folgenden Werte fest und behalten Sie die Standardwerte für die anderen Werte bei:

- Network (Netzwerk) – Wählen Sie eine vorhandene VPC mit öffentlichen und privaten Subnetzen aus, z. B. tutorial-dual-stack-vpc (vpc-*identifier*), die in Erstellen einer VPC mit privaten und öffentlichen Subnetzen erstellt wurde.
- Subnetz — Wählen Sie ein vorhandenes öffentliches Subnetz aus, z. B. subnet- ***identifier*** | tutorial-dual-stack-subnet -public1-us-east-2a | us-east-2a, erstellt in. Erstellen einer VPC-Sicherheitsgruppe für eine öffentliche Amazon-EC2-Instance
- Auto-assign Public IP (Öffentliche IP-Adresse automatisch zuweisen) – Wählen Sie Enable (Aktivieren) aus.
- Auto-assign IPv6 IP (IPv6-IP automatisch zuweisen) – Wählen Sie Enable (Aktivieren) aus.
- Firewall (security groups) (Firewall (Sicherheitsgruppen)) – Wählen Sie Select an existing security group (Eine vorhandene Sicherheitsgruppe auswählen) aus.
- Common security groups (Allgemeine Sicherheitsgruppen) – Wählen Sie eine vorhandene Sicherheitsgruppe aus, z. B. die Gruppe `tutorial-securitygroup`, die Sie in Erstellen einer VPC-Sicherheitsgruppe für eine öffentliche Amazon-EC2-Instance erstellt haben. Stellen Sie sicher, dass die von Ihnen gewählte Sicherheitsgruppe Regeln für eingehenden Datenverkehr für Secure Shell (SSH) und HTTP-Zugriff enthält.

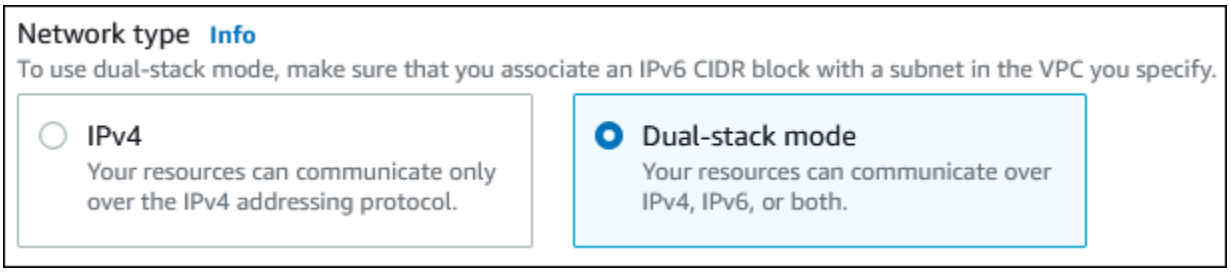
Erstellen eines DB-Clusters im Dual-Stack-Modus

In diesem Schritt erstellen Sie einen DB-Cluster zum Ausführen im Dual-Stack-Modus.

So erstellen Sie eine DB-Instance

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der oberen rechten Ecke der Konsole den Ort aus, AWS-Region an dem Sie den erstellen möchten. In diesem Beispiel wird die Region USA Ost (Ohio) verwendet.
3. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
4. Wählen Sie Create database (Datenbank erstellen) aus.
5. Stellen Sie auf der Seite Create database (Datenbank erstellen), die nachfolgend dargestellt ist, sicher, dass die Option Standard create (Standarderstellung) ausgewählt ist, und wählen Sie dann den DB-Engine-Typ Aurora MySQL aus.
6. Legen Sie im Abschnitt Connectivity folgende Werte fest:

   - Network type (Netzwerktyp) – Wählen Sie Dual-stack mode (Dual-Stack-Modus) aus.

   - Virtual Private Cloud (VPC) Wählen Sie eine vorhandene VPC mit öffentlichen und privaten Subnetzen aus, z. B. tutorial-dual-stack-vpc (vpc-*identifier*), die in Erstellen einer VPC mit privaten und öffentlichen Subnetzen erstellt wurde.

     Die VPC muss Subnetze in verschiedenen Availability Zones haben.

   - DB Subnet group (DB-Subnetzgruppe) – Wählen Sie eine DB-Subnetzgruppe für die VPC aus, z. B. tutorial-dual-stack-db-subnet-group, die in Erstellen einer DB-Subnetzgruppe erstellt wurde.
   - Public access (Öffentlicher Zugriff) – Wählen Sie No (Nein) aus.
   - VPC security group (firewall) (VPC-Sicherheitsgruppe (Firewall)) – Wählen Sie Choose existing (Vorhandene auswählen) aus.
   - Existing VPC security groups (Vorhandene VPC-Sicherheitsgruppen) – Wählen Sie eine vorhandene VPC-Sicherheitsgruppe aus, die für den privaten Zugriff konfiguriert ist, z. B. tutorial-dual-stack-db-securitygroup, die in Erstellen einer VPC-Sicherheitsgruppe für einen privaten DB-Cluster erstellt wurde.

Entfernen Sie andere Sicherheitsgruppen wie die Standardsicherheitsgruppe, indem Sie das jeweilige X wählen.

- Availability Zone – Wählen Sie us-west-2a aus.

  Um AZ-übergreifenden Datenverkehr zu vermeiden, stellen Sie sicher, dass sich die DB-Instance und die EC2-Instance in derselben Availability Zone befinden.

7. In den übrigen Abschnitten geben Sie die Einstellungen für Ihren DB-Cluster an. Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Einstellungen für Aurora-DB-Cluster.

Herstellen einer Verbindung mit Ihrer Amazon-EC2-Instance und dem DB-Cluster

Nachdem Ihre Amazon-EC2-Instance und den DB-Cluster im Dual-Stack-Modus erstellt wurden, können Sie sich über das IPv6-Protokoll mit jeder einzelnen Instance verbinden. Um mithilfe des IPv6-Protokolls eine Verbindung zu einer Amazon EC2 EC2-Instance herzustellen, folgen Sie den Anweisungen unter Connect to your Linux Instance im Amazon EC2 EC2-Benutzerhandbuch.

Um von der Amazon-EC2-Instance aus eine Verbindung zu Ihrem Aurora-MySQL-DB-Cluster herzustellen, folgen Sie den Anweisungen unter Verbindung mit einem DB-Cluster von Aurora MySQL herstellen.

Löschen der VPC

Nachdem Sie die VPC und andere Ressourcen für dieses Tutorial erstellt haben, können Sie sie löschen, wenn sie nicht mehr benötigt werden.

Wenn Sie in der VPC, die Sie für dieses Tutorial erstellt haben, Ressourcen hinzugefügt haben, müssen Sie diese möglicherweise löschen, bevor Sie die VPC löschen können. Beispiele für Ressourcen sind Amazon-EC2-Instances oder DB-Cluster. Weitere Informationen finden Sie unter Löschen Ihrer VPC im Amazon VPC User Guide.

So löschen Sie eine VPC und zugehörige Ressourcen

1. Löschen Sie die DB-Subnetzgruppe:

   a. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

   b. Wählen Sie im Navigationsbereich Subnetzgruppe aus.

c. Wählen Sie die DB-Subnetzgruppe aus, die Sie löschen möchten, z. B. tutorial-db-subnet-group.

d. Wählen Sie Löschen, und wählen Sie dann im Bestätigungsfenster Löschen.

2. Notieren Sie sich die VPC-ID.

a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

b. Wählen Sie VPC Dashboard und dann VPCs.

c. Suchen Sie die von Ihnen erstellte VPC in der Liste, z. B. tutorial-dual-stack-vpc.

d. Notieren Sie den Wert VPC ID (VPC-ID) der VPC, die Sie erstellt haben. Sie benötigen diese VPC-ID in den nachfolgenden Schritten.

3. Löschen der Sicherheitsgruppen:

a. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.

b. Wählen Sie VPC Dashboard und dann Sicherheitsgruppen.

c. Wählen Sie die Sicherheitsgruppe für die Amazon-RDS-DB-Instance aus, z. B. tutorial-dual-stack-db-securitygroup.

d. Wählen Sie unter Actions (Aktionen) Delete security groups (Sicherheitsgruppen löschen) und dann Delete (Löschen) auf der Bestätigungsseite aus.

e. Wählen Sie auf der Seite Security Groups (Sicherheitsgruppen) die Sicherheitsgruppe für die Amazon-EC2-Instance aus, z. B. tutorial-dual-stack-securitygroup.

f. Wählen Sie unter Actions (Aktionen) Delete security groups (Sicherheitsgruppen löschen) und dann Delete (Löschen) auf der Bestätigungsseite aus.

4. Löschen des NAT-Gateways:

a. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.

b. Wählen Sie VPC Dashboard und dann NAT Gateways.

c. Wählen Sie das NAT-Gateway der VPC aus, die Sie erstellt haben. Verwenden Sie die VPC-ID, um das richtige NAT-Gateway zu identifizieren.

d. Wählen Sie unter Actions (Aktionen) die Option Delete NAT gateway (NAT-Gateway löschen) aus.

e. Geben Sie auf der Bestätigungsseite **`delete`** ein, und wählen Sie die Option Delete (Löschen) aus.

5. Löschen der VPC:

a. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
b. Wählen Sie VPC Dashboard und dann VPCs.
c. Wählen Sie die VPC aus, die Sie löschen möchten, z. B.tutorial-dual-stack-vpc.
d. Wählen Sie unter Actions (Aktionen) die Option Delete VPC (VPC löschen) aus.

   Auf der Bestätigungsseite werden weitere Ressourcen angezeigt, die der VPC zugeordnet sind, die ebenfalls gelöscht werden, einschließlich der damit verknüpften Subnetze.
e. Geben Sie auf der Bestätigungsseite **`delete`** ein, und wählen Sie die Option Delete (Löschen) aus.

6. Freigeben der Elastic-IP-Adressen:

a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
b. Klicken Sie aufEC2-DashboardKlicken Sie auf und danach aufElastische IP-Adressenaus.
c. Wählen Sie die Elastic-IP-Adresse aus, die Sie freigeben möchten.
d. Wählen Sie unter Actions (Aktionen) die Option Release Elastic IP addresses (Elastic-IP-Adressenfreigeben) aus.
e. Wählen Sie auf der Bestätigungsseite Freigeben.

Kontingente und Beschränkungen für Amazon Aurora

Im Folgenden finden Sie eine Beschreibung der Ressourcenkontingente und Benennungseinschränkungen für Amazon Aurora.

Themen

Kontingente in Amazon Aurora

Jedes AWS Konto hat für jede AWS Region Kontingente für die Anzahl der Amazon Aurora Aurora-Ressourcen, die erstellt werden können. Nachdem das Kontingent für eine Ressource erreicht wurde, schlagen zusätzliche Aufrufe zum Erstellen dieser Ressource mit einer Ausnahme fehl.

In der folgenden Tabelle sind die Ressourcen und ihre Kontingente pro AWS Region aufgeführt.

Name	Standard	Anpas	Beschreibung
Autorisierungen pro DB-Sicherheitsgruppe	Jede unterstützte Region: 20	Nein	Anzahl der Sicherheitsgruppenberechtigungen pro DB-Sicherheitsgruppe
Kundenspezifische Motorversionen	Jede unterstützte Region: 40	Ja	Die maximale Anzahl von benutzerdefinierten Engine-Versionen, die in diesem Konto in der aktuellen Region zulässig sind
DB-Cluster-Parametergruppen	Jede unterstützte Region: 50	Nein	Die maximale Anzahl von DB-Cluster-Parametergruppen
DB-Cluster	Jede unterstützte Region: 40	Ja	Die maximale Anzahl von Aurora-Clustern

Name	Standard	Anpas	Beschreibung
			in diesem Konto in der aktuellen Region
DB-Instances	Jede unterstützte Region: 40	Ja	Die maximale Anzahl von DB-Instances, die in diesem Konto in der aktuellen Region zulässig ist
DB-Subnetzgruppen	Jede unterstützte Region: 50	Ja	Die maximale Anzahl von DB-Subnetzgruppen
Größe des HTTP-Anforderungstexts der Daten-API	Jede unterstützte Region: 4 Megabyte	Nein	Die maximal zulässige Größe für den HTTP-Anforderungstext.
Maximale Anzahl gleichzeitiger Cluster-Geheimnis-Paare der Daten-API	Jede unterstützte Region: 30	Nein	Die maximale Anzahl eindeutiger Paare von Aurora Serverless v1-DB-Clustern und Geheimnissen in gleichzeitigen Daten-API-Anfragen für dieses Konto in der aktuellen AWS Region.

Name	Standard	Anpas	Beschreibung
Maximale Anzahl gleichzeitiger Daten-API-Anforderungen	Jede unterstützte Region: 500	Nein	Die maximale Anzahl von Daten-API-Anfragen an einen Aurora Serverless v1-DB-Cluster, die dasselbe Geheimnis verwenden und gleichzeitig verarbeitet werden können. Zusätzliche Anforderungen werden in die Warteschlange gestellt und verarbeitet, sobald in Bearbeitung befindliche Anforderungen abgeschlossen sind.
Maximale Ergebnissatzgröße der Daten-API	Jede unterstützte Region: 1 Megabyte	Nein	Die maximale Größe der Datenbank-Ergebnismenge, die von der Daten-API zurückgegeben werden kann.
Maximale Daten-API-Größe der JSON-Antwortzeichenfolge	Jede unterstützte Region: 10 Megabyte	Nein	Die maximale Größe der vereinfachten JSON-Antwortzeichenfolge, die von der RDS-Daten-API zurückgegeben wird.

Name	Standard	Anpas	Beschreibung
Daten-API-Anforderungen pro Sekunde	Jede unterstützte Region: 1000 pro Sekunde	Nein	Die maximale Anzahl von Anfragen an die Daten-API pro Sekunde, die für dieses Konto in der aktuellen AWS Region zulässig ist. Dieses Kontingent gilt nur für Amazon Aurora Serverless v1-Cluster.
Ereignisabonnements	Jede unterstützte Region: 20	Ja	Die maximale Anzahl von Ereignisabonnements
IAM-Rollen pro DB-Cluster	Jede unterstützte Region: 5	Yes (Ja)	Die maximale Anzahl von IAM-Rollen, die mit einem DB-Cluster verknüpft werden können
IAM-Rollen pro DB-Instance	Jede unterstützte Region: 5	Yes (Ja)	Die maximale Anzahl von IAM-Rollen, die mit einer DB-Instance verknüpft werden können
Manuelle DB-Cluster-Snapshots	Jede unterstützte Region: 100	Yes (Ja)	Die maximale Anzahl manueller DB-Cluster-Snapshots
Manuelle DB-Instance-Snapshots	Jede unterstützte Region: 100	Yes (Ja)	Die maximale Anzahl manueller DB-Instance-Snapshots
Optionsgruppen	Jede unterstützte Region: 20	Ja	Die maximale Anzahl von Optionsgruppen
Parametergruppen	Jede unterstützte Region: 50	Ja	Die maximale Anzahl von Parametergruppen

Name	Standard	Anpas	Beschreibung
Proxys	Jede unterstützte Region: 20	Ja	Die maximale Anzahl von Proxys, die für dieses Konto in der aktuellen Region zulässig sind AWS
Read Replicas pro Primary	Jede unterstützte Region: 15	Ja	Die maximale Anzahl von Lesereplikaten pro primäre DB-Instance. Dieses Kontingent kann für Amazon Aurora nicht angepasst werden.
Reservierte DB-Instances	Jede unterstützte Region: 40	Ja	Die maximale Anzahl reservierter DB-Instan ces, die für dieses Konto in der aktuellen Region zulässig sind AWS
Regeln pro Sicherheitsgruppe	Jede unterstützte Region: 20	Nein	Die maximale Anzahl von Regeln pro DB-Sicher heitsgruppe
Sicherheitsgruppen	Jede unterstützte Region: 25	Ja	Die maximale Anzahl von DB-Sicherheitsgruppen
Sicherheitsgruppen (VPC)	Jede unterstützte Region: 5	Nein	Die maximale Anzahl von DB-Sicherheitsgruppen pro Amazon VPC
Subnetze pro DB-Subnetzgruppe	Jede unterstützte Region: 20	Nein	Die maximale Anzahl von Subnetzen pro DB-Subnetzgruppe

Name	Standard	Anpas	Beschreibung
Tags pro Ressource	Jede unterstützte Region: 50	Nein	Die maximale Anzahl von Tags pro Amazon-RDS-Ressource
Gesamtspeicher für alle DB-Instances	Jede unterstützte Region: 100 000 Gigabyte	Ja	Der maximale Gesamtspeicher (in GB) von EBS-Volumes für alle Amazon-RDS-DB-Instances zusammen. Dieses Kontingent gilt nicht für Amazon Aurora, das ein maximales Cluster-Volumen von 128 TiB für jeden DB-Cluster hat.

Note

Standardmäßig ist das Verwenden von bis zu insgesamt 40 DB-Instances möglich. RDS-DB-Instances, Aurora DB-Instances, Amazon Neptune-Instances und Amazon DocumentDB-Instances werden zu diesem Kontingent hinzugerechnet.
Wenn Ihre Anwendung mehr DB-Instances benötigt, können Sie zusätzliche DB-Instances anfordern, indem Sie die Konsole für Service Quotas öffnen. Wählen Sie im Navigationsbereich AWS -Services aus. Wählen Sie Amazon Relational Database Service (Amazon RDS) sowie ein Kontingent aus und folgen Sie den Anweisungen, um eine Kontingenterhöhung anzufordern. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service Quotas-Benutzerhandbuch.
Backups, AWS Backup die von verwaltet werden, gelten als manuelle DB-Cluster-Snapshots, werden aber nicht auf das Kontingent für manuelle Cluster-Snapshots angerechnet. Informationen dazu AWS Backup finden Sie im AWS Backup Entwicklerhandbuch.

Wenn Sie RDS-API-Operationen verwenden und das Standardkontingent für die Anzahl von Aufrufen pro Sekunde überschreiten, gibt die Amazon-RDS-API eine Fehlermeldung ähnlich der folgenden aus.

ClientError: Beim Aufrufen der Operation *API_Name* ist ein Fehler aufgetreten (ThrottlingException): Rate überschritten.

Reduzieren Sie in diesem Fall die Anzahl der Aufrufe pro Sekunde. Das Kontingent soll die meisten Anwendungsfälle abdecken. Wenn höhere Kontingente benötigt werden, können Sie eine Erhöhung des Kontingents beantragen, indem Sie eine der folgenden Optionen verwenden:

- Öffnen Sie von der Konsole aus die Service Quotas Quotas-Konsole.
- Verwenden Sie von der AWS CLI aus den request-service-quota-increase AWS CLI Befehl.

Weitere Informationen zu diesem Service finden Sie im Benutzerhandbuch für Service Quotas.

Benennungseinschränkungen in Amazon Aurora

In der folgenden Tabelle werden die Benennungseinschränkungen in Amazon Aurora beschrieben.

Ressource oder Element	Einschränkungen
DB Cluster ID	Für IDs gelten diese Namenseinschränkungen: • Sie müssen 1–63 alphanumerische Zeichen oder Bindestriche enthalten. • Muss mit einem Buchstaben beginnen. • Darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten. • Muss für alle DB-Instances pro AWS Konto und AWS Region eindeutig sein.
Initiale Datenbank Name	Die Beschränkungen für Datenbanknamen sind zwischen Aurora MySQL und PostgreSQL unterschiedlich. Weitere Informationen finden Sie in den verfügbaren Einstellu ngen beim Erstellen jedes DB Clusters.
Masterbenutzername	Die für den Hauptbenutzernamen geltenden Einschrän kungen sind bei jeder Datenbank-Engine unterschiedlich. Weitere Informationen finden Sie in den verfügbaren Einstellungen beim Erstellen jedes DB Clusters.

Ressource oder Element	Einschränkungen
Hauptpasswort	Das Passwort für den Master-Benutzer der Datenbank kann jedes druckbare ASCII-Zeichen außer `/`, `'`, `"`, `@` oder Leerzeichen enthalten. Für Oracle ist & eine zusätzliche Zeichenbeschränkung. Das Passwort hat die folgende Anzahl druckbarer ASCII-Zeichen abhängig von der DB-Engine: • Aurora MySQL 8–41 • Aurora PostgreSQL 8–99
Name der DB-Parametergruppe	Diese Namen haben diese Einschränkungen: • Sie müssen 1–255 alphanumerische Zeichen enthalten. • Muss mit einem Buchstaben beginnen. • Bindestriche sind erlaubt, aber der Name darf nicht mit einem Bindestrich enden oder zwei aufeinanderfolgende Bindestriche enthalten.
DB-Subnetzgruppenname	Diese Namen haben diese Einschränkungen: • Müssen 1–255 Zeichen enthalten. • Alphanumerische Zeichen, Leerzeichen, Bindestriche, Unterstriche und Punkte sind erlaubt.

Amazon Aurora-Größenbeschränkungen

Beschränkungen der Speichergröße

Ein Aurora Cluster-Volume kann für die folgenden Engine-Versionen auf eine maximale Größe von 128 tebibytes (TiB) anwachsen:

- Alle verfügbaren Aurora-MySQL-3-Versionen; Aurora-MySQL-Version 2, Versionen 2.09 und höher
- Alle verfügbaren Aurora-PostgreSQL-Versionen

Bei niedrigeren Engine-Versionen ist die maximale Größe eines Aurora-Cluster-Volume 64 TiB. Weitere Informationen finden Sie unter Wie sich die Größe des Aurora-Speichers automatisch ändert.

Sie können die `AuroraVolumeBytesLeftTotal`-Metrik verwenden, um den verbleibenden Speicherplatz zu überwachen. Weitere Informationen finden Sie unter Metriken auf Clusterebene für Amazon Aurora.

Beschränkungen der SQL-Tabellengröße

Bei einem Aurora MySQL-DB-Cluster beträgt die maximale Tabellengröße 64 Tebibyte (TiB). Bei einem Aurora PostgreSQL-DB-Cluster beträgt die maximale Tabellengröße 32 Tebibyte (TiB). Wir empfehlen Ihnen, beim Designen der Tabellen die bewährten Methoden zu befolgen, z. B. bei der Partitionierung von großen Tabellen.

Grenzen der Tabellenraum-ID

Die maximale Tabellenraum-ID für Aurora MySQL ist 2147483647. Wenn Sie häufig Tabellen erstellen und löschen, achten Sie auf Ihre Tabellenraum-IDs und planen Sie die Verwendung logischer Dumps. Weitere Informationen finden Sie unter Logische Migration von MySQL zu Amazon Aurora MySQL mithilfe von mysqldump.

Fehlerbehebung für Amazon Aurora

Verwenden Sie die folgenden Abschnitte, um Probleme zu beheben, die Sie mit DB-Instances in Amazon RDS und Amazon Aurora haben.

Themen

Informationen über das Beheben von Problemen mithilfe der Amazon RDS-API finden Sie unter Fehlerbehebung für Anwendungen in Aurora.

Verbindung zur Amazon RDS-DB-Instance kann nicht hergestellt werden

Wenn Sie keine Verbindung zu einer DB-Instance herstellen können, sind die folgenden Punkte häufige Ursachen:

- Regeln für eingehenden Datenverkehr – Die von Ihrer lokalen Firewall erzwungenen Zugriffsregeln und die für den Zugriff auf Ihre DB-Instance autorisierten IP-Adressen stimmen möglicherweise nicht überein. Das Problem sind höchstwahrscheinlich die Regeln für eingehenden Datenverkehr in Ihrer Sicherheitsgruppe.

  Standardmäßig erlauben DB-Instances keinen Zugriff. Zugriff wird über eine Sicherheitsgruppe gewährt, die der VPC zugeordnet ist und Datenverkehr in die und aus der DB-Instance zulässt. Fügen Sie der Sicherheitsgruppe bei Bedarf Regeln für eingehenden und ausgehenden Datenverkehr für Ihre besondere Situation hinzu. Sie können eine IP-Adresse, einen IP-Adressbereich oder eine andere VPC-Sicherheitsgruppe angeben.

> **Note**
>
> Wenn Sie eine neue Regel für eingehenden Datenverkehr hinzufügen, können Sie für Source (Quelle) die Option My IP (Meine IP) auswählen, um den Zugriff auf die DB-Instance von der in Ihrem Browser erkannten IP-Adresse zu ermöglichen.

Weitere Informationen zum Einrichten von Sicherheitsgruppen finden Sie unter Ermöglichen des Zugriffs auf den DB-Cluster in der VPC durch Erstellen einer Sicherheitsgruppe.

> **Note**
>
> Client-Verbindungen von IP-Adressen im Bereich 169.254.0.0/16 sind nicht erlaubt. Dies ist der APIPA-Bereich (Automatic Private IP Addressing), der für die Local-Link-Adressierung verwendet wird.

- Öffentliche Zugänglichkeit– Um eine Verbindung mit Ihrer DB-Instance von außerhalb der VPC herzustellen, z. B. mithilfe einer Client-Anwendung, muss der Instance eine öffentliche IP-Adresse zugewiesen sein.

  Um die Instance öffentlich zugänglich zu machen, ändern Sie sie und wählen Sie unter Public accessibility (Öffentlicher Zugriff) die Option Yes (Ja) aus. Weitere Informationen finden Sie unter Ausblenden einer DB-Clusters in einer VPC vor dem Internet.
- Port – Der Port, den Sie beim Erstellen der DB-Instance angegeben haben, kann aufgrund Ihrer lokalen Firewall-Beschränkungen nicht zum Senden oder Empfangen von Nachrichten verwendet werden. Wenden Sie sich an Ihren Netzwerkadministrator, um herauszufinden, ob Ihr Netzwerk den angegebenen Port für eingehende und ausgehende Kommunikation zulässt.
- Verfügbarkeit – Bei einer neu erstellten DB-Instance lautet ihr Status `creating`, bis die DB-Instance bereit für die Verwendung ist. Wenn sich der Status in `available` ändert, können Sie die Verbindung zur DB-Instance herstellen. Abhängig von der Größe Ihrer DB-Instance kann es bis zu 20 Minuten dauern, bevor eine Instance verfügbar ist.
- Internet-Gateway – Damit öffentlich auf eine DB-Instance zugegriffen werden kann, müssen die Subnetze in seiner DB-Subnetzgruppe über ein Internet-Gateway verfügen.

So konfigurieren Sie ein Internet-Gateway für ein Subnetz

1. Melden Sie sich bei der Amazon RDS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) und dann den Namen der DB-Instance aus.
3. Notieren Sie auf der Registerkarte Connectivity & security (Konnektivität und Sicherheit) die Werte der VPC-ID unter VPC und die Subnetz-ID unter Subnets (Subnetze).
4. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
5. Wählen Sie im Navigationsbereich Internet Gateways aus. Überprüfen Sie, ob Ihrer VPC ein Internet-Gateway angefügt ist. Falls nicht, wählen Sie Create Internet Gateway, um ein Internet-Gateway zu erstellen. Wählen Sie das Internet-Gateway aus, klicken Sie auf die Option Attach to VPC, und folgen Sie den Anleitungen, um das Gateway Ihrer VPC anzufügen.
6. Wählen Sie im Navigationsbereich die Option Subnets und dann Ihr Subnetz aus.
7. Überprüfen Sie, ob auf der Registerkarte Route Table eine Route mit `0.0.0.0/0` unter "Destination" und das Internet-Gateway für Ihre VPC unter „Target“ vorhanden ist.

   Wenn Sie eine Verbindung mit Ihrer Instance mithilfe der IPv6-Adresse herstellen, überprüfen Sie, dass eine Route für den gesamten IPv6-Datenverkehr (`::/0`) vorhanden ist, die zum Internet-Gateway führt. Andernfalls gehen Sie wie folgt vor:

   a. Wählen Sie die ID der Routing-Tabelle (rtb-xxxxxxxx) aus, um zur Routing-Tabelle zu gelangen.
   b. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten). Wählen Sie Add route (Route hinzufügen) aus, verwenden Sie `0.0.0.0/0` als Ziel und das Internet-Gateway als Ziel.

      Wählen Sie für IPv6 Add route (Route hinzufügen) aus, verwenden Sie `::/0` als Ziel und das Internet-Gateway als Ziel.
   c. Wählen Sie Save Rules (Routen speichern) aus.

   Wenn Sie versuchen, eine Verbindung mit dem IPv6-Endpunkt herzustellen, stellen Sie außerdem sicher, dass der IPv6-Adressbereich des Clients berechtigt ist, eine Verbindung mit der DB-Instance herzustellen.

Weitere Informationen finden Sie unter Arbeiten mit einer DB-Cluster in einer VPC.

Testen der Verbindung zu einer DB-Instance

Sie können Ihre Verbindung zu einer DB-Instance mit gängigen Linux- oder Microsoft Windows-Tools testen.

Sie können die Verbindung über ein Linux- oder Unix-Terminal testen, indem Sie Folgendes eingeben. Ersetzen Sie *DB-instance-endpoint* durch den Endpunkt und *port* durch den Port Ihrer DB-Instance.

```
nc -zv DB-instance-endpoint port
```

Das folgende Beispiel zeigt einen Beispielbefehl und den Rückgabewert.

```
nc -zv postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 8299

  Connection to postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 8299 port [tcp/
vvr-data] succeeded!
```

Windows-Benutzer können Telnet verwenden, um die Verbindung zu einer DB-Instance zu testen. Telnet-Aktionen werden nur zum Testen der Verbindung unterstützt. Wenn eine Verbindung erfolgreich ist, gibt die Aktion keine Nachricht zurück. Wenn eine Verbindung nicht erfolgreich ist, erhalten Sie eine Fehlermeldung wie die folgende.

```
C:\>telnet sg-postgresql1.c6c8mntfake0.us-west-2.rds.amazonaws.com 819

  Connecting To sg-postgresql1.c6c8mntfake0.us-west-2.rds.amazonaws.com...Could not
 open
  connection to the host, on port 819: Connect failed
```

Wenn Telnet-Aktionen erfolgreich sind, wurde Ihre Sicherheitsgruppe ordnungsgemäß konfiguriert.

> **Note**
>
> Internet Control Message Protocol (ICMP)-Datenverkehr, einschließlich Ping, wird von Amazon RDS nicht akzeptiert.

Fehlerbehebung bei der Verbindungsauthentifizierung

In einigen Fällen können Sie eine Verbindung mit Ihrer DB-Instance herstellen, erhalten jedoch Authentifizierungsfehler. In diesen Fällen sollten Sie das Hauptbenutzerpasswort für die DB-Instance zurücksetzen. Sie können dies tun, indem Sie die RDS-Instance ändern.

Amazon RDS-Sicherheitsprobleme

Um Sicherheitsprobleme zu vermeiden, sollten Sie niemals Ihren AWS Master-Benutzernamen und Ihr Passwort für ein Benutzerkonto verwenden. Es empfiehlt sich, Ihren Master zu verwenden AWS-Konto , um Benutzer zu erstellen und diese DB-Benutzerkonten zuzuweisen. Sie können Ihr Hauptkonto auch verwenden, um bei Bedarf andere Benutzerkonten zu erstellen.

Informationen zum Erstellen von Benutzern finden Sie unter Erstellen eines IAM-Benutzers in Ihrem AWS-Konto. Informationen zum Erstellen von Benutzern in AWS IAM Identity Center finden Sie unter Identitäten verwalten in IAM Identity Center.

Fehlermeldung „Failed to retrieve account attributes, certain console functions may be impaired (Fehler beim Abrufen von Kontoattributen, bestimmte Konsolenfunktionen können beeinträchtigt sein).“

Dieser Fehler kann verschiedene Ursachen haben. Es kann daran liegen, dass Ihrem Konto Berechtigungen fehlen oder Ihr Konto nicht ordnungsgemäß eingerichtet wurde. Wenn Ihr Konto neu ist, haben Sie möglicherweise nicht abgewartet, bis das Konto bereit ist. Wenn dies ein vorhandenes Konto ist, könnten Berechtigungen in Ihren Zugriffsrichtlinien fehlen, um bestimmte Aktionen auszuführen, wie z. B. das Erstellen einer DB-Instance. Um das Problem zu beheben, muss Ihr Administrator die erforderlichen Rollen für Ihr Konto bereitstellen. Weitere Informationen finden Sie in der IAM-Dokumentation.

Zurücksetzen des Besitzerpassworts der DB-Instance

Wenn Sie aus Ihrem DB--Cluster ausgesperrt werden, können Sie sich als Hauptbenutzer anmelden. Anschließend können Sie die Anmeldeinformationen für andere administrative Benutzer oder Rollen zurücksetzen. Wenn Sie sich nicht als Hauptbenutzer anmelden können, kann der AWS Kontoinhaber das Masterbenutzer-Passwort zurücksetzen. Weitere Informationen zu den Administratorkonten oder -rollen, die Sie möglicherweise zurücksetzen müssen, finden Sie unter Berechtigungen von Hauptbenutzerkonten.

Sie können das DB-Instance-Passwort ändern, indem Sie die Amazon RDS-Konsole, den AWS CLI Befehl modify-db-instanceoder den API-Vorgang ModifyDBInstance verwenden. Weitere Informationen zum Ändern einer DB-Instance in einen DB-Cluster finden Sie unter Ändern einer DB-Instance in einem DB-Cluster.

Ausfall oder Neustart einer Amazon RDS-DB-Instance

Ein Ausfall der DB-Instance kann auftreten, wenn eine DB-Instance neu gestartet wird. Er kann auch auftreten, wenn die DB-Instance in einen Zustand versetzt wird, der den Zugriff darauf verhindert, und wenn die Datenbank neu gestartet wird. Ein Neustart kann erfolgen, wenn Sie Ihre DB-Instance manuell neu starten. Ein Neustart kann auch auftreten, wenn Sie eine DB-Instance-Einstellung ändern, für die ein Neustart erforderlich ist, um wirksam zu werden.

Ein Neustart der DB-Instance tritt auf, wenn Sie eine Einstellung ändern, für die ein Neustart erforderlich ist, oder wenn Sie einen Neustart manuell durchführen. Ein Neustart kann sofort erfolgen, wenn Sie eine Einstellung ändern und die Änderung sofort wirksam werden soll. Oder er kann während des Wartungsfensters der DB-Instance auftreten.

Ein Neustart der DB-Instance wird sofort ausgeführt, wenn eine der folgenden Situationen eintritt:

- Sie ändern den Aufbewahrungszeitraum für Backups für eine DB-Instance von 0 auf einen Wert ungleich Null oder von einem Wert ungleich Null auf 0. Anschließend legen Sie Apply Immediately (Sofort anwenden) auf `true` fest.
- Sie ändern die DB-Instance-Klasse und Apply Immediately (Direkt anwenden) ist auf `true` eingestellt.

Ein Neustart der DB-Instance tritt während des Wartungsfensters auf, wenn eine der folgenden Situationen eintritt:

- Sie ändern den Aufbewahrungszeitraum für Backups für eine DB-Instance von 0 auf einen Wert ungleich Null oder von einem Wert ungleich Null auf 0 und Apply Immediately (Direkt anwenden) ist auf `false` festgelegt.
- Sie ändern die DB-Instance-Klasse und Apply Immediately (Direkt anwenden) ist auf `false` eingestellt.

Wenn Sie einen statischen Parameter in einer DB-Parametergruppe ändern, wird die Änderung erst wirksam, wenn die der Parametergruppe zugeordnete DB-Instance neu gestartet wird. Die Änderung

erfordert einen manuellen Neustart. Die DB-Instance wird während des Wartungsfensters nicht automatisch neu gestartet.

Amazon RDS-DB-Parameter Änderungen wirken sich nicht aus

In einigen Fällen können Sie einen Parameter in einer DB-Parametergruppe ändern, aber die Änderungen werden nicht wirksam. Wenn dies der Fall ist, müssen Sie wahrscheinlich die DB-Instance, die der DB-Parametergruppe zugeordnet ist, neu starten. Wenn Sie einen dynamischen Parameter ändern, wird die Änderung sofort wirksam. Wenn Sie einen statischen Parameter ändern, wird die Änderung erst wirksam, wenn Sie die der Parametergruppe zugeordnete DB-Instance neu starten.

Sie können eine DB-Instance mithilfe der RDS-Konsole neu starten. Oder Sie können die API-Operation `RebootDBInstance` explizit aufrufen. Sie können ohne Failover neu starten, wenn sich die DB-Instance in einer Multi-AZ-Bereitstellung befindet. Da die zugeordnete DB-Instance nach der Änderung eines statischen Parameters neu gestartet werden muss, wird das Risiko einer fehlerhaften Konfiguration gesenkt, die API-Aufrufe beeinträchtigen könnte. Ein Beispiel hierfür ist der Aufruf von `ModifyDBInstance` zur Änderung der DB-Instance-Klasse. Weitere Informationen finden Sie unter Ändern von Parametern in einer DB-Parametergruppe.

Probleme mit freisetzbarem Speicher in Amazon Aurora

Freisetzbarer Speicher ist der gesamte Random Access Memory (RAM, Arbeitsspeicher) einer DB-Instance, der der Datenbank-Engine zur Verfügung gestellt werden kann. Es ist die Summe aus dem freien Arbeitsspeicher des Betriebssystems und dem verfügbaren Puffer- und Seitencache-Speicher. Die Datenbank-Engine verwendet den größten Teil des Speichers auf dem Host, aber Betriebssystemprozesse verbrauchen ebenfalls RAM. Speicher, der derzeit der Datenbank-Engine zugewiesen oder von Betriebssystemprozessen verwendet wird, ist nicht im freisetzbaren Speicher enthalten. Wenn der Datenbank-Engine der Speicher ausgeht, kann die DB-Instance den temporären Speicherplatz nutzen, der normalerweise zum Puffern und Zwischenspeichern verwendet wird. Wie bereits erwähnt, ist dieser temporäre Speicherplatz im freisetzbaren Speicher enthalten.

Sie verwenden die `FreeableMemory` Metrik in Amazon CloudWatch , um den freien Speicher zu überwachen. Weitere Informationen finden Sie unter Übersicht über die Überwachung von Metriken in Amazon Aurora.

Wenn Ihre DB-Instance ständig wenig möglichen freien Speicher hat oder Auslagerungsbereiche verwendet, erwägen Sie, auf eine größere DB-Instance-Klasse hochzuskalieren. Weitere Informationen finden Sie unter Aurora DB-Instance-Klassen.

Sie können auch die Speichereinstellungen ändern. Beispiel: Bei Aurora MySQL können Sie die Größe des Parameters `innodb_buffer_pool_size` anpassen. Dieser Parameter ist standardmäßig auf 75 Prozent des physischen Speichers festgelegt. Weitere Tipps zur MySQL-Fehlerbehebung finden Sie unter Wie kann ich Probleme mit geringem freisetzbaren Speicher in einer Datenbank von Amazon RDS für MySQL beheben?

Bei Aurora Serverless v2 stellt `FreeableMemory` die Menge des nicht belegten Speichers dar, die verfügbar ist, wenn die Aurora Serverless v2-DB-Instance auf ihre maximale Kapazität skaliert wird. Möglicherweise haben Sie die Instance auf relativ niedrige Kapazität herunterskaliert, aber sie meldet immer noch einen hohen Wert für `FreeableMemory`, weil die Instance hochskalieren kann. Dieser Speicher ist derzeit nicht verfügbar, aber Sie können ihn bei Bedarf erhalten.

Für jede Aurora-Kapazitätseinheit (Aurora Capacity Unit, ACU), bei der die aktuelle Kapazität unter der maximalen Kapazität liegt, erhöht sich `FreeableMemory` ungefähr um 2 GiB. Daher nähert sich diese Metrik erst null, wenn die DB-Instance so hoch wie möglich hochskaliert ist.

Wenn sich diese Metrik dem Wert `0` nähert, ist die DB-Instance möglichst hoch skaliert. Sie nähert sich der Grenze des verfügbaren Speichers. Erwägen Sie, die maximale ACU-Einstellung für den Cluster zu erhöhen. Wenn sich diese Metrik dem Wert `0` nähert, erwägen Sie bei einer Reader-DB-Instance, dem Cluster weitere Reader-DB-Instances hinzuzufügen. Auf diese Weise können Sie den schreibgeschützten Teil der Workload auf mehrere DB-Instances verteilen und so die Speicherauslastung für jede Reader-DB-Instance reduzieren. Weitere Informationen finden Sie unter Wichtige CloudWatch Amazon-Metriken für Aurora Serverless v2.

Bei Aurora Serverless v1 können Sie den Kapazitätsbereich so ändern, dass mehr ACUs verwendet werden. Weitere Informationen finden Sie unter Ändern eines Aurora Serverless v1-DB-Clusters.

Replikationsprobleme mit Amazon Aurora MySQL

Einige MySQL-Replikationsprobleme gelten auch für Aurora MySQL. Sie können diese Probleme diagnostizieren und beheben.

Themen

- Diagnose und Lösung bei Verzögerungen zwischen Read Replicas (Lesereplikaten)
- Diagnose und Lösung eines Fehlers bei einer MySQL Read Replica

- Fehler „Replication stopped (Replikation gestoppt)“

Diagnose und Lösung bei Verzögerungen zwischen Read Replicas (Lesereplikaten)

Nachdem Sie ein MySQL-Lesereplikat erstellt haben und das Replikat verfügbar ist, repliziert Amazon RDS zunächst die an der Quell-DB-Instance vorgenommen Änderungen ab dem Zeitpunkt der Operation der Lesereplikaterstellung. Während dieser Phase ist die Verzögerungszeit der Replikation für das Lesereplikat größer als 0. Sie können diese Verzögerungszeit in Amazon überwachen, CloudWatch indem Sie sich die Amazon RDS-Metrik ansehen.

Diese `AuroraBinlogReplicaLag`-Metrik meldet den Wert des `Seconds_Behind_Master`-Feldes des `SHOW REPLICA STATUS`-Befehls von MySQL. Weitere Informationen finden Sie unter SHOW REPLICA STATUS-Anweisung in der MySQL-Dokumentation.

Wenn die Metrik `AuroraBinlogReplicaLag` 0 erreicht, hat das Replica den Stand der Quell-DB-Instance erreicht. Wenn die `AuroraBinlogReplicaLag` Metric auf -1 zurückgeht, ist die Replikation möglicherweise nicht aktiv. Um einen Replikationsfehler zu beheben, lesen Sie Diagnose und Lösung eines Fehlers bei einer MySQL Read Replica. Ein `AuroraBinlogReplicaLag`-Wert von -1 kann auch bedeuten, dass der `Seconds_Behind_Master`-Wert nicht bestimmt werden kann oder `NULL` ist.

> **Note**
>
> Frühere Versionen von Aurora MySQL verwenden `SHOW SLAVE STATUS` anstelle von `SHOW REPLICA STATUS`. Wenn Sie Aurora MySQL Version 1 oder 2 verwenden, verwenden Sie `SHOW SLAVE STATUS`. Verwenden Sie `SHOW REPLICA STATUS` für Aurora MySQL Version 3 und höher.

Die Metrik `AuroraBinlogReplicaLag` gibt während eines Netzwerkausfalls den Wert -1 an oder wenn ein Patch während des Wartungsfensters angewendet wird. Warten Sie in diesem Fall, bis die Netzwerkverbindung wiederhergestellt ist oder die Wartung beendet ist, bevor Sie die Metrik `AuroraBinlogReplicaLag` wieder überprüfen.

Die MySQL-Lesereplikationstechnologie ist asynchron. Daher können Sie gelegentliche Erhöhungen für die `BinLogDiskUsage`-Metrik in der Quell-DB-Instance und für die `AuroraBinlogReplicaLag`-Metrik auf dem Lesereplikat erwarten. Betrachten Sie beispielsweise

eine Situation, in der ein hohes Volumen von Schreiboperationen auf die Quell-DB-Instance parallel ausgeführt wird. Gleichzeitig werden Schreiboperationen in das Lesereplikat mit einem einzelnen I/O-Thread serialisiert. Eine solche Situation kann zu einer Verzögerung zwischen der Quell-Instance und dem Lesereplikat führen.

Weitere Informationen zu Read Replicas und MySQL finden Sie in unter Replication Implementation Details in der MySQL-Dokumentation.

Sie können die Verzögerung zwischen den Updates einer Quell-DB-Instance und den nachfolgenden Updates der Lesereplikate folgendermaßen reduzieren:

- Legen Sie für die DB-Instance-Klasse des Lesereplikats eine Speichergröße fest, die mit der Größe der Quell-DB-Instance vergleichbar ist.
- Stellen Sie sicher, dass die Parametereinstellungen in den DB-Parametergruppen, die von der Quell-DB-Instance und dem Lesereplikat verwendet werden, kompatibel sind. Weitere Informationen und ein Beispiel finden Sie zum Thema der `max_allowed_packet` Parameter im nächsten Abschnitt.
- Deaktivieren Sie den Anfrage-Cache. Bei Tabellen, die häufig geändert werden, kann die Verwendung des Anfragecaches die Replikationsverzögerung erhöhen, da der Cache häufig gesperrt und aktualisiert wird. Wenn dies der Fall ist, reduzieren Sie möglicherweise die Replikationsverzögerung durch die Deaktivierung des Anfragecaches. Sie können den Anfrage-Cache deaktivieren, indem Sie den `query_cache_type parameter` in der DB-Parametergruppe für die DB-Instance auf 0 setzen. Weitere Informationen zum Abfragecache finden Sie unter Abfragecache-Konfiguration.
- Wärmen Sie den Pufferpool auf dem Lesereplikat für InnoDB für MySQL auf. Nehmen wir beispielsweise an, Sie haben eine kleine Gruppe von Tabellen, die häufig aktualisiert werden, und Sie verwenden das InnoDB- oder XTraDB-Tabellenschema. Legen Sie in diesem Fall diese Tabellen auf dem Lesereplikat ab. Dies führt dazu, dass die Datenbank-Engine die Zeilen dieser Tabellen auf dem Datenträger durchsucht und sie dann im Pufferpool zwischenspeichert. Dieser Ansatz kann Replikatverzögerung reduzieren. Es folgt ein Beispiel.

  Für LinuxmacOS, oderUnix:

```
PROMPT> mysqldump \
    -h <endpoint> \
    --port=<port> \
    -u=<username> \
    -p <password> \
```

```
    database_name table1 table2 > /dev/null
```

Windows:

```
PROMPT> mysqldump ^
    -h <endpoint> ^
    --port=<port> ^
    -u=<username> ^
    -p <password> ^
    database_name table1 table2 > /dev/null
```

Diagnose und Lösung eines Fehlers bei einer MySQL Read Replica

Amazon RDS überwacht den Replikationsstatus Ihrer Lesereplikate. RDS aktualisiert das Feld Replication State (Replikationsstatus) der Lesereplikat-Instance auf `Error`, wenn die Replikation aus irgendeinem Grund angehalten wird. Die Einzelheiten des von den MySQL-Engines ausgelösten Fehlers finden Sie im Feld Replication Error (Replikationsfehler). Ereignisse, die den Status des Lesereplikats angeben, werden ebenfalls generiert, einschließlich RDS-EVENT-0045, RDS-EVENT-0046 und RDS-EVENT-0057. Weitere Informationen über Ereignisse und Abonnements zu Ereignissen finden Sie unter Arbeiten mit Amazon-RDS-Ereignisbenachrichtigungen. Wenn eine MySQL-Fehlermeldung zurückgegeben wird, lesen Sie den Fehler in der MySQL Fehlermeldungsdokumentation nach.

Die folgenden, allgemeinen Situationen können häufig zu Replikationsfehlern führen:

- Der Wert für den `max_allowed_packet`-Parameter für ein Lesereplikat ist niedriger als der `max_allowed_packet`-Parameter für die Quell-DB-Instance.

  Der `max_allowed_packet`-Parameter ist ein benutzerdefinierter Parameter, den Sie in einer DB-Parametergruppe festlegen können. Der `max_allowed_packet`-Parameter wird verwendet, um die maximale Größe der Data Manipulation Language (DML) anzugeben, die in der Datenbank ausgeführt werden kann. In einigen Fällen ist der `max_allowed_packet`-Wert für die Quell-DB-Instance möglicherweise größer als der `max_allowed_packet`-Wert des Lesereplikats. In diesen Fällen kann der Replikationsprozess einen Fehler ausgeben und die Replikation anhalten. Der häufigste Fehler ist `packet bigger than 'max_allowed_packet' bytes`. Sie können den Fehler beheben, indem Sie die DB-Parametergruppe der Quelle und des Lesereplikats mit denselben Parameterwerten für `max_allowed_packet` verwenden.

- Schreibvorgänge auf Tabellen in einem Lesereplikat. Wenn Sie Indizes für ein Lesereplikat erstellen, müssen Sie den `read_only`-Parameter auf 0 setzen, um die Indizes zu erstellen. Wenn Sie in Tabellen auf dem Lesereplikat schreiben, kann die Replikation unterbrochen werden.
- Die Verwendung einer nicht-transaktionalen Speicher-Engine wie MyISAM: Read Replicas erfordern eine transaktionale Speicher-Engine. Die Replikation wird nur für die folgenden Speicher-Engines unterstützt: InnoDB for MySQL oder MariaDB.

  Führen Sie zum Umwandeln einer MyISAM-Tabelle in eine InnoDB-Tabelle den folgenden Befehl aus:

  ```
  alter table <schema>.<table_name> engine=innodb;
  ```
- Verwenden von nicht-deterministischen Abfragen wie `SYSDATE()`. Weitere Informationen finden Sie unter Determination of Safe and Unsafe Statements in Binary Logging in der MySQL-Dokumentation.

Mit den folgenden Schritten können Sie Ihren Replikationsfehler beheben:

- Wenn Sie einen logischen Fehler feststellen und den Fehler sicher überspringen können, befolgen Sie die Schritte in Überspringen von Fehlern für die aktuelle Replikation. Ihre Aurora MySQL-DB-Instance muss eine Version ausführen, die das `mysql_rds_skip_repl_error`-Verfahren umfasst. Weitere Informationen finden Sie unter mysql_rds_skip_repl_error.
- Wenn ein Problem mit der Position des Binärprotokolls (Binlog) auftritt, können Sie die Replikatswiedergabeposition ändern. Bei Aurora-MySQL-Version 1 und 2 verwenden Sie dazu den Befehl `mysql.rds_next_master_log`. Bei Aurora-MySQL-Version 3 und höher verwenden Sie dazu den Befehl `mysql.rds_next_source_log`. Auf Ihrer Aurora MySQL-DB-Instance muss eine Version ausgeführt werden, die den -Befehl zum Ändern der Replikatswiedergabeposition unterstützt. Weitere Versionsinformationen finden Sie unter mysql_rds_next_master_log.
- Wenn aufgrund einer hohen DML-Last ein temporäres Leistungsproblem auftritt, können Sie den `innodb_flush_log_at_trx_commit`-Parameter in der DB-Parametergruppe auf dem Lesereplikat auf 2 stellen. Dies kann das Aufholen des Lesereplikats unterstützen, auch wenn es vorübergehend die Atomizität, die Konsistenz, die Isolation und die Haltbarkeit (Atomicity, Consistency, Isolation und Durability – ACID) verringert.
- Sie können das Lesereplikat löschen und eine Instance mit derselben DB-Instance-Kennung erstellen. Auf diese Weise bleibt der Endpunkt derselbe wie der Ihres alten Lesereplikats.

Wenn ein Replikationsfehler korrigiert wird, ändert sich der Wert unter Replication State (Replikationsstatus) zu Replicating (Replizierend). Weitere Informationen finden Sie unter Fehlerbehebung für ein Problem mit einem MySQL-Read Replica.

Fehler „Replication stopped (Replikation gestoppt)“

Wenn Sie den `mysql.rds_skip_repl_error` Befehl aufrufen, wird möglicherweise eine Fehlermeldung angezeigt, die besagt, dass die Replikation heruntergefahren oder deaktiviert ist.

Diese Fehlermeldung wird angezeigt, wenn die Replikation angehalten wird und nicht mehr neu gestartet werden kann.

Wenn Sie eine größere Anzahl von Fehlern ignorieren müssen, kann die Dauer der Verzögerung der Replikation den standardmäßigen Aufbewahrungszeitraum für binäre Protokolldateien überschreiten. In diesem Fall kann es zu einem schwerwiegenden Fehler kommen, weil binäre Protokolldateien bereinigt werden, bevor ihr Inhalt in der Replica repliziert wurde. Diese Bereinigung führt zur Beendigung der Replikation, und Sie können den Befehl `mysql.rds_skip_repl_error` nicht mehr aufrufen, um Replikationsfehler zu überspringen und zu ignorieren.

Sie können dieses Problem umgehen, indem Sie die Anzahl der Stunden erhöhen, für die binäre Protokolldateien in der Replikationsquelle beibehalten werden. Nachdem Sie die Aufbewahrungsdauer für binäre Protokolldateien verlängert haben, können Sie die Replikation neu starten und nach Bedarf den Befehl `mysql.rds_skip_repl_error` aufrufen.

Um den Aufbewahrungszeitraum für Binärprotokolle festzulegen, verwenden Sie das Verfahren mysql_rds_set_configuration. Geben Sie einen Konfigurationsparameter namens "binlog retention hours" und einen zugehörigen Wert in Stunden an, um festzulegen, wie viele Stunden binäre Protokolldateien auf dem DB-Cluster vorgehalten werden sollen (maximal 2160 Stunden = 90 Tage). Der Standardwert für Aurora MySQL ist 24 (1 Tag). Beim folgenden Beispiel wird die Aufbewahrungszeit für binäre Protokolle auf 48 Stunden festgelegt.

```
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

Amazon RDS-API-Referenz

Zusätzlich zur AWS Management Console und zur AWS Command Line Interface (AWS CLI) bietet Amazon RDS auch eine API. Mithilfe der API können Sie Aufgaben zur Verwaltung Ihrer DB-Instances und anderer Objekte in Amazon RDS automatisieren.

- Eine alphabetische Liste der API-Operationen finden Sie unter Aktionen.
- Eine alphabetische Liste der Datentypen finden Sie unter Datentypen.
- Eine Liste der häufigen Abfrageparameter finden Sie unter Häufige Parameter.
- Beschreibungen der Fehlercodes finden Sie unter Häufige Fehler.

Weitere Informationen zur AWS CLI finden Sie in der AWS Command Line Interface-Amazon-RDS-Referenz.

Themen

Verwenden der Abfrage-API

In den folgenden Abschnitten werden die Parameter und die Abfrageauthentifizierung beschrieben, die für die Abfrage-API verwendet werden.

Allgemeine Informationen zur Funktionsweise der Abfrage-API finden Sie unter Abfrageanforderungen im Amazon EC2 API Reference.

Abfrageparameter

HTTP-Query-basierte Anfragen sind HTTP-Anfragen, die das HTTP-Verb GET oder POST und einen Query-Parameter namens verwende `Action`.

Jede Query-Anfrage muss einige allgemeine Parameter enthalten, um die Authentifizierung und Auswahl einer Aktion zu bearbeiten.

Einige Operationen verwenden Parameterlisten. Diese Listen werden mit der Notation `param.`*n* definiert. Werte von *n* sind Ganzzahlen ab 1.

Informationen zu Amazon-RDS-Regionen und -Endpunkten finden Sie unter Amazon Relational Database Service (RDS) im Abschnitt zu Regionen und Endpunkten der Allgemeine Amazon Web Services-Referenz.

Authentifizierung von Abfrageanforderungen

Sie können Query-Anfragen nur über HTTPS senden und müssen in jede Query-Anfrage eine Signatur einschließen. Sie müssen entweder AWS-Signature Version 4 oder -Signature Version 2 verwenden. Weitere Informationen finden Sie unter Signaturprozess mit Signature Version 4 und Signaturprozess mit Signature Version 2.

Fehlerbehebung für Anwendungen in Aurora

Amazon RDS stellt spezifische und beschreibende Fehlermeldungen bereit, um Sie bei der Behebung von Problemen während der Interaktion mit der Amazon RDS-API zu unterstützen.

Themen

- Fehler bei Abrufen
- Tipps zur Problembehebung

Weitere Informationen zur Fehlerbehebung bei Amazon RDS-DB-Instances finden Sie unter Fehlerbehebung für Amazon Aurora.

Fehler bei Abrufen

In der Regel sollte Ihre Anwendung überprüfen, ob eine Anforderung einen Fehler verursacht hat, bevor Sie Zeit für die Verarbeitung von Ergebnissen aufwenden. Die einfachste Möglichkeit, herauszufinden, ob ein Fehler aufgetreten ist, besteht darin, nach einem `Error`-Knoten in der Antwort aus der Amazon RDS-API zu suchen.

Die XPath-Syntax bietet eine einfache Möglichkeit, nach einem `Error`-Knoten zu suchen. Darüber hinaus vereinfacht sie den Abruf von Fehlercode und Fehlermeldung. Der folgende Codeausschnitt verwendet Perl und das XML::XPath-Modul, um zu ermitteln, ob während einer Anfrage ein Fehler aufgetreten ist. Wenn ein Fehler aufgetreten ist, gibt der Code den ersten Fehlercode und die erste Fehlermeldung in der Antwort an.

```
use XML::XPath;
    my $xp = XML::XPath->new(xml =>$response);
```

```
    if ( $xp->find("//Error") )
    {print "There was an error processing your request:\n", " Error code: ",
    $xp->findvalue("//Error[1]/Code"), "\n", " ",
    $xp->findvalue("//Error[1]/Message"), "\n\n"; }
```

Tipps zur Problembehebung

Die folgenden Prozesse werden empfohlen, um Probleme mit der Amazon-RDS-API zu diagnostizieren und zu beheben.

- Überprüfen Sie, ob Amazon RDS in der AWS-Region normal ausgeführt wird, indem Sie http://status.aws.amazon.com aufrufen.
- Überprüfen Sie die Struktur Ihrer Anforderung.

  Jede Amazon RDS-Operation verfügt über eine Referenzseite in der Amazon RDS-API-Referenz. Prüfen Sie nochmals, dass Sie die Parameter korrekt verwenden. Betrachten Sie die Beispielanforderungen oder Benutzerszenarien, um zu sehen, ob ähnliche Operationen ausgeführt werden, und um eine Vorstellung von möglichen Fehlern zu erhalten.
- Prüfen Sie AWS re:Post.

  Amazon RDS besitzt ein Entwickler-Community, in der Sie nach Lösungen für Probleme suchen können, die andere Entwickler bereits hatten. Zum Anzeigen der Themen navigieren Sie zu AWS re:Post.

Dokumentverlauf

Aktuelle API-Version:2014-10-31

In der folgenden Tabelle werden wichtige Änderungen am Amazon Aurora Benutzerhandbuch beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren. Informationen zu Amazon Relational Database Service (Amazon RDS) finden Sie im Amazon Relational Database Service Benutzerhandbuch.

> **Note**
>
> Vor dem 31. August 2018 wurde Amazon Aurora im Amazon Relational Database Service Benutzerhandbuch dokumentiert. Informationen zum früheren Dokumentverlauf von Aurora finden Sie unter Dokumentverlauf im Amazon Relational Database Service-Benutzerhandbuch.

Sie können neue Amazon Aurora Funktionen auf der Was ist neu mit Datenbank?-Seite filtern. FürProdukte wählen Sie Amazon Aurora aus. Suchen Sie dann mit Schlüsselwörtern wie **`global database`** oder **`Serverless`**.

Änderung	Beschreibung	Datum
AWS Python-Treiber allgemein verfügbar	Der Amazon Web Services (AWS) Python-Treiber ist als fortschrittlicher Python-Wrapper konzipiert. Dieser Wrapper ergänzt den Open-Source-Treiber Psycopg und erweitert dessen Funktionalität. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Aurora-DB-Clustern mit den AWS Treibern.	23. Mai 2024

Zero-ETL-Integrationen sind in den Regionen Chinas verfügbar	Zero-ETL-Integrationen sind jetzt in AWS-Regionen China (Peking) und China (Ningxia) verfügbar. Weitere Informationen finden Sie unter Zero-ETL-Integrationen mit Amazon Redshift.	21. Mai 2024
RDS Proxy ist in mehr Regionen verfügbar	RDS Proxy ist jetzt in den Regionen Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Naher Osten (VAE), Israel (Tel Aviv), Kanada West (Calgary) und Europa (Zürich) verfügbar. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy.	21. Mai 2024

Amazon RDS Extended Support	Beim Erstellen oder Wiederherstellen einer Aurora MySQL Version 2 oder 3 oder Aurora PostgreSQL Version 11-Datenbank wird diese Datenbank jetzt automatisch bei Amazon RDS Extended Support registriert, sodass Ihre vorhandenen Anwendungen weiterhin so funktionieren, wie sie sind. Sie können sich vom RDS Extended Support abmelden, um Gebühren nach Ablauf des Standard-Supportdatums von Aurora für Ihre Datenbank-Engine zu vermeiden. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Extended Support.	21. März 2024
Datenfilterung für Zero-ETL-Integrationen	Amazon RDS unterstützt Datenfilterung auf Datenbank- und Tabellenebene für Zero-ETL-Integrationen mit Amazon Redshift. Weitere Informationen finden Sie unter Datenfilterung für Aurora Zero-ETL-Integrationen mit Amazon Redshift.	20. März 2024

Aurora MySQL-Integrationen mit Amazon Bedrock	Sie können jetzt Amazon Aurora MySQL-Datenbanken in Amazon Bedrock integrieren, um generative KI-Anwendungen zu unterstützen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Machine Learning mit Aurora MySQL.	8. März 2024
Neue AWS verwaltete Richtlinie	Amazon RDS hat eine neue verwaltete Richtlinie hinzugefügt `AmazonRDSCustomInstanceProfileRolePolicy`, mit der RDS Custom Automatisierungsaktionen und Datenbankverwaltungsaufgaben über ein EC2-Instance-Profil ausführen kann. Weitere Informationen finden Sie unter Änderungen von Amazon RDS an von AWS verwalteten Richtlinien.	27. Februar 2024
Amazon RDS-Unterstützung für AWS Secrets Manager die Region Israel (Tel Aviv)	Amazon RDS unterstützt Secrets Manager in der Region Israel (Tel Aviv). Weitere Informationen finden Sie unter Passwortverwaltung mit Amazon RDS und AWS Secrets Manager.	21. Februar 2024

Amazon RDS Extended Support	Amazon RDS aktiviert jetzt automatisch Amazon RDS Extended Support, wenn die wichtigsten Engine-Versionen von Aurora MySQL und Aurora PostgreSQL in Ihren DB-Clustern und globalen Clustern das Aurora-Enddatum des Standard-Supports erreichen . Weitere Informationen finden Sie unter Verwenden von Amazon RDS Extended Support.	15. Februar 2024
Aurora PostgreSQL 16.1 unterstützt Babelfish für Aurora PostgreSQL 4.0.0	Aurora PostgreSQL 16.1 unterstützt Babelfish 4.0.0. Eine Liste der neuen Funktionen finden Sie unter 16.1. Eine Liste der Funktionen, die in jeder Babelfish-Version unterstützt werden, finden Sie unter Unterstützte Funktionalität in Babelfish nach Version. Weitere Nutzungsinformationen finden Sie unter Arbeiten mit Babelfish für Aurora PostgreSQL.	31. Januar 2024
Aktualisieren Sie auf das standardmäßige CA-Zertifikat	Das Standard-CA-Zertifikat ist auf festgelegt. `rds-ca-rsa2048-g1` . Weitere Informationen finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung zu einem DB-Cluster.	26. Januar 2024

RDS Proxy ist in der Region Europa (Spanien) verfügbar	RDS Proxy ist jetzt in der Region Europa (Spanien) verfügbar. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy.	8. Januar 2024
RDS-Daten-API mit Aurora PostgreSQL Serverless v2 und bereitgestellt	Sie können jetzt die RDS-Daten-API mit Aurora PostgreSQL Serverless v2 und bereitgestellten DB-Clustern verwenden. Mit der RDS Data API können Sie über einen sicheren HTTP-Endpunkt auf Ihre Aurora-Cluster zugreifen und SQL-Anweisungen ausführen, ohne Datenbanktreiber zu verwenden oder Verbindungen zu verwalten. Weitere Informationen finden Sie unter Verwenden der RDS-Daten-API.	21. Dezember 2023
Aurora PostgreSQL-Integrationen mit Amazon Bedrock	Sie können jetzt Amazon Aurora PostgreSQL-Datenbanken in Amazon Bedrock integrieren, um generative KI-Anwendungen zu unterstützen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora Machine Learning mit Aurora PostgreSQL.	21. Dezember 2023

Amazon Aurora ist in der Region Kanada West (Calgary) verfügbar	Amazon Aurora ist jetzt in der Region Kanada West (Calgary) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	20. Dezember 2023
Amazon RDS unterstützt das Anzeigen und Beantworten von Empfehlungen	Amazon Aurora Aurora-Empfehlungen umfassen jetzt schwellenwertbasierte proaktive und auf maschinellem Lernen basierende reaktive Empfehlungen. Weitere Informationen finden Sie unter Amazon Aurora Aurora-Empfehlungen anzeigen und darauf reagieren.	19. Dezember 2023
Aurora PostgreSQL Zero-ETL-Integrationen mit Amazon Redshift (Vorschau)	Sie können jetzt Zero-ETL-Integrationen mit Amazon Redshift mithilfe eines Aurora PostgreSQL-Quell-DB-Clusters erstellen. Für die Vorschauversion müssen Sie alle Integrationen in der Amazon RDS Database Preview Environment im Osten der USA (Ohio) (us-east-2) erstellen. AWS-Region Weitere Informationen finden Sie unter Arbeiten mit Null-ETL-Integrationen von Aurora in Amazon Redshift.	28. November 2023

Amazon Aurora PostgreSQL unterstützt die globale Weiterleitung von Datenbank-Schreibvorgängen	Sie können jetzt die Schreibweiterleitung auf sekundären Clustern in einer globalen Datenbank auf der Grundlage von Aurora PostgreSQL aktivieren. Weitere Informationen finden Sie unter Verwenden der Schreibweiterleitung in einer globalen Aurora-PostgreSQL-Datenbank.	9. November 2023
Aurora-PostgreSQL-Unterstützung für optimierte Lesevorgänge	Mit Aurora-optimierten Lesevorgängen können Sie eine schnellere Abfrageverarbeitung mit Aurora PostgreSQL erreichen. Weitere Informationen finden Sie unter Verbesserung der Abfrageleistung für Aurora PostgreSQL mit Aurora-optimierten Lesevorgängen.	8. November 2023

Amazon RDS exportiert Performance Insights Insights-Metriken nach Amazon CloudWatch	Mit Performance Insights können Sie die vorkonfig urierten oder benutzerd efinierten Metrik-Dashboards nach Amazon exportieren. CloudWatch Die exportier ten Metrik-Dashboards können in der Konsole angezeigt werden. CloudWatc h Sie können auch ein ausgewähltes Performan ce Insights Insights-Metrik-Widget exportieren und die Metrikdaten in der CloudWatc h Konsole anzeigen. Weitere Informationen finden Sie unter Performance Insights Insights-Metriken exportieren nach CloudWatch.	8. November 2023
Allgemeine Verfügbarkeit von Aurora MySQL Null-ETL-Integrationen mit Amazon Redshift	Null-ETL-Integrationen mit Amazon Redshift sind jetzt allgemein für Aurora MySQL verfügbar. Weitere Informati onen finden Sie unter Arbeiten mit Null-ETL-Integrationen von Aurora in Amazon Redshift.	7. November 2023

Unterstützung von Aurora PostgreSQL für Blau/Grün-Bereitstellungen von RDS	Sie können jetzt eine Blau/Grün-Bereitstellung aus einem Aurora-PostgreSQL-DB-Cluster erstellen. Weitere Informationen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.	26. Oktober 2023
Aurora MySQL unterstützt serverseitige Verschlüsselung mit AWS KMS keys (SSE-KMS)	In Aurora MySQL Version 3.05 und höher können Sie SSE-KMS, einschließlich Von AWS verwaltete Schlüssel kundenverwalteter Schlüssel, für die serverseitige Verschlüsselung von Daten verwenden, die Sie aus Amazon S3 laden oder dort speichern. Weitere Informationen finden Sie unter Laden von Daten aus Textdateien in einem Amazon-S3-Bucket in einen Amazon-Aurora-MySQL-DB-Cluster und Speichern von Daten aus einem Amazon-Aurora-MySQL-DB-Cluster aus Textdateien in einem Amazon-S3-Bucket.	25. Oktober 2023

Aurora-MySQL-Optimierungen reduzieren die Neustartzeit der Datenbank	In Aurora MySQL Version 3.05 und höher haben wir Optimierungen eingeführt, die die Neustartzeit der Datenbank reduzieren. Diese Optimierungen sorgen für bis zu 65 % weniger Ausfallzeiten als ohne Optimierungen und weniger Unterbrechungen Ihrer Datenbank-Workloads nach einem Neustart. Weitere Informationen finden Sie unter Optimierungen zur Verkürzung der Datenbankneustartzeit.	25. Oktober 2023
Aktualisierung der verwalteten Richtlinien AWS	Die von `AmazonRDSPerformanceInsightsReadOnly` und `AmazonRDSPerformanceInsightsFullAccess` verwalteten Richtlinien enthalten jetzt `Sid` (Statement-ID) als Bezeichner in der Richtlinienerklärung. Weitere Informationen finden Sie unter Änderungen von Amazon RDS an von AWS verwalteten Richtlinien.	23. Oktober 2023

Amazon RDS veröffentlicht Performance Insights Insights-Zählermetriken auf Amazon CloudWatch	Die metrische Rechenfunktion DB_PERF_INSIGHTS in der CloudWatch Konsole ermöglicht es Ihnen, Amazon RDS nach Performance Insights Insights-Zählermetriken abzufragen. Weitere Informationen finden Sie unter CloudWatch Alarme zur Überwachung von Amazon Aurora erstellen.	20. September 2023
Amazon Aurora unterstützt point-in-time Recovery (PITR) mit AWS Backup	Sie können jetzt automatische (kontinuierliche) Aurora-Backups verwalten AWS Backup und von dort aus zu bestimmten Zeiten wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit mit AWS Backup.	07. September 2023
Amazon RDS Extended Support	Amazon Aurora kündigt die bevorstehende Möglichkeit an, die Engine-Hauptversionen von Aurora MySQL und Aurora PostgreSQL in Ihren DB-Instances auch nach dem Ende des Standard-Supports von Aurora weiter auszuführen. Weitere Informationen finden Sie unter Verwenden von Amazon RDS Extended Support.	1. September 2023

Amazon Aurora MySQL erweitert die Unterstützung für Percona XtraBackup	Sie können jetzt physische Migrationen von MySQL-8.0 -Datenbanken zu DB-Cluste rn in Aurora MySQL Version 3 durchführen. Weitere Informationen finden Sie unter Physische Migration von MySQL mithilfe von Percona XtraBackup und Amazon S3.	24. August 2023
Die globale Aurora-Da tenbank unterstü.tzt globales Datenbank-Failover	Die globale Aurora-Datenbank unterstützt jetzt verwaltetes globales Failover, sodass Sie sie nach einem echten regionalen Notfall oder einem vollständigen Service-Ausfall einfacher wiederherstellen können. Weitere Informati onen zu dieser Funktion finden Sie unter Ausführen von verwalteten Failovern für globale Aurora-Datenbanken .. Die Funktion, die zuvor als „verwaltetes geplantes Failover“ bezeichnet wurde, heißt jetzt „Umstellung“. Informationen zu Umstellun gen finden Sie unter Durchführ en von Umstellungen für Amazon Aurora Global Databases.	21. August 2023

Aktualisierung der AWS verwalteten Richtlinienberechtigungen	Die `AmazonRDSFullAccess` -verwaltete Richtlinie umfasst neue Berechtigungen, mit denen Sie den Leistungsanalysebericht für einen bestimmten Zeitraum erstellen, anzeigen und löschen können. Weitere Informationen finden Sie unter Amazon RDS-Updates für AWS verwaltete Richtlinien.	17. August 2023
Aktualisierung der AWS verwalteten Richtlinienberechtigungen	Das Hinzufügen neuer Berechtigungen zur `AmazonRDSPerformanceInsightsReadOnly` -verwalteten Richtlinie und das Hinzufügen einer neuen verwalteten Richtlinie `AmazonRDSPerformanceInsightsFullAccess` ermöglicht es Ihnen, einen DB-Lastanalysebericht für einen bestimmten Zeitraum zu erstellen. Weitere Informationen finden Sie unter Amazon RDS-Updates für AWS verwaltete Richtlinien.	16. August 2023

Amazon RDS unterstützt die Analyse von DB-Ladezeiträumen mit Performance Insights	Performance Insights ermöglicht Ihnen, einen Leistungsanalysebericht für einen bestimmten Zeitraum zu erstellen. Der Bericht enthält die identifizierten Einblicke und Empfehlungen zum Beheben von Leistungsproblemen. Weitere Informationen finden Sie unter Analysieren der DB-Last über einen bestimmten Zeitraum.	16. August 2023
Amazon Aurora unterstützt die Beibehaltung automatisierter Backups für DB-Cluster	Sie können jetzt automatisierte Backups für gelöschte Aurora-Cluster beibehalten und sie zu einem bestimmten Zeitpunkt wiederherstellen. Weitere Informationen finden Sie unter Beibehaltung automatisierter Backups.	4. August 2023
Amazon Aurora ist in der Region Israel (Tel Aviv) verfügbar	Amazon Aurora ist jetzt in der Region Israel (Tel Aviv) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	1. August 2023

Amazon Aurora MySQL unterstützt die lokale (clusterinterne) Schreibweiterleitung	Sie können jetzt Schreibvorgänge von einer Reader-DB-Instance an eine Writer-DB-Instance innerhalb eines DB-Clusters von Aurora MySQL weiterleiten. Weitere Informationen finden Sie unter Verwendung der Schreibweiterleitung in einem DB-Cluster von Amazon Aurora MySQL.	31. Juli 2023
Amazon Aurora unterstützt Aurora Serverless v2 zusätzlich AWS-Region	Sie können jetzt Aurora Serverless v2 DB-Cluster im asiatisch-pazifischen Raum (Melbourne) erstellen AWS-Region. Weitere Informationen zu Aurora Serverless v2 finden Sie unter Verwendung von Aurora Serverless v2.	28. Juni 2023
Amazon Aurora führt Null-ETL-Integrationen in Amazon Redshift ein (Vorschau)	Null-ETL-Integrationen bieten eine vollständig verwaltete Lösung, die Transaktionsdaten innerhalb von Sekunden, nachdem diese in einen Aurora-MySQL-DB-Cluster geschrieben wurden, in Amazon Redshift verfügbar macht. Weitere Informationen finden Sie unter Arbeiten mit Null-ETL-Integrationen von Aurora in Amazon Redshift.	28. Juni 2023

Amazon RDS bietet eine kombinierte Performance Insights- und CloudWatch Metrikansicht im Performance Insights Insights-Dashboard	Amazon RDS bietet jetzt eine konsolidierte Ansicht von Performance Insights und CloudWatch Metriken im Performance Insights Insights-Dashboard. Weitere Informationen finden Sie unter Anzeigen von kombinierten Metriken in der Amazon-RDS-Konsole.	24. Mai 2023
Amazon Aurora unterstützt die Instance-Klassen db.r7g	Sie können jetzt die Instance-Klassen vom Typ „db.r7g“ verwenden, um Aurora-DB-Cluster zu erstellen. Weitere Informationen finden Sie unter Aurora-DB-Instance-Klassen.	11. Mai 2023
Amazon Aurora unterstützt eine neue Speicherkonfiguration für DB-Cluster	Bei Aurora I/O-Optimized zahlen Sie nur für die Nutzung und Speicherung Ihrer DB-Cluster, ohne zusätzliche Gebühren für Lese- und Schreib-I/O-Operationen. Weitere Informationen finden Sie unter Speicherkonfigurationen für DB-Cluster von Amazon Aurora.	11. Mai 2023

Amazon Aurora unterstützt Aurora Serverless v2 zusätzlich AWS-Regionen	Sie können jetzt Aurora Serverless v2 DB-Cluster in den folgenden Ländern erstellen AWS-Regionen: Asien-Pazifik (Hyderabad), Europa (Spanien), Europa (Zürich) und Naher Osten (VAE). Weitere Informationen zu Aurora Serverless v2 finden Sie unter Verwendung von Aurora Serverless v2.	4. Mai 2023
Aurora Serverless v1 unterstützt die Konvertierung zu bereitgestellten Clustern	Sie können einen DB-Cluster von Aurora Serverless v1 direkt zu einem bereitgestellten DB-Cluster konvertieren. Weitere Informationen finden Sie unter Konvertieren eines DB-Clusters von Aurora Serverless v1 zu einem bereitgestellten Cluster.	27. April 2023
Aurora Serverless v1 unterstützt Amazon Aurora PostgreSQL Version 13	Sie können jetzt DB-Cluster von Aurora Serverless v1 erstellen, auf denen Aurora PostgreSQL Version 13 ausgeführt wird. Weitere Informationen finden Sie unter Aurora Serverless v1.	27. April 2023

Amazon Aurora Aurora-Unterstützung für AWS Secrets Manager die Regionen Chinas	Amazon Aurora unterstützt Secrets Manager in den Regionen China (Peking) und China (Ningxia). Weitere Informationen finden Sie unter Passwortverwaltung mit Amazon Aurora und AWS Secrets Manager.	20. April 2023
Amazon Aurora unterstützt das Veröffentlichen von Ereignissen mit Tags für Themen-Subscriber	Amazon Aurora Aurora-Ereignisbenachrichtigungen, die an Amazon Simple Notification Service (Amazon SNS) oder Amazon gesendet werden, enthalten EventBridge jetzt Ereignis-Tags im Nachrichtentext. Diese Tags liefern Daten über die Ressource, die vom Serviceereignis betroffen war. Weitere Informationen finden Sie unter Tags und Attribute von Amazon-RDS-Ereignisbenachrichtigungen.	17. April 2023
Aktualisieren auf Berechtigungen für serviceverknüpfte IAM-Rollen	Die `AmazonRDSReadOnlyAccess` Richtlinien `AmazonRDSFullAccess` und gewähren jetzt zusätzliche Berechtigungen, um die Anzeige von Amazon DevOps Guru-Ergebnissen in der RDS-Konsole zu ermöglichen. Weitere Informationen finden Sie unter Amazon RDS-Updates für AWS verwaltete Richtlinien.	30. März 2023

Amazon Aurora unterstützt globale Datenbanken in der Region Asien-Pazifik (Melbourne)	Sie können jetzt globale Aurora-Datenbanken in der Region Asien-Pazifik (Melbourne) erstellen. Weitere Informationen zu globalen Aurora-Datenbanken finden Sie unter Verwenden von globalen Amazon-Aurora-Datenbanken.	22. März 2023
Aktualisierung der AWS verwalteten Richtlinienberechtigungen	Die `AmazonRDSReadOnlyAccess` Richtlinien `AmazonRDSFullAccess` und gewähren Amazon jetzt zusätzliche Berechtigungen CloudWatch. Weitere Informationen finden Sie unter Amazon RDS-Updates für AWS verwaltete Richtlinien.	16. März 2023
RDS Proxy ist in den chinesischen Regionen verfügbar	RDS Proxy ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy.	15. März 2023
Amazon Aurora unterstützt Aurora Serverless v2 in den chinesischen Regionen	Aurora Serverless v2 ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar. Weitere Informationen finden Sie unter Aurora Serverless v2.	15. März 2023

RDS Proxy ist in der Region Asien-Pazifik (Jakarta) verfügbar	RDS Proxy ist jetzt in der Region Asien-Pazifik (Jakarta) verfügbar. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy.	08. März 2023
Amazon Aurora MySQL unterstützt die Kerberos-Authentifizierung	Sie können jetzt die Kerberos-Authentifizierung verwenden, um Benutzer zu authentifizieren, wenn sie sich mit Ihren Aurora-MySQL-DB-Clustern verbinden. Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung für Aurora MySQL.	08. März 2023
Amazon Aurora unterstützt zusätzlich globale Datenbanken AWS-Regionen	Sie können jetzt globale Aurora-Datenbanken in den folgenden Regionen erstellen: Afrika (Kapstadt), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), Asien-Pazifik (Jakarta), Europa (Mailand), Europa (Spanien), Europa (Zürich), Naher Osten (Bahrain) und Naher Osten (VAE). Weitere Informationen zu globalen Aurora-Datenbanken finden Sie unter Verwenden von globalen Amazon-Aurora-Datenbanken.	6. März 2023

Amazon Aurora unterstützt zusätzlich das Kopieren von DB-Cluster-Snapshots AWS-Regionen	Sie können jetzt DB-Cluster-Snapshots in den foglenden Regionen kopieren: Afrika (Kapstadt), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), Asien-Paz ifik (Jakarta), Asien-Paz ifik (Melbourne), Europa (Mailand), Europa (Spanien), Europa (Zürich), Naher Osten (Bahrain) und Naher Osten (VAE). Informationen zum Kopieren von DB-Cluster-Snapshots finden Sie unter Kopieren eines DB-Cluster-Snapshots.	6. März 2023
Amazon DevOps Guru for RDS unterstützt proaktive Einblicke	Amazon DevOps Guru for RDS veröffentlicht proaktive Einblicke mit Empfehlungen, die Ihnen helfen, Probleme in Ihren Aurora-Datenbanken zu beheben, bevor sie voraussic htlich auftreten. Weitere Informationen finden Sie unter So funktioniert DevOps Guru for RDS.	28. Februar 2023
Amazon-Aurora-MySQL-Version 1 ist veraltet	Aurora-MySQL-Version 1 (mit MySQL 5.6 kompatibel) ist veraltet. Weitere Informationen finden Sie unter Wie lange bleiben Amazon-Aurora-Haup tversionen verfügbar?	28. Februar 2023

Aurora Serverless v1 unterstützt die Einstellung des DB-Cluster-Wartungsfensters	Sie können jetzt das Wartungsfenster für Aurora Serverless v1-DB-Cluster festlegen. Weitere Informationen finden Sie unter Anpassen des bevorzugten DB-Cluster-Wartungsfensters.	27. Februar 2023
Amazon Aurora unterstützt Datenbank-Aktivitätsstreams in den Regionen Asien-Pazifik (Hyderabad), Europa (Spanien) und Naher Osten (VAE).	Weitere Informationen finden Sie unter Datenbankaktivitäts-Streams.	27. Januar 2023
Amazon Aurora ist in der Region Asien-Pazifik (Melbourne) verfügbar	Amazon Aurora ist jetzt in der Region Asien-Pazifik (Melbourne) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	23. Januar 2023
Angeben der Zertifizierungsstelle (CA) bei der DB-Cluster-Erstellung	Sie können jetzt bei der Erstellung des DB-Clusters angeben, welche CA für das Serverzertifikat eines DB-Clusters verwendet werden soll. Weitere Informationen finden Sie unter Zertifizierungsstellen.	5. Januar 2023

Aurora MySQL 3.*-Unterstützung für die Rückverfolgung	Aurora MySQL 3.*-Versionen unterstützen jetzt die schnelle Wiederherstellung nach Benutzerfehlern wie Löschen der falschen Tabelle oder Löschen der falschen Zeile. Mithilfe de Rückverfolgung können Sie Ihre Datenbank zu einem früheren Zeitpunkt verschieben, ohne dass eine Wiederherstellung aus einem Backup erforderlich ist. Der Vorgang ist selbst bei großen Datenbanken innerhalb weniger Sekunden abgeschlossen. Einzelheiten finden Sie unter Rückverfolgen eines Aurora-DB-Clusters.	4. Januar 2023
Verwenden Sie Amazon RDS Blue/Green Deployments, die zusätzlich verfügbar sind AWS-Regionen	Die Funktion „Blau/Grün-Bereitstellungen“ ist jetzt in den Regionen China (Peking) und China (Ningxia) verfügbar. Weitere Informationen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.	22. Dezember 2022

Aktualisieren auf Berechtigungen für serviceverknüpfte IAM-Rollen	Die ServiceRolePolicy AmazonRDS-Richtlinie gewährt jetzt zusätzliche Berechtigungen für. AWS Secrets Manager Weitere Informationen finden Sie unter Amazon RDS-Updates für AWS verwaltete Richtlinien.	22. Dezember 2022
Amazon Aurora lässt sich AWS Secrets Manager für die Passwortverwaltung integrieren	Aurora kann das Hauptbenutzerpasswort für einen DB-Cluster in Secrets Manager verwalten. Weitere Informationen finden Sie unter Passwortverwaltung mit Amazon Aurora und AWS Secrets Manager.	22. Dezember 2022
Amazon Aurora unterstützt Aurora Serverless v2 zusätzlich AWS-Regionen	Aurora Serverless v2 ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar. Weitere Informationen finden Sie unter Aurora Serverless v2.	21. Dezember 2022
Aurora PostgreSQL unterstützt RDS Proxy mit PostgreSQL 14	Sie können jetzt einen RDS-Proxy mit einem DB-Cluster von Aurora PostgreSQL 14 erstellen. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy.	13. Dezember 2022

Amazon Aurora informiert Sie über kürzlich von Amazon Guru entdeckte Anomalien DevOps	Auf der Seite mit den Datenbankdetails der Konsole werden Sie sowohl über aktuelle als auch über Anomalien informiert, die in den letzten 24 Stunden aufgetreten sind. Weitere Informationen finden Sie unter So funktioniert DevOps Guru for RDS.	13. Dezember 2022
Amazon RDS Proxy unterstützt globale Datenbanken	Sie können jetzt RDS Proxy mit globalen Aurora-Datenbanken verwenden. Weitere Informationen finden Sie unter Verwenden von RDS Proxy mit globalen Aurora-Datenbanken.	7. Dezember 2022
DB-Cluster von Aurora PostgreSQL unterstützen Trusted Language Extensions für PostgreSQL	Trusted Language Extensions für PostgreSQL ist ein Open-Source-Entwicklungskit, mit dem Sie leistungsstarke PostgreSQL-Erweiterungen erstellen und diese sicher auf Ihrem DB-Cluster von Aurora PostgreSQL ausführen können. Weitere Informationen finden Sie unter Arbeiten mit Trusted Language Extensions für PostgreSQL.	30. November 2022

Amazon GuardDuty RDS Protection überwacht auf Zugriffsbedrohungen	Wenn Sie GuardDuty RDS Protection aktivieren, verarbeitet GuardDuty RDS-Anmeldeereignisse aus Ihren Aurora-Datenbanken, überwacht diese Ereignisse und erstellt Profile für potenzielle Insider-Bedrohungen oder externe Akteure. Wenn GuardDuty RDS Protection eine potenzielle Bedrohung erkennt, GuardDuty generiert es ein neues Ergebnis mit Details über die potenziell gefährdete Datenbank. Weitere Informationen finden Sie unter Überwachen von Bedrohungen mit GuardDuty RDS Protection.	30. November 2022

Verwenden von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen	Sie können Änderungen an einem DB-Cluster in einer Staging-Umgebung vornehmen und die Änderungen testen, ohne dass sich dies auf Ihren Produktions-DB-Cluster auswirkt. Wenn Sie bereit sind, können Sie die Staging-Umgebung zur neuen Produktionsdatenbankumgebung hochstufen, wobei die Ausfallzeit minimal ist. Weitere Informationen finden Sie unter Verwendung von Blau/Grün-Bereitstellungen von Amazon RDS für Datenbankaktualisierungen.	27. November 2022
Amazon Aurora ist in der Region Asien-Pazifik (Hyderabad) verfügbar	Amazon Aurora ist jetzt in der Region Asien-Pazifik (Hyderabad) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	22. November 2022
Amazon Aurora ist in der Region Europa (Spanien) verfügbar	Amazon Aurora ist jetzt in der Region Europa (Spanien) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	16. November 2022

Amazon Aurora ist in der Region Europa (Zürich) verfügbar	Amazon Aurora ist jetzt in der Region Europa (Zürich) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	9. November 2022
Amazon Aurora unterstützt das Exportieren von Daten aus DB-Clustern nach Amazon S3	Sie können Aurora-Cluster-Daten jetzt direkt nach S3 exportieren, ohne zuerst einen Snapshot erstellen zu müssen. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Daten nach Amazon S3.	27. Oktober 2022
Amazon Aurora MySQL unterstützt schnellere Exporte nach Amazon S3	Sie können jetzt von einer bis zu zehnmal schnelleren Leistung beim Export von DB-Cluster-Snapshot-Daten nach S3 für MySQL 5.7- und 8.0-kompatible Aurora-MySQL-Cluster profitieren. Weitere Informationen finden Sie unter Exportieren von DB-Cluster-Snapshot-Daten nach Amazon S3.	20. Oktober 2022

Amazon Aurora unterstützt die automatische Einrichtung der Konnektivität zwischen einem Aurora-DB-Cluster und einer EC2-Instance	Sie können den verwenden AWS Management Console , um Konnektivität zwischen einem vorhandenen Aurora-DB-Cluster und einer EC2-Instance einzurichten. Weitere Informationen finden Sie unter Automatisches Verbinden einer EC2-Instance und eines Aurora-DB-Clusters.	14. Oktober 2022
AWS JDBC-Treiber für PostgreSQL allgemein verfügbar	Der AWS JDBC-Treiber für PostgreSQL ist ein Client-Treiber, der für Aurora PostgreSQL entwickelt wurde. Der AWS JDBC-Treiber für PostgreSQL ist jetzt allgemein verfügbar. Weitere Informationen finden Sie unter Verbindung mit dem AWS JDBC-Treiber für PostgreSQL herstellen.	6. Oktober 2022
Amazon Aurora unterstützt das direkte Upgrade für MySQL-5.7-kompatibles Aurora MySQL	Sie können ein direktes Upgrade vornehmen, um einen vorhandenen mit MySQL 5.7 kompatiblen Aurora-MySQL-Cluster in einen mit MySQL 8.0 kompatiblen Aurora-MySQL-Cluster zu ändern. Weitere Informationen finden Sie unter Upgrade von Aurora MySQL 2.x auf 3.x.	26. September 2022

Performance-Insights zeigt die 25 wichtigsten SQL-Abfragen	Auf der Registerkarte Top SQL (Top-SQL) werden die 25 SQL-Abfragen angezeigt, die am meisten zur DB-Last beitragen. Weitere Informationen finden Sie unter Übersicht über die Registerkarte „Top SQL“ (Top-SQL).	13. September 2022
Aurora MySQL unterstützt eine neue DB-Instance-Klasse	Sie können jetzt die DB-Instance-Klasse db.r6i für DB-Cluster von Aurora MySQL verwenden. Weitere Informationen finden Sie unter DB-Instance-Klassen.	13. September 2022
Amazon Aurora ist in der Region Naher Osten (VAE) verfügbar	Amazon Aurora ist jetzt in der Region Naher Osten (VAE) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	30. August 2022
Amazon Aurora unterstützt die automatische Einrichtung der Konnektivität mit einer EC2-Instance	Wenn Sie einen Aurora-DB-Cluster erstellen, können Sie den verwenden, AWS Management Console um die Konnektivität zwischen einer Amazon Elastic Compute Cloud-Instance und dem neuen DB-Cluster einzurichten. Weitere Informationen finden Sie unter Automatische Netzwerkkonnektivität mit einer EC2-Instance konfigurieren.	22. August 2022

Amazon RDS unterstützt den Dual-Stack-Modus	DB-Cluster können jetzt im Dual-Stack-Modus ausgeführt werden. Im Dual-Stack-Modus können Ressourcen mit der DB-Cluster über IPv4, IPv6 oder beidem kommunizieren. Weitere Informationen finden Sie unter Amazon Aurora-IP-Adressierung.	17. August 2022
Amazon Aurora unterstützt In-Place-Upgrade für PostgreSQL-kompatible Aurora Serverless v1	Sie können ein In-Place-Upgrade für einen PostgreSQL 10-kompatiblen Aurora Serverless v1 Cluster durchführen, um einen bestehenden Cluster in einen PostgreSQL 11-kompatiblen Aurora Serverless v1 Cluster zu verwandeln. Informationen zum In-Place-Upgrade-Verfahren finden Sie unter Ändern eines Aurora Serverless v1 DB-Clusters.	08. August 2022
Performance Insights unterstützt die Region Asien-Pazifik (Jakarta)	Bisher konnten Sie Performance Insights in der Region Asien-Pazifik (Jakarta) nicht verwenden. Diese Einschränkung wurde entfernt. Weitere Informationen finden Sie unter Support der AWS-Region für Performance Insights.	21. Juli 2022

Amazon Aurora unterstützt eine neue DB-Instance-Klasse	Sie können jetzt die db.r6i DB-Instance-Klasse für Aurora PostgreSQL DB-Cluster verwenden. Weitere Informationen finden Sie unter DB-Instance-Klassen.	14. Juli 2022
RDS Performance Insights unterstützt zusätzliche Aufbewahrungsfristen	Bisher bot Performance Insights nur zwei Aufbewahrungsfristen an: 7 Tage (Standard) oder 2 Jahre (731 Tage). Wenn Sie Ihre Leistungsdaten jetzt länger als 7 Tage aufbewahren müssen, können Sie zwischen 1 und 24 Monaten angeben. Weitere Informationen finden Sie unterPreisgestaltung und Datenspeicherung für Performance Insights.	01. Juli 2022
Amazon Aurora unterstützt das In-Place-Upgrade für MySQL-kompatible Aurora Serverless v1	Sie können ein direktes Upgrade für einen mit MySQL 5.6 kompatiblen Aurora Serverless v1-Cluster vornehmen, um einen vorhandenen Cluster in einen mit MySQL 5.7 kompatiblen Aurora Serverless v1-Cluster zu ändern. Informationen zum In-Place-Upgrade-Verfahren finden Sie unter Ändern eines Aurora Serverless v1 DB-Clusters.	16. Juni 2022

Aurora unterstützt das Einschalten von Amazon DevOps Guru in der RDS-Konsole	Sie können die DevOps Guru-Abdeckung für Ihre Aurora-Datenbanken von der RDS-Konsole aus aktivieren. Weitere Informationen finden Sie unter DevOpsGuru für RDS einrichten.	9. Juni 2022
Amazon Aurora unterstützt das Veröffentlichen von Ereignissen in verschlüsselten Amazon-SNS-Themen	Amazon Aurora kann jetzt Ereignisse in Amazon Simple Notification Service (Amazon-SNS)-Themen veröffentlichen, bei denen serversei tige Verschlüsselung (SSE) aktiviert ist, um Ereignisse, die sensible Daten enthalten , zusätzlich zu schützen. Weitere Informationen finden Sie unter Abonniere n von Amazon-RDS-Ereignisbenachrichtigungen.	1. Juni 2022
Amazon RDS veröffentlicht Nutzungsmetriken auf Amazon CloudWatch	Der `AWS/Usage` Namespace in Amazon CloudWatch enthält Nutzungsmetriken auf Kontoebene für Ihre Amazon RDS-Servicekonting enten. Weitere Informationen finden Sie unter CloudWatch Amazon-Nutzungsmetriken für Amazon Aurora.	28. April 2022

Daten-API-Ergebnissätze im JSON-Format	Ein optionaler Parameter für die Funktion `ExecuteStatement` bewirkt, dass der Abfrageergebnissatz als Zeichenfolge im JSON-Format zurückgegeben wird. Der JSON-Ergebnissatz lässt sich einfach und bequem in eine Datenstruktur in der Sprache Ihrer Anwendung umwandeln. Weitere Informationen finden Sie unter Verarbeiten von Abfrageergebnissen im JSON-Format.	27. April 2022
Amazon Aurora Serverless v2 ist jetzt allgemein verfügbar.	Amazon Aurora Serverless v2 ist für alle Benutzer allgemein verfügbar. Weitere Informationen finden Sie unter Verwendung von Aurora Serverless v2.	21. April 2022
Aurora MySQL unterstützt konfigurierbare Cipher-Suites	Mit Aurora MySQL können Sie nun konfigurierbare Cipher-Suites verwenden, um die Verbindungsverschlüsselung zu steuern, die Ihr Datenbankserver akzeptiert. Weitere Informationen finden Sie unter Konfigurieren von Cipher-Suites für Verbindungen mit Aurora-MySQL-DB-Clustern.	15. April 2022

Aurora PostgreSQL unterstützt RDS-Proxy mit PostgreSQL 13	Sie können jetzt einen RDS-Proxy mit einem Aurora PostgreSQL 13-DB-Cluster erstellen. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy.	4. April 2022
Versionshinweise für Aurora PostgreSQL	Es gibt jetzt einen separaten Leitfaden für die Versionshinweise von Amazon Aurora PostgreSQL. Weitere Informationen finden Sie unter Versionshinweise für Aurora PostgreSQL.	22. März 2022
Versionshinweise für Aurora MySQL	Es gibt jetzt einen separaten Leitfaden für die Versionshinweise von Amazon Aurora MySQL. Weitere Informationen finden Sie unter Versionshinweise für Aurora MySQL.	22. März 2022
Aurora PostgreSQL unterstützt Upgrades auf Multi-Hauptversionen	Sie können jetzt Versionsupgrades von Aurora-PostgreSQL-DB-Clustern über mehrere Hauptversionen hinweg durchführen. Weitere Informationen finden Sie unter So führen Sie ein Hauptversionsupgrade durch.	4. März 2022

Aurora PostgreSQL unterstützt konfigurierbare Cipher-Suites	Mit Aurora PostgreSQL Version 11.8 und höher können Sie jetzt konfiguri erbare Cipher-Suites verwenden, um die Verbindun gsverschlüsselung zu steuern, die Ihr Datenbankserver akzeptiert. Weitere Informati onen zur Verwendung konfigurierbarer Cipher-Suites mit Aurora PostgreSQL finden Sie unter Konfigurieren von Cipher-Suites für Verbindun gen mit Aurora-PostgreSQL-DB-Clustern.	4. März 2022
AWS JDBC-Treiber für MySQL allgemein verfügbar	Der AWS JDBC-Treiber für MySQL ist ein Client-Treiber, der für die Hochverfügbarkeit von Aurora MySQL entwickel t wurde. Der AWS JDBC-Treiber für MySQL ist jetzt allgemein verfügbar. Weitere Informationen finden Sie unter Herstellen einer Verbindun g mit dem Amazon Web Services JDBC-Treiber für MySQL.	2. März 2022

Aurora PostgreSQL 13.5 unterstützt Babelfish für Aurora PostgreSQL 1.1.0	Aurora PostgreSQL 13.5 unterstützt Babelfish 1.1.0. Eine Liste der neuen Funktionen finden Sie unter 13.5. Eine Liste der Funktionen, die in jeder Babelfish-Version unterstützt werden, finden Sie unter Unterstützte Funktionalität in Babelfish nach Version. Weitere Nutzungsinformationen finden Sie unter Arbeiten mit Babelfish für Aurora PostgreSQL.	28. Februar 2022
Amazon Aurora unterstützt Datenbank-Aktivitäts-Streams in der Region Asien-Pazifik (Jakarta)	Weitere Informationen finden Sie unter Support AWS-Regionen für Datenbankaktivitätsstreams.	16. Februar 2022
Performance Insights unterstützt neue API-Operationen	Performance Insights unterstützt die folgenden API-Operationen: `GetResourceMetadata`, `ListAvailableResourceDimensions` und `ListAvailableResourceMetrics`. Weiteren Informationen finden Sie unter Abrufen von Metriken mit der Performance Insights API in diesem Handbuch und in der Referenz zur Amazon RDS Performance Insights API.	12. Januar 2022

Amazon RDS Proxy unterstützt Ereignisse	RDS Proxy generiert jetzt Ereignisse, die Sie abonnieren und unter CloudWatch Ereignisse anzeigen oder so konfigurieren können, dass sie an Amazon gesendet EventBridge werden. Weitere Informationen finden Sie unter Arbeiten mit RDS-Proxy-Ereignissen.	11. Januar 2022
RDS Proxy ist zusätzlich erhältlich AWS-Regionen	RDS Proxy ist jetzt in den folgenden Regionen erhältlich: Afrika (Kapstadt), Asien-Pazifik (Hongkong, Osaka), Europa (Milan, Paris, Stockholm), Naher Osten (Bahrain) und Südamerika (São Paulo). Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy.	5. Januar 2022
Amazon Aurora ist in der Region Asien-Pazifik (Jakarta) verfügbar	Amazon Aurora ist jetzt in der Region Asien-Pazifik (Jakarta) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	13. Dezember 2021

DevOpsGuru for Amazon RDS bietet detaillierte Einblicke und Empfehlungen für Amazon Aurora	DevOpsGuru for RDS nutzt Performance Insights für leistungsbezogene Daten. Anhand dieser Daten analysiert der Service die Leistung Ihrer Amazon Aurora DB-Instances und kann Ihnen bei der Lösung von Leistungsproblemen helfen. Weitere Informationen finden Sie unter Analysieren von Leistungsanomalien mit DevOps Guru for RDS in diesem Handbuch und unter Überblick über DevOps Guru for RDS im Amazon DevOps Guru-Benutzerhandbuch.	1. Dezember 2021
Aurora PostgreSQL unterstützt RDS-Proxy mit PostgreSQL 12	Sie können jetzt einen RDS-Proxy mit einem Aurora PostgreSQL 12-Datenbank-Cluster erstellen. Weitere Informationen zu RDS Proxy finden Sie unter Verwenden von Amazon RDS Proxy.	22. November 2021
Aurora unterstützt AWS Graviton2-Instanzklassen für Datenbankaktivitätsstreams	Sie können Datenbank-Aktivitätsstreams mit der Instance-klasse db.r6g für Aurora MySQL und Aurora PostgreSQL verwenden. Weitere Informationen finden Sie unter Unterstützte DB-Instance-Klassen.	3. November 2021

Amazon Aurora Aurora-Unterstützung für kontoüber greifende Konten AWS KMS keys	Sie können einen KMS-Schlüssel von einem anderen AWS-Konto für die Verschlüsselung verwenden, wenn Sie DB-Snapshots nach Amazon S3 exportieren. Weitere Informationen finden Sie unter Exportieren von DB-Snapshot-Daten nach Amazon S3.	3. November 2021
Amazon Aurora unterstützt Babelfish für Aurora PostgreSQL	Babelfish for Aurora PostgreSQL erweitert Ihre Amazon Aurora PostgreSQL-kompatible Edition-Datenbank um die Möglichkeit, Datenbankverbindungen von Microsoft SQL Server-Clients zu akzeptieren. Weitere Informationen finden Sie unter Arbeiten mit Babelfish für Aurora PostgreSQL.	28. Oktober 2021
Aurora Serverless v1 kann SSL für Verbindungen benötigen	Die Aurora-Clusterparameter `force_ssl` für PostgreSQL und `require_secure_transport` für MySQL werden für Aurora Serverless v1 jetzt unterstützt. Weitere Informationen finden Sie unter Verwendung von TLS/SSL mit Aurora Serverless v1.	26. Oktober 2021

Amazon Aurora unterstützt Performance Insights zusätzlich AWS-Regionen	Performance Insights ist in den Regionen Naher Osten (Bahrain), Afrika (Kapstadt), Europa (Mailand) und Asien-Pazifik (Osaka) verfügbar. Weitere Informationen finden Sie unter Support der AWS-Region für Performance Insights.	5. Oktober 2021
Konfigurierbares Autoskalierungs-Timeout für Aurora Serverless v1	Sie können auswählen, wie lange Aurora Serverless v1 wartet, um einen Punkt für die automatische Skalierung zu finden. Wenn in diesem Zeitraum kein Autoskalierungspunkt gefunden wird, bricht Aurora Serverless v1 das Skalierungsereignis ab oder erzwingt die Kapazitätsänderung, je nach der von Ihnen ausgewählten Timeout-Aktion. Weitere Informationen finden Sie unter Autoskalierung für Aurora Serverless v1.	10 September 2021

Aurora unterstützt X2g- und T4g-Instance-Klassen	Sowohl Aurora MySQL als auch Aurora PostgreSQL können jetzt X2g- und T4g-Instance-Klassen verwenden . Die Instance-Klassen, die Sie verwenden können, hängen von der Version von Aurora MySQL oder Aurora PostgreSQL ab. Informationen zu den unterstützten Instance-Typen finden Sie unter DB-Instance-Klassen.	10. September 2021
Amazon RDS unterstützt RDS Proxy in einer gemeinsam genutzten VPC	Jetzt können Sie einen RDS Proxy in einer gemeinsam genutzten Virtual Private Cloud (VPC) erstellen. Weitere Informationen zu RDS Proxy finden Sie unter „Verwalten von Verbindungen mit Amazon RDS Proxy“ im Amazon RDS-Benutzerhandbuch oder im Aurora-Benutzerhandbuch.	6. August 2021
Aurora-Versionsrichtlinienseite	Das Amazon-Aurora-Benutzerhandbuch enthält jetzt einen Abschnitt mit allgemeinen Informationen zu Aurora-Versionen und den zugehörigen Richtlinien. Details dazu finden Sie unter Amazon-Aurora-Versionen.	14. Juli 2021

Schließt Daten-API-Ereignisse von einem AWS CloudTrail Trail aus	Sie können Daten-API-Ereignisse von einem CloudTrail Trail ausschließen. Weitere Informationen finden Sie unter Daten-API-Ereignisse aus einem AWS CloudTrail Trail ausschließen.	2. Juli 2021
Amazon Aurora PostgreSQL-kompatible Edition unterstützt zusätzliche Erweiterungen	Zu den neu unterstützten Erweiterungen gehören pg_bigm, pg_cron, pg_partman und pg_proctab. Weitere Informationen finden Sie unter Erweiterungsversionen für Amazon-Aurora-PostgreSQL-kompatible Edition.	17. Juni 2021
Klonen für Aurora Serverless-Cluster	Sie können jetzt geklonte Cluster erstellen, die Aurora Serverless sind. Weitere Informationen zum Klonen finden Sie unter Klonen eines Aurora-DB-Clusters.	16. Juni 2021
Aurora globale Datenbanken sind in China (Peking)- und China (Ningxia)-Regionen verfügbar	Sie können jetzt Aurora globale Datenbanken in den Regionen China (Peking) und China (Ningxia) erstellen. Weitere Informationen zu globalen Aurora-Datenbanken finden Sie unter Arbeiten mit globalen Amazon Aurora-Datenbanken.	19. Mai 2021

FIPS 140-2-Unterstützung für Daten-API	Die Daten-API unterstützt die Federal Information Processing Standard Publication 140-2 (FIPS 140-2) für SSL/TLS-Verbindungen. Weitere Informationen finden Sie unter Verfügbarkeit der Daten-API .	14. Mai 2021
AWS JDBC-Treiber für PostgreSQL (Vorschau)	Der AWS JDBC-Treiber für PostgreSQL, der jetzt als Vorschauversion verfügbar ist, ist ein Client-Treiber, der für die Hochverfügbarkeit von Aurora PostgreSQL entwickelt wurde. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Amazon Web Services JDBC-Treiber für PostgreSQL (Vorschau).	27. April 2021
Die Daten-API ist zusätzlich verfügbar AWS-Regionen	Die Daten-API ist jetzt in den Regionen Asien-Pazifik (Seoul) und Kanada (Zentral) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit der Daten-API.	9. April 2021
Amazon Aurora unterstützt die Graviton2 DB-Instance-Klassen	Sie können jetzt die Graviton2-DB-Instance-Klassen db.r6g.x verwenden, um DB-Cluster mit MySQL oder PostgreSQL zu erstellen. Weitere Informationen finden Sie unter DB-Instance-Klassenarten.	12. März 2021

Erweiterungen des RDS-Proxy-Endpunkts	Sie können zusätzliche Endpunkte erstellen, die jedem RDS-Proxy zugeordnet sind. Das Erstellen eines Endpunkts in einer anderen VPC ermöglicht den VPC-übergreifenden Zugriff für den Proxy. Proxies für Aurora MySQL-Cluster können auch schreibgeschützte Endpunkte haben. Diese Reader-Endpunkte stellen eine Verbindung zu Reader-DB-Instances in den Clustern her und können die Leseskalierbarkeit und Verfügbarkeit für abfragein tensive Anwendungen verbessern. Weitere Informationen zu RDS Proxy finden Sie unter „Verwalten von Verbindungen mit Amazon RDS Proxy“ im Amazon RDS-Benutzerhandbuch oder im Aurora-Benutzerhandbuch.	8. März 2021
Amazon Aurora ist in der Region Asien-Pazifik (Osaka) verfügbar	Amazon Aurora ist jetzt in der Region Asien-Pazifik (Osaka) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	1. März 2021

Aurora PostgreSQL unterstützt die Aktivierung von IAM- und Kerberos-Authentifizierung auf demselben DB-Cluster	Aurora PostgreSQL unterstützt jetzt die Aktivierung sowohl der IAM-Authentifizierung als auch der Kerberos-Authentifizierung auf demselben DB-Cluster. Weitere Informationen finden Sie unter Datenbank-Authentifizierung mit Amazon Aurora .	24. Februar 2021
Die globale Aurora-Datenbank unterstützt jetzt verwaltetes geplantes Failover	Die globale Aurora-Datenbank unterstützt jetzt verwaltetes geplantes Failover, sodass Sie die primäre AWS -Region Ihrer globalen Aurora-Datenbank einfacher ändern können. Sie können das verwaltete geplante Failover nur mit fehlerfreien globalen Aurora-Datenbanken verwenden . Weitere Informationen finden Sie unter Notfallwiederherstellung und globale Amazon Aurora-Datenbanken . Referenzinformationen finden Sie im Amazon RDS API Reference unter `FailoverGlobalCluster` .	11. Februar 2021

Die Daten-API für Aurora Serverless unterstützt jetzt mehr Datentypen	Mit der Daten-API für Aurora Serverless können Sie jetzt `UUID`- und `JSON`-Datentypen als Eingabe für die Datenbank verwenden. Auch mit der Daten-API für Aurora Serverless können Sie jetzt den Typwert `LONG` als `STRING`-Wert aus Ihrer Datenbank zurückgeben lassen. Weitere Informationen finden Sie unter Aufrufen der Daten-API. Referenzinformationen zu unterstützten Datentypen finden Sie im Data Service-API-Referenz von Amazon RDS unter `SqlParameter`.	2. Februar 2021
Aurora PostgreSQL unterstützt Upgrades auf Hauptversionen für PostgreSQL 12	Mit Aurora PostgreSQL können Sie nun die DB-Engine auf Hauptversion 12 aktualisieren. Weitere Informationen finden Sie unter Aktualisieren der PostgreSQL-DB-Engine für Aurora PostgreSQL.	28. Januar 2021

Aurora MySQL unterstützt ein direktes Upgrade	Sie können Ihren Aurora MySQL 1.x-Cluster auf Aurora MySQL 2.x upgraden, wobei die DB-Instances, Endpunkte usw. des ursprünglichen Clusters erhalten bleiben. Diese integrierte Upgrade-Technik vermeidet die Unannehmlichkeit beim Einrichten eines ganz neuen Clusters durch Wiederherstellen eines Snapshots. Sie vermeidet auch den Aufwand beim Kopieren aller Ihrer Tabellendaten in einen neuen Cluster. Weitere Informationen finden Sie unter Upgrade der Hauptversion eines Aurora MySQL DB-Clusters von 1.x auf 2.x.	11. Januar 2021
AWS JDBC-Treiber für MySQL (Vorschau)	Der AWS JDBC-Treiber für MySQL, der jetzt als Vorschauversion verfügbar ist, ist ein Client-Treiber, der für die hohe Verfügbarkeit von Aurora MySQL entwickelt wurde. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit dem Amazon Web Services JDBC-Treiber für MySQL (Vorschau).	7. Januar 2021

Aurora unterstützt Datenbank aktivitäts-Streams auf sekundären Clustern einer globalen Datenbank	Sie können eine Datenbank mit einem Datenbankaktivität sstream auf einem primären oder sekundären Cluster von Aurora PostgreSQL oder Aurora MySQL starten. Informationen zu unterstützten Engine-Versionen finden Sie unter Einschränkungen der globalen Aurora-Datenbanken.	22. Dezember 2020
Multi-Master-Cluster mit 4 DB-Instances	Die maximale Anzahl von DB-Instances in einem Aurora MySQL Multi-Master-Clust er beträgt jetzt vier. Früher waren zwei DB-Instances das Maximum. Weitere Informati onen finden Sie unter Arbeiten mit Aurora-Multi-Master-Clustern.	17. Dezember 2020
Aurora PostgreSQL unterstützt Funktionen AWS Lambda	Sie können jetzt die AWS Lambda Funktion für Ihre Aurora PostgreSQL-DB-Clus ter aufrufen. Weitere Informati onen finden Sie unter Aufrufen einer Lambda-Funktion aus einem Aurora PostgreSQL-DB-Cluster.	11. Dezember 2020

Amazon Aurora unterstützt die Graviton2 DB-Instance-Klassen in der Vorschau	Sie können jetzt die Graviton2 -DB-Instance-Klassen db.r6g.x in der Vorschau verwenden , um DB-Cluster mit MySQL oder PostgreSQL zu erstellen . Weitere Informationen finden Sie unter DB-Instance-Klassenarten.	11. Dezember 2020
Amazon Aurora Serverless v2 ist jetzt in der Vorschauversion erhältlich.	Amazon Aurora Serverless v2 ist in der Vorschauversion verfügbar. Fordern Sie Zugriff an, um mit Amazon Aurora Serverless v2 arbeiten zu können. Weitere Informationen finden Sie auf der Seite für Aurora Serverless v2.	1. Dezember 2020

Aurora PostgreSQL ist jetzt für Aurora Serverless in weiteren AWS-Regionen verfügbar.	Aurora PostgreSQL ist jetzt für Aurora Serverless in weiteren AWS-Regionen verfügbar. Sie können jetzt wählen, ob Sie dasselbe Aurora PostgreSQL Serverless v1 AWS-Regionen Angebot verwenden möchten. Aurora MySQL Serverless v1 Zu den weiteren AWS-Regionen Aurora Serverless Unterstützungsangeboten gehören USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Seoul), Asien-Pazifik (Mumbai), Kanada (Mittel-) Europa (London) und Europa (Paris). Eine Liste aller Regionen und unterstützten Aurora-DB-Engines für Aurora Serverless finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v1. Die Amazon-RDS-Daten-API für Aurora Serverless ist jetzt auch in denselben AWS-Regionen verfügbar. Eine Liste aller Regionen, die die Daten-API für unterstützenAurora Serverless, finden Sie unter Daten-API mit Aurora MySQL Serverless v1	24. November 2020

Amazon RDS-Performance Insights führt neue Dimensionen ein	Sie können die Datenbanklast nach den Dimensionsgruppen für Datenbank, Anwendung (PostgreSQL) und Sitzungstyp (PostgreSQL) gruppieren. Amazon RDS unterstützt auch die Dimensionen db.name, db.application.name (PostgreSQL) und db.session_type.name (PostgreSQL). Weitere Informationen finden Sie unter Hauptlast-Tabelle.	24. November 2020
Aurora Serverless unterstützt jetzt Version 10.12 von Aurora PostgreSQL	Aurora PostgreSQL für Aurora Serverless wurde in allen AWS -Regionen, in denen Aurora PostgreSQL für Aurora Serverless unterstützt wird, auf Aurora PostgreSQL Version 10.12 aktualisiert. Weitere Informationen finden Sie unter Unterstützte Regionen und Aurora-DB-Engines für Aurora Serverless v1.	4. November 2020

Die Daten-API unterstützt jetzt die Tag-basierte Autorisierung	Die Daten-API unterstützt die Tag-basierte Autorisierung. Wenn Sie Ihre RDS-Clusterressourcen mit Tags gekennzeichnet haben, können Sie diese Tags in Ihren Richtlinienanweisungen verwenden, um den Zugriff über die Daten-API zu steuern. Weitere Informationen finden Sie unter Autorisieren des Zugriffs auf die Daten-API.	27. Oktober 2020
Amazon Aurora erweitert Unterstützung für den Export von Snapshots nach Amazon S3	Sie können jetzt in allen kommerziellen AWS-Regionen DB-Snapshot-Daten nach Amazon S3 exportieren. Weitere Informationen finden Sie unter Exportieren von DB-Snapshot-Daten nach Amazon S3.	22. Oktober 2020

Die Globale Aurora-Datenbank unterstützt das Klonen	Sie können jetzt Klone der primären und sekundären DB-Cluster Ihrer globalen Aurora-Datenbanken erstellen. Sie können dies tun, indem Sie die Menüoption Create Clone verwenden AWS Managemen t Console und auswählen. Sie können auch den Befehl verwenden AWS CLI und den `restore-db-cluster -to-point-in-time` Befehl mit der `--restore -type copy-on-write` Option ausführen. Mit dem AWS Management Console oder dem AWS CLI können Sie auch DB-Cluster aus Ihren globalen Aurora-Datenbanken AWS kontenübergreifend klonen. Weitere Informati onen zum Klonen finden Sie unter Klonen eines Aurora DB-Cluster-Volumes.	19. Oktober 2020

Amazon Aurora unterstützt die dynamische Größenanpassung für das Cluster-Volume	Beginnend mit Aurora MySQL 1.23 und 2.09 sowie Aurora PostgreSQL 3.3.0 und Aurora PostgreSQL 2.6.0 reduziert Aurora die Größe des Cluster-Volumes nach dem Entfernen von Daten über Operationen wie `DROP TABLE`. Um diese Erweiterung nutzen zu können, aktualisieren Sie auf eine der entsprechenden Versionen, abhängig von der Datenbank-Engine, die Ihr Cluster verwendet. Weitere Informationen zu dieser Funktion und zur Überprüfung des verwendeten und verfügbaren Speicherplatzes für einen Aurora-Cluster finden Sie unter Verwalten von Performance und Skalierung für Aurora DB-Cluster.	13. Oktober 2020
Amazon Aurora unterstützt Volumegrößen bis zu 128 TiB	Neue und bestehende Aurora-Cluster-Volumes können jetzt auf eine maximale Größe von 128 tebibytes (TiB) erweitert werden. Weitere Informationen finden Sie unter Informationen zum Anwachsen des Aurora-Speichers.	22. September 2020

Aurora PostgreSQL unterstützt die DB-Instance-Klassen db.r5 und db.t3 in der Region China (Ningxia)	Sie können jetzt Aurora–PostgreSQL-DB-Cluster in der Region China (Ningxia) erstellen, die die DB-Instance-Klassen db.r5 und db.t3 verwenden. Weitere Informationen finden Sie unter DB-Instance-Klassen.	3. September 2020

Aurora-Erweiterungen für parallele Abfragen	Ab Aurora MySQL 2.09 und 1.23 können Sie die Vorteile der Verbesserungen für die Funktion für parallele Abfragen nutzen. Für das Erstellen eines parallele n Abfrageclusters ist kein spezieller Engine-Modus mehr erforderlich. Sie können die parallele Abfrage jetzt mithilfe der Konfigurationsopti on `aurora_parallel_qu ery` für jeden bereitges tellten Cluster aktivieren und deaktivieren, auf dem eine kompatible Aurora MySQL-Version ausgeführ t wird. Sie können einen vorhandenen Cluster auf eine kompatible Aurora MySQL-Version aktualisieren und eine parallele Abfrage verwenden, anstatt einen neuen Cluster zu erstellen und in diesen Daten zu importier en. Sie können Performan ce Insights für parallele Abfragecluster verwenden . Sie können parallele Abfragecluster stoppen und starten. Sie können parallele Aurora-Abfragecluster erstellen, die mit MySQL 5.7 kompatibel sind. Die parallele Abfrage funktioniert für Tabellen, die das Zeilenfor	2. September 2020

	mat `DYNAMIC` verwenden . Parallele Abfragecluster können die AWS Identity and Access Managemen t (IAM-) Authentifizierung verwenden. DB-Reader -Instances in parallelen Abfrageclustern können die Vorteile der Isolation sstufe `READ COMMITTED` nutzen. Sie können jetzt auch parallele Abfrage-C luster in zusätzlichen AWS-Regionen erstellen. Weitere Informationen zur Funktion für parallele Abfragen und zu diesen Verbesserungen finden Sie unter Arbeiten mit parallele n Abfragen für Aurora MySQL.	
Änderungen am Aurora MySQL-Parameter binlog_ro ws_query_log_events	Sie können nun den Wert des Aurora MySQL-Kon figurationsparameters ändern `binlog_rows_query_ log_events` . Früher war dieser Parameter nicht veränderbar.	26. August 2020

Unterstützung für automatische Nebenversions-Upgrades für Aurora MySQL	Mit Aurora MySQL wird die Einstellung Enable auto minor version upgrade (Automatisches Nebenversions-Upgrade aktivieren) jetzt wirksam, wenn Sie sie für einen Aurora MySQL-DB-Cluster angeben. Wenn Sie das automatische Nebenversions-Upgrade aktivieren, wird Aurora automatisch auf neue Nebenversionen aktualisiert, sobald diese veröffentlicht werden. Die automatischen Upgrades erfolgen während des Wartungsfensters für die Datenbank. Für Aurora MySQL gilt diese Funktion nur für Aurora MySQL Version 2, die mit MySQL 5.7 kompatibel ist. Zunächst bringt das automatische Upgrade-Verfahren Aurora MySQL-DB-Cluster auf Version 2.07.2. Weitere Informationen zur Funktionsweise dieser Funktion mit Aurora MySQL finden Sie unter Datenbank-Upgrades und Patches für Amazon Aurora MySQL.	3. August 2020

Aurora PostgreSQL unterstützt Upgrades auf Hauptversionen für PostgreSQL Version 11	Mit Aurora PostgreSQL können Sie nun die DB-Engine auf Hauptversion 11 aktualisieren. Weitere Informationen finden Sie unter Aktualisieren der PostgreSQL-DB-Engine für Aurora PostgreSQL.	28. Juli 2020
Amazon Aurora unterstützt AWS PrivateLink	Amazon Aurora unterstützt jetzt die Erstellung von Amazon VPC-Endpunkten für Amazon RDS-API-Aufrufe, um den Verkehr zwischen Anwendungen und Aurora im AWS Netzwerk aufrechtzuerhalten. Weitere Informationen finden Sie unter Amazon Aurora und Schnittstellen-VPC-Endpunkte (AWS PrivateLink).	9. Juli 2020
RDS Proxy allgemein verfügbar	RDS Proxy ist jetzt allgemein verfügbar. Sie können RDS Proxy mit RDS MySQL, Aurora MySQL, RDS for PostgreSQL und Aurora PostgreSQL für Produktions-Workloads verwenden. Weitere Informationen zu RDS Proxy finden Sie unter „Verwalten von Verbindungen mit Amazon RDS Proxy“ im Amazon RDS-Benutzerhandbuch oder im Aurora-Benutzerhandbuch.	30. Juni 2020

Schreibweiterleitung in der globalen Aurora-Datenbank	Sie können jetzt die Schreibfunktion für sekundäre Cluster in einer globalen Datenbank aktivieren. Bei der Schreibweiterleitung geben Sie DML-Anweisungen in einem sekundären Cluster aus, Aurora leiten die Schreiboperation an den primären Cluster weiter, und die aktualisierten Daten werden auf alle sekundären Cluster repliziert. Weitere Informationen finden Sie unter Schreibweiterleitung für sekundäre Zwecke AWS-Regionen mit einer globalen Aurora-Datenbank.	18. Juni 2020
Aurora unterstützt die Integration mit AWS Backup	Sie können es verwenden AWS Backup , um Backups von Aurora-DB-Clustern zu verwalten. Weitere Informationen finden Sie unter Übersicht über das Sichern und Wiederherstellen eines Aurora-DB-Clusters.	10. Juni 2020
Aurora PostgreSQL unterstützt DB-Instance-Klassen vom Typ „db.t3.large“	Sie können jetzt Aurora PostgreSQL-DB-Cluster erstellen, die DB-Instance-Klassen vom Typ „db.t3.large“ verwenden. Weitere Informationen finden Sie unter DB-Instance-Klassen.	5. Juni 2020

Die globale Aurora-Datenbank unterstützt PostgreSQL-Version 11.7 und die verwaltete Recovery Point Objective (RPO)	Sie können jetzt globale Aurora-Datenbanken für die PostgreSQL-Datenbank-Engine-Version 11.7. erstellen. Sie können auch verwalten, wie eine globale PostgreSQL-Datenbank mithilfe eines Recovery Point Objective (RPO, Definition eines Zeitraums zwischen zwei Datensicherungen) nach einem Ausfall wiederhergestellt wird. Weitere Informationen finden Sie unter Überregionale Notfallwiederherstellung für globale Aurora-Datenbanken.	4. Juni 2020
Aurora MySQL unterstützt Datenbanküberwachung mit Datenbankaktivitäts-Streams	Aurora MySQL enthält jetzt Datenbankaktivitätsstreams, die einen near-real-time Datenstrom der Datenbankaktivität in Ihrer relationalen Datenbank bereitstellen. Weitere Informationen finden Sie unter Verwenden von Datenbankaktivitäts-Streams.	2. Juni 2020
Der Abfrage-Editor ist zusätzlich verfügbar AWS-Regionen	Der Abfrage-Editor für Aurora Serverless ist jetzt zusätzlich AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit des Abfrage-Editors.	28. Mai 2020

Die Daten-API ist zusätzlich verfügbar AWS-Regionen	Die Daten-API ist jetzt zusätzlich verfügbar AWS-Regionen. Weitere Informationen finden Sie unter Verfügbarkeit der Daten-API.	28. Mai 2020
RDS-Proxy verfügbar in Region Kanada (Zentral)	Sie können nun die RDS-Proxy-Vorschau in der Region Region Kanada (Zentral) verwenden. Weitere Informationen zu RDS-Proxy finden Sie unter Verwalten von Verbindungen mit Amazon RDS-Proxy (Vorschau).	28. Mai 2020
Globale Aurora-Datenbank und regionsübergreifende Read Replicas (Lesereplikate)	Sie können für eine globale Aurora-Datenbank nun ein regionsübergreifendes Aurora MySQL-Read Replica erstellen, wenn sich der primäre Cluster in derselben Region wie ein sekundärer Cluster befindet. Weitere Informationen zu Aurora Globale Datenbank und regionsübergreifenden Read Replicas finden Sie unter Arbeiten mit Amazon Aurora Global Database und Replizieren von Amazon Aurora MySQL DB.	18. Mai 2020

RDS Proxy ist in weiteren Sprachen verfügbar AWS-Regionen	Sie können nun die RDS-Proxy-Vorversion in der Region USA West (Nordkalifornien), der Region Europa (London), der Region Europa (Frankfurt), der Region Asien-Pazifik (Seoul), der Region Asien-Pazifik (Mumbai), der Region Asien-Pazifik (Singapur) und der Region Asien-Pazifik (Sydney) verwenden. Weitere Informationen zu RDS-Proxy finden Sie unter Verwalten von Verbindungen mit Amazon RDS-Proxy (Vorschau).	13. Mai 2020
Aurora PostgreSQL-kompatible Edition unterstützt On-Premise- oder selbstgehostetes Microsoft Active Directory	Sie können nun ein lokales oder selbstgehostetes Active Directory für die Kerberos-Authentifizierung von Benutzern verwenden, wenn sie eine Verbindung zu Ihren Aurora PostgreSQL-DB-Clustern herstellen. Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung mit Aurora PostgreSQL.	7. Mai 2020

Aurora MySQL-Multimaster-Cluster sind in mehr verfügbar AWS-Regionen	Sie können jetzt Aurora-Multi-Master-Cluster in der Region Asien-Pazifik (Seoul), der Region Asien-Pazifik (Tokio), der Region Asien-Pazifik (Mumbai) und der Region Europa (Frankfurt) erstellen . Weitere Informationen zu Multi-Master-Clustern finden Sie unter Arbeiten mit Aurora-Multi-Master-Clustern.	7. Mai 2020
Performance Insights unterstützt die Analyse von Statistiken zu laufenden Aurora MySQL-Abfragen	Sie können jetzt Statistiken laufender Abfragen mit Performance Insights für Aurora MySQL-DB-Instances analysieren. Weitere Informationen finden Sie unter Analysieren von Statistiken zu laufenden Abfragen.	5. Mai 2020
Java-Client-Bibliothek für Daten-API allgemein verfügbar	Die Java-Client-Bibliothek für die Daten-API ist jetzt allgemein verfügbar. Sie können eine Java Client-Bibliothek für Data API herunterladen und verwenden. Mithilfe dieser Bibliothek können Sie Ihre clientseitigen Klassen zu Anforderungen und Antworten der Daten-API zuweisen. Weitere Informationen finden Sie unter Verwenden der Java Client-Bibliothek für die Daten-API.	30. April 2020

Amazon Aurora ist in der Region Europa (Mailand) verfügbar	Amazon Aurora ist jetzt in der Region Europa (Mailand) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	28. April 2020
Amazon Aurora ist in der Region Europa (Mailand) verfügbar	Amazon Aurora ist jetzt in der Region Europa (Mailand) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	27. April 2020
Amazon Aurora ist in der Region Afrika (Kapstadt) verfügbar	Amazon Aurora ist jetzt in der Region Afrika (Kapstadt) verfügbar. Weitere Informationen finden Sie unter Regionen und Availability Zones.	22. April 2020
Aurora PostgreSQL unterstützt jetzt DB-Instance-Klassen db.r5.16xlarge und db.r5.8xlarge	Sie können jetzt Aurora PostgreSQL-DB-Cluster mit PostgreSQL erstellen, die die DB-Instance-Klassen db.r5.16xlarge und db.r5.8xlarge verwenden. Weitere Informationen finden Sie unter Hardware-Spezifikationen für DB-Instance-Klassen für Aurora.	8. April 2020

Amazon RDS-Proxy für PostgreSQL	Amazon RDS-Proxy ist jetzt für PostgreSQL verfügbar. Sie können den RDS-Proxy verwenden, um den Overhead für die Verbindungsverwaltung in Ihrem Cluster zu reduzieren und auch die Wahrscheinlichkeit des Fehlers „zu viele Verbindungen“ zu reduzieren. Der RDS-Proxy ist derzeit als öffentliche Vorversion für PostgreSQL verfügbar. Weitere Informationen finden Sie unter Verwalten von Verbindungen mit Amazon RDS Proxy (Vorversion).	8. April 2020
Globale Aurora-Datenbanken unterstützen jetzt Aurora PostgreSQL	Sie können jetzt globale Aurora-Datenbanken für das PostgreSQL-Datenbank-Engine erstellen. Eine globale Aurora-Datenbank erstreckt sich über mehrere AWS-Regionen und ermöglicht globale Lesevorgänge mit geringer Latenz und Notfallwiederherstellung nach regionalen Ausfällen. Weitere Informationen finden Sie unter Arbeiten mit Amazon Aurora Global Database.	10. März 2020

Unterstützung für Upgrades von Hauptversionen für Aurora PostgreSQL	Mit Aurora PostgreSQL können Sie nun die DB-Engine auf eine Hauptversion aktualisieren. Auf diese Weise können Sie zu einer neueren Hauptversion springen, wenn Sie ausgewählte PostgreSQL-Engine-Versionen aktualisieren. Weitere Informationen finden Sie unter Aktualisieren der PostgreSQL-DB-Engine für Aurora PostgreSQL.	4. März 2020
Aurora PostgreSQL unterstützt die Kerberos-Authentifizierung	Sie können jetzt die Kerberos-Authentifizierung verwenden, um Benutzer zu authentifizieren, wenn sie sich mit Ihren Aurora PostgreSQL-DB-Clustern verbinden. Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung mit Aurora PostgreSQL.	28. Februar 2020
Die Daten-API unterstützt AWS PrivateLink	Die Daten-API unterstützt jetzt die Erstellung von Amazon VPC-Endpunkten für Daten-API-Aufrufe, um den Verkehr zwischen Anwendungen und der Daten-API im AWS Netzwerk aufrechtzuerhalten. Weitere Informationen finden Sie unter Erstellen eines Amazon-VPC-Endpunkts (AWS PrivateLink) für die Daten-API.	6. Februar 2020

Unterstützung von Aurora Machine Learning in Aurora PostgreSQL	Die `aws_ml` Aurora PostgreSQL-Erweiterung bietet Funktionen, die Sie in Ihren Datenbankabfragen verwenden, um Amazon Comprehend zur Stimmungsanalyse aufzurufen und Ihre eigenen SageMaker Machine-Learning-Modelle auszuführen. Weitere Informationen finden Sie unter Verwenden von Machine Learning (ML)-Funktionen mit Aurora.	5. Februar 2020
Aurora PostgreSQL unterstützt das Exportieren von Daten nach Amazon S3	Sie können Daten aus einem Aurora PostgreSQL-DB-Cluster abfragen und direkt in Dateien exportieren, die in einem Amazon S3-Bucket gespeichert sind. Weitere Informationen finden Sie unter Exportieren von Daten aus einem Aurora PostgreSQL-DB-Cluster zu Amazon S3.	5. Februar 2020
Unterstützung für den Export von DB-Snapshot-Daten nach Amazon S3	Amazon Aurora unterstützt den Export von DB-Snapshot-Daten nach Amazon S3 for MySQL und PostgreSQL. Weitere Informationen finden Sie unter Exportieren von DB-Snapshot-Daten zu Amazon S3.	9. Januar 2020

Aurora MySQL-Versionshinweise im Dokumentverlauf	Dieser Abschnitt enthält nun Verlaufseinträge für Aurora MySQL-kompatible Edition-Versionshinweise für Versionen, die nach dem 31. August 2018 veröffentlicht wurden. Wählen Sie den Link in der ersten Spalte des Verlaufseintrags, um die vollständigen Versionshinweise für eine spezifische Version anzuzeigen.	13. Dezember 2019
Amazon RDS Proxy	Sie können den Overhead für die Verbindungsverwaltung in Ihrem Cluster reduzieren und die Wahrscheinlichkeit des Fehlers "zu viele Verbindungen" reduzieren, indem Sie Amazon RDS Proxy verwenden. Sie ordnen jeden Proxy einer RDS DB-Instance oder einem Aurora DB-Cluster zu. Dann verwenden Sie den Proxy-Endpunkt in der Verbindungszeichenfolge für Ihre Anwendung. Der Amazon RDS-Proxy ist derzeit als öffentliche Vorversion verfügbar. Die Aurora MySQL-Datenbank-Engine wird unterstützt. Weitere Informationen finden Sie unter Verwalten von Verbindungen mit Amazon RDS Proxy (Vorversion).	03. Dezember 2019

Data API for Aurora Serverless v1 unterstützt Datentyp-Mapping-Hinweise	Sie können nun einen Hinweis verwenden, damit die Data API for Aurora Serverless v1 einen `String`-Wert als einen anderen Typ zur Datenbank sendet. Weitere Informationen finden Sie unter Aufrufen der Daten-API.	26. November 2019
Data API for Aurora Serverless v1 unterstützt eine Java-Clientbibliothek (Vorversion)	Sie können eine Java Client-Bibliothek für Data API herunterladen und verwenden. Mithilfe dieser Bibliothek können Sie Ihre clientseitigen Klassen zu Anforderungen und Antworten der Daten-API zuweisen. Weitere Informationen finden Sie unter Verwenden der Java Client-Bibliothek für die Daten-API.	26. November 2019
Aurora PostgreSQL ist mit FedRAMP HIGH konform	Aurora PostgreSQL ist mit FedRAMP HIGH konform. Einzelheiten zu den Maßnahmen AWS und zur Einhaltung der Vorschriften finden Sie unter AWS Services im Umfang der einzelnen Compliance-Programme.	26. November 2019

Isolationsstufe READ COMMITTED für Amazon Aurora MySQL-Replikate aktiviert	Sie können jetzt die Isolationsstufe `READ COMMITTED` für Aurora MySQL-Replikate aktivieren. Hierzu müssen Sie die Konfigurationseinstellung `aurora_read_replica_read_committed_isolation_enabled` auf Sitzungsebene aktivieren. Die Verwendung der Isolationsstufe `READ COMMITTED` für langfristig ausgeführte Abfragen auf OLTP-Clustern kann helfen, Probleme mit der Länge der Verlaufsliste zu lösen. Vor der Aktivierung dieser Einstellung müssen Sie verstehen, wie sich das Isolationsverhalten auf Aurora-Replikaten von der gewöhnlichen MySQL-Implementierung von unterscheide `READ COMMITTED` . Weitere Informationen finden Sie unter Aurora MySQL-Isolationsstufen.	25. November 2019
Performance Insights unterstützt die Analyse von Statistiken zu laufenden Aurora PostgreSQL-Abfragen	Sie können jetzt Statistiken laufender Abfragen mit Performance Insights für Aurora PostgreSQL-DB-Instances analysieren. Weitere Informationen finden Sie unter Analysieren von Statistiken zu laufenden Abfragen.	25. November 2019

Mehr Cluster in einer globalen Aurora-Datenbank	Sie können jetzt einer globalen Aurora-Datenbank mehrere sekundäre Regionen hinzufügen. Sie können globale Lesevorgänge mit niedriger Latenz und Notfallwiederherstellungen in einem größeren geografischen Bereich nutzen. Weitere Informationen zu globalen Aurora-Datenbanken finden Sie unter Arbeiten mit Amazon Aurora Global Databases.	25. November 2019
Unterstützung von Aurora Machine Learning in Aurora MySQL	In Aurora MySQL 2.07 und höher können Sie Amazon Comprehend für Stimmungsanalysen und für eine Vielzahl von Algorithmen SageMaker für maschinelles Lernen aufrufen. Sie können die Ergebnisse direkt in Ihrer Datenbankanwendung verwenden, indem Sie Aufrufe an gespeicherte Funktionen in Ihre Abfragen einbetten. Weitere Informationen finden Sie unter Verwenden von Machine Learning (ML)-Funktionen mit Aurora.	25. November 2019

Die globale Aurora-Datenbank erfordert keine Engine-Modus-Einstellung mehr	Sie müssen nicht mehr `--engine-mode=global` angeben, wenn Sie ein Cluster erstellen, das Teil einer globalen Aurora-Datenbank sein soll. Alle Aurora-Cluster, die die Kompatibilitätsanforderungen erfüllen, können Teil einer globalen Datenbank sein. Der Cluster muss beispielsweise zurzeit Aurora MySQL Version 1 mit MySQL 5.6-Kompatibilität verwenden. Weitere Informationen zu globalen Aurora-Datenbanken finden Sie unter Arbeiten mit globalen Amazon Aurora-Datenbanken.	25. November 2019
Die globale Aurora-Datenbank ist für Aurora MySQL Version 2 verfügbar	Ab Aurora MySQL 2.07 können Sie eine globale Aurora-Datenbank erstellen, die mit MySQL 5.7 kompatibel ist. Sie müssen den Engine-Modus `global` für die primären oder sekundären Cluster nicht angeben. Sie können jedes neue bereitgestellte Cluster mit Aurora MySQL 2.07 oder höher zu einer Aurora Global Database hinzufügen. Weitere Informationen zu Aurora Global Database finden Sie unter Arbeiten mit Amazon Aurora Global Database.	25. November 2019

Aurora MySQL Hot-Row-Contention-Optimierung ohne Labor-Modus verfügbar	Die Hot Row Contention-Optimierung ist jetzt allgemein für Aurora MySQL verfügbar und erfordert kein Festlegen des Aurora-Labor-Modus auf „ON (EIN)“. Diese Funktion sorgt für eine deutliche Verbesserung des Durchsatzes bei Workloads mit zahlreichen Transaktionen, die um Zeilen auf derselben Seite konkurrieren. Diese Verbesserung umfasst die Veränderung des von Aurora MySQL verwendeten Entsperrungsalgorithmus.	19. November 2019
Aurora MySQL Hash Joins ohne Labor-Modus verfügbar	Die Hash Join-Funktion ist jetzt allgemein für Aurora MySQL verfügbar und erfordert kein Festlegen des Aurora-Labor-Modus-auf „ON (EIN)“. Diese Funktion kann die Abfrageleistung verbessern, wenn Sie eine große Datenmenge mithilfe eines Equijoins verbinden müssen. Weitere Informationen zum Verwenden dieser Funktion finden Sie unter Arbeiten mit Hash Joins in Aurora MySQL.	19. November 2019

Aurora MySQL 2.*-Unterstützung für weitere db.r5-Instance-Klassen	Aurora MySQL-Cluster unterstützen jetzt die Instance-Typen db.r5.8xlarge, db.r5.16xlarge und db.r5.24xlarge. Weitere Informationen zu Instance-Typen für Aurora MySQL-Cluster finden Sie unter Auswahl der DB-Instance-Klasse.	19. November 2019
Aurora MySQL 2.*-Unterstützung für die Rückverfolgung	Aurora MySQL 2.*-Versionen unterstützen jetzt die schnelle Wiederherstellung nach Benutzerfehlern wie Löschen der falschen Tabelle oder Löschen der falschen Zeile. Mithilfe de Rückverfolgung können Sie Ihre Datenbank zu einem früheren Zeitpunkt verschieben, ohne dass eine Wiederherstellung aus einem Backup erforderlich ist. Der Vorgang ist selbst bei großen Datenbanken innerhalb weniger Sekunden abgeschlossen. Einzelheiten finden Sie unter Rückverfolgen eines Aurora-DB-Clusters.	19. November 2019

Unterstützung von Abrechnungstags für Aurora	Sie können nun Tags verwenden, um die Kostenverrechnung für Ressourcen wie Aurora-Cluster, DB-Instances innerhalb von Aurora-Clustern, I/O, Backups, Snapshots usw. zu verfolgen. Mit dem Cost Explorer können Sie sich die mit jedem Tag verbundenen AWS Kosten anzeigen lassen. Weitere Informationen zur Verwendung von Tags mit Aurora finden Sie unter Tagging von Amazon RDS-Ressourcen. Allgemeine Informationen zu Tags und deren Verwendung für die Kostenanalyse finden Sie unter Verwendung von Kostenzuordnungs-Tags und Benutzerdefinierte Kostenzuordnungs-Tags.	23. Oktober 2019
Daten-API für Aurora PostgreSQL	Aurora PostgreSQL unterstützt jetzt die Verwendung der Data API mit Amazon Aurora Serverless v1-DB-Clustern. Weitere Informationen finden Sie unter Verwenden der Data API for Aurora Serverless v1.	23. September 2019

Aurora PostgreSQL unterstützt das Hochladen von Datenbankprotokollen in Protokolle CloudWatch	Sie können Ihren Aurora PostgreSQL-DB-Cluster so konfigurieren, dass Protokolldaten in einer Protokollgruppe in Amazon CloudWatch Logs veröffentlicht werden. Mit CloudWatch Logs können Sie eine Echtzeitanalyse der Protokolldaten durchführen und diese CloudWatch zum Erstellen von Alarmen und zum Anzeigen von Metriken verwenden. Sie können CloudWatch Logs verwenden, um Ihre Protokolldatensätze in einem äußerst langlebigen Speicher zu speichern. Weitere Informationen finden Sie unter Veröffentlichen von Aurora PostgreSQL-Protokollen in Amazon CloudWatch Logs.	9. August 2019
Multi-Master-Cluster für Aurora MySQL	Sie können Aurora MySQL Multi-Master-Cluster einrichten. In diesen Clustern verfügt jede DB-Instance über Lese- und Schreibfähigkeit. Weitere Informationen finden Sie unter Arbeiten mit Aurora-Multi-Master-Clustern.	8. August 2019

Aurora PostgreSQL unterstützt Aurora Serverless v1	Sie können jetzt Amazon Aurora Serverless v1 mit Aurora PostgreSQL verwenden. Ein Aurora Serverless DB-Cluster kann abhängig von Ihren Anwendungsanforderungen automatisch starten, herunterfahren und die Kapazität steigern oder senken. Weitere Informationen finden Sie unter Verwendung von Amazon Aurora Serverless v1.	9. Juli 2019
Kontoübergreifendes Klonen für Aurora MySQL	Sie können jetzt das Cluster-Volume für einen Aurora MySQL-DB-Cluster zwischen AWS Konten klonen. Sie autorisieren die gemeinsame Nutzung über AWS Resource Access Manager (AWS RAM). Das geklonte Cluster-Volume verwendet einen copy-on-write Mechanismus, der nur zusätzlichen Speicherplatz für neue oder geänderte Daten benötigt. Weitere Informationen zum Klonen für Aurora finden Sie unter Klonen von Datenbanken in einem Aurora-DB-Cluster.	2. Juli 2019

Aurora PostgreSQL unterstützt db.t3-DB-Instance-Klassen	Sie können jetzt Aurora PostgreSQL-DB-Cluster erstellen, die DB-Instance-Klassen vom Typ "db.t3" verwenden. Weitere Informationen finden Sie unter DB-Instance-Klasse.	20. Juni 2019
Unterstützung für den Import von Daten aus Amazon S3 for Aurora PostgreSQL	Sie können nun Daten aus einer Amazon S3-Datei in eine Tabelle in einem Aurora PostgreSQL DB-Cluster importieren. Weitere Informationen finden Sie unter Importieren von Amazon S3-Daten in einen Aurora PostgreSQL DB-Cluster.	19. Juni 2019
Aurora PostgreSQL jetzt mit schneller Failover-Wiederherstellung und Cluster-Cacheverwaltung	Aurora PostgreSQL bietet jetzt eine Cluster-Cacheverwaltung, um im Falle eines Failovers eine schnelle Wiederherstellung der primären DB-Instance sicherzustellen. Weitere Informationen finden Sie unter Schnelle Wiederherstellung nach Failover mit Cluster-Cacheverwaltung.	11. Juni 2019
Data API for Aurora Serverless v1 allgemein verfügbar	Sie können mit Webservice-basierten Anwendungen über die Data API auf Aurora Serverless v1-Cluster zugreifen. Weitere Informationen finden Sie unter Verwenden der Data API for Aurora Serverless v1.	30. Mai 2019

Aurora PostgreSQL unterstützt die Datenbanküberwachung mit Datenbankaktivitäts-Streams	Aurora PostgreSQL enthält jetzt Datenbankaktivitätsstreams, die einen near-real-time Datenstrom der Datenbankaktivität in Ihrer relationalen Datenbank bereitstellen. Weitere Informationen finden Sie unter Verwenden von Datenbankaktivitäts-Streams.	30. Mai 2019
Amazon-Aurora-Empfehlungen	Amazon Aurora bietet nun automatisierte Empfehlungen für Aurora-Ressourcen. Weitere Informationen finden Sie unter Verwenden von Amazon Aurora-Empfehlungen.	22. Mai 2019
Performance Insights-Support für Aurora Global Database	Sie können Performance Insights jetzt mit Aurora Global Database nutzen. Weitere Informationen über Performance-Insights für Aurora finden Sie unter Verwenden von Amazon RDS Performance Insights. Weitere Informationen zu Aurora Global Databases finden Sie unter Arbeiten mit Aurora Global Database.	13. Mai 2019

Performance Insights ist für Aurora MySQL 5.7 verfügbar	Amazon RDS Performance Insights ist jetzt für Aurora MySQL-Versionen 2.x verfügbar, die mit MySQL 5.7 kompatibel sind. Weitere Informationen finden Sie unter Verwenden von Amazon RDS-Performance-Insights.	3. Mai 2019
Die globalen Aurora-Datenbanken sind in weiteren Sprachen verfügbar AWS-Regionen	Sie können jetzt globale Aurora-Datenbanken in den meisten Ländern erstellen, in AWS-Regionen denen Aurora verfügbar ist. Weitere Informationen zu globalen Aurora-Datenbanken finden Sie unter Arbeiten mit globalen Amazon Aurora-Datenbanken.	30. April 2019
Mindestkapazität 1 für Aurora Serverless v1	Für einen Aurora Serverless v1-Cluster müssen Sie eine Mindestkapazitätseinstellung von 1 verwenden. Zuvor betrug die Mindestkapazität 2. Weitere Informationen zum Angeben von Aurora-Serverless-Kapazitätswerten finden Sie unter Festlegen der Kapazität eines Aurora Serverless v1-Serverless-DB-Clusters.	29. April 2019

Aurora Serverless v1-Timeout-Aktion	Sie können jetzt die Aktion angeben, die ausgeführt werden soll, wenn für eine Aurora Serverless v1-Kapazitätsänderung ein Timeout eintritt. Weitere Informationen finden Sie unter Timeout-Aktion für Kapazitätsänderungen.	29. April 2019
Sekundengenaue Abrechnung	Amazon RDS wird jetzt in allen On-Demand-Instances in 1-Sekunden-Schritten abgerechnet, AWS-Regionen mit Ausnahme von AWS GovCloud (USA). Weitere Informationen finden Sie unter Abrechnung von DB-Instances für Aurora.	25. April 2019
Schnappschüsse teilen Aurora Serverless v1AWS-Regionen	Im Fall von Aurora Serverless v1 werden Snapshots stets verschlüsselt. Wenn Sie den Snapshot mit Ihrem eigenen verschlüsseln AWS KMS key, können Sie den Snapshot jetzt kopieren oder teilen. AWS-Regionen Informationen zu Snapshots von Aurora Serverless v1-DB-Clustern finden Sie unter Aurora Serverless v1 und Snapshots.	17. April 2019

Wiederherstellen von MySQL 5.7-Backups aus Amazon S3	Sie können jetzt ein Backup Ihrer MySQL Version 5.7-Datenbank erstellen und auf Amazon S3 speichern und die Sicherungsdatei anschließend auf einem neuen Aurora MySQL DB-Cluster wiederherstellen. Weitere Informationen finden Sie unter Migrieren von Daten aus einer externen MySQL-Datenbank in einen Aurora MySQL-DB-Cluster.	17. April 2019
Teilen von Aurora Serverless v1-Snapshots über Regionen hinweg	Im Fall von Aurora Serverless v1 werden Snapshots stets verschlüsselt. Wenn Sie den Snapshot mit Ihrem eigenen verschlüsseln AWS KMS key, können Sie den Snapshot jetzt regionsübergreifend kopieren oder teilen. For information on snapshots of Aurora Serverless v1-DB clusters, see Aurora Serverless und Snapshots.	16. April 2019
proof-of-concept Aurora-Anleitung	Sie können lernen, wie ein Machbarkeitsnachweis durchgeführt wird, um Ihre Anwendung und Workload mit Aurora auszuprobieren. Ein komplettes Tutorial finden Sie unter Durchführen eines Aurora-Machbarkeitsnachweises.	16. April 2019

Aurora Serverless v1 unterstützt das Wiederherstellen aus einem Amazon S3-Backup	Sie können jetzt Backups von Amazon S3 in einen Aurora Serverless-Cluster importieren. Einzelheiten zu diesem Verfahren finden Sie unter Migrieren von Daten aus MySQL mithilfe eines Amazon S3-Buckets.	16. April 2019
Neue modifizierbare Parameter für Aurora Serverless v1	Sie können jetzt die folgenden DB-Parameter für einen Aurora Serverless v1-Cluster modifizieren: `innodb_file_format` , `innodb_file_per_table` , `innodb_large_prefix` , `innodb_lock_wait_timeout` , `innodb_monitor_disable` , `innodb_monitor_enable` , `innodb_monitor_reset` , `innodb_monitor_reset_all` , `innodb_print_all_deadlocks` , `log_warnings` , `net_read_timeout` , `net_retry_count` , `net_write_timeout` , `sql_mode` und `tx_isolation` . Weitere Informationen zu Konfigurationsparametern für Aurora Serverless v1-Cluster finden Sie unter Aurora Serverless v1 und Parametergruppen.	4. April 2019

Aurora PostgreSQL unterstützt db.r5-DB-Instance-Klassen	Sie können jetzt Aurora PostgreSQL-DB-Cluster erstellen, die DB-Instance-Klassen vom Typ "db.r5" verwenden. Weitere Informationen finden Sie unter DB-Instance-Klasse.	4. April 2019
Logische Aurora PostgreSQL-Replikation	Sie können nun die logische PostgreSQL-Replikation nutzen, um Teile einer Datenbank für einen Aurora PostgreSQL-DB-Cluster zu replizieren. Weitere Informationen finden Sie unter Verwenden der logischen Replikation von PostgreSQL.	28. März 2019

GTID-Unterstützung für Aurora MySQL 2.04	Sie können die Replikation nun mit der Funktion der globalen Transaktions-ID (GTID) von MySQL 5.7 verwenden. Diese Funktion vereinfacht das Durchführen der Binärprotokoll-(binlog)Replikation zwischen Aurora MySQL und einer externen MySQL 5.7-kompatiblen Datenbank. Die Replikation kann den Aurora MySQL-Cluster als Quelle oder als Ziel verwenden. Diese Funktion ist für Aurora MySQL 2.04 und höher verfügbar. Weitere Informationen über GTID-basierte Replikation und Aurora MySQL finden Sie unter Verwenden der GTID-basierten Replikation für Aurora MySQL.	25. März 2019

Aurora Serverless v1Logs auf Amazon hochladen CloudWatch	Sie können Aurora jetzt Datenbankprotokolle CloudWatch für einen Aurora Serverless v1 Cluster hochladen lassen. Weitere Informationen finden Sie unter Anzeigen von Aurora Serverless-DB-Clustern. Als Teil dieser Erweiterung können Sie nun Werte für Parameter auf Instance-Ebene in einer DB-Clusterparamete rgruppe definieren und diese Werte auf alle DB-Instances im Cluster anwenden, sofern sie nicht in der DB-Parame tergruppe überschrieben werden. Weitere Informationen finden Sie unter Arbeiten mit DB-Parametergruppen und DB-Clusterparametergruppen.	25. Februar 2019
Aurora MySQL unterstützt db.t3-DB-Instance-Klassen	Sie können jetzt Aurora MySQL-DB-Cluster erstellen , die DB-Instance-Klassen vom Typ "db.t3" verwenden. Weitere Informationen finden Sie unter DB-Instance-Klasse.	25. Februar 2019
Aurora MySQL unterstützt db.r5-DB-Instance-Klassen	Sie können jetzt Aurora MySQL-DB-Cluster erstellen , die DB-Instance-Klassen vom Typ "db.r5" verwenden. Weitere Informationen finden Sie unter DB-Instance-Klasse.	25. Februar 2019

Performance Insights-Zähler für Aurora MySQL	Sie können nun Leistungszähler zu Ihren Performance Insights-Diagrammen für Aurora MySQL-DB-Instances hinzufügen. Weitere Informationen finden Sie unter Verwenden der Performance-Insights-Dashboard-Komponenten .	19. Februar 2019
Amazon RDS Performance Insights unterstützt Anzeige von mehr SQL-Text für Aurora MySQL	Amazon RDS Performance Insights unterstützt jetzt die Anzeige von mehr SQL-Text im Performance Insights-Dashboard für Aurora MySQL-DB-Instances. Weitere Informationen finden Sie unter Anzeigen von mehr SQL-Text im Performance-Insights-Dashboard.	6. Februar 2019
Amazon RDS Performance Insights unterstützt Anzeige von mehr SQL-Text für Aurora PostgreSQL	Amazon RDS Performance Insights unterstützt jetzt die Anzeige von mehr SQL-Text im Performance Insights-Dashboard für Aurora PostgreSQL-DB-Instances. Weitere Informationen finden Sie unter Anzeigen von mehr SQL-Text im Performance-Insights-Dashboard.	24. Januar 2019

Aurora-Sicherungsfakturierung	Sie können die CloudWatch Amazon-Metriken `TotalBackupStorageBilled` , und verwenden `SnapshotStorageUsed` , `BackupRetentionPeriodStorageUsed` um die Speicherbelegung Ihrer Aurora-Backups zu überwachen. Weitere Informationen zur Verwendung von CloudWatch Metriken finden Sie unter Überblick über die Überwachung. Weitere Informationen über die Verwaltung von Sicherungsdaten finden Sie unter Grundlegendes zur Aurora-Sicherungsspeichernutzung.	3. Januar 2019
Performance Insights-Zähler	Sie können nun Leistungsindikatoren zu Ihren Performance Insights-Diagrammen hinzufügen. Weitere Informationen finden Sie unter Verwenden der Performance-Insights-Dashboard-Komponenten .	6. Dezember 2018

Globale Aurora-Datenbank	Sie können jetzt globale Aurora-Datenbanken erstellen . Eine globale Aurora-Da tenbank erstreckt sich über mehrere AWS-Regionen und ermöglicht globale Lesevorgä nge mit geringer Latenz und Notfallwiederherstellung nach regionalen Ausfällen. Weitere Informationen finden Sie unter Arbeiten mit Amazon Aurora Global Database.	28. November 2018
Abfrageplanverwaltung in Aurora PostgreSQL	Aurora PostgreSQL bietet nun eine Abfrageplanverwalt ung, mit der Sie PostgreSQ L-Abfrageausführungspläne verwalten können. Weitere Informationen finden Sie unter Verwalten von Abfrageau sführungsplänen für Aurora PostgreSQL.	20. November 2018
Abfrage-Editor für Aurora Serverless v1 (Beta)	Sie können SQL-Anweisungen in der Amazon RDS-Konso le auf Aurora Serverless v1-Clustern ausführen. Weitere Informationen finden Sie unter Verwenden des Abfrage-E ditors für Aurora Serverless v1.	20. November 2018

Data API für Aurora Serverless v1 (Beta)	Sie können mit Webservice-basierten Anwendungen über die Data API auf Aurora Serverless v1-Cluster zugreifen. Weitere Informationen finden Sie unter Using the Data API for Aurora Serverless.	20. November 2018
TLS-Unterstützung für Aurora Serverless v1	Aurora Serverless v1-Cluster unterstützen TLS-/SSL-Verschlüsselung. Weitere Informationen finden Sie unter TLS/SSL für Aurora Serverless.	19. November 2018
Benutzerdefinierte Endpunkte	Sie können nun Endpunkte erstellen, die einer beliebigen Menge von DB-Instances zugeordnet sind. Diese Funktion hilft beim Lastausgleich und der Hochverfügbarkeit für Aurora-Cluster, bei denen einige DB-Instances eine andere Kapazität oder Konfiguration haben als andere. Sie können benutzerdefinierte Endpunkte verwenden, anstatt eine Verbindung zu einer bestimmten DB-Instance über deren Instance-Endpunkt herzustellen. Weitere Informationen finden Sie unter Amazon Aurora-Verbindungsmanagement.	12. November 2018

Unterstützung der IAM-Authentifizierung in Aurora PostgreSQL	Aurora PostgreSQL unterstützt nun die IAM-Authentifizierung. Weitere Informationen finden Sie unter IAM-Datenbankauthentifizierung.	8. November 2018
Benutzerdefinierte Parametergruppen für die Wiederherstellung und zeitpunktbezogene Wiederherstellung	Sie können jetzt bei einer Snapshot-Wiederherstellung oder einer zeitpunktbezogenen Wiederherstellung eine benutzerdefinierte Parametergruppe angeben. Weitere Informationen finden Sie unter Wiederherstellen aus einem DB-Cluster-Snapshot und Wiederherstellen eines DB-Clusters zu einer bestimmten Zeit.	15. Oktober 2018
Löschschutz für Aurora-DB-Cluster	Wenn Sie für einen DB-Cluster Löschschutz aktivieren, kann die Datenbank von keinem Benutzer gelöscht werden. Weitere Informationen finden Sie unter Löschen eines DB-Clusters.	26. September 2018
Stoppen/Starten-Funktion für Aurora	Sie können jetzt mit einer einzelnen Operation einen kompletten Aurora-Cluster stoppen oder starten. Weitere Informationen finden Sie im Abschnitt zum Stoppen und Starten eines Aurora-Clusters.	24. September 2018

Parallelabfrage-Funktion für Aurora MySQL	Aurora MySQL bietet jetzt eine Option zur parallelen Ausführung von I/O-Arbeiten für Abfragen in der gesamten Aurora-Speicherinfrastruktur. Mit dieser Funktion können datenintensive analytische Abfragen, die häufig die zeitaufwendigsten Vorgänge in einer Workload darstellen, beschleunigt werden. Weitere Informationen finden Sie im Abschnitt zum Arbeiten mit einer parallelen Abfrage für Aurora MySQL.	20. September 2018
Neues Handbuch	Dies ist die erste Version des Amazon Aurora-Benutzerhandbuchs.	31. August 2018

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.

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.